TUGAS AKHIR
SKEMA MAGANG

PENGUJIAN KEAMANAN PADA APLIKASI WEB INTERNAL BERBASIS PYTHON
(STUDI KASUS: SISTEM MANAJEMEN SISWA)

MUHAMMAD LUKMAN

NIM : 225610018

PROGRAM STUDI SISTEM INFORMASI
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2025

TUGAS AKHIR
SKEMA MAGANG

PENGUJIAN KEAMANAN PADA APLIKASI WEB INTERNAL BERBASIS PYTHON (STUDI KASUS: SISTEM MANAJEMEN SISWA)

Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada

Program Sarjana

Program Studi Sistem Informasi Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Disusun Oleh

MUHAMMAD LUKMAN

NIM : 225610018

PROGRAM STUDI SISTEM INFORMASI
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Pengujian Keamanan Pada Aplikasi Web Internal Berbasis Python (Studi Kasus: Sistem Manajemen Siswa)
Nama	:	Muhammad Lukman
NIM	:	225610018
Program Studi	:	Sistem Informasi
Program	:	Sarjana
Semester	:	Semester 6
Tahun Akademik	:	Genap (2024/2025)

Telah diperiksa dan disetujui untuk diujikan
di hadapan Dewan Penguji Tugas Akhir

Yogyakarta ,29 Agustus 2025
Dosen Pembimbing,

Yudhi Kusnanto, S.T., M.T
NIDN : 0531127002

HALAMAN PENGESAHAN

PENGUJIAN KEAMANAN PADA APLIKASI WEB INTERNAL BERBASIS PYTHON (STUDI KASUS: SISTEM MANAJEMEN SISWA)

Telah dipertahankan di depan Dewan Penguji dan dinyatakan diterima untuk memenuhi sebagian persyaratan guna memperoleh
Gelar Sarjana Komputer
Program Studi Sistem Informasi
Fakultas Teknologi Informasi
Universitas Teknologi Digital Indonesia

Yogyakarta, 31 Juli 2025

Dewan Penguji	NIDN	Tandatangan
1. Yudhi Kusnanto, S.T., M.T	0531127002	.....
2. Dr. L.N. Harnaningrum,S.Si, M.T.	0513057101	.....
3. Ariesta Damayanti, S.Kom., M.Cs.	0020047801	.....

Mengetahui
Ketua Program Studi Sistem Informasi

Deborah Kurniawati, S.Kom., M.Cs.
NIDN : 0511107301

PERNYATAAN KEASLIAN TUGAS AKHIR

Dengan ini saya menyatakan bahwa naskah Tugas Akhir ini belum pernah diajukan untuk memperoleh gelar Sarjana Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 23 Juli 2025

Muhammad Lukman
NIM: 225610018

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan kerendahan hati, penulis mempersembahkan Tugas Akhir yang berjudul:

"Pengujian Keamanan pada Aplikasi Web Internal Berbasis Python (Studi Kasus: Sistem Manajemen Siswa)"

Karya ini penulis persembahkan untuk:

1. Allah SWT, yang telah memberikan rahmat, kesehatan, dan kekuatan hingga penulis dapat menyelesaikan pendidikan ini.
2. Ayahanda Fauzi dan Ibunda Rahayu, yang selalu menjadi sumber semangat, kasih sayang, doa, dan dukungan tanpa henti sepanjang perjalanan hidup dan pendidikan penulis.
3. Bapak Yudhi Kusnanto, S.T., M.T selaku dosen pembimbing yang telah membimbing dan mendukung penulis dengan penuh kesabaran dan keikhlasan.
4. Seluruh keluarga besar PT. Sekuriti Siber Indonesia yang telah memberikan ilmu, kesempatan, dan dukungan dalam proses penelitian ini.

Karya sederhana ini adalah wujud dedikasi dan ungkapan terima kasih penulis kepada semua pihak yang telah menjadi bagian dari perjalanan ini. Semoga setiap langkah dan ilmu yang diperoleh dapat bermanfaat bagi diri penulis, keluarga, masyarakat, dan bangsa.

PRAKATA

Dengan penuh rasa syukur, penulis menyadari bahwa penyusunan Tugas Akhir yang berjudul *"Pengujian Keamanan pada Aplikasi Web Internal Berbasis Python (Studi Kasus: Sistem Manajemen Siswa)"* tidak akan dapat terselesaikan tanpa adanya bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan arahan, motivasi, dan dukungan selama proses penyusunan Tugas Akhir ini. Penulis berharap karya ini dapat memberikan manfaat dan kontribusi nyata dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan aplikasi web. Penulis juga sangat terbuka terhadap kritik dan saran yang membangun untuk perbaikan di masa mendatang.

Ucapan terima kasih yang tulus penulis persembahkan kepada:

1. Ibu Sri Redjeki, S.Si., M.Kom., Ph.D. selaku Rektor Universitas Teknologi Digital Indonesia yang telah memberikan kesempatan kepada penulis untuk menempuh pendidikan di universitas ini.
2. Deborah Kurniawati, S.Kom., M.Cs. selaku ketua program studi mahasiswa Sistem Informas.
3. Yudhi Kusnanto, S.T., M.T selaku dosen pembimbing yang telah dengan sabar memberikan bimbingan, arahan, serta dukungan dari awal hingga selesainya Tugas Akhir ini.
4. Seluruh Keluarga besar PT. Siber Sekuriti Indonesia
5. Orang tua tercinta, Ayah Fauzi dan Terkhusus Ibunda saya Rahayu yang selalu memberikan cinta, dukungan, doa, serta dorongan moril maupun materil selama penulis menempuh pendidikan hingga saat ini.
6. Seluruh pihak lain yang tidak dapat penulis sebutkan satu per satu, tetapi telah memberikan kontribusi dalam penyelesaian skripsi ini.

Penulis sepenuhnya menyadari bahwa karya ini masih jauh dari sempurna dan memiliki berbagai kekurangan. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran yang membangun untuk memperbaiki dan mengembangkan

penelitian di masa yang akan datang. Semoga Tugas Akhir ini dapat menjadi referensi dan memberikan manfaat bagi penulis, pembaca, serta menjadi kontribusi positif dalam bidang keamanan informasi di Indonesia.

Akhir kata, penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak atas segala dukungan yang telah diberikan. Semoga Tuhan Yang Maha Esa senantiasa melimpahkan rahmat, keberkahan, dan kemudahan kepada kita semua.

Yogyakarta, 23 Juli 2025

Muhammad Lukman

INTISARI

Perkembangan teknologi informasi mendorong penggunaan aplikasi web dalam berbagai bidang, termasuk dalam pengelolaan data siswa di lingkungan pendidikan. Namun, tingginya ketergantungan terhadap aplikasi berbasis web juga meningkatkan potensi ancaman keamanan informasi. Oleh karena itu, penelitian ini dilakukan untuk menguji keamanan pada aplikasi web internal berbasis Python dengan studi kasus Sistem Manajemen Siswa yang digunakan oleh sebuah instansi pendidikan.

Pengujian keamanan dalam penelitian ini dilakukan menggunakan metode uji penetrasi dengan mengacu pada standar *Open Web Application Security Project Application Security Verification Standard* (OWASP ASVS). Beberapa potensi kerentanan diuji menggunakan alat bantu seperti Burp Suite, dengan fokus pada tiga jenis serangan umum, yaitu *SQL Injection*, *Insecure Direct Object References* (IDOR), dan kerentanan pada mekanisme *file upload*. Setiap temuan dianalisis untuk menilai dampak, tingkat risiko, serta langkah mitigasi yang dapat diterapkan.

Hasil penelitian menunjukkan adanya celah keamanan yang berpotensi dieksploitasi oleh pihak yang tidak bertanggung jawab. Temuan ini kemudian dimitigasi agar aplikasi memenuhi standar keamanan yang telah ditetapkan, sekaligus meningkatkan integritas data dan kepercayaan pengguna.

Kata kunci: *file upload, IDOR, OWASP ASVS, pengujian keamanan, SQL Injection*

ABSTRACT

The development of information technology encourages the use of web applications in various fields, including in managing student data in an educational environment. However, the high dependence on web-based applications also increases the potential for information security threats. Therefore, this research was conducted to test the security of Python-based internal web applications with a case study of the Student Management System used by an educational institution.

Security testing in this research was conducted using the penetration test method with reference to the Open Web Application Security Project Application Security Verification Standard (OWASP ASVS) standard. Several potential vulnerabilities were tested using tools such as Burp Suite, focusing on three common types of attacks, namely SQL Injection, Insecure Direct Object References (IDOR), and vulnerabilities in the file upload mechanism. Each finding was analyzed to assess the impact, risk level, and applicable mitigation measures.

The results showed that there were security gaps that could potentially be exploited by irresponsible parties. These findings are then mitigated so that the application meets established security standards, while improving data integrity and user trust.

Keywords: *file upload, IDOR, OWASP ASVS, security testing, SQL Injection*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL