ANALISIS KEAMANAN SISTEM INFORMASI DENGAN *PENETRATION TESTING* DAN ISO 27001:2013 (STUDI KASUS SISTEM INFORMASI MANAJEMEN ASET MUHAMMADIYAH PWM DIY)

Skripsi untuk memenuhi salah satu syarat memperoleh gelar strata satu
Program Studi Teknik Informatika

Disusun oleh
Anwaruddin Kamal Ibrahim
12650072

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA
2019

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-2441/Un.02/DST/PP.00.9/08/2019

Tugas Akhir dengan judul	:	ANALISIS KEAMANAN SISTEM INFORMASI DENGAN PENETRATION TESTING DAN ISO 27001:2013 (STUDI KASUS SISTEM INFORMASI MANAJEMEN ASET MUHAMMADIYAH PWM DIY)
Yang dipersiapkan dan disusun oleh	:	
Nama	:	ANWARUDDIN KAMAL IBRAHIM
NIM	:	12650072
Telah diujikan pada	:	Selasa, 25 Juni 2019
Nilai Ujian Tugas Akhir	:	A/B

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Muhammad Taufiq Nuruzzaman, S.T., M.Eng
NIP. 19791118 200501 1 003

Penguji I

Dr. Bambang Sugiantoro, S.Si., M.T
NIP.19751024 200912 1 002

Penguji II

Maria Ulfah S, S.Kom, MIT, Ph.D
NIP.19780106 200212 2 001

Yogyakarta, 5 Agustus 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Plh. Dekan

Dr. Agung Fatwanto, S.Si, M.Kom
NIP. 19770103 200501 1 003

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Anwaruddin kamal Ibrahim
NIM	: 12650072
Judul Skripsi	: Analisis Keamanan Sistem Informasi Dengan Penetration Testing dan ISO 27001:2013 (Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah PWM DIY)

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum ***wr. wb.***

Yogyakarta, 18 Juni 2019
Pembimbing

Muhammad Taufiq Nuruzzaman, S.T. M.Eng.
NIP. 19791118 200501 1 003

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Anwaruddin Kamal Ibrahim
NIM	: 12650072
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **" Analisis Keamanan Sistem Informasi Dengan Penetration Testing dan ISO 27001:2013 (Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah PWM DIY)"** tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 18 Juni 2019

Yang Menyatakan

Anwaruddin Kamal Ibrahim
NIM. 12650072

KATA PENGANTAR

Bismillahirrahmanirrahim, puji syukur atas kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah serta inayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Keamanan Sistem Informasi Dengan Penetration Testing dan ISO 27001:2013 (Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah PWM DIY)" ini dengan baik sesuai dengan kewajiban dalam memenuhi gelar Strata 1 Komputer (S.Kom) di Jurusan Teknik Informatika Fakultas Sains dan teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Tidak lupa shalawat serta salam tetap tercurah kepada junjungan Nabi Muhammad SAW dan semoga kelak kita mendapat syafaat darinya.

Oleh karena itu, penulis ingin mengucapkan terima kasih sebesarbesarnya kepada:

1. Bapak Prof. Drs. K.H. Yudian Wahyudi, M.A., Ph.D. selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Bapak Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
3. Bapak Sumarsono, S.T., M.Kom., selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
4. Bapak Aulia Faqih Rifa'i, M.Kom., selaku dosen pembimbing akademik kelas reguler Teknik Informatika 2012.
5. Bapak Muhammad Taufiq Nuruzzaman, S.T. M.Eng., selaku Dosen Pembimbing skripsi yang telah memberikan arahan, saran, waktu serta masukan kepada penulis dalam menyusun skripsi.
6. Bapak dan Ibu Dosen Program Studi Informatika UIN Sunan Kalijaga yang telah memberikan banyak bekal ilmu kepada penulis.

7. Pihak Pimpinan Wilayah Muhammadiyah Yogyakarta yang telah memberikan izin penelitian.
8. Orang tua dan keluarga tercinta yang senantiasa memberikan motivasi serta dukungan baik moril maupun materiil kepada penulis dengan sumua kasih sayangnya.
9. Teman-teman Teknik Informatika yang tidak dapat disebutkan satu persatu yang telah memberikan bantuan, dukungan, serta motivasi kepada penulis.
10. Semua pihak yang telah memberikan bantuan dan dukungan selama menempuh strata satu teknik informatika khususnya dalam penyusunan skripsi ini yang tidak dapat disebut satu persatu. Terima kasih.

Semoga Allah SWT memlalas amal kebaikan dari seluru pihak yang telah membantu penulis menyelesaikan skripsi. Penulis menyadari sepenuhnya masih banyak kesalahan dan kekurangan dalam skripsi ini, maka dari itiu berbagai saran dan kritik sangat diharapkan demi perbaikan. Semoga skripsi ini dapat bermanfaat bagi penyusun sendiri pada khususnya dan bagi para pembaca pada umumnya. Terima kasih.

Yogyakarta, 25 Juni 2019

Penulis

HALAMAN PERSEMBAHAN

Laporan skripsi ini saya persembahkan kepada:

1. Kedua Orang tua, Bapak Muhammad Luqman dan Ibu Syarifah.
2. Kakak dan Adik, Alvina Dian Firdausi dan Arya Choirul Fikri.
3. Teman – teman yang selalu memberikan dukungan dalam pembuatan skripsi Faizin, Alfian Gautama, Pamuji, Alif Aziz, Siti Fatimah, Fauzi, Wahib, Robin, Alfian Nur Jayanto.
4. Teman-teman Teknik Informatika 2012
5. Teman-teman guru dan karyawan di SMP Muhammadiyah 1 Depok

HALAMAN MOTTO

لَنْ تَرْجِعَ الأَيَّامُ الَّتِي مَضَتْ

Tidak akan kembali hari-hari yang telah berlalu

HIDUP SEKALI HIDUPLAH YANG BERARTI

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ANALISIS KEAMANAN SISTEM INFORMASI DENGAN PENETRATION TESTING DAN ISO 27001:2013 (STUDI KASUS SISTEM INFORMASI MANAJEMEN ASET MUHAMMADIYAH PWM DIY)

Anwaruddin Kamal Ibrahim
NIM 12650072

INTISARI

Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) adalah sistem informasi berbasis web yang dikembangkan Majelis Wakaf dan Kehartabendaan PWM DIY untuk membantu proses pengelolaan aset Muhammadiyah. Tentunya, data yang tersimpan dalam SIMAM merupakan data penting yang harus dilindungi. Untuk mengetahui tingkat keamanan SIMAM, pengujian keamanan diperlukan untuk mengetahui celah keamanan dalam sistem, sehingga dapat dilakukan perbaikan pada SIMAM. Dan perlu dilakukan audit keamanan sistem informasi untuk memastikan kebijakan keamanan informasi diterapkan sesuai prosedur.

Penelitian ini dilakukan dengan melakukan *penetration testing* terhadap SIMAM menggunakan *tools* berupa perangkat lunak antara lain *Dmitry, Nmap, OWASP ZAP, Acunetix, Metasploit, SQLmap,* dan *XSSer*. Sedangkan audit keamanan sistem informasi kami menggunakan ISO/IEC 27001 yang merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) yang secara umum membahas mengenai apa yang seharusnya dilakukan dalam usaha mengimplementasikan konsep – konsep keamanan informasi.

Hasil penetration testing terhadap Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) sebagai berikut. Nmap menemukan 4 port terbuka. OWASP ZAP menemukan total 9 kerentanan. Acunetix menemukan total 25 kerentanan. Metasploit telah menemukan 1 kerentanan. Dalam eksploitasi kami tidak berhasil melakukan serangan dengan Sqlmap dan XSSer. Sedangkan hasil audit terhadap Majelis Wakaf dan Kehartabendaan PWM DIY selaku penanggung jawab SIMAM, memperoleh nilai kematangan 2.32 (*Repeatable But Intuitive*).

Kata kunci: *Penetration Testing, Dmitry, Nmap, OWASP ZAP, Acunetix, Metasploit, SQLmap, XSSer, Audit Sistem Informasi, ISO/IEC 27001*.

ANALYSIS OF INFORMATION SYSTEM SECURITY WITH PENETRATION TESTING AND ISO 27001: 2013 (CASE STUDY OF MUHAMMADIYAH ASSET MANAGEMENT INFORMATION SYSTEM)

Anwaruddin Kamal Ibrahim
NIM 12650072

ABSTRACT

Muhammadiyah Asset Management Information System (SIMAM) is a web-based information system developed by the PWM DIY Waqf Assembly to assist the process of asset management of Muhammadiyah. The data stored in SIMAM is important data that must be protected. Security testing is needed to find security holes in the system, that improvements can be made to SIMAM. And it is necessary to conduct an information system security audit to ensure that information security policies are implemented according to the procedure.

This research is carried out by conducting penetration testing of SIMAM using tools such as software including Dmitry, Nmap, OWASP ZAP, Acunetix, Metasploit, SQLmap, and XSSer. While our information system security audit uses ISO / IEC 27001 which is a standard document of the Information Security Management System (ISMS) which generally discusses what should be done in an effort to implement information security concepts.

Penetration testing results for the Case Study of the Muhammadiyah Asset Management Information System (SIMAM). Nmap finds 4 open ports. OWASP ZAP found a total of 9 vulnerabilities. Acunetix found a total of 25 vulnerabilities. Metasploit has found 1 vulnerability. In exploitation we did not succeed in carrying out attacks with Sqlmap and XSSer. While the results of the audit of the PWM DIY Wakaf Assembly as the person in charge of SIMAM, obtained a maturity value of 2.32 (Repeatable But Intuitive).

Keywords: *Penetration Testing, Dmitry, Nmap, OWASP ZAP, Acunetix, Metasploit, SQLmap, XSSer, Information System Audit, ISO / IEC 27001.*

BAB I
PENDAHULUAN

1.1 Latar Belakang

John D Howard mengatakan dalam Disertasinya *An Analysis of Security Incident on the Internet* 1989-1995, " *Computer Security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks."* (Howard, 1997)

Sedangkan fakta yang sampaikan oleh pakar keamanan siber Pratama Persadha dari ID-SIRTII/CC mengatakan, "Kejadian di 2017 menjadi penanda bagi semua pihak khususnya pemerintah untuk lebih serius memperhatikan isu keamanan siber. Terlebih, *Indonesian Security Incident Response Team on Internet Infrastructure/Coordinator Center* (Id-SIRTII/CC) mencatat, hingga November 2017, Indonesia mendapat sebanyak 205.502.159 serangan keamanan siber." (Nugraheny, 2017)

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan sering kali berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan.

Saat ini informasi sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial, organisasi non-komersial, perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Jaringan komputer seperti internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai berbondong-bondong membuat sistem informasinya dan menghubungkan ke Internet. Terhubungnya komputer ke Internet membuka potensi adanya lubang keamanan yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit untuk mengakses informasi.

Majelis Wakaf dan Kehartabendaan PWM DIY adalah salah satu organisasi yang menggunakan sistem informasi untuk membantu meringankan tugas mereka. Majelis Wakaf dan Kehartabendaan PWM DIY memanfaatkan sistem informasi untuk mempermudah pengelolaan aset dengan membuat SIMAM (Sistem Informasi Manajemen Aset Muhammadiyah). SIMAM dibuat untuk mempermudah Majelis Wakaf dan Kehartabendaan PWM DIY untuk mendata dan mengelola aset yang dimuliki PWM DIY yang berada di seluruh wilayah Daerah Istimewa Yogyakarta.

Untuk menanggulangi resiko keamanan pada SIMAM maka diperlukan beberapa proses penanggulangan resiko. Dalam penelitian ini proses penanggulangan resiko yang akan kami lakukan adalah *penetration testing*. *Penetration testing* adalah penilaian dengan mengevaluasi kerentanan yang teridentifikasi untuk memverifikasi adanya kerentanan. *Penetration testing* akan mencoba menyerang kerentanan tersebut dengan cara yang sama seperti peretas untuk memverifikasi kerentanan mana yang sebenarnya merupakan ancaman keamanan sistem.

Langkah menanggulangi resiko keamanan pada SIMAM yang kedua adalah melakukan audit keamanan sistem informasi menggunakan standar ISO 27001. Dengan audit keamanan menggunakan ISO 27001 diharapkan organisasi dapat membangun dan memelihara sistem manajemen keamanan informasi. ISO 27001

merupakan dokumen standar untuk Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan gambaran umum mengenai apa saja yang harus dilakukan untuk implementasi konsep-konsep keamanan informasi dalam sebuah perusahaan. ISO 27001 sangat fleksibel dikembangkan karena tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai, dan ukuran struktur organisasi.

1.2 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang didapat adalah sebagai berikut :

1. Bagaimana merencanakan dan melaksanakan analisis keamanan sistem informasi manajemen aset muhammadiyah menggunakan *penetration testing* dan ISO 27001:2013?
2. Bagaimana mengetahui kerentanan pada keamanan sistem informasi manajemen aset muhammadiyah menggunakan *penetration testing*?
3. Bagaimana melaksanakan audit keamanan sistem informasi manajemen aset muhammadiyah berdasarkan standar ISO 27001: 2013?
4. Bagaimana menyusun hasil analisis keamanan sistem informasi manajemen aset muhammadiyah menggunakan *penetration testing* dan ISO 27001: 2013?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Data yang digunakan dalam analisis dan pembahasan masalah adalah data yang diperoleh dari *penetration testing*, observasi dan wawancara.
2. *Penetration testing* dilakukan menggunakan alat yang terdapat dalam Kali Linux. Alat yang akan digunakan adalah Dmitry dan Nmap untuk mengumpulkan informasi . OWASP ZAP, Acunetix, dan Metasloit untuk mendeteksi kerentanan. SQLmap dan XSSer untuk eksploitasi kerentanan.
3. Klausul ISO 27001:2013 yang digunakan adalah:

a) Kebijakan Keamanan Informasi A.5
b) Pengelolaan Aset A.8
c) Pengendalian Akses A.9
d) Keamanan Fisik Dan Lingkungan A.11

4. Metode penilaian yang digunakan adalah metode *scoring* dengan pendekatan sesuai standar ISO 27001 yaitu *maturity level model*.

1.4 Tujuan Penelitian

Berdasar latar belakang serta rumusan masalah di atas, maka tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Melaksanakan analisis keamanan sistem informasi manajemen aset muhammadiyah menggunakan *penetration testing* dan ISO 27001:2013.
2. Melaporkan hasil kerentanan pada keamanan sistem informasi manajemen aset Muhammadiyah berdasarkan hasil *penetration testing*.
3. Mendapatkan hasil pengukuran audit keamanan sistem informasi manajemen aset Muhammadiyah sesuai standar ISO 27001:2013.
4. Menyusun hasil analisis keamanan sistem informasi manajemen aset Muhammadiyah berdasarkan hasil *penetration testing* dan ISO 27001:2013 yang berupa temuan dan rekomendasi yang dapat digunakan untuk perbaikan dan peningkatan keamanan sistem informasi aset.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Pihak Pimpinan Wilayah Muhammadiyah DIY dapat mengetahui kerentanan pada keamanan sistem informasi manajemen aset Muhammadiyah berdasarkan *penetration testing*.
2. Pihak Pimpinan Wilayah Muhammadiyah DIY dapat mengetahui kekurangan mereka dalam manajemen keamanan sistem informasi berdasarkan audit keamanan sistem informasi manajemen aset Muhammadiyah berdasarkan standar ISO 27001:2013.

3. Mandapatkan laporan dan rekomendasi hasil analisis keamanan sistem informasi manajemen aset muhammadiyah dari *penetration testing* dan hasil analisis manajemen pengelolaan sistem informasi manajemen aset muhammadiyah berdasarkan ISO 27001:2013.

1.6 Keaslian Penelitian

Penelitian sejenis mengenai analisis keamanan sistem informasi sebelumnya sudah banyak dilakukan oleh beberapa peneliti. Namun penelitian tentang " Analisis Keamanan Sistem Informasi dengan Penetration Testing dan ISO 27001:2013 untuk Sistem Informasi Manajemen Aset Muhammadiyah PWM DIY" belum pernah dilakukan sebelumnya.

BAB VI
PENUTUP

6.1. Kesimpulan

Setalah proses penelitian Analisis Keamanan Sistem Informasi Dengan *Penetration Testing* Dan ISO 27001:2013 (Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah PWM DIY), yang dimulai dengan penetration testing dan dilanjutkan dengan audit menggunakan ISO 27001. Kami menyimpulkan hasil penelitian sebagai berikut:

a) Hasil *penetration testing* terhadap Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) sebagai berikut. Dalam *information gathering*, ditemukan 4 *port* yang terbuka yaitu *port* 80, 443, 3306, dan 10123. Dalam *vulnerability assesment* ditemukan beberapa kerentanan antara lain. OWASP ZAP menemukan total 9 kerentanan melalui 2 kali pemindaian. Dengan rincian 3 kerentanan menengah, dan 6 kerentanan rendah. Acunetix menemukan total 25 kerentanan melalui 2 kali pemindaian. Dengan rincian 2 kerentanan tinggi, 7 kerentanan menengah, 13 kerentanan rendah, dan 3 informasi. Metasploit telah menemukan 1 kerentanan. Dalam eksploitasi kami tidak berhasil melakukan serangan dengan Sqlmap dan XSSer.
b) Hasil audit yang telah kami lakukan terhadap pimpinan majelis wakaf dan kehartabendaan PWM DIY selaku penanggung jawab Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) kami mendapatkan hasil Maturity level sebesar 2.32 (*Repeatable But Intuitive)*.

c) Rekomendasi dari hasil penetration testing dan audit menggunakan ISO 27001 telah kami susun. Rekomendasi tersebut kami susun berdasarkan temuan yang kami dapatkan selama penelitian.

6.2. Saran

Setelah semua proses penelitian yang telah kami laksanakan, kami masih merasa ada banyak kekurangan yang harus diperbaiki. Sehingga kami berharap untuk penelitian lebih lanjut, kamimemberikan saran sebagai berikut:

a) Kami merekomendasikan majelis wakaf dan kehartabendaan PWM DIY untuk menerapkan standar ISO 27001 secara menyeluruh.
b) Diharapkan penelitian lebih lanjut mengenai Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) dapat menggunakan semua klausul yang ada pada ISO 27001. Sehingga nilai kematangan dapat menyeluruh pada semua proses manajemen keamanan informasi.
c) Kami berharap rekomendasi kami kepada majelis wakaf dan kehartabendaan PWM DIY baik rekomendasi hasil penetration testing maupun hasil audit ISO 27001 dapat dilaksanakan untuk meningkatkan keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM).

DAFTAR PUSTAKA

Ahmad, A. (2012). Bakuan Audit Keamanan Informasi Kemenpora. Dalam M. Dr. H. Amar Ahmad, *Bakuan Audit Keamanan Informasi Kemenpora.* Jakarta: Kementerian Pemuda dan Olahraga.

Baloch, R. (2015). *Ethical Hacking and Penetration Testing Guide.* CRC Press.

Beggs, R. W. (2014). *Mastering Kali Linux for Advanced Penetration Testing.* Packt Publishing.

Calder, A., & Watkins, S. (2008). *It Governance: A Manager's Guide To Data Security And ISO 27001 ISO 27002 4th Edition.* Kogan Page.

DMitry. (2019). *https://mor-pah.net/software/dmitry-deepmagic-information-gathering-tool/*. Diambil kembali dari Mor-Pah.net: https://mor-pah.net/software/dmitry-deepmagic-information-gathering-tool/

Howard, J. D. (1997). An Analysis of Security Incident on the Internet 1989-1995. *Carnegie Mellon University*.

iso27001security.com. (2018). *iso27001security*. Diambil kembali dari iso27001security.com: http://www.iso27001security.com/html/27001.html

Juhdan. (2016). *Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001.* Yogyakarta: Skripsi Thesis, Uin Sunan Kalijaga .

Kadir, A. (2003). *Pengenalan Sistem Informasi.* Yogyakarta : Andi.

Kristanto, A. (2008). *Perancangan Sistem Informasi Dan Aplikasinya.* Yogyakarta: Gava Media.

Kurniawan, E. (2018). *Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013*

Menggunakan SSE-CMM. Yogyakarta: Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.

Metasari, D. (2014). *Analisis Keamanan Website Di Universitas Muhammadiyah Surakarta.* Skripsi thesis, Universitas Muhammadiyah Surakarta.

Metasploit. (2019). *Geting started*. Diambil kembali dari Metasploit Rapid7: https://metasploit.help.rapid7.com/docs

Mulyanto, A. (2009). *Sistem Informasi Konsep & Aplikasi.* Yogyakarta: Pustaka Pelajar.

Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing with Kali Linux.* Packt Publishing.

Nmap. (2019). *nmap scurity scanner*. Diambil kembali dari nmap: https://nmap.org/

Nugraheny, D. E. (2017, Desember 27). *Kasus Keamanan Siber Ini Bikin Heboh Sepanjang 2017*. Diambil kembali dari https://www.republika.co.id: https://www.republika.co.id/berita/trendtek/internet/17/12/27/p1livw414-kasus-keamanan-siber-ini-bikin-heboh-sepanjang-2017

OWASP. (2017). *OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks.* Diambil kembali dari owasp.org: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main

Permatasari, D. I. (2016). *Audit Keamanan Informasi Berdasarkan Standar Sni-Iso 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.* Yogyakarta: Skripsi Thesis, Uin Sunan Kalijaga .

Prasad, P. (2016). *Mastering Modern Web Penetration Testing.* Packt Publishing.

Raharjo, B. (1999). *Keamanan Sistem Informasi Berbasis Internet.* Diambil kembali dari PT Insan Komunikasi: http://www.geocities.ws/hme_istn/Efiles/handbook.pdf

Sarno, R. (2009). Audit Sistem Informasi dan Teknologi Informasi. Dalam R. Sarno, *Audit Sistem Informasi dan Teknologi Informasi.* Bandung: Itspress.

SQLmap. (2019). *sqlmap introduction*. Diambil kembali dari http://sqlmap.org/: http://sqlmap.org/

Taufiq, F. M. (2017). *Vulnerability Analisis Untuk Peningkatan Sistem Keamanan Website (Studi Kasus Di Lingkungan UMM).* Malang: Fakultas Teknik Universitas Muhammadiyah Malang.

Wecan, P. P. (2017). *Pengujian Keamanan Sistem Informasi Akademik UIN Sunan Kalijaga Yogyakarta.* YOGYAKARTA: Skripsi thesis, UIN SUNAN KALIJAGA.

Weidman, G. (2014). *Penetration Testing A Hands On Introduction to Hacking.* No Starch Press.

Wibirama, S. (2013, April 30). *Bagaimana Membuat Studi Pustaka yang Baik*. Diambil kembali dari http://wibirama.staff.ugm.ac.id: http://wibirama.staff.ugm.ac.id/2013/04/30/sunu-wibirama-bagaimana-membuat-studi-pustaka-yang-baik/

Williams, J., & wichers, d. (2013). OWASP top 10 2013 The Ten Most Critical Web Aplication Security Risk. Dalam D. W. Jeff Williams, *OWASP top 10 2013 The Ten Most Critical Web Aplication Security Risk* (hal. 20). Bel Air, Los Angeles: OWASP Foundation.

ZAP, O. (2019). *owasp zap*. Diambil kembali dari owasp: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

LAMPIRAN

JADWAL PENETILIAN

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

No	Kegiatan	Januari				Februari				Maret				April			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Studi Literatur																
2.	Pengambilan Data																
3	Penetration testing																
4	Audit Sistem Informasi																
5	Rekomendasi																
6	Kesimpulan Penelitian																
7	Penyusunan Laporan Hasil Penelitian																

SURAT IZIN PENELITIAN

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA
FAKULTAS SAINS DAN TEKNOLOGI
Alamat: Jln. Marsda Adisucipto telephon 0274519739 fax 0274540971
http://saintek.uin-suka.ac.id Yogyakarta 55281

Nomor : B- 144/Un 02/DST 1/PP.05.3/01/2019 14 Januari 2019
Sifat : Penting
Lamp. : 1 bendel Proposal
Hal : Permohonan Izin Penelitian

Kepada:
Yth. H.Jarot Wahyudi, S.H.,M.A.
Ketua Majelis Wakaf dan Kehartabendaan PWM DIY
Di Yogyakarta

Assalamu'alaikum Wr.Wb.

Kami beritahukan bahwa untuk memenuhi penyusunan tugas akhir/skripsi yang berjudul : Analisis Keamanan Sistem Informasi dengan Penetrotion Testing dan SNI ISO/IEC 270012013 (Studi Kasus Sistem Informasi Manajemen Aset Muhammadiyah PWM DIY) diperlukan penelitian.Oleh karena itu, kami mengharap kiranya Bapak/Ibu berkenan memberikan izin penelitian bagi mahasiswa kami :

Nama : Anwaruddin Kamal Ibrahim
NIM : 12650072
Program Studi : Teknik Informatika
Semester : XIV
Alamat : Jl.Utama gang Graskap Pugeran, Maguwaharjo, Depok, Sleman DIY.
Untuk Melakukan penelitian di : Pimpinan Wilayah Muhammadiyah DIY
Metode pengumpulan data : Pengujian SIMAM, Observasi dan Wawancara
Adapun waktunya mulai tgl : 14 Januari 2019 s.d 31 Maret 2019

Demikian surat permohonan ini disampaikan, atas diperkenankannya diucapkan terimakasih.

Wassalamu'alaikum Wr.Wb.

Dekan,
Wakil Dekan Bidang Akademik

Agung Fatwanto

Tembusan:
Dekan (sebagai laporan)

LAMPIRAN *PENETRATION TESTING*

Sistem Informasi Manajemen Aset Muhammadiyah

HASIL SCAN NMAP

<?xml version="1.0" encoding="iso-8859-1"?>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?><nmaprun start="1548309050" profile_name="Intense scan, all TCP ports" xmloutputversion="1.04" scanner="nmap" version="7.70" startstr="Thu Jan 24 12:50:50 2019" args="nmap -p 1-65535 -T4 -A -v 103.19.180.123"><scaninfo services="1-65535" protocol="tcp" numservices="65535" type="syn"></scaninfo><verbose level="1"></verbose><debugging level="0"></debugging><output type="interactive">Starting Nmap 7.70 (https://nmap.org) at 2019-01-24 12:50 WIB
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:50
Completed NSE at 12:50, 0.00s elapsed
Initiating NSE at 12:50
Completed NSE at 12:50, 0.00s elapsed
Initiating Ping Scan at 12:50
Scanning 103.19.180.123 [4 ports]
Completed Ping Scan at 12:50, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:50
Completed Parallel DNS resolution of 1 host. at 12:51, 13.00s elapsed
Initiating SYN Stealth Scan at 12:51
Scanning 103.19.180.123 [65535 ports]
Discovered open port 80/tcp on 103.19.180.123
Discovered open port 443/tcp on 103.19.180.123
Discovered open port 3306/tcp on 103.19.180.123
Discovered open port 10123/tcp on 103.19.180.123
Completed SYN Stealth Scan at 12:51, 17.45s elapsed (65535 total ports)
Initiating Service scan at 12:51
Scanning 4 services on 103.19.180.123
Completed Service scan at 12:51, 12.14s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 103.19.180.123
Retrying OS detection (try #2) against 103.19.180.123
Initiating Traceroute at 12:51
Completed Traceroute at 12:51, 3.02s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 12:51
Completed Parallel DNS resolution of 4 hosts. at 12:51, 13.00s elapsed
NSE: Script scanning 103.19.180.123.
Initiating NSE at 12:51
Completed NSE at 12:51, 5.15s elapsed

```
Initiating NSE at 12:51
Completed NSE at 12:51, 0.01s elapsed
Nmap scan report for 103.19.180.123
Host is up (0.010s latency).
Not shown: 65526 closed ports
PORT     STATE    SERVICE  VERSION
25/tcp   filtered smtp
80/tcp   open     http     nginx 1.10.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.10.3
|_http-title: QASS UAD v2
443/tcp  open     ssl/http nginx 1.10.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.10.3
|_http-title: Did not follow redirect to https://simam.wakafmu.org/login
| ssl-cert: Subject: commonName=simam.wakafmu.org
| Subject Alternative Name: DNS:simam.wakafmu.org,
DNS:www.simam.wakafmu.org
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's
Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-11-10T15:37:47
| Not valid after:  2019-02-08T15:37:47
| MD5:   dbc5 d086 6517 775a 9c13 6d48 6e19 d8f8
|_SHA-1: a947 fa6c db74 f888 cfc4 dfe1 3f84 30aa a0a7 bfbb
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
1720/tcp  filtered h323q931
3306/tcp  open     mysql    MySQL 5.5.5-10.1.26-MariaDB-0+deb9u1
|_mysql-info: ERROR: Script execution failed (use -d to debug)
7547/tcp  filtered cwmp
10123/tcp open     ssh      OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
| ssh-hostkey:
|   2048 a6:de:f6:ce:e9:59:7d:af:6f:89:15:d2:c3:fe:5d:52 (RSA)
|   256 24:74:56:60:76:c9:7c:24:0c:6c:f7:b1:ff:11:8e:4f (ECDSA)
```

```
|_  256 87:ee:56:60:26:a0:d8:0a:c4:55:84:a9:8a:3f:d2:f0 (ED25519)
30005/tcp filtered unknown
58000/tcp filtered unknown
Device type: general purpose|broadband
router|WAP|printer|webcam|specialized
Running (JUST GUESSING): Linux 2.6.X|2.4.X (89%), Asus embedded
(89%), Lexmark embedded (88%), AXIS embedded (86%), Crestron 2-
Series (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:asus:rt-ac66u cpe:/h:asus:rt-
n16 cpe:/h:lexmark:x644e cpe:/o:linux:linux_kernel:2.4
cpe:/h:axis:211_network_camera cpe:/o:linux:linux_kernel:2.6.20
cpe:/o:crestron:2_series
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (89%), Asus RT-AC66U
router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%), Asus RT-
N66U WAP (Linux 2.6) (89%), Tomato 1.28 (Linux 2.6.22) (89%), Lexmark
X644e printer (88%), Linux 2.6.24 (87%), OpenWrt 0.9 - 7.09 (Linux 2.4.30
- 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%),
OpenWrt Kamikaze 7.09 (Linux 2.6.22) (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Thu Jan 24 12:51:35 2019)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Random positive increments
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   ...
2   12.19 ms 36.73.64.1
3   12.36 ms 125.160.1.197
4   2.24 ms  192.168.107.2 (192.168.107.2)
5   2.28 ms  103.19.180.123

NSE: Script Post-scanning.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.45 seconds
```

Raw packets sent: 66129 (2.911MB) | Rcvd: 66225 (2.656MB)
</output><host comment=""><status state="up"></status><address
addrtype="ipv4" vendor=""
addr="103.19.180.123"></address><hostnames></hostnames><ports><extr
aports count="65526" state="closed"></extraports><port protocol="tcp"
portid="25"><state reason="admin-prohibited" state="filtered"
reason_ttl="254"></state><service method="table" conf="3"
name="smtp"></service></port><port protocol="tcp" portid="80"><state
reason="syn-ack" state="open" reason_ttl="251"></state><service
product="nginx" version="1.10.3" method="probed" conf="10"
name="http"></service></port><port protocol="tcp" portid="443"><state
reason="syn-ack" state="open" reason_ttl="53"></state><service
product="nginx" version="1.10.3" method="probed" conf="10"
name="http"></service></port><port protocol="tcp" portid="1720"><state
reason="no-response" state="filtered" reason_ttl="0"></state><service
method="table" conf="3" name="h323q931"></service></port><port
protocol="tcp" portid="3306"><state reason="syn-ack" state="open"
reason_ttl="53"></state><service product="MySQL" version="5.5.5-
10.1.26-MariaDB-0+deb9u1" method="probed" conf="10"
name="mysql"></service></port><port protocol="tcp"
portid="7547"><state reason="no-response" state="filtered"
reason_ttl="0"></state><service method="table" conf="3"
name="cwmp"></service></port><port protocol="tcp"
portid="10123"><state reason="syn-ack" state="open"
reason_ttl="53"></state><service product="OpenSSH" name="ssh"
extrainfo="protocol 2.0" version="7.4p1 Debian 10+deb9u4" conf="10"
method="probed"></service></port><port protocol="tcp"
portid="30005"><state reason="no-response" state="filtered"
reason_ttl="0"></state><service method="table" conf="3"
name="unknown"></service></port><port protocol="tcp"
portid="58000"><state reason="no-response" state="filtered"
reason_ttl="0"></state><service></service></port></ports><os><portused
state="open" portid="80" proto="tcp"></portused><portused state="closed"
portid="1" proto="tcp"></portused><portused state="closed"
portid="39289" proto="udp"></portused><osmatch line="49721"
name="Linux 2.6.18 - 2.6.22" accuracy="89"><osclass type="general
purpose" osfamily="Linux" vendor="Linux" osgen="2.6.X"
accuracy="89"></osclass></osmatch><osmatch line="8205" name="Asus
RT-AC66U router (Linux 2.6)" accuracy="89"><osclass type="broadband
router" osfamily="Linux" vendor="Linux" osgen="2.6.X"
accuracy="89"></osclass></osmatch><osmatch line="60654" name="Asus
RT-N16 WAP (Linux 2.6)" accuracy="89"><osclass type="WAP"

osfamily="embedded" vendor="Asus" osgen=""
accuracy="89"></osclass></osmatch><osmatch line="60695" name="Asus
RT-N66U WAP (Linux 2.6)" accuracy="89"><osclass type="WAP"
osfamily="embedded" vendor="Asus" osgen=""
accuracy="89"></osclass></osmatch><osmatch line="61392"
name="Tomato 1.28 (Linux 2.6.22)" accuracy="89"><osclass type="WAP"
osfamily="Linux" vendor="Linux" osgen="2.6.X"
accuracy="89"></osclass></osmatch><osmatch line="43254"
name="Lexmark X644e printer" accuracy="88"><osclass type="printer"
osfamily="embedded" vendor="Lexmark" osgen=""
accuracy="88"></osclass></osmatch><osmatch line="51944" name="Linux
2.6.24" accuracy="87"><osclass type="general purpose" osfamily="Linux"
vendor="Linux" osgen="2.6.X"
accuracy="87"></osclass></osmatch><osmatch line="46532"
name="OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34)" accuracy="87"><osclass
type="WAP" osfamily="Linux" vendor="Linux" osgen="2.4.X"
accuracy="87"></osclass></osmatch><osmatch line="46571"
name="OpenWrt White Russian 0.9 (Linux 2.4.30)"
accuracy="87"><osclass type="WAP" osfamily="Linux" vendor="Linux"
osgen="2.4.X" accuracy="87"></osclass></osmatch><osmatch
line="61315" name="OpenWrt Kamikaze 7.09 (Linux 2.6.22)"
accuracy="87"><osclass type="WAP" osfamily="Linux" vendor="Linux"
osgen="2.6.X" accuracy="87"></osclass></osmatch></os><uptime
lastboot="Thu Jan 24 12:51:35 2019"
seconds="24"></uptime><tcpsequence index="262"
values="74168C3C,953C82B7,D3641FC0,7214ABF8,D5D66E19,D546941
4" difficulty="Good luck!"></tcpsequence><ipidsequence
values="F50,2A50,42AA,5AA8,7590,9190" class="Random positive
increments"></ipidsequence><tcptssequence
values="D5699C02,10B3E402,B6325800,D529E802,B313D402,3FDA1002
" class="other"></tcptssequence><trace port="80" proto="tcp"><hop
rtt="12.19" host="" ipaddr="36.73.64.1" ttl="2"></hop><hop rtt="12.36"
host="" ipaddr="125.160.1.197" ttl="3"></hop><hop rtt="2.24"
host="192.168.107.2" ipaddr="192.168.107.2" ttl="4"></hop><hop
rtt="2.28" host="" ipaddr="103.19.180.123"
ttl="5"></hop></trace></host><runstats><finished timestr="Thu Jan 24
12:51:59 2019" time="1548309119"></finished><hosts down="0" total="1"
up="1"></hosts></runstats></nmaprun>

HASIL SCAN OWASP ZAP

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	6
Informational	0

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://103.19.180.123
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://simam.wakafmu.org/login
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://simam.wakafmu.org
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://103.19.180.123
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://103.19.180.123
Method	GET
Parameter	X-XSS-Protection
URL	http://103.19.180.123/robots.txt
Method	GET
Parameter	X-XSS-Protection
URL	http://103.19.180.123/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
Instances	3
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
Other information	X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://simam.wakafmu.org/static/images/favicon-32x32.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://simam.wakafmu.org/static/images/apple-touch-icon.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://simam.wakafmu.org/login
Method	GET
Parameter	X-Content-Type-Options
URL	https://simam.wakafmu.org/static/images/favicon-16x16.png
Method	GET
Parameter	X-Content-Type-Options
Instances	4
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://simam.wakafmu.org/robots.txt
Method	GET
Parameter	X-XSS-Protection
URL	https://simam.wakafmu.org/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	https://simam.wakafmu.org/login
Method	GET
Parameter	X-XSS-Protection
Instances	3
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss
Other information	The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://simam.wakafmu.org
Method	GET
Parameter	X-XSS-Protection
Instances	1
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss
Other information	The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://simam.wakafmu.org
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

ACUNETIX

Scan of simam.wakafmu.org

Scan details

Scan information	
Start time	10/04/2019, 19:00:40
Start url	https://simam.wakafmu.org
Host	simam.wakafmu.org
Scan time	35 minutes, 27 seconds
Profile	Full Scan
Server information	nginx/1.10.3
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	13
High	1
Medium	3
Low	7
Informational	2

Affected items

Web Server	
Alert group	nginx Integer Overflow
Severity	High
Description	A security issue was identified in nginx range filter. A specially crafted request might result in an integer overflow and incorrect processing of ranges, potentially resulting in sensitive information leak (CVE-2017-7529). When using nginx with standard modules this allows an attacker to obtain a cache file header if a response was returned from cache. In some configurations a cache file header may contain IP address of the backend server or other sensitive information. Besides, with 3rd party modules it is potentially possible that the issue may lead to a denial of service or a disclosure of a worker process memory.
Recommendations	Upgrade nginx to the latest version or apply the patch provided by the vendor.
Alert variants	
Details	Not available in the free trial

Web Server	
Alert group	.htaccess file readable
Severity	Medium
Description	This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. .htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.
Recommendations	Restrict access to the .htaccess file by adjusting the web server configuration.
Alert variants	
Details	Not available in the free trial

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**TLS 1.0 enabled**
Severity	Medium
Description	The web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.
Recommendations	It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial
[illegible]	
Web Server	
Alert group	**Login page password-guessing attack**
Severity	Low
Description	A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
Recommendations	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.
Alert variants	
Details	Not available in the free trial
[illegible]	
Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial
[illegible]	

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Possible sensitive files**
Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Possible sensitive files**
Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Content Security Policy (CSP) not implemented**
Severity	Informational

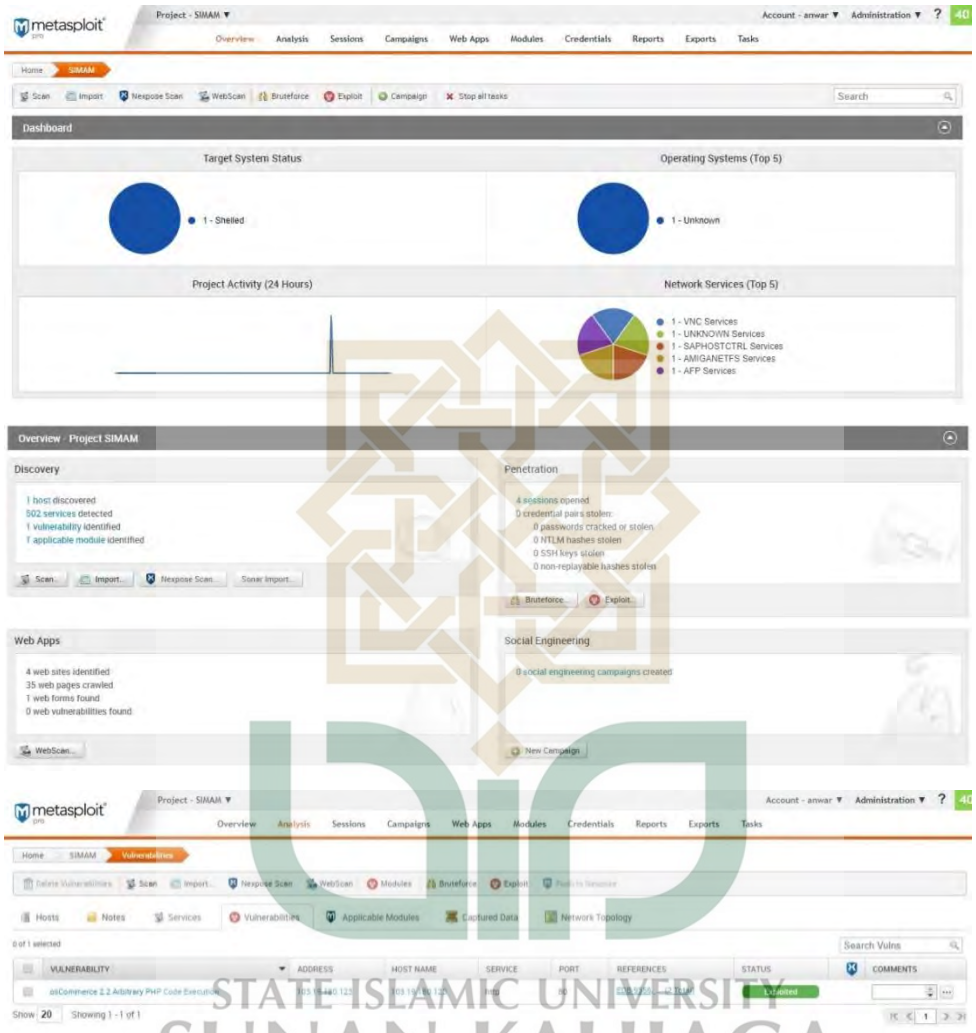
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following: [illegible] It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.
Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	Not available in the free trial
[illegible]	

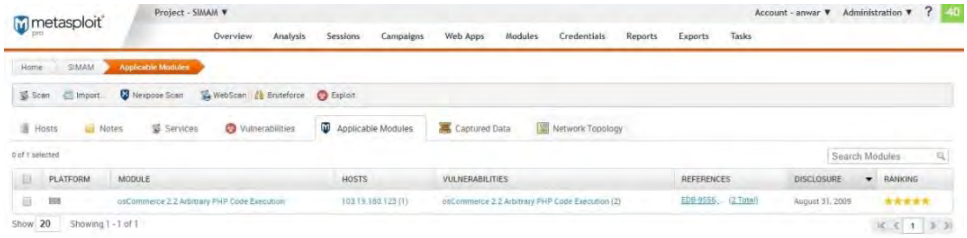
Web Server	
Alert group	**TLS 1.1 enabled**
Severity	Informational
Description	The web server supports encryption through TLS 1.1. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended (although at the time of writing not required) to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.
Recommendations	It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.
Alert variants	
Details	Not available in the free trial
[illegible]	

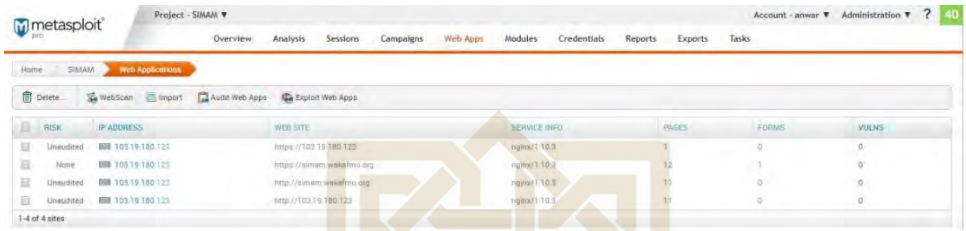
Scanned items (coverage report)

https://simam.wakafmu.org/
https://simam.wakafmu.org/login
https://simam.wakafmu.org/private
https://simam.wakafmu.org/private/
https://simam.wakafmu.org/private/.htaccess
https://simam.wakafmu.org/static/
https://simam.wakafmu.org/static/fonts/
https://simam.wakafmu.org/static/images/
https://simam.wakafmu.org/static/js/
https://simam.wakafmu.org/static/js/plugins/
https://simam.wakafmu.org/system
https://simam.wakafmu.org/system/
https://simam.wakafmu.org/system/.htaccess
https://simam.wakafmu.org/system/core/
https://simam.wakafmu.org/system/core/compat/
https://simam.wakafmu.org/system/database
https://simam.wakafmu.org/system/database/
https://simam.wakafmu.org/system/fonts/

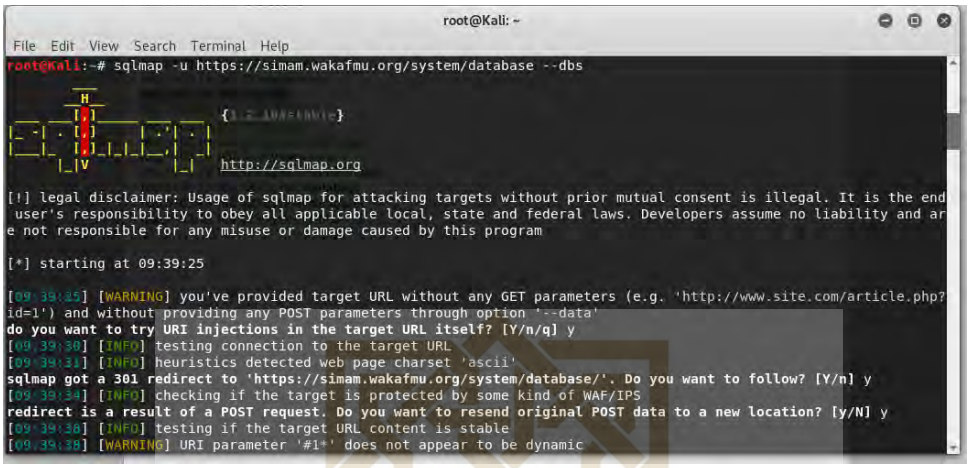
METASPLOIT

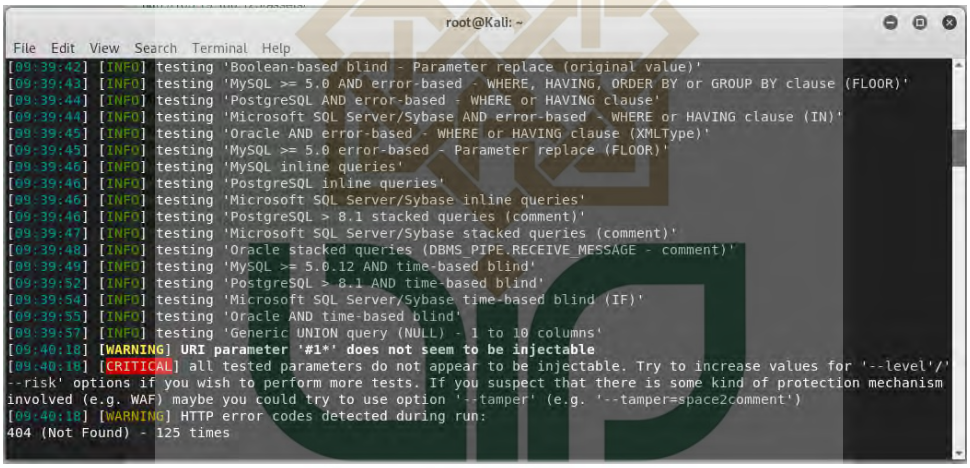


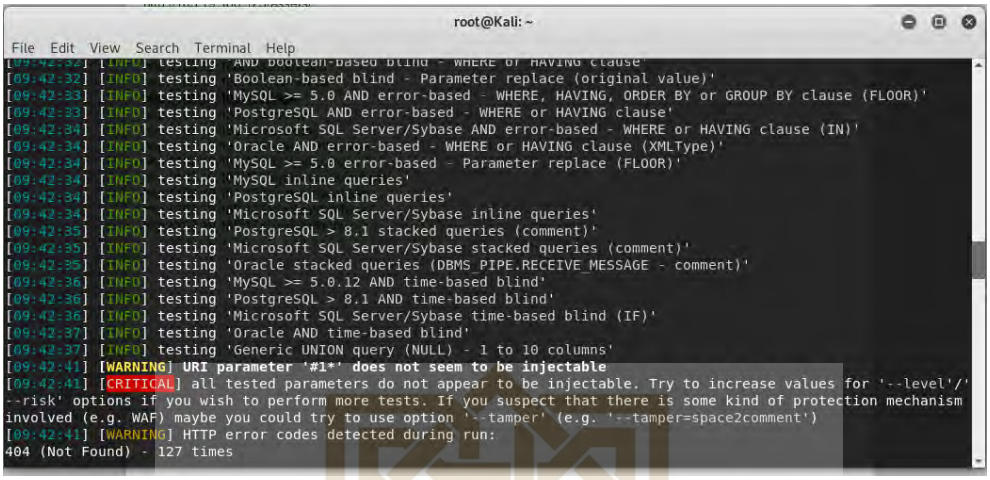


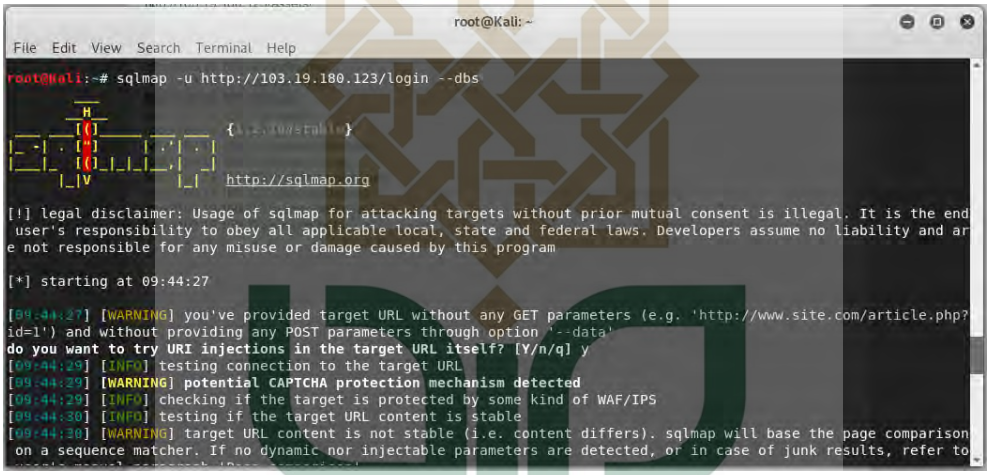


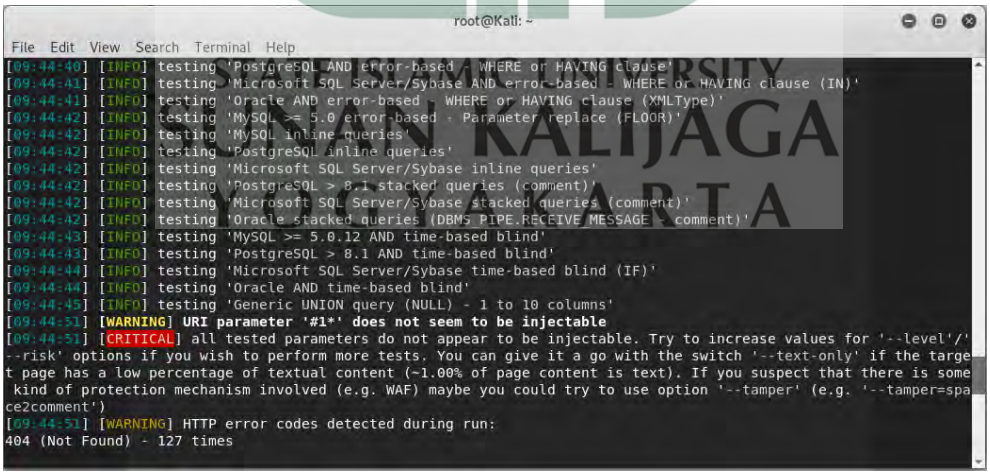
SQLMAP

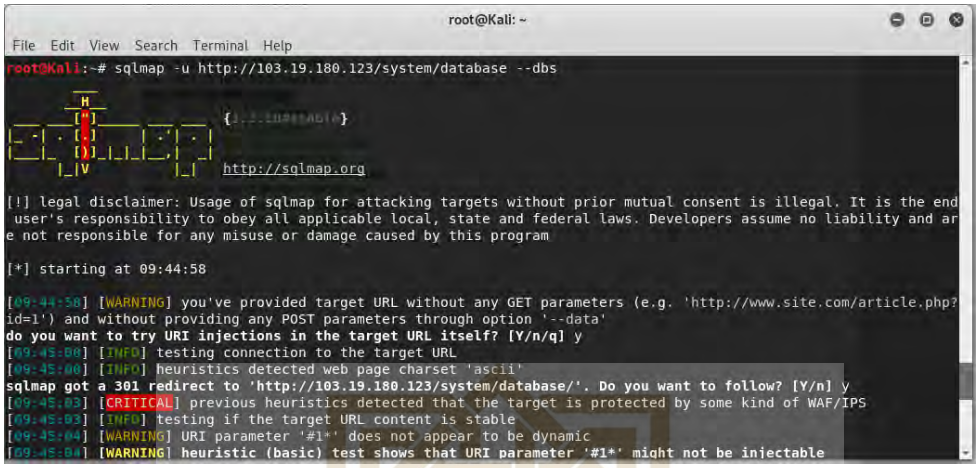


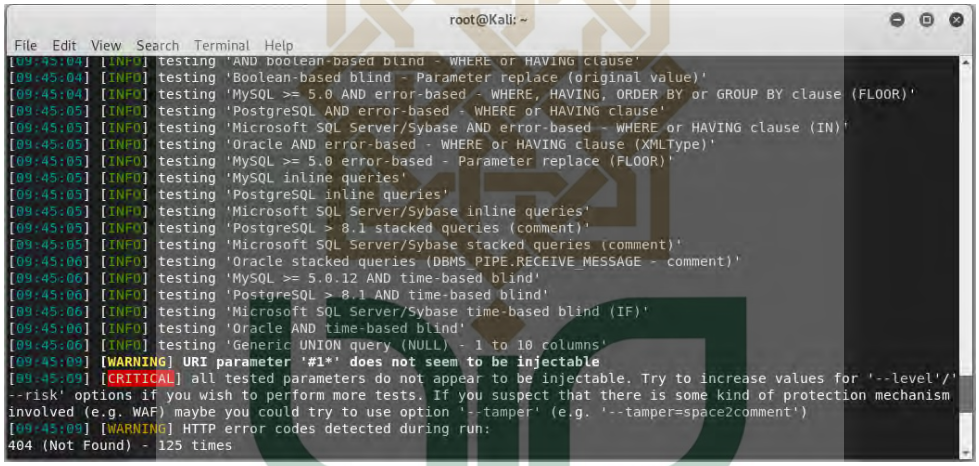



root@Kali: ~
File Edit View Search Terminal Help
[09:42:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:42:33] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[09:42:33] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:42:34] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:42:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:42:34] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[09:42:34] [INFO] testing 'MySQL inline queries'
[09:42:34] [INFO] testing 'PostgreSQL inline queries'
[09:42:34] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[09:42:35] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:42:35] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:42:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[09:42:36] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[09:42:36] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[09:42:36] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[09:42:37] [INFO] testing 'Oracle AND time-based blind'
[09:42:37] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[09:42:41] [WARNING] URI parameter '#1*' does not seem to be injectable
[09:42:41] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'
--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism
involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment')
[09:42:41] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 127 times

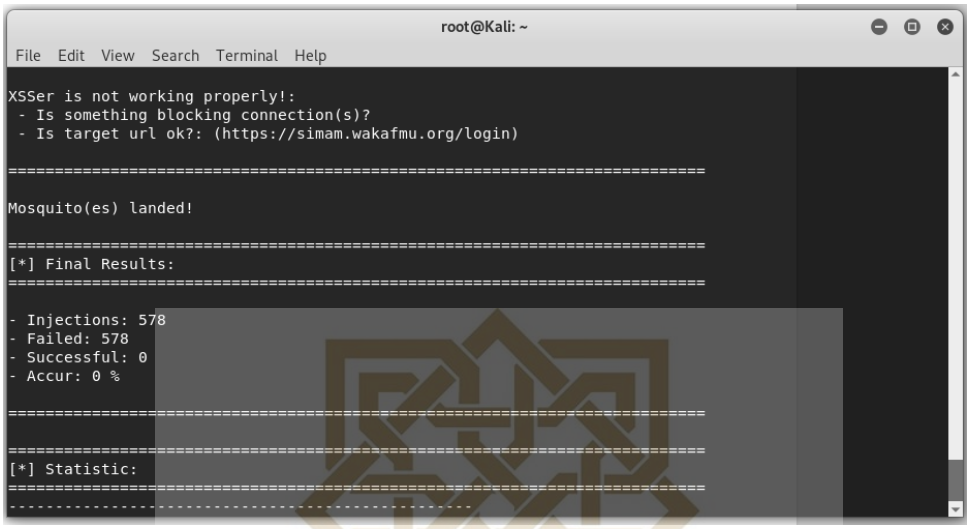

root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~# sqlmap -u http://103.19.180.123/login --dbs
{1.2.10#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end
user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program
[*] starting at 09:44:27
[09:44:27] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?
id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[09:44:29] [INFO] testing connection to the target URL
[09:44:29] [WARNING] potential CAPTCHA protection mechanism detected
[09:44:29] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:44:30] [INFO] testing if the target URL content is stable
[09:44:30] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison
on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to

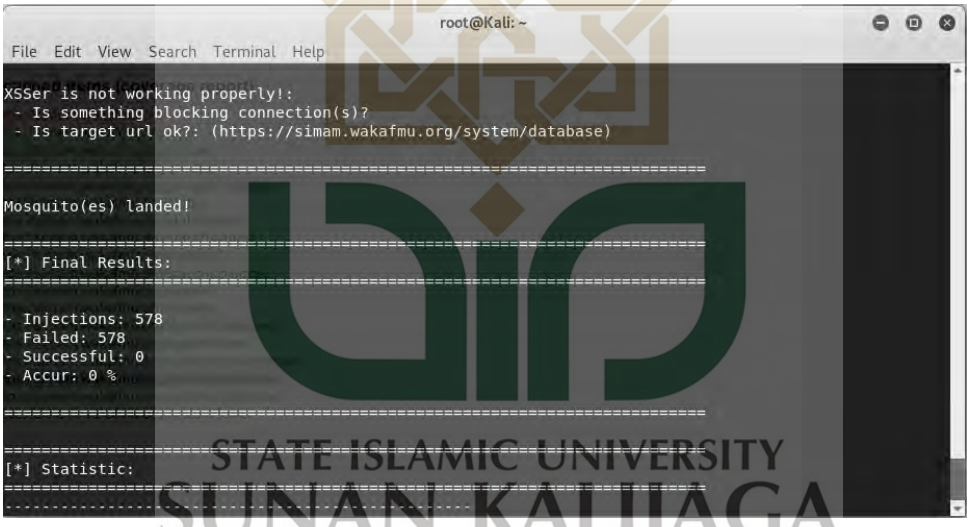

root@Kali: ~
File Edit View Search Terminal Help
[09:44:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:44:41] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:44:41] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:44:42] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[09:44:42] [INFO] testing 'MySQL inline queries'
[09:44:42] [INFO] testing 'PostgreSQL inline queries'
[09:44:42] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[09:44:42] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:44:42] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:44:42] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[09:44:43] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[09:44:43] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[09:44:44] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[09:44:44] [INFO] testing 'Oracle AND time-based blind'
[09:44:45] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[09:44:51] [WARNING] URI parameter '#1*' does not seem to be injectable
[09:44:51] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'
--risk' options if you wish to perform more tests. You can give it a go with the switch '--text-only' if the targe
t page has a low percentage of textual content (~1.00% of page content is text). If you suspect that there is some
kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=spa
ce2comment')
[09:44:51] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 127 times

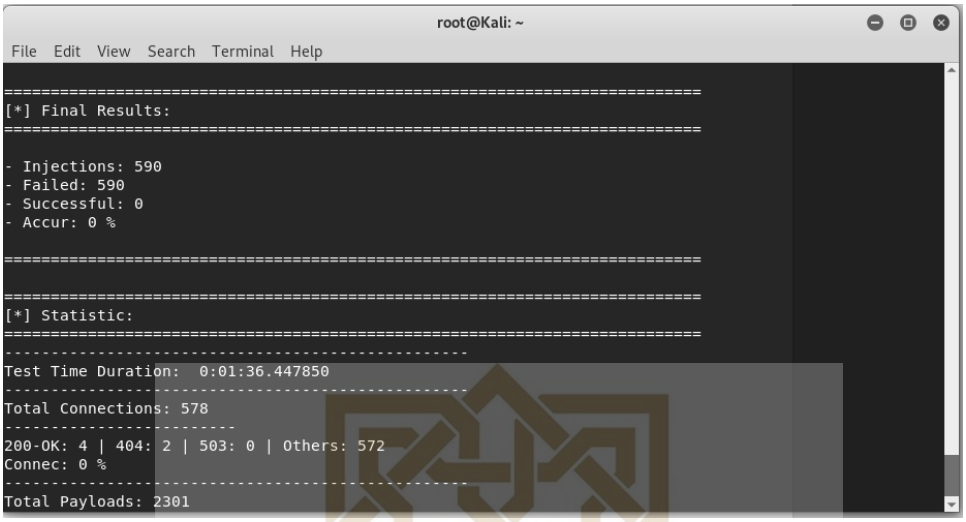


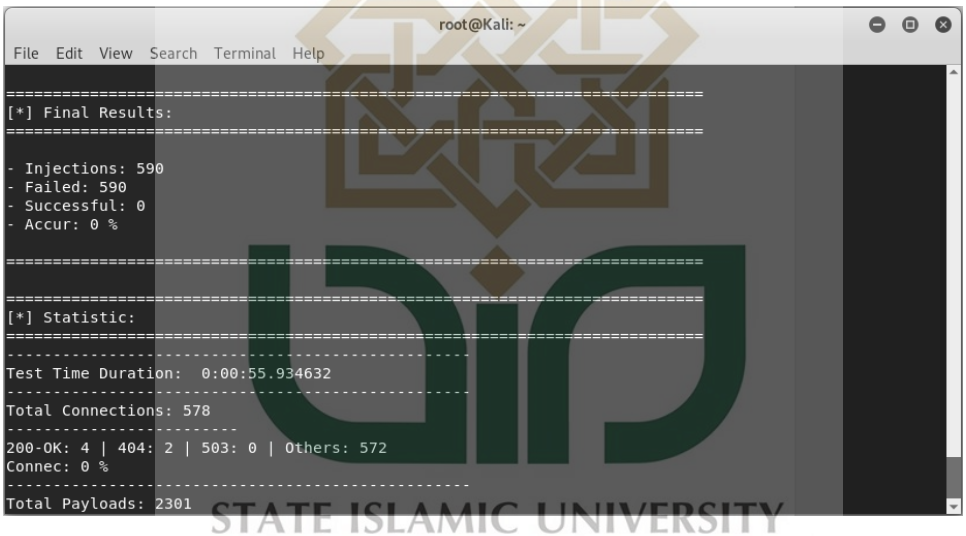


XSSER









LAMPIRAN AUDIT KEAMANAN

Sistem Informasi Manajemen Aset Muhammadiyah

Audit Charter

Project ID : ISO/IEC 27001:2013-Audit 01
Project Name : Audit Keamanan Sistem Informasi
Auditor : Anwaruddin Kamal Ibrahim
Project Description :

Penelitian melakukan audit keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) Pimpinan Wilayah Muhammadiyah Daerah Istimewa Yogyakarta menggunakan standar ISO/IEC 27001:2013. Audit keamanan informasi menggunakan 4 klausul dalam ISO/IEC 27001:2013 yaitu Kebijakan Keamanan Informasi, Pengelolaan Aset, Pengendalian Akses, Keamanan Fisik Dan Lingkungan.

Project Schedule : Februari - April 2019
Stakeholder list :

Jabatan	**Responden**	**Klausul Pengendalian**
Ketua Majelis Wakaf Dan Kehartabendaan PWM DIY	H. Jarot Wahyudi, S.H., M.A	Kebijakan Keamanan Informasi A.5
Staf Majelis Wakaf Dan Kehartabendaan PWM DIY	Ana Rahmawati Wibowo, S.E	Pengelolaan Aset A.8 Pengendalian Akses A.9
Kepala Urusan Pengelolan Infrastruktur dan Komunikasi BISKOM UAD	Wahyu Prio Wicaksono, S.Kom.	Keamanan Fisik Dan Lingkungan A.11

Yogyakarta, 19 Februari 2019

Mengetahui,
Ketua Majelis Wakaf dan
Kehartabendaan PWM DIY

H. Jarot Wahyudi, S.H., M.A.
NIP.

Auditor

Anwaruddin Kamal Ibrahim
NIM: 12650072

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Project Name	: Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Menggunakan Standar ISO/IEC 27001:2013
Auditor	: Anwaruddin Kamal Ibrahim
Audite	: H. Jarot Wahyudi, S.H., M.A
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian Tugas Akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY
Date	: 24 Februari 2019
Jabatan	: Ketua Majelis Wakaf Dan Kehartabendaan PWM DIY

Approved by Auditor

H. Jarot Wahyudi, S.H., M.A Anwaruddin K I

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Project Name	: Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Menggunakan Standar ISO/IEC 27001:2013
Auditor	: Anwaruddin Kamal Ibrahim
Audite	: Ana Rahmawati Wibowo, S.E
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian Tugas Akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY
Date	: 24 Februari 2019
Jabatan	: Staf Majelis Wakaf Dan Kehartabendaan PWM DIY

Approved by Auditor

Ana Rahmawati Wibowo, S.E Anwaruddin K I

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Project Name	: Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO 27001
Auditor	: Anwaruddin Kamal Ibrahim
Audite	: Wahyu Prio Wicaksono, S.Kom.
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian Tugas Akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY
Date	: 1 Maret 2019
Jabatan	: Kepala Urusan Pengelolan Infrastruktur dan Komunikasi BISKOM UAD

Approved by Auditor

Wahyu Prio Wicaksono, S.Kom. Anwaruddin K I

ACUAN KONTROL AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

NO	KLAUSUL	DESKRIPSI	AUDITE
1.	**A5**	Kebijakan keamanan informasi	H. Jarot Wahyudi, S.H., M.A
2.	**A.8**	Pengelolaan Aset	Ana Rahmawati Wibowo, S.E
3.	**A.9**	Pengendalian Akses	Ana Rahmawati Wibowo, S.E
4.	**A.11**	keamanan fisik dan lingkungan	Wahyu Prio Wicaksono, S.Kom.

KLAUSUL, OBJEKTIF KONTROL dan KONTROL dalam Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Klausul	Objektif Kontrol	Kontrol
5 Kebijakan Keamanan	5.1 Arah manajemen untuk keamanan informasi	5.1.1 Kebijakan untuk informasi
		5.1.2 Tinjauan kebijakan untuk keamanan informasi
8 Manajemen aset	8.1 Tanggung jawab atas aset	8.1.1 Inventarisasi aset
		8.1.2 Kepemilikan aset
		8.1.3 Penggunaan aset yang dapat diterima
		8.1.4 Pengembalian aset
	8.2 Klasifikasi informasi	8.2.1 Klasifikasi informasi
		8.2.2 Pelabelan informasi
		8.2.3 Penanganan aset
9 Kontrol akses	9.1 Persyaratan bisnis kontrol akses	9.1.1 Kebijakan kontrol akses
		9.1.2 Akses ke jaringan dan layanan jaringan
	9.2 Manajemen akses pengguna	9.2.1 Registrasi dan de-registrasi pengguna
		9.2.2 Penyediaan akses pengguna
		9.2.3 Pengelolaan hak akses istimewa
		9.2.4 Manajemen informasi otentikasi rahasia pengguna
		9.2.5 Tinjauan hak akses pengguna
		9.2.6 Penghapusan atau penyesuaian hak akses
	9.3 Tanggung jawab pengguna	9.3.1 Penggunaan informasi otentikasi rahasia
	9.4 Kontrol akses sistem dan aplikasi	9.4.1 Pembatasan akses informasi

		9.4.2 Prosedur masuk yang aman
		9.4.3 Sistem manajemen kata sandi
		9.4.4 Penggunaan program utilitas istimewa
		9.4.5 Kontrol akses ke kode sumber program
11 Keamanan fisik dan lingkungan	11.1 Area aman	11.1.1 Batas keamanan fisik
		11.1.2 Kontrol entri fisik
		11.1.3 Mengamankan kantor, kamar dan fasilitas
		11.1.4 Melindungi dari ancaman lingkungan ujung eksternal
		11.1.5 Bekerja di area yang aman
		11.1.6 Area pengiriman dan pemuatan
	11.2 Peralatan	11.2.1 Penempatan dan perlindungan peralatan
		11.2.2 Utilitas pendukung
		11.2.3 Keamanan kabel
		11.2.4 Perawatan peralatan
		11.2.5 Penghapusan aset
		11.2.6 Keamanan peralatan dan aset di luar lokasi
		11.2.7 Mengamankan pembuangan atau penggunaan kembali peralatan
		11.2.8 Peralatan pengguna tanpa pengawasan
		11.2.9 Hapus meja dan hapus kebijakan layar

PERTANYAAN WAWANCARA DALAM PROSES AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

NO	Kontrol	Pertanyaan	Kode
1.	5.1.1 Kebijakan untuk informasi	Apakah sudah ada kebijakan terkait keamanan informasi?	Q1
		Sudahkah kebijakan tersebut didokumentasikan?	Q2
		Apakah kebujakan tersebut telah dipublikasikan kepada pihak yang terkait?	Q3
2.	5.1.2 Tinjauan kebijakan untuk keamanan informasi	Apakah pernah dilakukan peninjauan terhadap kebijakan tersebut?	Q4
		Apakah tinjauan kebijakan dilakukan secara terjadwal?	Q5
		Apakah perubahan kebijakan tersebut telah dipublikasikan?	Q6
3.	8.1.1 Inventarisasi aset	Apakah sudah dilakukan inventarisasi aset?	Q7
		Apakah inventarisasi aset sudah didokumentasikan?	Q8
		Adakah kebijakan dalam pengelolaan aset?	Q9
4.	8.1.2 Kepemilikan aset	Adakah petugas yang mengontrol dan memelihara terhadap semua informasi aset?	Q10
		Apakah dilakukan pengecekan inventaris aset secara berkala?	Q11
		Apakah sudah di identifikasi nilai dan tingkat kepentingan aset?	Q12
5.	8.1.3 Penggunaan aset yang dapat diterima	Adakah peraturan dalam penggunaan dan pengelolaan aset?	Q13
		Adakah peraturan tersebut sudah didokumentasikan?	Q14
		Adakah dokumentasi dari penggunaan atau pengelolaan aset?	Q15

6.	8.1.4 Pengembalian aset	Bagaimana pengelolaan dari pengembalian aset?	Q16
		Bagaimana penanganan aset yang hilang?	Q17
7.	8.2.1 Klasifikasi informasi	Apakah pada informasi aset sudah lakukan klasifikasi dan pengamanan?	Q18
8.	8.2.2 Pelabelan informasi	Apakah ada prosedur pelabelan informasi dalam bentuk fisik dan elektronik?	Q19
		Apakah prosedur pelabelan sudah sesuai dengan kebijakan klasifikasi informasi?	Q20
9.	8.2.3 Penanganan aset	Sehubungan dengan informasi rahasia yang diterima dari sumber eksternal: apakah tingkat klasifikasi mereka dipetakan dengan tepat ke tingkat klasifikasi organisasi sendiri?	Q21
10.	9.1.1 Kebijakan kontrol akses	Apakah sudah menerapkan kontrol akses bagi siapa saja yang berhak mengakses ruang informasi?	Q22
		Apakah ada aturan tertentu ketika memasuki ruang informasi?	Q23
11.	9.1.2 Akses ke jaringan dan layanan jaringan	Apakah ada kontrol keamanan untuk akses dalam jaringan?	Q24
12.	9.2.1 Registrasi dan de-registrasi pengguna	Apakah ada ID pengguna unik untuk setiap pengguna?	Q25
		Apakah ada tinjauan berkala untuk mengidentifikasi ID pengguna yang sudah tidak terpakai?	Q26
		Apakah ID sudah tidak terpakai dihapus setelah mengonfirmasi bahwa mereka tidak lagi diperlukan?	Q27
		Adakah mekanisme yang mencegah ID pengguna dipindahkan ke pengguna lain?	Q28
13.	9.2.2 Penyediaan akses pengguna	Apakah akses yang disediakan untuk setiap pengguna sama?	Q29

		Bagaimana proses mengajukan akses tambahan di luar akses dasar?	Q30
14.	9.2.3 Pengelolaan hak akses istimewa	Adakah pengguna istimewa yang memiliki hak akses khusus?	Q31
		Bagaimana prosedur bagi pengguna istimewa?	Q32
15.	9.2.4 Manajemen informasi otentikasi rahasia pengguna	Bagaimana pengguna mendapatkan username dan kata sandi?	Q33
		Bagaimana proses bila pengguna melupakan kata sandi?	Q34
		Apakah pemberian kata sandi baru manual, semi atau sepenuhnya otomatis?	Q35
		Apakah kata sandi dalam sistem / perangkat dan aplikasi disimpan dalam terenkripsi?	Q36
16.	9.2.5 Tinjauan hak akses pengguna	Apakah tinjauan berkala atas hak akses pengguna pada sistem?	Q37
		Apakah tinjauan dilakukan secara berkala?	Q38
		Apakah hak akses dan izin disesuaikan atau diotorisasi ulang sesuai?	Q39
17.	9.2.6 Penghapusan atau penyesuaian hak akses	Apakah ada prosedur untuk melakukan penghapusan dan penyesuian hak akses?	Q40
18.	9.3.1 Penggunaan informasi otentikasi rahasia	Adakah kebijakan tentang penggunaan informasi rahasia?	Q41
19.	9.4.1 Pembatasan akses informasi	Adakah sistem memiliki kontrol untuk membatasi akses informasi?	Q42
20.	9.4.2 Prosedur masuk yang aman	apakah proses masuk/ identifikasi pengguna dan otentikasi diamankan?	Q43
		Apakah kata sandi yang tidak valid memicu penguncian?	Q44

21.	9.4.3 Sistem manajemen kata sandi	apakah sistem memberlakukan persyaratan kekuatan kata sandi yang tercantum dalam kebijakan dan standar organisasi?	Q45
22.	9.4.4 Penggunaan program utilitas istimewa	Siapa yang mengendalikan utilitas istimewa? Siapa yang dapat mengaksesnya, dalam kondisi apa dan untuk tujuan apa?	Q46
23.	9.4.5 Kontrol akses ke source code program	Apakah source code disimpan di satu atau lebih sumber atau repositori?	Q47
		Bagaimana keamanan akses, kontrol versi, pemantauan, dan pencatatan dilakukan?	Q48
		Apakah akses dan perubahan log disimpan dan ditinjau?	Q49
24.	11.1.1 Batas keamanan fisik	Apakah bangunan dipastikan menggunakan konstruksi yang kokoh?	Q50
		Apakah semua titik akses eksternal dilindungi secara memadai terhadap akses tidak sah?	Q51
		Apakah kontrol keamanan fisik sudah mematuhi standar dan hukum di Indonesia	Q52
25.	11.1.2 Kontrol entri fisik	Apakah sudah menggunakan sistem kontrol akses yang sesuai (kunci keamanan, pemantauan CCTV)?	Q53
		Adakah prosedur akses terhadap pusat data, ruang komunikasi dan area penting lainnya?	Q54
		Apakah semua pihak berwenang memiliki dan menggunaka tanda pengenal saat akses ruang pusat data, ruang komunikasi dan area penting lainnya?	Q55
26.	11.1.3 Mengamankan kantor, kamar dan fasilitas	Adakah pengamanan yang dilakukan terhadap kantor dan fasilitas yang terdapat dalam lingkungan organisasi secara keseluruhan?	Q56

27.	11.1.4 Melindungi dari ancaman lingkungan ujung eksternal	Bagaimana kontrol dan perlindungan gedung terhadap api, banjir, petir?	Q57
28.	11.1.5 Bekerja di area yang aman	Apakah ada prsedur untuk memastikan keamanan area bekerja?	Q58
		Apakah ada pemeriksaan terjadwal untuk keamanan area kerja?	Q59
29.	11.1.6 Area pengiriman dan pemuatan	Apakah barang yang masuk diperiksa dan rinciannya dicatat sesuai dengan kebijakan dan prosedur keamanan?	Q60
30.	11.2.1 Penempatan dan perlindungan peralatan	Bagaimana peralatan TIK dan peralatan terkait (server, komputer, printer. dll) dipastikan aman dari api, banjir, petir, bahan peledak,gangguan listrik, gangguan komunikasi, dan kerusakan kriminal?	Q61
31.	11.2.2 Utilitas pendukung	Apakah pengaturan daya ruang server dan komputer sudah menggunakan UPS, Generator listrik atau pemasok daya lainnya?	Q62
		Apakah instalasi pendingin udara sudah diinstal dan ditempatkan dengan benar?	Q63
32.	11.2.3 Keamanan kabel	Adakah perlindungan fisik yang sesuai untuk kabel eksternal?	Q64
		Apakah kabel daya terpisah dari kabel komunikasi untuk mencegah interferensi?	Q65
		Apakah akses ke panel patch dan ruang kabel dikontrol terlindung dari penyadapan?	Q66
33.	11.2.4 Perawatan peralatan	Adakah personel khusus berkualifikasi yang melakukan pemeliharaan peralatan?	Q67
		Adakah jadwal dan laporan pemeliharaan?	Q68

34.	11.2.5 Penghapusan aset	Bagaimana kebijakan dan prosedur mengenai penghapusan aset informasi?	Q69
		Adakah persetujuan atau otorisasi yang terdokumentasi?	Q70
		Adakah prosedur untuk melacak pergerakan aset bernilai tinggi atau berisiko tinggi?	Q71
35.	11.2.6 Keamanan peralatan dan aset di luar lokasi	Adakah kebijakan penggunaan untuk semua perangkat seluler atau portabel yang digunakan dari lokasi rumah?	Q72
		Bagaimana semua ini dicapai dan dipastikan dalam praktik?	Q73
36.	11.2.7 Mengamankan pembuangan atau penggunaan kembali peralatan	Adakah kebijakan dan catatan terkait yang berkaitan dengan bagaimana peralatan TIK digunakan kembali atau dibuang?	Q74
		Apakah kebijakan dan proses mencakup semua perangkat dan media TIK?	Q75
37.	11.2.8 Peralatan pengguna tanpa pengawasan	Apakah sistem sudah menggunakan sesi time out?	Q76
		Adakah prodesur atau kebijakan untuk tidak meniggalkan server/komputer dalam keadaan menyala?	Q77
38.	11.2.9 Hapus meja dan hapus kebijakan layar	Ulasan kebijakan, standar, prosedur dan pedoman dalam bidang ini. Seberapa baik itu bekerja dalam praktek?	Q78

PEMETAAN PERTANYAAN WAWANCARA DALAM PROSES AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Form Question 1

Q1, Q2, Q3, Q4, Q5, Q6.

Form Question 2

Q7, Q8, Q9, Q10, Q11, Q12, Q13, Q14, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q46, Q47, Q48, Q49.

Form Question 3

Q50, Q51, Q52, Q53, Q54, Q55, Q56, Q57, Q58, Q59, Q60, Q61, Q62, Q63, Q64, Q65, Q66, Q67, Q68, Q69, Q70, Q71, Q72, Q73, Q74, Q75, Q76, Q77, Q78.

HASIL PERHITUNGAN AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Klausul A5 Kebijakan keamanan informasi

NO	Kontrol	Pertanyaan	Score
1	5.1.1 Kebijakan untuk informasi	Apakah sudah ada kebijakan terkait keamanan informasi?	**2**
		Sudahkah kebijakan tersebut didokumentasikan?	**2**
		Apakah kebujakan tersebut telah dipublikasikan kepada pihak yang terkait?	**2**
Rara-rata			**2**
2	5.1.2 Tinjauan kebijakan untuk keamanan informasi	Apakah pernah dilakukan peninjauan terhadap kebijakan tersebut?	**1**
		Apakah tinjauan kebijakan dilakukan secara terjadwal?	**1**
		Apakah perubahan kebijakan tersebut telah dipublikasikan?	**2**
Rara-rata			**1.33**
Rata-rata keseluruhan			**1.67**

Klausul A.8 Pengelolaan Aset

NO	Kontrol	Pertanyaan	Score
1	8.1.1 Inventarisasi aset	Apakah sudah dilakukan inventarisasi aset?	**4**
		Apakah inventarisasi aset sudah didokumentasikan?	**4**
		Adakah kebijakan dalam pengelolaan aset?	**4**
Rata-rata			**4**
2	8.1.2 Kepemilikan aset	Adakah petugas yang mengontrol dan memelihara terhadap semua informasi aset?	**3**

		Apakah dilakukan pengecekan inventaris aset secara berkala?	**2**
		Apakah sudah di identifikasi nilai dan tingkat kepentingan aset?	**3**
Rata-rata			**2.667**
3	8.1.3 Penggunaan aset yang dapat diterima	Adakah prosedur yang mengatur penggunaan dan pengelolaan aset?	**3**
		Apakah prosedur yang mengatur penggunaan dan pengelolaan aset sudah didokumentasikan?	**2**
		Adakah dokumentasi dari penggunaan atau pengelolaan aset?	**2**
Rata-rata			**2.333**
4	8.1.4 Pengembalian aset	Adakah prosedur dari pengembalian aset?	**2**
		Adakah prosedur dalam penanganan aset yang hilang?	**3**
			2.5
5	8.2.1 Klasifikasi informasi	Apakah pada informasi aset sudah lakukan klasifikasi dan pengamanan?	**2**
Rata-rata			**2**
6	8.2.2 Pelabelan informasi	Apakah ada prosedur pelabelan informasi dalam bentuk fisik dan elektronik?	**3**
		Apakah prosedur pelabelan sudah sesuai dengan kebijakan klasifikasi informasi?	**3**
Rata-rata			**3**
7	8.2.3 Penanganan aset	Sehubungan dengan informasi rahasia yang diterima dari sumber eksternal: apakah tingkat klasifikasi mereka dipetakan dengan tepat ke tingkat klasifikasi organisasi sendiri?	**1**
Rata-rata			**1**
Rata-rata keseluruhan			**2.5**

Klausul A.9 Pengendalian Akses

NO	Kontrol	Pertanyaan	Score
1	9.1.1 Kebijakan kontrol akses	Apakah sudah menerapkan kontrol akses bagi siapa saja yang berhak mengakses ruang informasi?	**3**
		Apakah ada aturan tertentu ketika memasuki ruang informasi?	**1**
Rata-rata			**2**
2	9.1.2 Akses ke jaringan dan layanan jaringan	Apakah ada kontrol keamanan untuk akses dalam jaringan?	**1**
Rata-rata			**1**
3	9.2.1 Registrasi dan de-registrasi pengguna	Apakah ada ID pengguna unik untuk setiap pengguna?	**2**
		Apakah ada tinjauan berkala untuk mengidentifikasi ID pengguna yang sudah tidak terpakai?	**1**
		Apakah ID sudah tidak terpakai dihapus setelah mengonfirmasi bahwa mereka tidak lagi diperlukan?	**1**
		Adakah mekanisme yang mencegah ID pengguna dipindahkan ke pengguna lain?	**1**
Rata-rata			**1.25**
4	9.2.2 Penyediaan akses pengguna	Apakah akses yang disediakan untuk setiap pengguna sama?	**3**
		Bagaimana proses mengajukan akses tambahan di luar akses dasar?	**3**
Rata-rata			**3**
5	9.2.3 Pengelolaan hak akses istimewa	Adakah pengguna istimewa yang memiliki hak akses khusus?	**3**
		Bagaimana prosedur bagi pengguna istimewa?	**3**
Rata-rata			**3**

6	9.2.4 Manajemen informasi otentikasi rahasia pengguna	Bagaimana pengguna mendapatkan username dan kata sandi?	**2**
		Bagaimana proses bila pengguna melupakan kata sandi?	**2**
		Apakah pemberian kata sandi baru manual, semi atau sepenuhnya otomatis?	**1**
		Apakah kata sandi dalam sistem / perangkat dan aplikasi disimpan dalam terenkripsi?	**3**
Rata-rata			**2**
7	9.2.5 Tinjauan hak akses pengguna	Apakah tinjauan berkala atas hak akses pengguna pada sistem?	**2**
		Apakah tinjauan dilakukan secara berkala?	**2**
		Apakah hak akses dan izin disesuaikan atau diotorisasi ulang sesuai?	**2**
Rata-rata			**2**
8	9.2.6 Penghapusan atau penyesuaian hak akses	Apakah ada prosedur untuk melakukan penghapusan dan penyesuian hak akses?	**1**
Rata-rata			**1**
9	9.3.1 Penggunaan informasi otentikasi rahasia	Adakah kebijakan tentang penggunaan informasi rahasia?	**2**
Rata-rata			**2**
10	9.4.1 Pembatasan akses informasi	Adakah sistem memiliki kontrol untuk membatasi akses informasi?	**3**
Rata-rata			**3**
11	9.4.2 Prosedur masuk yang aman	apakah proses masuk/ identifikasi pengguna dan otentikasi diamankan?	**3**
		Apakah kata sandi yang tidak valid memicu penguncian?	**2**

Rata-rata			**2.5**
12	9.4.3 Sistem manajemen kata sandi	apakah sistem memberlakukan persyaratan kekuatan kata sandi yang tercantum dalam kebijakan dan standar organisasi?	**1**
Rata-rata			**1**
13	9.4.4 Penggunaan program utilitas istimewa	Siapa yang mengendalikan utilitas istimewa? Siapa yang dapat mengaksesnya, dalam kondisi apa dan untuk tujuan apa?	**3**
Rata-rata			**3**
14	9.4.5 Kontrol akses ke source code program	Apakah source code disimpan di satu atau lebih sumber atau repositori?	**3**
		Bagaimana keamanan akses, kontrol versi, pemantauan, dan pencatatan dilakukan?	**3**
		Apakah akses dan perubahan log disimpan dan ditinjau?	**3**
Rata-rata			**3**
Rata-rata keseluruhan			**2.125**

Klausul A.11 keamanan fisik dan lingkungan

NO	Kontrol	Pertanyaan	Score
1	11.1.1 Batas keamanan fisik	Apakah bangunan dipastikan menggunakan konstruksi yang kokoh?	**4**
		Apakah semua titik akses eksternal dilindungi secara memadai terhadap akses tidak sah?	**4**
		Apakah kontrol keamanan fisik sudah mematuhi standar dan hukum di Indonesia	**4**
Rata-rata			**4**
2	11.1.2 Kontrol entri fisik	Apakah sudah menggunakan sistem kontrol akses yang sesuai (kunci keamanan, pemantauan CCTV)?	**3**

		Adakah prosedur akses terhadap pusat data, ruang komunikasi dan area penting lainnya?	**3**
		Apakah semua pihak berwenang memiliki dan menggunaka tanda pengenal saat akses ruang pusat data, ruang komunikasi dan area penting lainnya?	**3**
Rata-rata			**3**
3	11.1.3 Mengamankan kantor, kamar dan fasilitas	Adakah pengamanan yang dilakukan terhadap kantor dan fasilitas yang terdapat dalam lingkungan organisasi secara keseluruhan?	**3**
Rata-rata			**3**
4	11.1.4 Melindungi dari ancaman lingkungan eksternal	Bagaimana kontrol dan perlindungan gedung terhadap api, banjir, petir?	**3**
Rata-rata			**3**
5	11.1.5 Bekerja di area yang aman	Apakah ada prsedur untuk memastikan keamanan area bekerja?	**3**
		Apakah ada pemeriksaan terjadwal untuk keamanan area kerja?	**3**
Rata-rata			**3**
6	11.1.6 Area pengiriman dan pemuatan	Apakah barang yang masuk diperiksa dan rinciannya dicatat sesuai dengan kebijakan dan prosedur keamanan?	**3**
Rata-rata			**3**
7	11.2.1 Penempatan dan perlindungan peralatan	Bagaimana peralatan TIK dan peralatan terkait (server, komputer, printer. dll) dipastikan aman dari api, banjir, petir, bahan peledak, gangguan listrik, gangguan komunikasi, dan kerusakan kriminal?	**3**
Rata-rata			**3**

8	11.2.2 Utilitas pendukung	Apakah pengaturan daya ruang server dan komputer sudah menggunakan UPS, Generator listrik atau pemasok daya lainnya?	**4**
		Apakah instalasi pendingin udara sudah diinstal dan ditempatkan dengan benar?	**4**
Rata-rata			**4**
9	11.2.3 Keamanan kabel	Adakah perlindungan fisik yang sesuai untuk kabel eksternal?	**4**
		Apakah kabel daya terpisah dari kabel komunikasi untuk mencegah interferensi?	**4**
		Apakah akses ke panel patch dan ruang kabel dikontrol terlindung dari penyadapan?	**2**
Rata-rata			**3.33**
10	11.2.4 Perawatan peralatan	Adakah personel khusus berkualifikasi yang melakukan pemeliharaan peralatan?	**3**
		Adakah jadwal dan laporan pemeliharaan?	**3**
Rata-rata			**3**
11	11.2.5 Penghapusan aset	Bagaimana kebijakan dan prosedur mengenai penghapusan aset informasi?	**3**
		Adakah persetujuan atau otorisasi yang terdokumentasi?	**3**
		Adakah prosedur untuk melacak pergerakan aset bernilai tinggi atau berisiko tinggi?	**3**
Rata-rata			**3**
12	11.2.6 Keamanan peralatan dan aset di luar lokasi	Adakah kebijakan penggunaan untuk semua perangkat seluler atau portabel yang digunakan dari lokasi rumah?	**2**
		Bagaimana semua ini dicapai dan dipastikan dalam praktik?	**2**
Rata-rata			**2**

13	11.2.7 Mengamankan pembuangan atau penggunaan kembali peralatan	Adakah kebijakan dan catatan terkait yang berkaitan dengan bagaimana peralatan TIK digunakan kembali atau dibuang?	**3**
		Apakah kebijakan dan proses mencakup semua perangkat dan media TIK?	**3**
Rata-rata			**3**
14	11.2.8 Peralatan pengguna tanpa pengawasan	Apakah sistem sudah menggunakan sesi time out?	**3**
		Adakah prodesur atau kebijakan untuk tidak meniggalkan komputer dalam keadaan menyala?	**3**
Rata-rata			**3**
15	11.2.9 Clear desk and clear screen policy	Adakah prosedur yang memastikan bahwa informasi sensitif baik format digital dan fisik terjaga kerahasiaannya?	**2**
Rata-rata			**2**
Rata-rata keseluruhan			**3.0**

Klausul	**Keterangan**	**Score**
5	**Kebijakan Keamanan**	**1.67**
8	**Manajemen aset**	**2.5**
9	**Kontrol akses**	**2.125**
11	**Keamanan fisik dan lingkungan**	**3**
Rata-rata score		**2.324**

HASIL WAWANCARA AUDIT

Audit Charter

Project ID : ISO/IEC 27001:2013-Audit 01

Project Name : Audit Keamanan Sistem Informasi

Auditor : Anwaruddin Kamal Ibrahim

Project Description :

Penelitian melakukan audit keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) Pimpinan Wilayah Muhammadiyah Daerah Istimewa Yogyakarta menggunakan standar ISO/IEC 27001:2013. Audit keamanan informasi menggunakan 4 klausul dalam ISO/IEC 27001:2013 yaitu Kebijakan Keamanan Informasi, Pengelolaan Aset, Pengendalian Akses, Keamanan Fisik Dan Lingkungan.

Project Schedule : Februari - April 2019

Stakeholder list :

Jabatan	Responden	Klausul Pengendalian
Ketua Majelis Wakaf Dan Kehartabendaan PWM DIY	H. Jarot Wahyudi, S.H., M.A	Kebijakan Keamanan Informasi A.5
Staf Majelis Wakaf Dan Kehartabendaan PWM DIY	Ana Rahmawati Wibowo, S.E	Pengelolaan Aset A.8 Pengendalian Akses A.9

Kepala Urusan Pengelolan Infrastruktur dan Komunikasi BISKOM UAD	Wahyu Prio Wicaksono, S.Kom.	Keamanan Fisik Dan Lingkungan A.11

Yogyakarta, 19 Februari 2019

Mengetahui,

Ketua Majelis Wakaf dan
Kehartabendaan PWM DIY

H. Jarot Wahyudi, S.H., M.A.

NIP.

Auditor

Anwaruddin Kamal Ibrahim

NIM: 12650072

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah

(SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Project Name	: Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Menggunakan Standar ISO/IEC 27001:2013
Auditor	: Anwaruddin Kamal Ibrahim
Audite	: H. Jarot Wahyudi, S.H., M.A
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian Tugas Akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY
Date	: 24 Februari 2019
Jabatan	: Ketua Majelis Wakaf Dan Kehartabendaan PWM DIY

Approved by | Auditor

H. Jarot Wahyudi, S.H., M.A | Anwaruddin K I

PERTANYAAN WAWANCARA DALAM PROSES AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah

(SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

NO	Kontrol	Pertanyaan	Jawaban	Score
1.	5.1.1 Kebijakan untuk informasi	Apakah sudah ada kebijakan terkait keamanan informasi?	Sudah ada	2
		Sudahkah kebijakan tersebut didokumentasikan?	Sudah	2
		Apakah kebijakan tersebut telah dipublikasikan kepada pihak yang terkait?	Sudah	2
2.	5.1.2 Tinjauan kebijakan untuk keamanan informasi	Apakah pernah dilakukan peninjauan terhadap kebijakan tersebut?	Sudah Pernah LX	1
		Apakah tinjauan kebijakan dilakukan secara terjadwal?	tidak terjadwal/sesuai masalah	1
		Apakah perubahan kebijakan tersebut telah dipublikasikan?	Secara di Publikasi setelah ada Perubahan	2

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah

(SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Project Name	: Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Menggunakan Standar ISO/IEC 27001:2013
Auditor	: Anwaruddin Kamal Ibrahim
Audite	: Ana Rahmawati Wibowo, S.E
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian Tugas Akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY
Date	: 24 Februari 2019
Jabatan	: Staf Majelis Wakaf Dan Kehartabendaan PWM DIY

Approved by

Ana Rahmawati Wibowo, S.E

Auditor

Anwaruddin K I

PERTANYAAN WAWANCARA DALAM PROSES AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah

(SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

NO	Kontrol	Pertanyaan	Jawaban	Score
1.	8.1.1 Inventarisasi aset	Apakah sudah dilakukan inventarisasi aset?	Sudah	4
		Apakah inventarisasi aset sudah didokumentasikan?	Sudah	4
		Adakah kebijakan dalam pengelolaan aset?	Sudah	4
	8.1.2 Kepemilikan aset	Adakah petugas yang mengontrol dan memelihara terhadap semua informasi aset?	Ada	3
2.		Apakah dilakukan pengecekan inventaris aset secara berkala?	Dilaksanakan masing-masing penanggung jawab aset	2

		Apakah sudah di identifikasi nilai dan tingkat kepentingan aset?	Sudah	3
3.	8.1.3 Penggunaan aset yang dapat diterima	Adakah peraturan dalam penggunaan dan pengelolaan aset?	Sudah	3
		Adakah peraturan tersebut sudah didokumentasikan?	Sudah	2
		Adakah dokumentasi dari penggunaan atau pengelolaan aset?	Belum	2
4.	8.1.4 Pengembalian aset	Bagaimana pengelolaan dari pengembalian aset?	Sudah ada	2
		Bagaimana penanganan aset yang hilang?	Sudah ada	3
5.	8.2.1 Klasifikasi informasi	Apakah pada informasi aset sudah lakukan klasifikasi dan pengamanan?	Belum ada penanganan	2

6.	8.2.2 Pelabelan informasi	Apakah ada prosedur pelabelan informasi dalam bentuk fisik dan elektronik?	Sudah, fisik dan elektronik	3
		Apakah prosedur pelabelan sudah sesuai dengan kebijakan klasifikasi informasi?	Sudah	3
7.	8.2.3 Penanganan aset	Sehubungan dengan informasi rahasia yang diterima dari sumber eksternal: apakah tingkat klasifikasi mereka dipetakan dengan tepat ke tingkat klasifikasi organisasi sendiri?	Belum ada	1
8.	9.1.1 Kebijakan kontrol akses	Apakah sudah menerapkan kontrol akses bagi siapa saja yang berhak mengakses ruang informasi?	Sudah	3

		Apakah ada aturan tertentu ketika memasuki ruang informasi?	Belum ada	1
9.	9.1.2 Akses ke jaringan dan layanan jaringan	Apakah ada kontrol keamanan untuk akses dalam jaringan?	Belum ada	1
10.	9.2.1 Registrasi dan de-registrasi pengguna	Apakah ada ID pengguna unik untuk setiap pengguna?	Ada	2
		Apakah ada tinjauan berkala untuk mengidentifikasi ID pengguna yang sudah tidak terpakai?	Belum	1
		Apakah ID sudah tidak terpakai dihapus setelah mengonfirmasi bahwa mereka tidak lagi diperlukan?	Belum	1

		Adakah mekanisme yang mencegah ID pengguna dipindahkan ke pengguna lain?	Belum	1
11.	9.2.2 Penyediaan akses pengguna	Apakah akses yang disediakan untuk setiap pengguna sama?	Tidak sama, adanya beberapa tingkat	3
		Bagaimana proses mengajukan akses tambahan di luar akses dasar?	Pilakukan oleh pimpinan. Persetujuan pimpinan	3
12.	9.2.3 Pengelolaan hak akses istimewa	Adakah pengguna istimewa yang memiliki hak akses khusus?	Ada	3
		Bagaimana prosedur bagi pengguna istimewa?	Ditentukan langsung oleh pimpinan	3
13.	9.2.4 Manajemen informasi otentikasi rahasia pengguna	Bagaimana pengguna mendapatkan username dan kata sandi?	Dibuat oleh pimpinan	2

	Bagaimana proses bila pengguna melupakan kata sandi?	Reset dilakukan oleh admin	2
	Apakah pemberian kata sandi baru manual, semi atau sepenuhnya otomatis?	Pemberian manual default	1
	Apakah kata sandi dalam sistem / perangkat dan aplikasi disimpan dalam terenkripsi?	Sudah terenkripsi	3
14.	9.2.5 Tinjauan hak akses pengguna Apakah tinjauan berkala atas hak akses pengguna pada sistem?	Setiap update	2
	Apakah tinjauan dilakukan secara berkala?	tidak terjadwal	2
	Apakah hak akses dan izin disesuaikan atau diotorisasi ulang sesuai?	disesuaikan	2

15.	9.2.6 Penghapusan atau penyesuaian hak akses	Apakah ada prosedur untuk melakukan penghapusan dan penyesuian hak akses?	Tidakada	1
16.	9.3.1 Penggunaan informasi otentikasi rahasia	Adakah kebijakan tentang penggunaan informasi rahasia?	Ada	2
17.	9.4.1 Pembatasan akses informasi	Adakah sistem memiliki kontrol untuk membatasi akses informasi?	Ada	3
18.	9.4.2 Prosedur masuk yang aman	apakah proses masuk/ identifikasi pengguna dan otentikasi diamankan?	Sudahdiamankan	3
		Apakah kata sandi yang tidak valid memicu penguncian?	setiap 3 kali salah memasukkan 3 menit	2
19.	9.4.3 Sistem manajemen kata sandi	apakah sistem memberlakukan persyaratan kekuatan kata sandi yang tercantum dalam kebijakan dan standar organisasi?	Belum	1

20.	9.4.4 Penggunaan program utilitas istimewa	Siapa yang mengendalikan utilitas istimewa? Siapa yang dapat mengaksesnya, dalam kondisi apa dan untuk tujuan apa?	Plm Pivan	3
21.	9.4.5 Kontrol akses ke source code program	Apakah source code disimpan di satu atau lebih sumber atau repositori?	Iya	3
		Bagaimana keamanan akses, kontrol versi, pemantauan, dan pencatatan dilakukan?	dilakukan setiap update	3
		Apakah akses dan perubahan log disimpan dan ditinjau?	Perubahan disimpan	3

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah

(SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

Project Name	: Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO 27001
Auditor	: Anwaruddin Kamal Ibrahim
Audite	: Wahyu Prio Wicaksono, S.Kom.
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian Tugas Akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY
Date	: 1 Maret 2019
Jabatan	: Kepala Urusan Pengelolan Infrastruktur dan Komunikasi BISKOM UAD

Approved by	Auditor
Wahyu Prio Wicaksono, S.Kom.	Anwaruddin K I

PERTANYAAN WAWANCARA DALAM PROSES AUDIT

Audit Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) PWM DIY Berdasarkan Standar ISO/IEC 27001:2013

NO	Kontrol	Pertanyaan	Jawaban	Score
1.	11.1.1 Batas keamanan fisik	Apakah bangunan dipastikan menggunakan konstruksi yang kokoh?	Sudah	4
		Apakah semua titik akses eksternal dilindungi secara memadai terhadap akses tidak sah?	Sudah	4
		Apakah kontrol keamanan fisik sudah mematuhi standar dan hukum di Indonesia	Sudah	4
2.	11.1.2 Kontrol entri fisik	Apakah sudah menggunakan sistem kontrol akses yang sesuai (kunci keamanan, pemantauan CCTV)?	Sudah	3

	Adakah prosedur akses terhadap pusat data, ruang komunikasi dan area penting lainnya?	Ada	3
	Apakah semua pihak berwenang memiliki dan menggunaka tanda pengenal saat akses ruang pusat data, ruang komunikasi dan area penting lainnya?	Sudah	3
3.	11.1.3 Mengamankan kantor, kamar dan fasilitas	Adakah pengamanan yang dilakukan terhadap kantor dan fasilitas yang terdapat dalam lingkungan organisasi secara keseluruhan?	Sudah	3
4.	11.1.4 Melindungi dari ancaman lingkungan ujung eksternal	Bagaimana kontrol dan perlindungan gedung terhadap api, banjir, petir?	Sudah, tetapi harus teknologi lama	3

5.	11.1.5 Bekerja di area yang aman	Apakah ada prsedur untuk memastikan keamanan area bekerja?	Sudah	3
		Apakah ada pemeriksaan terjadwal untuk keamanan area kerja?	Ada	3
6.	11.1.6 Area pengiriman dan pemuatan	Apakah barang yang masuk diperiksa dan rinciannya dicatat sesuai dengan kebijakan dan prosedur keamanan?	Sudah	3
7.	11.2.1 Penempatan dan perlindungan peralatan	Bagaimana peralatan TIK dan peralatan terkait (server, komputer, printer. dll) dipastikan aman dari api, banjir, petir, bahan peledak,gangguan listrik, gangguan komunikasi, dan kerusakan kriminal?	Sudah aman	3

8.	11.2.2 Utilitas pendukung	Apakah pengaturan daya ruang server dan komputer sudah menggunakan UPS, Generator listrik atau pemasok daya lainnya?	ada UPS dan Genset	4
		Apakah instalasi pendingin udara sudah diinstal dan ditempatkan dengan benar?	Sudah aman	4
9.	11.2.3 Keamanan kabel	Adakah perlindungan fisik yang sesuai untuk kabel eksternal?	Sudah	4
		Apakah kabel daya terpisah dari kabel komunikasi untuk mencegah interferensi?	Sudah terpisah	4
		Apakah akses ke panel patch dan ruang kabel dikontrol terlindung dari penyadapan?	Ada kemungkinan Penyadapan	2

10.	11.2.4 Perawatan peralatan	Adakah personel khusus berkualifikasi yang melakukan pemeliharaan peralatan?	Ada	3
		Adakah jadwal dan laporan pemeliharaan?	Setiap bulan	3
11.	11.2.5 Penghapusan aset	Bagaimana kebijakan dan prosedur mengenai penghapusan aset informasi?	Sudah ada	3
		Adakah persetujuan atau otorisasi yang terdokumentasi?	Ada	3
		Adakah prosedur untuk melacak pergerakan aset bernilai tinggi atau berisiko tinggi?	Ada	

12.	11.2.6 Keamanan peralatan dan aset di luar lokasi	Adakah kebijakan penggunaan untuk semua perangkat seluler atau portabel yang digunakan dari lokasi rumah?	Belum	2
		Bagaimana semua ini dicapai dan dipastikan dalam praktik?	Belum bisa dipastikan	2
13.	11.2.7 Mengamankan pembuangan atau penggunaan kembali peralatan	Adakah kebijakan dan catatan terkait yang berkaitan dengan bagaimana peralatan TIK digunakan kembali atau dibuang?	Sudah ada	3
		Apakah kebijakan dan proses mencakup semua perangkat dan media TIK?	Sudah ada	3
14.	11.2.8 Peralatan pengguna tanpa pengawasan	Apakah sistem sudah menggunakan sesi time out?	Sudah ada	3

		Adakah prodesur atau kebijakan untuk tidak meniggalkan server/komputer dalam keadaan menyala?	Sudah ada	3
15.	11.2.9 Hapus meja dan hapus kebijakan layar	Ulasan kebijakan, standar, prosedur dan pedoman dalam bidang ini. Seberapa baik itu bekerja dalam praktek?	Belum ada	2

BIODATA

Nama : Anwaruddin Kamal Ibrahim

Tempat Lahir : Pati

Tanggal Lahir : 12 April 1993

Golongan Darah : AB

Agama : Islam

Kewarganegaraan : Indonesia

Alamat Asal : Ds Margotuhu, rt 01, rw 04, Margomulyo,Tayu, Pati

Email : anwar.ibrahim0072@gmail.com

No. HP : 089654422333

Riwayat Pendidikan :

1999-2005 SD Muhammadiyah Margomulyo

2005-2011 Pondok Modern Darussalam Gontor

2012-2019 S1 Teknik Informatika.

Universitas Islam Negeri Sunan Kalijaga Yogyakarta