EVALUASI KEAMANAN WEBSITE AKADEMIK UNIVERSITAS X: STUDI KASUS SQL INJECTION, CROSS-SITE SCRIPTING (XSS), DAN DIRECTORY ENUMERATION

TUGAS AKHIR

Dosen Pembimbing:
Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
NIP : (19751024 200912 1 002)

Disusun Oleh :
Fariz Fitroturrohman
NIM. 21106050062

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2025

LEMBAR 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-1469/Un.02/DST/PP.00.9/07/2025

Tugas Akhir dengan judul : Evaluasi Keamanan Website Akademik Universitas X: Studi Kasus SQL Injection, Cross-Site Scripting (XSS), dan Directory Enumeration

yang dipersiapkan dan disusun oleh:

Nama : FARIZ FITROTURROHMAN
Nomor Induk Mahasiswa : 21106050062
Telah diujikan pada : Kamis, 10 Juli 2025
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. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 6885d481b3558

Penguji I

Ir. Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Ph.D.
SIGNED

Valid ID: 6882d8cd92642

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 6881ecfd94fb9

Yogyakarta, 10 Juli 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

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

Valid ID: 6887216b84b32

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama	: Fariz Fitroturrohman
NIM	: 21106050062
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi
Pembimbing	: Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.

Menyatakan dengan sesungguhnya bahwa Tugas Akhir saya yang berjudul **"Evaluasi Keamanan Website Akademik Universitas X: Studi Kasus SQL Injection, Cross-Site Scripting (XSS), dan Directory Enumeration"** merupakan hasil karya saya sendiri, tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar akademik di perguruan tinggi mana pun, dan sepanjang pengetahuan saya, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berdasarkan pernyataan tersebut, Tugas Akhir ini saya ajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana bidang Informatika pada Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Yogyakarta, 30 Juni 2025

Yang menyatakan,

Fariz Fitroturrohman

NIM. 21106050062

LEMBAR PERSETUJUAN

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

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp : -

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

Assalammu'alaikum wr. wb.

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

Nama	:	Fariz Fitroturrohman
NIM	:	21106050062
Judul Skripsi	:	Evaluasi Keamanan Website Akademik Universitas X: Studi Kasus SQL Injection, Cross-Site Scripting (XSS), dan Directory Enumeration

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

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara dapat segera dimunaqasyahkan. Atas perhatiannya saya ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 30 Juni 2025
Pembimbing

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
NIP. 19751024200912100 2

INTISARI

Website akademik merupakan sistem informasi penting yang digunakan oleh mahasiswa, dosen, dan staf untuk mengakses serta mengelola data akademik. Namun, sistem ini seringkali tidak dirancang dengan standar keamanan yang memadai, sehingga rentan terhadap berbagai jenis serangan siber. Oleh karena itu, evaluasi terhadap keamanan website akademik perlu dilakukan untuk mencegah potensi kebocoran data dan penyalahgunaan akses.

Penelitian ini menggunakan pendekatan black-box penetration testing dengan kerangka kerja NIST SP 800-115 yang terdiri dari tahap planning, discovery, attack, dan reporting. Pengujian difokuskan pada tiga jenis kerentanan yaitu Blind-Based SQL Injection, Reflected Cross-Site Scripting (XSS), dan Directory Enumeration. Alat bantu yang digunakan dalam pengujian ini meliputi XRAY, SQLMap, dan Burp Suite.

Hasil pengujian menunjukkan bahwa sistem mengandung kerentanan dengan tingkat keparahan sedang hingga tinggi. SQL Injection memiliki skor CVSS sebesar 8.2 (High), XSS sebesar 6.1 (Medium), dan Directory Enumeration sebesar 6.5 (Medium). Setiap kerentanan dianalisis dan diberikan rekomendasi perbaikan agar tidak dapat dieksploitasi oleh pihak tidak berwenang.

Kata Kunci: SQL Injection, XSS, Directory Enumeration, NIST SP 800-115, CVSS

ABSTRACT

Academic websites are critical information systems used by students, lecturers, and staff to access and manage academic data. However, many of these systems are not built with adequate security standards, making them vulnerable to cyberattacks. Therefore, it is essential to evaluate the security of academic websites to prevent potential data breaches and unauthorized access.

This study uses a black-box penetration testing approach based on the NIST SP 800-115 framework, which includes planning, discovery, attack, and reporting phases. The assessment focuses on three main vulnerabilities: Blind-Based SQL Injection, Reflected Cross-Site Scripting (XSS), and Directory Enumeration. Tools used in the testing process include XRAY, SQLMap, and Burp Suite.

The results indicate that the system contains vulnerabilities with medium to high severity levels. The SQL Injection scored 8.2 (High), XSS scored 6.1 (Medium), and Directory Enumeration scored 6.5 (Medium) based on the CVSS v3.1 metric. Each vulnerability was analyzed and provided with technical recommendations to prevent further exploitation.

Keywords: *SQL Injection, XSS, Directory Enumeration, NIST SP 800-115, CVSS*

MOTTO

“Lanange jagad, dadi o koyo Arjuno, ra kakean crito, susah seneng adepono.”

Ndarboy Genk – Lanang Tenan

“Wes kadung lahir lanang rasah gur piya-piye wae, sekirane ra entuk dalan ngecor dewe.”

Anonymous

“Jika kau menderita nikmatilah. Sebab penderitaan membersihkan hati, dan membuka jalan bagi masuknya cahaya Tuhan.”

Jalaluddin Rumi

“Hidup tidak usah dibuat sulit, tidak usah ruwet. Asal tidak maksiat, bisa menjadi pribadi yang menyenangkan dan bermanfaat bagi banyak orang serta tidak mengusik hidup orang lain, itu sudah cukup.”

Gus Baha

HALAMAN PERSEMBAHAN

Segala puji syukur kepada Allah SWT dan atas dukungan dan doa dari orang-orang tersayang, skripsi ini akhirnya dapat diselesaikan dengan baik dan tepat waktu. Oleh karena itu, dengan rasa bangga, penulis persembahkan rasa syukur dan terima kasih kepada:

1. Allah SWT yang atas izin dan karunia-Nya, skripsi ini dapat dibuat dan diselesaikan dengan baik dan tepat waktu.
2. Alm. Bapak Edy Haryadi Aziz dan Ibu Farihah Arifyati sebagai orang tua saya yang selalu mendukung, mendoakan, dan juga menyemangati dalam setiap proses kehidupan yang penulis jalani.
3. Bapak Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng. yang telah memberikan bimbingan dan menuntun penulis dalam proses pengerjaan dan perbaikan skripsi.
4. Teman-teman seperjuangan yang mau diajak oleh penulis untuk mengerjakan skripsi bersama-sama.

LEMBAR PEDOMAN PENGGUNAAN SKRIPSI

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga, yang diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta

KATA PENGANTAR

Alhamdulillahirabbil'alamin, segala puji dan syukur penulis panjatkan kehadirat Allah SWT atas rahmat dan karunia-Nya sehingga skripsi dengan judul "Evaluasi Keamanan Website Akademik Universitas X: Studi Kasus SQL Injection, Cross-Site Scripting (XSS), dan Directory Enumeration" ini bisa diselesaikan dengan baik dan tepat pada waktunya. Skripsi ini dibuat sebagai tugas akhir dan syarat untuk memperoleh gelar Sarjana Strata 1 Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri 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 atau teknologi. Skripsi ini juga bisa selesai atas bimbingan, saran, masukan, dan dukungan dari banyak pihak, baik dari keluarga, dosen, maupun teman seperjuangan. Oleh karena itu, penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Prof. Noorhaidi, M.A, M.Phil., Ph.D., selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
3. Dr. Muhammad Mustakim, S.T. M.T., selaku Ketua Program Studi Informatika UIN Sunan Kalijaga Yogyakarta.
4. Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng., selaku Dosen Pembimbing yang telah membantu memberikan bimbingan dan dukungan selama proses penulisan skripsi ini.
5. Dr. Ir. Sumarsono, S.T., M.Kom., selaku Dosen Pembimbing Akademik yang telah membersamai dan memberikan informasi selama perkuliahan.
6. Bapak Eko Hadi Gunawan, M.Eng., selaku Dosen Informatika yang sudah penulis anggap sebagai teman dekat bahkan teman curhat yang telah

memberikan banyak dukungan, bantuan, motivasi dan ilmu seputar kehidupan.

7. Kedua orang tua penulis atas doa, kasih sayang, dan dukungan dalam bentuk apapun selama ini.
8. Saudara Ahmad Ghozali, saudara Hikmah Nursidik, dan saudari Defany Khoirunnisa atas bantuan dan dukungannya selama ini karena sudah mau direpotkan untuk diajak menemani dan membantu penulis dalam proses pengerjaan skripsi.
9. Teman-teman Grup Tim Pilihan yang sudah membuat kehidupan perkuliahan ini menjadi lebih berwarna dengan tingkah laku konyol masing-masing.
10. Teman-teman seperjuangan, Informatika angkatan 2021 Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
11. Seluruh pihak yang telah membantu dan berkontribusi dalam penyusunan skripsi yang tidak bisa disebutkan satu persatu.

Penulis berharap semoga semua dukungan, motivasi, serta kontribusi yang telah diberikan oleh banyak pihak mendapatkan balasan dari Allah SWT dan penelitian ini dapat bermanfaat bagi kita semua. *Aamiin Ya Rabbal 'Aalamiin.*

Yogyakarta, 30 Juni 2025

Penulis,

Fariz Fitroturrohman

NIM. 21106050062

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan adanya kemajuan pada era industri 4.0, tentunya tidak terlepas dari kemajuan teknologi informasi dan digital yang ada. Hal itu tentunya semakin memudahkan umat manusia dalam beraktifitas ataupun melakukan banyak hal. Namun, dibalik itu semua, masih banyak orang yang belum sadar akan keamanan pada bidang siber. Dalam beberapa tahun belakang ini banyak terjadi kejahatan dalam dunia siber, baik itu ancaman serangan pada bidang pendidikan, ekonomi, ketahanan negara, maupun yang lainnya [1].

Kejahatan siber adalah istilah yang digunakan untuk menggambarkan kejahatan yang terjadi di internet. Ancaman kejahatan siber adalah jenis ancaman perang modern atau non militer yang memiliki kemampuan untuk menghancurkan negara melalui kepentingan individu atau kelompok tertentu. Teknologi informasi saat ini menjadi pedang bermata dua karena, selain membantu meningkatkan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi tempat yang ideal untuk kegiatan illegal [2].

Sangat penting untuk meningkatkan kesadaran dan kewaspadaan terhadap ancaman *cybercrime* di era teknologi saat ini. Beberapa elemen yang mendasari kebutuhan ini termasuk perkembangan digitalisasi dan teknologi. Kemajuan ini, bersama dengan peningkatan penggunaan internet di seluruh dunia, telah mengubah cara kita berinteraksi, bekerja, dan berbelanja. Dengan meningkatnya ketergantungan pada teknologi digital, risiko kejahzatan siber juga meningkat [3].

Semakin banyaknya kasus kejahatan internet di Indonesia telah mendorong pemerintah untuk mengesahkan undang-undang yang dapat

digunakan untuk menghukum para pelaku kejahatan internet. Pemerintah Indonesia memasukkan UU kejahatan siber (atau UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dengan harapan dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan internet [4].

Selain membantu banyak orang, kemajuan teknologi informasi juga dimanfaatkan oleh orang-orang yang melakukan kejahatan. SQL Injection adalah teknik yang sering digunakan oleh penyerang untuk memanfaatkan kelemahan aplikasi web. Teknik ini memanfaatkan celah di basis data, yang memungkinkan penyisipan kode dalam pernyataan SQL karena kelemahan dalam kode aplikasi tanpa penyaringan yang cukup [5].

Metode penyerangan yang dikenal sebagai SQL Injection menargetkan server web dengan memanfaatkan kode SQL untuk memanipulasi database. Serangan ini dapat merugikan banyak pihak karena memungkinkan penyerang untuk mencuri atau mengubah data yang tersimpan di web server dan memanipulasi logika perintah SQL untuk mendapatkan akses ke database dan informasi penting lainnya. Penyerang dapat mengubah sintaks SQL, kekuatan, dan fleksibilitas database, serta sistem operasi yang mendukungnya [6].

Cross-site scripting (XSS) adalah eksploitasi keamanan di mana penyerang memasukkan kode berbahaya (biasanya JavaScript) ke sisi klien suatu halaman web. Ketika kode berbahaya ini ditampilkan dalam klien web (seperti Internet Explorer, Mozilla, dll.), hacker dapat mendapatkan akses yang lebih besar ke halaman web. Serangan eksploitasi kerentanan XSS dapat mencuri data, mengontrol sesi pengguna, menjalankan kode berbahaya, atau digunakan dalam phishing scam [7].

Data BSSN menunjukkan bahwa sebanyak 714.170.967 serangan siber terjadi di sepanjang tahun 2022. Angka serangan tertinggi terjadi pada Januari, dengan 272.962.734 serangan, atau lebih dari sepertiga total serangan yang terjadi selama semester pertama tahun itu. Namun, pada

Februari, angka serangan turun lebih dari setengahnya, dengan hanya sekitar 111 juta serangan terjadi. Bulan-bulan berikutnya juga menunjukkan penurunan serangan siber; pada April, jumlah serangan siber hanya kurang dari 100 juta. Dengan 1,3 juta kasus, Indonesia menempati urutan pertama di antara negara-negara ASEAN dalam hal serangan malware, menurut data ASEAN Cyber Threat 2021 yang dirilis oleh Interpol. Jumlah ini hampir setengah dari total ancaman ransomware di antara negara-negara ASEAN. Vietnam menempati peringkat kedua dengan 886.874 kasus, sementara Brunei menempati peringkat terendah dengan 257 kasus [8].

Institusi Pendidikan menjadi institusi nomor dua yang mengalami serangan terbanyak selama 2021, menurut laporan BSSN. Data menunjukkan 83 stakeholder, dengan 41 stakeholder pemerintah, 10 stakeholder pendidikan, 8 stakeholder keuangan, 6 stakeholder e-commerce, 5 stakeholder kesehatan, 5 stakeholder swasta, 4 stakeholder media sosial, 3 jasa ekspedisi, dan 1 stakeholder energi. Kelemahannya termasuk kurangnya pengetahuan, keterampilan SDM, dan kurangnya kesadaran akan pentingnya keamanan siber [9].

Mengacu pada kasus di atas, penulis mengambil target website institusi pendidikan tinggi, yaitu website akademik universitas X. Website akademik universitas X adalah web yang digunakan oleh hampir semua elemen yang ada di universitas tersebut, khususnya mahasiswa dan dosen di mana web tersebut digunakan untuk mengakses hal yang penting, seperti isi data diri, input kartu rencana studi (KRS), melihat jadwal kuliah, dan masih banyak yang lainnya. Teknik penetrasi yang diambil ada tiga jenis yaitu injeksi SQL, XSS, dan *Directory Enumeration.* SQL Injection dipilih karena teknik serangan tersebut termasuk serangan yang sangat berbahaya karena penyerang bisa masuk dan mengakses database yang tidak sembarang orang bisa mengakses dari web target. Serangan XSS bekerja dengan cara menyisipkan script berbahaya ke dalam sistem dan kemudian dieksekusi, dan serangan ini bisa berakibat pada pencurian data dan yang

paling parah bisa sampai pada *defacement web*. *Directory Enumeration* adalah teknik serangan yang memungkinkan *hacker* untuk masuk ke dalam direktori dan file tersembunyi dari suatu sistem dan serangan ini bisa menyebabkan terekspos nya file konfigurasi atau backup sistem dan juga menjadi pintu masuk untuk serangan selanjutnya.

Proses penetrasi akan dilakukan di sistem operasi Kali Linux karena sistem operasi tersebut merupakan sistem operasi yang biasa digunakan untuk melakukan uji penetrasi karena di dalamnya sudah terdapat banyak alat bantu untuk melakukan pengujian. Evaluasi dari celah kerentanan yang ditemukan akan menggunakan metode CVSS agar mendapatkan penjelasan secara detail dan juga akurat. Hasil yang diharapkan yaitu serangan yang telah dilakukan dapat tembus ke dalam sistem sehingga nantinya bisa memberikan saran perbaikan agar serangan serupa tidak terjadi kembali.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas rumusan masalah yang akan diselesaikan pada penelitian kali ini adalah bagaimana hasil evaluasi keamanan terhadap website akademik universitas X berdasarkan perhitungan CVSS dan apa solusi perbaikan terhadap celah keamanan yang ditemukan pada website akademik universitas X.

1.3 Batasan Masalah

Batasan masalah yang ditetapkan pada projek penetration testing web ini dibatasi pada beberapa objek sebagai berikut:

1. Objek penelitian terbatas pada website Sistem Informasi Akademik Universitas X, tidak mencakup website atau situs lainnya.
2. Pengujian hanya akan berfokus pada serangan SQL Injection, XSS, dan *Directory Enumeration*.
3. Alat yang digunakan untuk pengujian adalah *tools* yang umum digunakan dalam melakukan uji keamanan website, yaitu XRAY, SQLMap, dan Burp Suite Community Edition.

4. Proses pengujian SQL Injection hanya sampai pada tahap menampilkan hasil database yang muncul setelah melakukan proses eksploitasi website.
5. Proses pengujian XSS hanya sebatas reflected.
6. Proses pengujian Directory Enumeration hanya sampai pada tahap menampilkan form login dari direktori *phpMyAdmin*.
7. Saran perbaikan hanya akan diberikan pada kerentanan yang telah ditemukan melalui proses pengujian.

1.4 Tujuan Penelitian

Tujuan penelitian yang akan dilakukan penulis untuk menjawab rumusan masalah adalah mengidentifikasi dan mengevaluasi tingkat keamanan pada website akademik universitas X melalui celah keamanan yang berhasil ditemukan dan memberikan solusi perbaikan pada celah keamanan yang ditemukan agar celah kerentanan dapat ditutup.

1.5 Manfaat Penelitian

Ada beberapa manfaat yang dapat diambil dari projek yang dibuat ini adalah sebagai berikut:

1. Bagi developer: memberikan panduan teknis dan bukti nyata mengenai potensi kerentanan umum pada aplikasi web akademik, sehingga dapat dijadikan referensi dalam membangun sistem yang aman melalui penerapan validasi input, pengamanan direktori, dan metode pengujian keamanan berbasis standar seperti NIST SP 800-115.
2. Bagi akademisi: Menjadi referensi ilmiah dalam bidang keamanan siber yang mengombinasikan metode penetration testing dan evaluasi risiko kuantitatif menggunakan CVSS v3.1, serta dapat digunakan sebagai studi kasus empiris untuk pembelajaran dan pengembangan penelitian lanjutan.
3. Bagi institusi terkait: Sebagai masukan strategis untuk meningkatkan keamanan sistem informasi akademik, melalui identifikasi celah

keamanan aktual dan rekomendasi perbaikan yang dapat dijadikan dasar penguatan kebijakan keamanan digital institusi.

4. Bagi masyarakat: Meningkatkan kesadaran masyarakat, khususnya pengguna layanan digital pendidikan, akan pentingnya keamanan data pribadi serta ancaman nyata dari serangan siber terhadap sistem yang digunakan secara luas dalam aktivitas akademik.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap website akademik Universitas X, dapat disimpulkan bahwa sistem tersebut mengandung tiga jenis celah keamanan utama, yaitu Blind-Based SQL Injection, Reflected Cross-Site Scripting (XSS), dan Directory Enumeration. Ketiga kerentanan ini berhasil ditemukan dan dieksploitasi melalui tahapan pengujian menggunakan framework NIST SP 800-115, yang mencakup tahap perencanaan, penemuan, serangan, dan pelaporan. Pengujian dilakukan dengan pendekatan black-box, tanpa akses terhadap kode sumber sistem.

Evaluasi tingkat keparahan setiap kerentanan dilakukan dengan menggunakan metode Common Vulnerability Scoring System (CVSS) versi 3.1. Hasil penilaian menunjukkan bahwa SQL Injection memiliki skor 8.2 (High), XSS sebesar 6.1 (Medium), dan Directory Enumeration sebesar 6.5 (Medium). Nilai-nilai ini menunjukkan bahwa sistem memiliki celah yang cukup serius dan berpotensi dimanfaatkan oleh pihak tidak berwenang untuk mengakses, mencuri, atau memanipulasi data penting, serta mengetahui struktur direktori yang bersifat sensitif.

Sebagai tindak lanjut atas temuan tersebut, telah disusun rekomendasi teknis perbaikan yang disesuaikan dengan masing-masing jenis kerentanan. Untuk SQL Injection, disarankan penggunaan prepared statement atau parameterized query serta validasi input untuk mencegah injeksi perintah ke dalam query. Untuk Reflected XSS, diperlukan sanitasi input dan penerapan kebijakan Content Security Policy (CSP) agar skrip berbahaya tidak dapat dijalankan di sisi klien. Adapun untuk Directory Enumeration, perbaikan dapat dilakukan dengan membatasi akses direktori

sensitif melalui konfigurasi server, menyembunyikan jalur default, dan menonaktifkan direktori yang tidak digunakan.

Dengan demikian, penelitian ini telah menjawab rumusan masalah dan mencapai tujuan yang telah ditetapkan, yaitu mengevaluasi keamanan pada website akademik Universitas X berdasarkan hasil temuan kerentanan, menganalisis tingkat keparahannya, serta memberikan solusi perbaikan yang dapat diterapkan untuk meningkatkan keamanan sistem secara menyeluruh.

5.2 Saran

Berdasarkan hasil temuan dan analisis yang telah dilakukan, penulis menyarankan:

1. Penerapan praktik pengembangan aman (secure coding) perlu diterapkan secara ketat oleh pengelola Sistem Informasi Akademik, termasuk penggunaan prepared statements untuk query SQL dan penyaringan input pengguna.
2. Setiap parameter input pengguna wajib melalui proses validasi dan encoding sebelum ditampilkan kembali ke pengguna untuk mencegah eksekusi skrip berbahaya (XSS prevention).
3. Akses ke direktori sensitif seperti *phpMyAdmin* harus dibatasi melalui konfigurasi server (IP whitelisting, otentikasi tambahan, atau penggantian path default) serta pembaruan rutin terhadap perangkat lunak yang digunakan.
4. Pihak Universitas disarankan untuk melakukan audit keamanan berkala dan menerapkan prosedur manajemen kerentanan berbasis standar seperti NIST dan CVSS, guna menjaga keberlanjutan sistem yang aman.
5. Untuk penelitian lanjutan, disarankan mengembangkan pengujian pada vektor serangan lainnya, serta mengevaluasi kerentanan dan *authentication bypass* sebagai bentuk ancaman yang lebih kompleks. Selain itu juga disarankan untuk menggunakan *tools* yang

lain agar bisa menganalisis perbandingannya antara hasil pengujian menggunakan *tools* satu dengan *tools* yang lainnya dalam hal kemudahan penggunaan dan hasil pengujian yang diperoleh ketika menggunakan *tools* tersebut.

DAFTAR PUSTAKA

[1] C. Rahmawati, "Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0," vol. 1, no. 1, 2019.

[2] S. Ariyaningsih, A. A. Andrianto, A. S. Kusuma, and R. A. Prastyanti, "Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia," *Justisia J. Ilmu Huk.*, vol. 1, no. 1, pp. 1–11, May 2023, doi: 10.56457/jjih.v1i1.38.

[3] Y. Siagian, A. Z. Syah, and N. Irawati, "Peningkatan Kesadaran dan Kewaspadaan Terhadap Ancaman Cybercrime Bagi Masyarakat di Era Digital," vol. 2, no. 2, 2024.

[4] M. Y. Dm and J. Lim, "Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia," vol. 4, no. 5, pp. 8018–8023, 2022.

[5] D. U. Khabibah, Y. Nurrohman, K. Dewandaru, S. J. D. H. Balian, and A. Setiawan, "Strategi Mitigasi SQL Injection dengan Implementasi SQLMap dan Web Application Firewall," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 12, Jun. 2024, doi: 10.47134/jtsi.v1i4.2656.

[6] A. Riyanti, B. M. Rahmanto, D. R. Hardianto, R. D. A. Yuristiawan, and A. Setiawan, "Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 9, Jun. 2024, doi: 10.47134/pjise.v1i4.2623.

[7] S. Suroto and A. Asman, "ANCAMAN TERHADAP KEAMANAN INFORMASI OLEH SERANGAN CROSS-SITE SCRIPTING (XSS) DAN METODE PENCEGAHANNYA," vol. 11, no. 1, Apr. 2021.

[8] CNNIndonesia, "RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan," 2022. [Online]. Available: https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan

[9] W. W, W. W, H. Prasetyo, B. Harjito, and S. W. Sihwi, "KEPUASAN SHARING KNOWLEDGE TEKNIK EARLY WARNING PENCEGAHAN BLACK SEO DALAM WEBSITE PEMERINTAH DAERAH," *J. Dharma*

Bhakti Ekuitas, vol. 8, no. 2, pp. 195–206, May 2024, doi: 10.52250/p3m.v8i2.759.

[10] M. A. Z. Risky and Y. Yuhandri, "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS," *J. Sistim Inf. Dan Teknol.*, pp. 215–220, Aug. 2021, doi: 10.37034/jsisfotek.v3i4.68.

[11] I. M. Raazi, M. Malahayati, B. Basrul, R. Malia, and M. Fadhli, "Analysis Server Security Assessment of Staffing Management Information System Using the NIST SP 800-115 Method at UIN Ar-Raniry Banda Aceh," *Circuit J. Ilm. Pendidik. Tek. Elektro*, vol. 8, no. 1, pp. 46–58, Feb. 2024, doi: 10.22373/crc.v8i1.20808.

[12] M. R. Abdallah, P. Hatta, and C. W. Budiyanto, "Security Analysis of Web-based Information Systems Through Vulnerability Assessment Using the Framework of OWASP Web Security Testing Guide and Common Vulnerability Scoring System," *J. Inform. Vocat. Educ.*, vol. 7, no. 3, Art. no. 3, Nov. 2024, doi: 10.20961/joive.v7i3.2411.

[13] M. Rozali and M. D. Sinaga, "DIAGNOSIS KEAMANAN WEB MENGGUNAKAN METODE UJI PENETRASI WEBSITE SEKOLAH," vol. 2, no. 1, Jan. 2024.

[14] H. A. Almaj Duddin and A. S. Fitrani, "Securing Input and Output Processes on The Web to Minimize SQL-Injection and XSS Attacks Using IDS and IPS Methods," *JOINCS J. Inform. Netw. Comput. Sci.*, vol. 4, no. 1, Apr. 2021, doi: 10.21070/joincs.v4i1.1577.

[15] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, May 2022, doi: 10.31933/jemsi.v3i5.992.

[16] V. B. A. Pardosi, B. Deta, F. Nugroho, and A. Y. Vandika, *Sistem keamanan informasi*. Solok: PT MAFY MEDIA LITERASI INDONESIA, 2024. Accessed: Jun. 20, 2025. [Online]. Available: https://repository.um.ac.id/5536/

[17] M. R. Nowak, M. Walkowski, and S. Sujecki, "Support for the Vulnerability Management Process Using Conversion CVSS Base Score 2.0 to 3.x," *Sensors*, vol. 23, no. 4, Art. no. 4, Jan. 2023, doi: 10.3390/s23041802.

[18] 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, Dec. 2021, doi: 10.30998/string.v6i2.11477.

[19] F. Sinlae, I. Maulana, F. Setiyansyah, and M. Ihsan, "Pengenalan Pemrograman Web: Pembuatan Aplikasi Web Sederhana Dengan PHP dan MYSQL," vol. 2, no. 2, Jul. 2024.

[20] V. Abdullayev and Dr. A. S. Chauhan, "SQL Injection Attack: Quick View," *Mesopotamian J. Cyber Secur.*, pp. 30–34, Feb. 2023, doi: 10.58496/MJCS/2023/006.

[21] N. M. Kevin, "Analisis Kerentanan Cross Site Scripting (XSS): Metode Serangan, Dampak, dan Strategi Pengamanan," *Pros. Semin. Nas. Inform.*, vol. 2, pp. 650–657, Jul. 2024.

[22] V. L. Hambaya, Q. H. Hidayah, N. Erzed, and B. A. Sekti, "Analisis Dan Perancangan Keamanan Frontend Dalam Aplikasi Web: XSS dan CSRF," *Pros. SISFOTEK*, vol. 8, no. 1, Art. no. 1, Oct. 2024.

[23] "Forced browsing | OWASP Foundation." Accessed: Mar. 09, 2025. [Online]. Available: https://owasp.org/www-community/attacks/Forced_browsing

[24] D. N. F. Fitriana, P. Elfa Mas'udia, and M. Kusumawardani, "NIST SP 800-115 Framework Implementation using Black Box Method on Security Gaps Testing on JTD Polinema's Official Website," *jartel*, vol. 13, no. 4, pp. 328–335, Dec. 2023, doi: 10.33795/jartel.v13i4.557.