ANALISIS METODE UJI PENETRASI KEAMANAN WEBSITE (STUDI KASUS E-LEARNING UIN SUNAN KALIJAGA)

SKRIPSI

FATIH NUR MUHAMMAD

NIM. 20106050027

PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA
2024

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1033/Un.02/DST/PP.00.9/07/2024

Tugas Akhir dengan judul : ANALISIS METODE UJI PENETRASI KEAMANAN WEBSITE (STUDI KASUS: E-LEARNING UIN SUNAN KALIJAGA)

yang dipersiapkan dan disusun oleh:

Nama : FATIH NUR MUHAMMAD
Nomor Induk Mahasiswa : 20106050027
Telah diujikan pada : Kamis, 20 Juni 2024
Nilai ujian Tugas Akhir : A-

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Sumarsono, S.T., M.Kom.
SIGNED

Valid ID: 6682b3cbe406e

Penguji I

Dr. Agus Mulyanto, S.Si., M.Kom., ASEAN Eng.
SIGNED

Valid ID: 667e79140cf04

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 667eed969ba4d

Yogyakarta, 20 Juni 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6683985874187

SURAT PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Fatih Nur Muhammad
Nomor Induk Mahasiswa	: 20106050027
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi

Menyatakan dengan sesungguhnya bahwa skripsi saya yang berjudul :

"Analisis Metode Uji Penetrasi Keamanan Website (Studi Kasus: *E-Learning* Uin Sunan Kalijaga)" adalah hasil karya pribadi yang tidak mengandung plagiarisme dan tidak berisi materi yang dipublikasikan atau ditulis orang lain, kecuali bagian-bagian tertentu yang penulis ambil sebagai acuan dengan tata cara yang dibenarkan secara ilmiah.

Jika terbukti pernyataan ini tidak benar, maka penulis siap mempertanggungjawabkan sesuai hukum yang berlaku.

Yogyakarta, 11 Juni 2024

Yang menyatakan,

Fatih Nur Muhammad

NIM. 20106050027

SURAT PERSETUJUAN SKRIPSI

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 515856 Yogyakarta 55281

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : -

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

Assalamualaikum Wr. Wb.

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

Nama	:	Fatih Nur Muhammad
NIM	:	20106050027
Judul Skripsi	:	ANALISIS METODE UJI PENETRASI KEAMANAN WEBSITE **(STUDI KASUS: E-LEARNING UIN SUNAN KALIJAGA)**

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 Program Studi Teknik Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara dapat segera di-*munaqasyah*-kan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamualaikum Wr. Wb.

Yogyakarta, 11 Juni 2024
Pembimbing,

Dr. Ir. Sumarsono, S.T., M.Kom.
NIP. 19710209 200501 1 003

INTISARI

Keamanan internet adalah aspek kritis dalam era digital yang semakin maju, di mana perlindungan terhadap data pribadi, informasi sensitif, dan integritas sistem menjadi sangat penting. Uji penetrasi adalah metode yang sering digunakan untuk mendeteksi kerentanan pada sebuah website atau aplikasi, sehingga kerentanan tersebut dapat diperbaiki sebelum dieksploitasi dan data dicuri.

Penelitian ini ditujukan untuk meneliti analisis penggunaan metode uji penetrasi terhadap keamanan website serta menguji. Metode yang digunakan untuk melakukan penelitian ini adalah uji penetrasi untuk pengumpulan data, pengujian, mengumpulkan hasi pengujian, merekap hasil pengujian dan menganalisis cara serta hasil pengujian. Pengujian dilakukan dengan 4 serangan yaitu *bruteforce, SQL Injection, XSS (Cross-site scripting), Directory Transversal.*

Hasil penelitian menunjukkan bahwa dari empat percobaan uji penetrasi, hanya serangan *brute force* yang berhasil mengambil alih akun. Tiga serangan lainnya mengalami kegagalan. Serangan *SQL injection* gagal karena tidak ditemukan celah parameter, penggunaan *honeypots* sebagai tameng, dan *Web Application Firewall* (WAF) yang efektif menghalau serangan. Serangan XSS tipe *stored XSS* juga gagal karena adanya filter yang menyaring kata-kata yang mengandung *JavaScript*. Terakhir, serangan *directory traversal* gagal karena validasi input yang baik, sehingga kode berbahaya tidak dapat disusupkan melalui search tab untuk mengakses direktori secara langsung.

Kata Kunci : Uji Penetrasi, *Bruteforce,* SQL *Injection, Cross site Scripting, Directory transversal.*

ABSTRACT

Internet security is a critical aspect in the increasingly advanced digital age, where the protection of personal data, sensitive information, and system integrity is of paramount importance. Penetration testing is a method that is often used to detect vulnerabilities in a website or application, so that these vulnerabilities can be fixed before they are exploited and data is stolen.

This research is aimed at examining the analysis of the use of penetration test methods for website security and testing. The method used to conduct this research is a penetration test for data collection, testing, collecting test results, recapitulating test results and analyzing methods and test results. Testing is done with 4 attacks namely brute force, SQL Injection, XSS (Cross-site scripting), Directory Transversal.

The results showed that of the four penetration test experiments, only the brute force attack succeeded in taking over the account. The other three attacks failed. The SQL injection attack failed because no parameter loopholes were found, the use of honeypots as a shield, and the Web Application Firewall (WAF) which effectively blocks attacks. The stored XSS attack also failed due to filters that filter out words containing JavaScript. Finally, the directory traversal attack failed due to good input validation, so malicious code could not be infiltrated through the search tab to access the directory directly.

Keyword : Penetration Testing, Bruteforce, SQL Injection, Cross site Scripting, Directory transversal.

MOTTO

"When in doubt, use brute force".

Kenneth Lane Thompson

"The act of breaking into a computer system has to have the same social stigma as breaking into a neighbor's house."

Kenneth Lane Thompson

‘‘The secret to success is consistency in effort’’

Benjamin Disraeli.

PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat dirampungkan dengan baik dan tepat pada waktunya. Oleh karena itu, dengan rasa bangga dan bahagia saya ucapkan rasa syukur dan terimakasih saya kepada:

1. Allah SWT karena hanya atas izin dan karuniaNyalah maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan penguasa alam yang meridhoi dan mengabulkan segala doa.

2. Bapak Drs. Slamet Widodo, dan Ibu Fraida Usriyah sebagai orang tua saya yang selalu mendukung, medoakan dan menyemangati dalam proses pengerjaan skripsi

3. Bapak Dr.Ir.Sumarsono, S.T., M.Kom. yang telah meluangkan waktunya untuk menuntun dan membimbing saya dalam proses pengerjaan dan perbaikan skripsi.

4. Teman-Teman seperjuangan(Kontrakan) yang mengajak saya bermain *game* ketika merasa jenuh dan buntu dengan skripsi.

5. Panggih Gumelaring Praja yang selalu membantu saya menjawab pertanyaan-pertanyaan terkait dengan skripsi.

6. Otniel Dewangga yang selalu membantu saya dalam memperbaiki masalah terkait laptop saya.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillahirabbil'alamin, segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga skripsi dengan judul "analisis metode uji penetrasi terhadap keamanan website (studi kasus: *e-learning* UIN Sunan Kalijaga)" ini bisa diselesaikan tepat waktu. Skripsi ini hadir sebagai tugas akhir perkuliahan serta persyaratan untuk memperoleh gelar Sarjana Strata 1 Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.

Melalui penelitian ini, penulis berharap kontribusi ilmiah yang dilakukan dapat memberikan manfaat bagi perkembangan ilmu pengetahuan dan praktik khususnya dalam bidang informatika/teknologi. Skripsi ini juga bisa selesai atas bimbingan, arahan, masukan, serta dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Bapak Prof. Dr. Phil. Al Makin, S.Ag., MA., selaku Rektor Universitas Islam Negri Sunan Kalijaga Yogyakarta.
2. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.
3. Ibu Maria Ulfah Siregar, S.Kom., MIT., Ph.D. selaku Ketua Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.
4. Bapak Mandahadi Kusuma, M.Eng. selaku Dosen Pembimbing Akademik yang telah membarengi serta memberikan informasi selama perkuliahan.
5. Bapak Dr. Ir. Sumarsono, S.T., M.Kom. selaku Dosen Pembimbing Skripsi yang telah meluangkan waktunya untuk mengarahkan dan mengevalusi selama proses skripsi.

6. Orang tua saya tercinta, Drs. Slamet Widodo dan Farida Usriah yang selalu memberikan kasih sayang, nasehat, dan doa untuk keberhasilan serta kelancaran anakmu ini.
7. Kakak, Dzakwan Murtadlo Mukti, yang telah memberikan dukungan berupa motivasi dan membantu penulisan skripsi.
8. Beberapa Café di Kota Yogyakarta yang telah menjadi tempat singgah untuk pengambilan data, dan penulisan skripsi.
9. Teman SMA saya yang selalu menemani saya ketika melakukan penelitian.
10. Teman-teman seperjuangan, Informatika angkatan 2020 Universitas Islam Negri Sunan Kalijaga Yogyakarta.
11. Semua pihak yang telah membantu dalam penyusunan skripsi yang tidak bisa disebutkan satu persatu. Penulis berharap semoga dukungan serta kontribusi yang diberikan oleh pihak terkait mendapatkan balasan dari Allah SWT dan penelitian ini dapat bermanfaat bagi kita semua.

Penulis berharap semoga dukungan serta kontribusi yang diberikan oleh pihak terkait mendapatkan balasan dari Allah SWT dan penelitian ini dapat bermanfaat bagi kita semua.

Wassalamu'alaikum Wr. Wb

Yogyakarta, 11 Juni 2024

Penyusun,

Fatih Nur Muhammad

NIM. 20106050027

DAFTAR ISI

HALAMAN PENGESAHAN ii
SURAT PERNYATAAN KEASLIAN iii
SURAT PERSETUJUAN SKRIPSI iv
INTISARI v
ABSTRACT vi
MOTTO vii
PERSEMBAHAN viii
KATA PENGANTAR ix
DAFTAR ISI xi
DAFTAR TABEL xiv
DAFTAR GAMBAR xv
DAFTAR LAMPIRAN xvi
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 5
1.3. Batasan Masalah 5
1.4. Tujuan Penelitian 6
1.5. Manfaat Penelitian 7
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI 8
2.1. Tinjauan Pustaka 8
2.2. Landasan Teori 10
2.2.1. Website 10
2.2.2. E-learning 11
2.2.3. Uji Penetrasi 11
2.2.4. Bruteforce Attack 12
2.2.5. SQL Injection 14
2.2.6. XSS (Cross Site Scripting) 14
2.2.7. Directory Tranversal 17
BAB III METODE PENELITIAN 20
3.1. Alat dan Bahan 20

3.1.1. Alat Penelitian 20
3.1.2. Bahan Penelitian 21
3.2. Metode Penelitian 22
3.2.1. Identifikasi Masalah 23
3.2.2. Pengumpulan data 23
3.3. Metode Pengujian 24
3.3.1. Bruteforce Attack 24
3.3.2. SQL Injection 24
3.3.3. *Cross-site Scripting* (XSS) 26
3.3.4. Directory Transversal 26
3.4. Waktu dan Tempat Penelitian 26
BAB IV PEMBAHASAN 21
4.1. Pengumpulan Data 21
4.2. Pengujian 33
4.2.1. Bruteforce Attack 33
4.2.2. SQL *Injection* 38
4.2.3. *Cross Site Scripting* (XSS) 42
4.2.4. Directory Tranversal 44
4.3. Menjabarkan Hasil Penelitian 46
4.3.1. Bruteforce Attack 46
4.3.2. SQL Injection 50
4.3.3. Cross Site Scripting 52
4.3.4. Directory Transversal 53
BAB V PENUTUP 64
5.1. Kesimpulan 64
5.2. Saran 65
DAFTAR PUSTAKA 67
LAMPIRAN 66
1. Lampiran Surat Perizinan Penelitian 66
2. Lampiran Kumpulan-Kumpulan Percobaan *Password* 70
3. Lampiran Bukti Serangan *Bruteforce* (serangan gagal) 86
4. Lampiran Bukti Serangan *Bruteforce* (berhasil) 87
5. Lampiran Bukti Serangan *Sql Injection* 88
6. Lampiran Bukti Serangan *Cross Site Scripting* 88

7. Lampiran Bukti Serangan *Directory Transversal* 89
DAFTAR RIWAYAT HIDUP 90

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka 9
Tabel 3.1 Bahan Penelitian 21
Tabel 4.1 Data Dosen 21
Tabel 4.2 Data Mahasiswa 29
Tabel 4.3 List *Password* Data Diri 29
Tabel 4.4 List *Password* buah, sayur, hewan, komputer 31

DAFTAR GAMBAR

Gambar 3.1 Tahapan Penelitian[22] 22
Gambar 4.1 Infografis Bruteforce 33
Gambar 4.2 tab proxy bursuite 34
Gambar 4.3 hasil intercept foxyproxy 35
Gambar 4.4 intruder burpsuite 35
Gambar 4.5 set payload burpusite 36
Gambar 4.6 percobaan uji password 37
Gambar 4.7 infografis sql injection 39
Gambar 4.8 mengecek celah parameter 40
Gambar 4.9 hasil intercept 41
Gambar 4.10 hasil copy intercept 41
Gambar 4.11 penggunaan SQLMap 42
Gambar 4.12 Infografis Stored xss 43
Gambar 4.13 percobaan xss 43
Gambar 4.14 mengupload script xss 44
Gambar 4.15 Infografis directory transversal 45
Gambar 4.16 pengujian kode directory transversal 45
Gambar 4.17 hasil directory transversal 45
Gambar 4.18. Gambar serangan bruteforce gagal. 47
Gambar 4.19 Password tertebak milik mahasiswa dalam prodi 48
Gambar 4.20 Password tertebak milik mahasiswa dalam prodi 49
Gambar 4.21 percobaan menggunakan payload 51
Gambar 4.22 Serangan SQL dialihkan menggunakan WAF 52
Gambar 4.23 Kata-kata terfilter 53

DAFTAR LAMPIRAN

Lampiran 1 Surat Perizinan Penelitian

Lampiran 2 Bukti Serangan *Bruteforce* (Serangan gagal)

Lampiran 3 Bukti Serangan *Bruteforce* (Serangan berhasil)

Lampiran 4 Bukti Serangan SQL *Injection*

Lampiran 5 Bukti Serangan *Cross Site Scripting*

Lampiran 6 Bukti Serangan *Directory Tramsversal*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan internet adalah aspek kritis dalam era digital yang semakin maju, di mana perlindungan terhadap data pribadi, informasi sensitif, dan integritas sistem menjadi sangat penting. Dengan meningkatnya ancaman dari serangan siber seperti *malware, phishing,* dan *ransomware*, penerapan langkah-langkah keamanan yang kuat menjadi suatu keharusan[1]. Keamanan data adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi. Karena hal itu diperlukan adanya kesiapan dari sisi pengguna untuk memahami apa-apa saja hal yang dilakukan untuk mengamankan data.[1]

Ancaman terhadap keamanan siber saat ini terus berkembang dan seiring dengan berkembangnya teknologi. Ketergantungan dengan internet juga semakin meningkat hingga untuk keperluan kehidupan sehari-hari[2]. Serangan-serangan komplek seperti *ransomware*, serangan *DDoS*, dan eksploitasi *zero-day* terus beradaptasi dan menargetkan berbagai sektor, mulai dari individu hingga perusahaan besar. Pelaku kejahatan siber juga semakin berkembang dengan memanfaatkan teknik serangan berupa rekayasa sosial untuk mendapatkan data dari target yang mereka incar. Ancaman siber juga menyerang keamanan nasional yaitu ancaman perang

siber atau dikenal sebagai *cyber war*[2]. Beberapa contoh perang atau serangan siber yaitu *Bruteforce attack, SQL Injection, XSS (Cross-Site Scripting), Directory Transversal.* Ketidaksadaran masyarakat terhadap kejahatan siber juga menyebabkan semakin mudahnya penjahat dalam menyerang dan mengeksploitasi data-data masyarakat yang berada di internet. [2]

Uji penetrasi adalah sebuah simulasi serangan nyata untuk menilai risiko yang terkait dengannya potensi pelanggaran keamanan. Pada saat melakukan uji penetrasi, penguji tidak hanya menemukan kerentanan yang ada dapat dimanfaatkan, namun juga harus mengeksploitasi kerentanan, dan menilai hal apa yang akan didapatkan ketika berhasil mengeksploitasi celah yang ada.[3].

Selama ini uji penetrasi digunakan untuk menguji keamanan berbagai sistem komputer. Uji penetrasi terdapat berbagai jenis pengujian, antara lain uji penetrasi website, uji penetrasi aplikasi atau *software* dan uji penetrasi jaringan. Uji penetrasi sering dilakukan oleh beberapa perusahaan-perusahaan besar guna mengetahui kerentanan-kerentanan yang didapatkan pada target dan mengeksploitasi kerentanan yang ada. Selain itu uji penetrasi ini mempunyai banyak metode serangan dan memiliki dampak yang macam-macam. Dampak yang diberikan juga memiliki tingkatan berbahaya yang berbeda-beda. Uji penetrasi sering digunakan guna menemukan celah kerentanan pada berbagai macam produk-produk baru ataupun produk yang melakukan pembaruan terbarukan mengenai aplikasi, website ataupun jaringan[3].

Dengan berbagai macam serangan yang digunakan pada saat uji penetrasi maka didapatkan celah-celah yang beresiko untuk diekploitasi dan menimbulkan

kerugian untuk korban baik secara waktu ataupun finansial. Kelebihan dari uji penetrasi adalah ketika sistem mengalami kerusakan pasca penyerangan/pengujian, data yang dimiliki target kemungkinan kecil tidak akan terambil karena penyerangan sudah terencanakan. Dan seringkali ancaman keamanan siber mengancam keamanan yang dimiliki suatu *website.*

Melalui analisis ancaman ini, metode yang tepat digunakan adalah uji penetrasi terhadap *website* daring milik Universitas Islam Negeri Sunan Kalijaga. Metode ini secara langsung mesimulasikan serangan siber yang sebenarnya dan juga memberikan pemahaman yang mendalam tentang sistem keamanan yang diuji. Dengan demikian dapat dilakukan analisis potensi-potensi serangan yang mungkin dilakukan oleh pihak-pihak yang tidak sah. Dengan pengamatan yang dilakukan sebelum penelitian, peneliti memutuskan untuk menggunakan 4 cara dalam melakukan yaitu *Bruteforce, SQL Injection, XSS (Cross-site Scripting), Directory Transversal*.

Alasan peneliti memilih empat metode dalam melakukan uji penetrasi adalah sebagai berikut: Serangan *brute force* sudah memiliki celah berupa, saat login, dosen UIN Sunan Kalijaga menggunakan NIP sebagai *username* dan memasukkan *password* agar bisa *login*. Selain itu, dalam percobaan yang dilakukan dalam login di *website* daring.uin-suka.ac.id ?, tidak terdapat batas jumlah toleransi percobaan *login*, sehingga penyerang dapat mencoba terus menerus tanpa harus khawatir bahwa akun akan terblokir. Sedangkan, serangan *SQL Injection* dipilih untuk menguji apakah website telah melakukan pengamanan terhadap kerentanan parameter. Pada serangan *XSS (Cross-site Scripting)* berupa *stored XSS*, peneliti

ingin menguji apakah *website* akan mengeksekusi dan mengizinkan unggahan pengumuman berupa *JavaScript* secara langsung tanpa melalui file atau materi lain. Dalam pengujian *directory traversal*, peneliti ingin menguji apakah website telah melakukan validasi *input* terhadap kode-kode berbahaya yang bisa disusupkan ke dalam *search tab* pada link daring.uin-suka.ac.id ?.

Penggunaan *automatic tools* pada penelitian kali ini mencakup 2 *automatic tools* yaitu untuk serangan *brute force* dan *sql injection.* Penggunaan *automatic tools* dalam pengujian *brute force* adalah *burpsuite community edition. Burpsuite* adalah sebuah aplikasi berbasis java yang berguna untuk melakukan uji keamanan pada aplikasi berbasis web[4]. Penggunaan aplikasi ini lebih digunakan karena yang diuji adalah aplikasi berbasis web dan pengujian serangan tidak bisa dilakukan secara besar yang dapat memicu sistem keamanan. Sedangkan pada pengujian *sql injection automatic tools* yang digunakan adalah *SQLMap. SQLMap* digunakan dalam pengujian *sql injection* karena *tools* tersebut dapat meningkatkan keberhasilan serangan dan mengekstarsi data-data yang ada didalam *database* secara langsung[5]. Selain itu *sqlmap* juga dapat membuat memilih untuk menggunakan bagian tertentu untuk dijadikan celah parameter sehingga kemungkinan serangan berhasil jauh lebih tinggi. Keunggulan lainnya adalah *sqlmap* dapat mengatur tingkat kekuatan yang digunakan yaitu *verbosity* dan *risk.* Fitur verbosity tersebut bertujuan untuk menampilkan detail *output* yang ditampilkan selama proses pengujian dan fitur risk dapat mengontrol seberapa agresif sqlmap mengirimkan payload dan mengeksploitasi kerentanan[5].

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas rumusan masalah yang akan diselesaikan pada penelitian kali ini adalah

1. Bagaimana Analisis hasil pengujian keamanan *website* dengan studi kasus daring.uin-suka.ac.id ?
2. Bagaimana performa yang ditunjukkan dari penggunaan *automatic tools* yang digunakan dalam uji penetrasi ?

Dengan demikian diharapkan dengan penelitian ini dapat membantu pengembang untuk menguji *website-website* yang baru dikembangkan atau *website* yang telah mengalami pembaruan.

1.3. Batasan Masalah

Penelitian kali ini membatasi analisis keamanan pada celah-celah keamanan yang mungkin muncul pada *website* Daring UIN Sunan Kalijaga Yogyakarta. Fokus utama pada penelitian kali ini ada pada identifikasi dan mitigasi serangan yang dapat terjadi pada *website* Daring UIN Sunan Kaliaga Yogyakarta. Dengan mempertimbangkan pada waktu penelitian, jumlah sample yang diteliti dan juga beberapa teknik serangan yang dilakukan guna mengetahui celah-celah yang dipunyai dari *website*.

Batasan masalah pada penelitian ini mencakup beberapa batasan:

1. Serangan yang dilakukan berupa serangan-serangan pada *website* yaitu *Bruteforce Attack*, SQL *Injection*, XSS (*Cross Site Scripting*), *Directory Transversal*.

2. Serangan yang dilakukan hanya berfokus pada *website* uin sunan kalijaga Yogyakarta berupa daring.uin-suka.ac.id.
3. Pengambilan sample sebanyak 12 orang dosen dan 6 mahasiswa berdasarkan data dari akademik. Terdiri dari: 3 dosen dalam prodi aktif mengajar, 3 dosen dalam prodi tidak aktif mengajar, 3 dosen luar prodi aktif mengajar, dan 3 dosen luar prodi tidak aktif mengajar. Dan 6 mahasiswa terdiri dari 3 mahasiswa dalam prodi dan 3 mahasiswa luar prodi. dengan pertimbangan waktu penelitian serta waktu pengujian.
4. Melakukan pengujian keamanan *website* menggunakan metode uji penetrasi dengan menggunakan perangkat lunak yaitu burpsuite *community edition* dan SQLMap.
5. Pada saat pengujian menggunakan burpsuite *community edition* cara yang digunakan hanya menggunakan *sniper attack.*
6. Pada saat pengujian *cross-site scripting* hanya menguji keamanan *website* dengan cara *stored xss.*

1.4. Tujuan Penelitian

Tujuan penelitian yang akan dilakukan penulis untuk menjawab rumusan masalah adalah

1. Menjabarkan hasil yang didapatkan setelah melakukan uji penetrasi.
2. Menjelaskan kelebihan dan kekurangan yang dimiliki *automatic tools* dalam melakukan uji penetrasi.

Selain dua tujuan penelitian diatas peneliti juga berharap agar para pembuat *website* ataupun pengguna *website* lebih waspada terkait hal-hal yang mengancam keamanan *website.*

1.5. Manfaat Penelitian

Secara teoritis manfaat dari penelitian yang saya kerjakan adalah untuk membantu mendeteksi ancaman-ancaman serangan yang bisa terjadi pada *website-website* universitas. Serta memberikan pengetahuan pada para *developer website* tentang beberapa bagian yang harus diuji dalam sisi keamanan ketika mempublikasikan *website*-nya. Mengedukasi pengguna *website* agar selalu waspada terhadap berbagai macam ancaman serangan yang akan terjadi. Secara praktis penelitian ini memiliki manfaat sebagai salah satu media belajar bagi yang berminat dalam keamanan *website.*

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil uji coba menggunakan metode uji penetrasi menggunakan 4 jenis serangan yaitu *bruteforce attack, sql injection, cross site scripting (XSS), directory transversal* didapatkan kesimpulan sebagai berikut :

a. *Website* https://daring.uin-suka.ac.id/ tidak dapat diserang menggunakan 3 serangan yaitu sql *injection, cross site scripting, directory transversal* sebagian besar kegagalan serangan disebabkan oleh tidak adanya celah paramater yang dimiliki *website* https://daring.uin-suka.ac.id/.

b. Serangan *bruteforce* adalah satu-satunya serangan yang mampu membobol pertahanan *website* https://daring.uin-suka.ac.id/. Dari 18 kali pengujian penetrasi akun daring hanya 2 akun yang rentan dibobol dikarenakan penggunaan *password* yang masih umum.

c. Dalam penggunaan *tools* peneliti lebih memilih menggunakan *tools* Burpsuite *Community edition* dibanding *tools* yang lain seperti *hydra*

karena burpsuite cenderung untuk melakukan penyerangan *bruteforce* kepada aplikasi web.

d. Penggunaan burpsuite *community edition* cenderung lebih lama dalam melakukan penyerangan sehingga tidak mudah terdeteksi. Namun karena, percobaan yang lama maka tidak dapat dilakukan untuk penyerangan dalam skala besar.

e. Penggunaan SQLMap dalam melakukan SQL *Injection* cukup membantu dalam melakukan serangan SQL *Injection.* Namun, penggunaan SQLMap juga tergantung pada tingkat keamanan *website*. Jika *website* tidak menampilkan celah parameter maka kemungkinan serangan akan gagal.

5.2. Saran

Saran yang diberikan peneliti terkait penggunaan metode uji penetrasi untuk mengamankan *website* adalah sebagai berikut:

a. Selalu amankan parameter dan tidak memperlihatkan *transfer protocol* seperti menggunakan *GET request* dan *POST request.* Dengan memperlihatkan *protocol* pengiriman data penyerang dapat melihat informasi yang ada pada data.

b. Selalu gunakan *protocol* https untuk mengenkripsi lalu lintas http, baik untuk *GET* ataupun *POST request* agar informasi tidak dapat langsung disadap.

c. Gunakan *password* yang unik dan sulit ditebak. Gunakan kombinasi antara huruf kecil, kapital, angka dan simbol agar *password* lebih bervariatif.

d. Secara teratur memperbarui *password* akan meningkatkan kesulitan bagi penyerang dalam menebak kata sandi yang digunakan.

e. Tambahkan batas toleransi yang dapat dilakukan saat melakukan kesalahan pada saat *login*.

DAFTAR PUSTAKA

[1] N. I. Erzed, "Keamanan di Internet," pp. 1–14.

[2] T. Vimy, S. Wiranto, R. Rudiyanto, P. Widodo, and ..., "Ancaman Serangan Siber Pada Keamanan Nasional Indonesia," *J. …*, vol. 6, no. 1, pp. 2319–2327, 2022, [Online]. Available: http://journal.upy.ac.id/index.php/pkn/article/view/2989

[3] T. W. Edgar and D. O. Manz, *Research Methods for Cyber Security*. 2017. doi: 10.1016/s1353-4858(18)30053-9.

[4] R. Indera, A. Budiono, and U. Y. K. S. Hediyanto, "Vulnerability Assessment Pada Situs Web KPPM FRI Dengan Burp Suite dan Intruder," *e-Proceeding Eng.*, vol. 10, no. 2, p. 1623, 2023.

[5] R. Hermawan, "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 6, no. 2, p. 210, 2021, doi: 10.30998/string.v6i2.11477.

[6] M. Nur Fikri, B. Parga Zen, R. Adhitama, and E. Ahmad Firdaus, "Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES)," *J. Inform.*, vol. 2, no. 2, pp. 19–27, 2023, doi: 10.57094/ji.v2i2.1046.

[7] H. A. A. Duddin and A. S. Fitrani, "Pengamanan Proses Input Output Pada Web Untuk Meminimalisir Serangan SQL-Injection dan XSS Menggunakan Metode IDS dan IPS," *Network, Comput. Sci.* |, vol. 4, no. 1, pp. 6–12, 2021.

[8] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 52–55, 2016, doi: 10.30743/infotekjar.v1i1.48.

[9] M. Z. Maharani, H. R. A. S. T, S. Juli, I. Ismail, F. I. Terapan, and U. Telkom, "Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks Analysis Website Security Using Scanning Method and," *Anal. Keamanan Website Menggunakan Metod.*

Acanning Dan Perhitungan Aecurity Metr., vol. 3, no. 3, pp. 1775–1782, 2017.

[10] S. Andriyani, M. F. Sidiq, and B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," *J. Inform. Inf. Technol.*, vol. 8798, pp. 1–13, 2023.

[11] B. A. B. Ii and A. K. E-learning, "Bab ii landasan teori e learning," pp. 13–76.

[12] A. Budiman, S. Ahdan, and M. Aziz, "Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment," *J. Komputasi*, vol. 9, no. 2, pp. 1–10, 2021, [Online]. Available: https://jurnal.fmipa.unila.ac.id/komputasi/article/view/2800

[13] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[14] Eril BSSN, "Mengenal Sql Injection," *Bssn*, 2019, [Online]. Available: https://bssn.go.id/wp-content/uploads/2019/09/Proteksi-terhadap-Kerentanan-SQL-Injection-2019-v.1.3.1_sign.pdf

[15] T. A. C. H. A. Ahmad Sultan Hakim, "Serangan Cross-site Scripting (XSS) Berdasarkan Base Metric CVSS V.2," *Muhammadiyah Jember*, vol. 2, no. 1, pp. 1–10, 2020.

[16] S. Suroto and A. Asman, "Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (XSS) Dan Metode Pencegahannya," *Zo. Komput.*, vol. 11, no. 1, pp. 11–19, 2021, [Online]. Available: http://ejurnal.univbatam.ac.id/index.php/komputer/article/view/658

[17] N. Ita Sopia Fazriani, B. Cut, and Sanusi, "Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendataan Warga," *Kandidat*, vol. 1, no. 1, pp. 15–20, 2019, [Online]. Available: http://jurnal.abulyatama.ac.id/index.php/kandidat

[18] E. L. Pratiwi, M. Z. Azhari, and M. R. Ariyandi, "ijns.org Indonesian Journal on Networking and Security - Volume 11 No 4 – 2022," vol. 11, no. 4, pp. 225–228, 2022.

[19] R. Hermawan, "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 6, p. 210, 2021, doi: 10.30998/string.v6i2.11477.

[20] R. Firmansyah and W. S. Prasetya, "Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery," *J. Enter*, vol. 1, pp. 294–306, 2018.

[21] M. I. Akhsin, M. Awaluddin, and A. Suprayogi, "Pemetaan Multi Bencana Kota Semarang," *J. Geod. Undip*, vol. 5, no. 4, pp. 132–139, 2016.

[22] H. Hasanah, "TEKNIK-TEKNIK OBSERVASI (Sebuah Alternatif Metode Pengumpulan Data Kualitatif Ilmu-ilmu Sosial)," *At-Taqaddum*, vol. 8, no. 1, p. 21, 2017, doi: 10.21580/at.v8i1.1163.

[23] Purwono, *25-53-1-SM.pdf*. 2008.

[24] A. Aryapranata, "Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id," *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 4, no. 1, pp. 55–59, 2020, doi: 10.55886/infokom.v4i1.321.