LAMPIRAN

1. Lampiran A - Transkrip/Penilaian dari tempat magang

PT SEKURITI SIBER INDONESIA
18 Office Park Building 21 Floor Unit C.
Jl. TB Simatupang Kav. 18, Jakarta ,12520
Telp : +62811-4441-1988; email: info@nemosecurity.com
https://nemosecurity.com/

FORM PENILAIAN KERJA MAGANG

Nama Mahasiswa : Zaki Nedhiansyah
NIM : 215410141
Tempat Pelaksanaan : PT Sekuriti Siber Indonesia
Periode Pelaksanaan : Februari - Juli

NO	ASPEK YANG DINILAI	NILAI (0-100)
1	Kemampuan pemecahan masalah	90
2	Kemampuan teknis	95
3	Kualitas hasil kerja	95
4	Perilaku dan etika kerja (kedisiplinan, tanggung jawab, dan adaptasi)	95
5	Komunikasi interpersonal	90
6	Inisiatif kerja (kontribusi ide dan pendapat)	90
7	Pemahaman sebagai SOC analyst dan Penestration Testing	95

Komentar:
- Sangat baik dalam mengidentifikasi masalah dan menemukan solusi yang efektif
- Memiliki pengetahuan teknis yang sangat baik dan dapat mengaplikasikannya dengan efisien
- Hasil kerja sangat memuaskan dan sesuai dengan standar yang diharapkan
- Sangat proaktif dan sering memberikan ide-ide yang konstruktif.

Nama Pembimbing : Nezim
Posisi/Jabatan : Direktur
No. Handphone : +62 812-9923-2285
Alamat Email : nezimlufni@nemosecurity.com

Yogyakarta, 10 Juli 2025
Pembimbing Lapangan,

(Nezim)

Gambar Lampiran A.1 Transkip Nilai

2. Lampiran B - Sertifikat Magang

Gambar Lampiran B.1 Sertifikat Magang

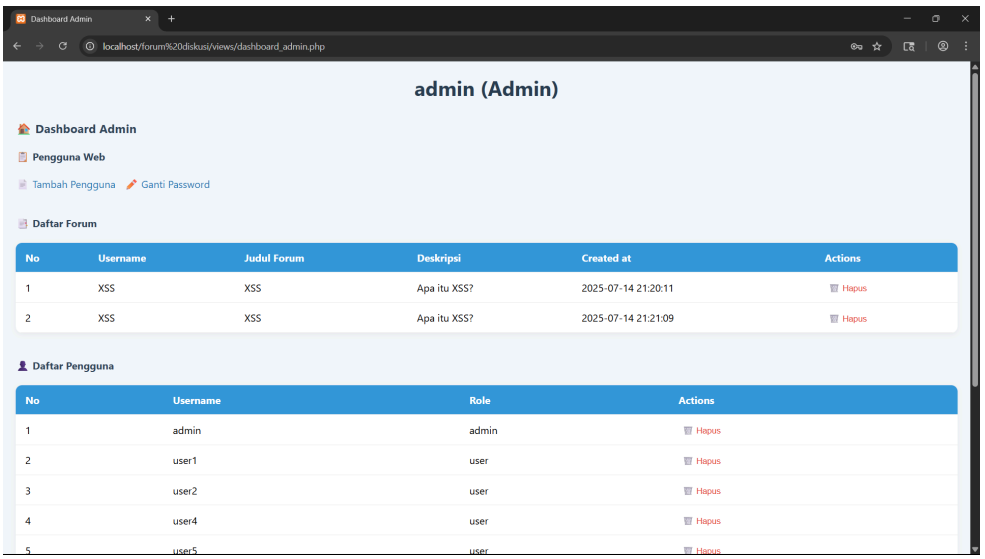
3. Lampiran C - Source Code

https://github.com/zakinedhiansyah/web-diskusi

4. Lampiran D - Proof of Concept (POC)

Tabel Lampiran D.1 Deskripsi *SQL Injection* Form Login

Title	*Structured Query Language Injection (SQLI)* login sebagai admin
Issue details	Pada halaman login terdapat celah *SQL Injection* yang memungkinkan penyerang untuk melewati proses autentikasi. Dengan memasukkan payload ' OR '1'='1 pada kolom username atau password, login tetap berhasil tanpa kredensial yang valid.
Serverity	*CRITICAL*
Impact	Penyerang dapat masuk sebagai user lain bahkan admin tanpa mengetahui *username* dan *password* sebenarnya. Ini memungkinkan akses penuh terhadap sistem.
Path	
Param/Inventory	Form Login (username, password)
Step POC	1. Buka halaman login. 2. Masukkan pada kolom username: ' OR '1'='1 3. Masukkan sembarang password. 4. Login berhasil tanpa kredensial yang valid.



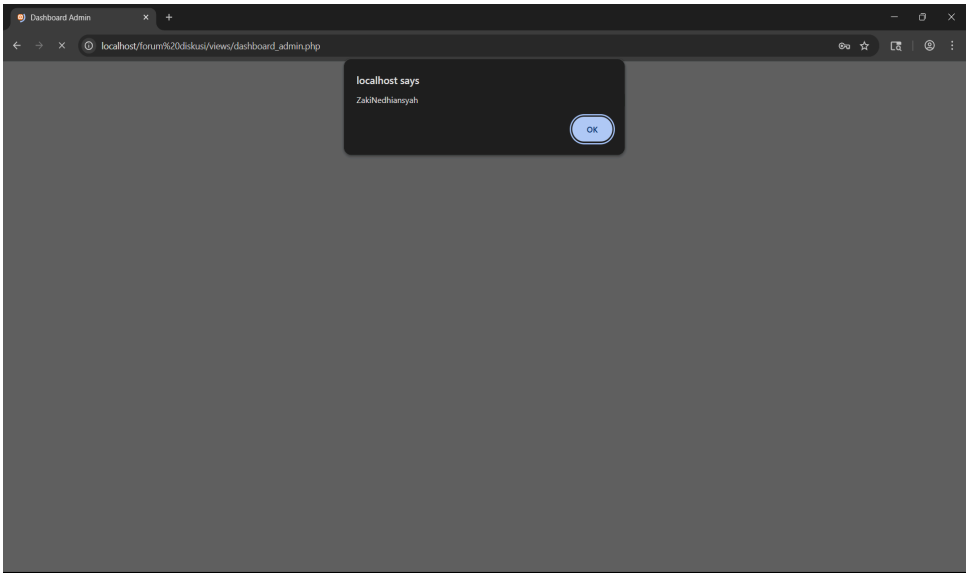
Gambar Lampiran D.1 SQL Injection

Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Tabel Lampiran D.2 Deskripsi XSS Form Register

Title	*XSS* pada Form Register
Issue details	Pada form register, input seperti nama atau username disimpan dan ditampilkan kembali tanpa disanitasi. Ini memungkinkan *Stored XSS*, di mana skrip seperti <script>alert('ZakiNedhiansyah')</script> akan dijalankan saat data ditampilkan kembali, misalnya di halaman profil.
Serverity	HIGH
Impact	Penyerang dapat menyerang admin atau pengguna lain melalui data yang disimpan, misalnya mencuri *cookie*, melakukan *CSRF*, atau mengambil alih sesi.
Path	
Param/Inventory	Form Register *(username, password)*

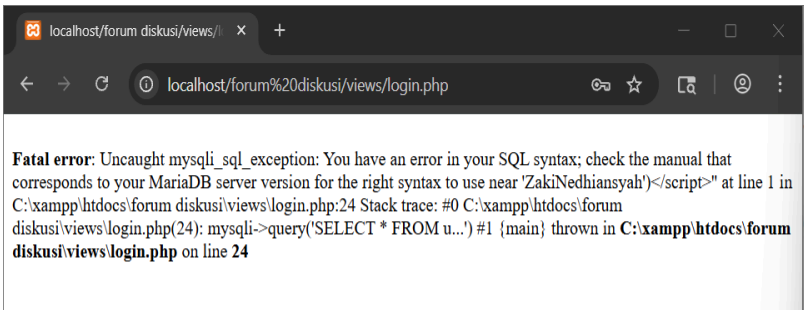
Step POC	1. Masukkan <script>alert(‘ZakiNedhiansyah’)</script> pada kolom nama saat mendaftar. 2. Login sebagai admin atau buka halaman profil pengguna. 3. Jika muncul *pop-up alert*, maka data ditampilkan tanpa *escape*.



Gambar Lampiran D.2 Hasil dari payload XSS

Reference	https://owasp.org/www-community/attacks/xss/

Tabel Lampiran D.3 Deskripsi XSS Form Login

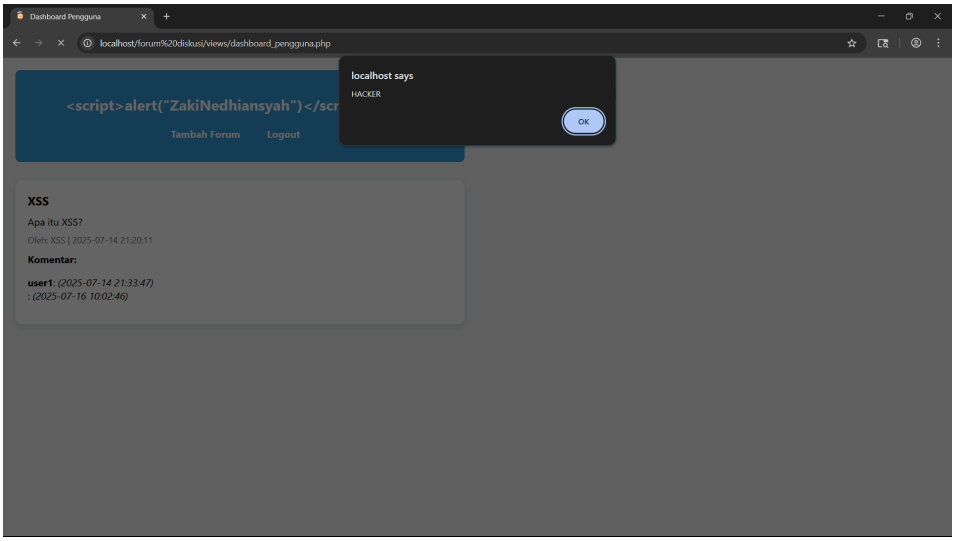
Title	*XSS* pada form Login
Issue details	Kolom input di form login (seperti username atau password) menampilkan kembali input pengguna tanpa filter. Jika penyerang memasukkan <script>alert('ZakiNedhiansyah')</script>, maka skrip dapat dijalankan ketika sistem memproses pesan error.
Serverity	*HIGH*
Impact	Penyerang dapat menjalankan skrip di browser korban, seperti mencuri *cookie*, menyisipkan keylogger, atau mengarahkan ke situs berbahaya.
Path	
Param/Inventory	Form Login (input error handling)
Step POC	1. Masukkan payload <script>alert('ZakiNedhiansyah')</script> pada kolom *username* atau *password*. 2. Submit form. 3. Jika skrip dieksekusi di halaman error/login gagal, maka form rentan terhadap *Reflected XSS*. 

Gambar Lampiran D.3 Halaman Error

Reference	https://owasp.org/www-community/attacks/xss/#stored-xss-attacks

Tabel Lampiran D.4 Deskripsi XSS Form Komentar

Title	*XSS* pada Form Komentar	
Issue details	Komentar pengguna disimpan ke database dan ditampilkan di halaman tanpa disanitasi.	
Serverity	*HIGH*	
Impact	Semua pengguna yang mengakses komentar akan terkena dampaknya. Dapat digunakan untuk mencuri informasi pengguna atau menyisipkan konten palsu.	
Path	Komentar pengguna	
Param/Inventory		
Step POC	1. Kirim komentar dengan isi: <script>alert(‘HACKER’')</script>. 2. Kunjungi halaman tempat komentar ditampilkan. 3. Jika skrip dieksekusi, maka celah *Stored XSS* telah terbukti.	



Gambar Lampiran D.4 Hasil dari payload XSS

Reference	https://owasp.org/www-community/attacks/xss/#stored-xss-attacks

5. Lampiran E - Kartu Bimbingan

KARTU BIMBINGAN
SKRIPSI – PROGRAM SARJANA
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

Nama : Zaki Nadhiancyah
NIM/Prodi : 21sy1014 / Informatika
Pembimbing : Dini fatta Sari S.T., M.T.
Judul : Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS

Kisi-Kisi Bimbingan	NO	TANGGAL	CATATAN KEGIATAN*	PARAF PEMBIMBING
1.Topik/Permasalahan 2. Seminar Proposal 3. Latar Belakang Masalah 4. Rumusan Masalah, Ruang Lingkup, Tujuan dan manfaat 5. Tinjauan Pustaka 6. Dasar Teori 7. Bahan/Data 8. Peralatan 9. Prosedur 10. Pengumpulan Data 11. Analisis dan Rancangan Sistem. 12. Implementasi dan Ujicoba Sistem 13. Pembahasan 14. Kesimpulan 15. Saran 16. Daftar Pustaka 17. Lampiran	1	12/5/2025	Pengajuan Judul	
	2	23/5/2025	Konsultasi BAB I	
	3	19/6/2025	Konsultasi BAB II	
	4	30/6/2025	Dan BAB III	
	5	1/7/2025	Konsultasi BAB IV dan V	
	6	11/7/2025	Perbaikan tulisan dan	
	7		format laporan	
	8	16/7/2025	Revisi final	
	9	19/7/2025	Penulisan Daftar	
	10		Pustaka	
	11	23/7/2025	ACC dan Pendaf-	
	12		taran Pendadaran	

Naskah ini disetujui untuk Ujian Pendadaran Skripsi
Yogyakarta, 19-07-2025
Dosen Pembimbing Skripsi

Dini fatta Sari S.T., M.T

*) Mohon diisikan catatan kegiatan pada saat bimbingan dengan kisi-kisi bimbingan sebagai refrensi pada saat membimbing

6. Lampiran F - Surat Keterangan Publikasi

SURAT KETERANGAN
PERSETUJUAN PUBLIKASI

Bahwa yang bertada tangan dibawah ini:

Nama	: Zaki Nedhiansyah
Nim	: 215410141
Jurusan	: Informatika
Jenjang	: Sarjana
Judul	: Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS

Menyerahkan karya ilmiah kepada pihak perpustakaan UTDI dan menyetujui untuk **diunggah ke Digital Library/Repository** UTDI sesuai dengan ketentuan yang berlaku untuk kepentingan riset dan pendidikan.

Yogyakarta, 19 Agustus 2025
Penulis

Zaki Nedhiansyah
215410141

7. Lampiran G - Keputusan Sidang

KEPUTUSAN HASIL UJIAN PENDADARAN

Sesuai dengan hasil sidang pendadaran pada tanggal 29 Juli 2025 maka

Nama Mahasiswa	Zaki Nedhiansyah
NIM / Program Studi	215410141 / Informatika
Jenjang	S1
	dinyatakan LULUS
Ketua Penguji	Indra Yatini Buryadi, S.Kom., M.Kom.

8. Lampiran H - Catatan Sidang

Hari, tanggal	:	Selasa, 29 Juli 2025
Waktu	:	08.00
Nama	:	Zaki Nedhiansyah
No. Mahasiswa / Prodi	:	215410141 / Informatika

No	Hal yang harus diperbaiki	Pemberi Catatan
1.	1. Deskripsi pekerjaan dibuat hanya di Bab 1, di bab 2 tidak ada deskripsi pekerjaan --> cek panduan penulisan 2. spasi dalam naskah belum seragam 3 judul berkaitan dengan optimalisasi dihilangkan, cukup penetrasi pada web yang dilakukan 4. nomor halaman urutnya dari bab 1 sampai akhir, bukan nomor per bab 5. tambahkan penjelasan di bab 4 pada bagian sql injection	Bu indra
2.	1. di bahas sebelum dilakukan penetrasi dan setelah penetrasi 2. rekomendasi yang diberikan, harus diuji terlebih dahulu. jika tidak dilakukan pengujian, tidak bisa memberikan rekomendasi. 3. perlu memberikan kode program yang rentan yang selaras dengan pengujian dan rekomendasi yang diberikan 4. foto foto yang di lampiran hilang, dan log activity magang dihilangkan --> sesuaikan isi lampiran dengan tempalte penulisan dan berikan gambar yang relevan 5. tambahkan sekenario pengujian 6. di bab 4, gambarnya di buat proporsional ukurannya 7. kesimpulan disesuaikan dengan tujuan	Pak Yudhi
3.		
4.		

9. Lampiran I - Ketentuan Sidang

PEMBERITAHUAN SEBELUM UJIAN :
Jika pengumpulan dokumen Tugas Akhir di perpustakaan melewati batas akhir semester berjalan, maka mahasiswa harus menyelesaikan registrasi dan KRS semester berikutnya.

KRITERIA KELULUSAN UJIAN TUGAS AKHIR

1. Lulus dengan memperhatikan catatan ujian tugas akhir, dan atau melakukan perbaikan atau penyempurnaan naskah dan atau produk dalam waktu maksimum dua bulan dari tanggal ujian tugas akhir, yaitu
mulai Selasa, 29 Juli 2025 sampai dengan Senin, 29 September 2025
Jika dalam waktu yang ditentukan mahasiswa tersebut tidak dapat menyelesaikan, maka mahasiswa yang bersangkutan dianggap tidak lulus ujian.
2. Tidak lulus, disarankan oleh Ketua Tim Penguji untuk mempelajari ulang materi, merombak produk/naskah, atau mengganti judul.

Ketentuan bagi peserta yang tidak lulus ujian tugas akhir.
1) Mahasiswa wajib menempuh ujian tugas akhir ulang
2) Kesempatan ujian tugas akhir ulang hanya diberikan dalam rentang waktu maksimum 6 bulan, setelah ujian sidang/pendadaran
3) Jika sampai batas waktu maksimum 6 bulan tersebut belum dapat diajukan/diselesaikan, maka calon peserta ujian dinyatakan sebagai mahasiswa peserta Tugas Akhir baru, dengan segala ketentuan yang berlaku bagi peserta baru
4) Mahasiswa yang akan menempuh ujian tugas akhir ulang ini diwajibkan membayar biaya ujian sesuai tarif yang ditetapkan.

Yogyakarta, 19 Agustus 2025
Memahami dan bersedia
Mematuhi peraturan di atas,

Zaki Nedhiansyah

10. Lampiran J - Ketentuan telah melakukan revisi

SURAT KETERANGAN TELAH MELAKUKAN REVISI

Yang bertanda tangan di bawah ini, saya :

Nama : Indra Yatini Buryadi, S.Kom., M.Kom.

NIDN : 0511046702

Sebagai : Ketua Penguji/Penguji Pendadaran

Menyatakan telah menyetujui revisi atas naskah dan/atau peranti lunak/peranti keras/rancangan, atas nama :

Nama : ZAKI NEDHIANSYAH

NIM : 215410141

Prodi : Informatika

Tanggal Pendadaran : Selasa, 29 Juli 2025

Pada Tugas Akhir berjudul :

PENETRASI TESTING KEAMANAN WEBSITE MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS

Demikian surat keterangan ini untuk menjadi periksa.

Yogyakarta, 19 Agustus 2025

Ketua Penguji/Penguji

Indra Yatini Buryadi, S.Kom., M.Kom.

NIDN: 0511046702

11.