PENETRATION TESTING

Proyek Akhir Praktikum Keamanan Jaringan

Oleh Kelompok 15

netlab

ANGGOTA KELOMPOK 15

Ryan Adidaru E. B.
2306266994

Fathan Yazid S.
2306250560

PENDAHULUAN

RUANG LINGKUP

Tujuan:
Melakukan demonstrasi penetrasi keamanan, analisis dampak, dan remediasi pada aplikasi web.

Target:
Aplikasi Web lokal (Node.js) yang dirancang khusus dengan kerentanan (Port 3001) dan versi aman (Port 3002).

TOPIK - TOPIK

INSECURE FILE UPLOAD

Menguji validasi server terhadap berkas yang diunggah.

INSECURE CHANGE PASSWORD

Menguji mekanisme reset password berbasis OTP.

METODOLOGI PENETRATION TESTING

Target Creation	Enumeration	Exploitation	Remediation	Proof
Pembuatan sistem vulnerable (tanpa DVWA/source code jadi).	*Pengumpulan informasi (Port scanning, tech stack analysis).*	*Eksekusi serangan dan pembuktian akses.*	*Penerapan patch keamanan dan best practices.*	*Validasi ulang bahwa celah telah tertutup.*

VULNERABILITY 1

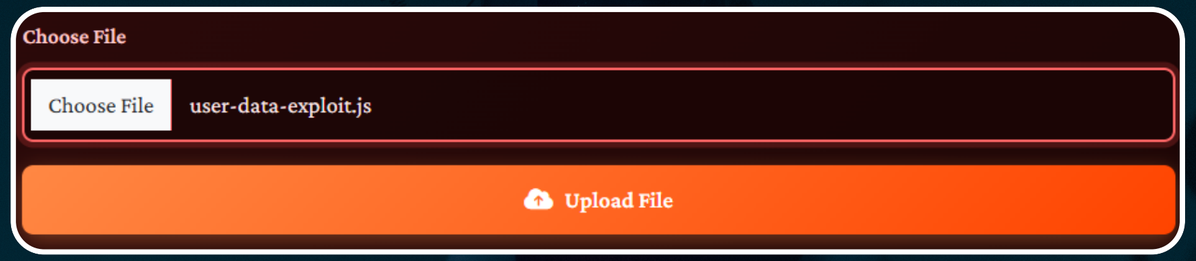
Insecure File Upload

Deskripsi

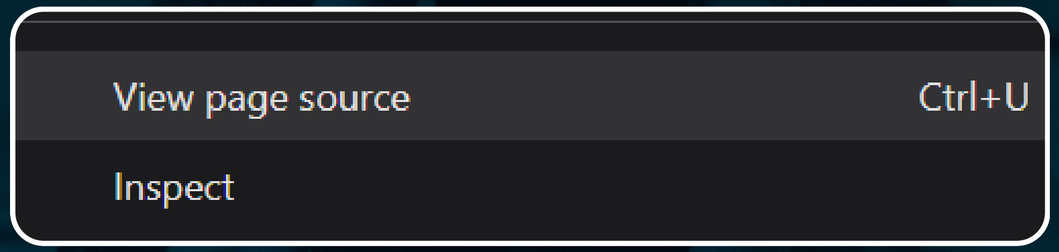
Server mengizinkan pengunggahan berkas tanpa validasi tipe, ekstensi, atau isi yang memadai.

Temuan Enumerasi

- Form upload tidak membatasi ekstensi file.
- Ditemukan debug endpoint /api/users melalui View Page Source yang mengekspos data user.



Pentester menemukan bahwa bisa upload file apa saja



Pentester mencoba mencari endpoint tidak tersnaitasi dari page source

Pentester menemukan endpoint untuk mendapatkan informasi users

VULNERABILITY 1

Insecure File Upload

Metode 1: Data Extraction

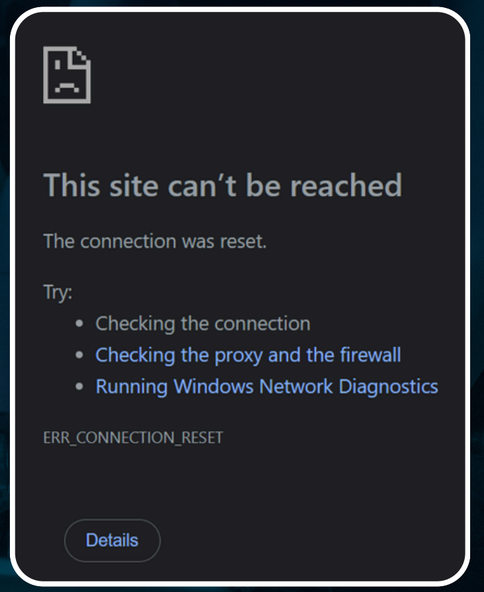
- Upload ***user-data-exploit.js.***
- **Hasil:** Server mengeksekusi script dan menampilkan database dump (Username, Email, Password Hash & Plaintext).

Metode 2: Denial of Service (DoS)

- Upload ***server-shutdown.js.***
- **Hasil:** Server crash/mati total, memutus koneksi seluruh pengguna.

Username	Email	Password Hash
fathan	fathan@kemjar.ac.id	$2a$10$FjgEsicO87tAV2EL.8FB
ryan	ryan@kemjar.ac.id	$2a$10$c/WZExbN0pFtzsJB/01p
admin	admin@kemjar.ac.id	$2a$10$xoiFYninyhrO/200cOOJ

Pentester memperoleh seluruh data database user



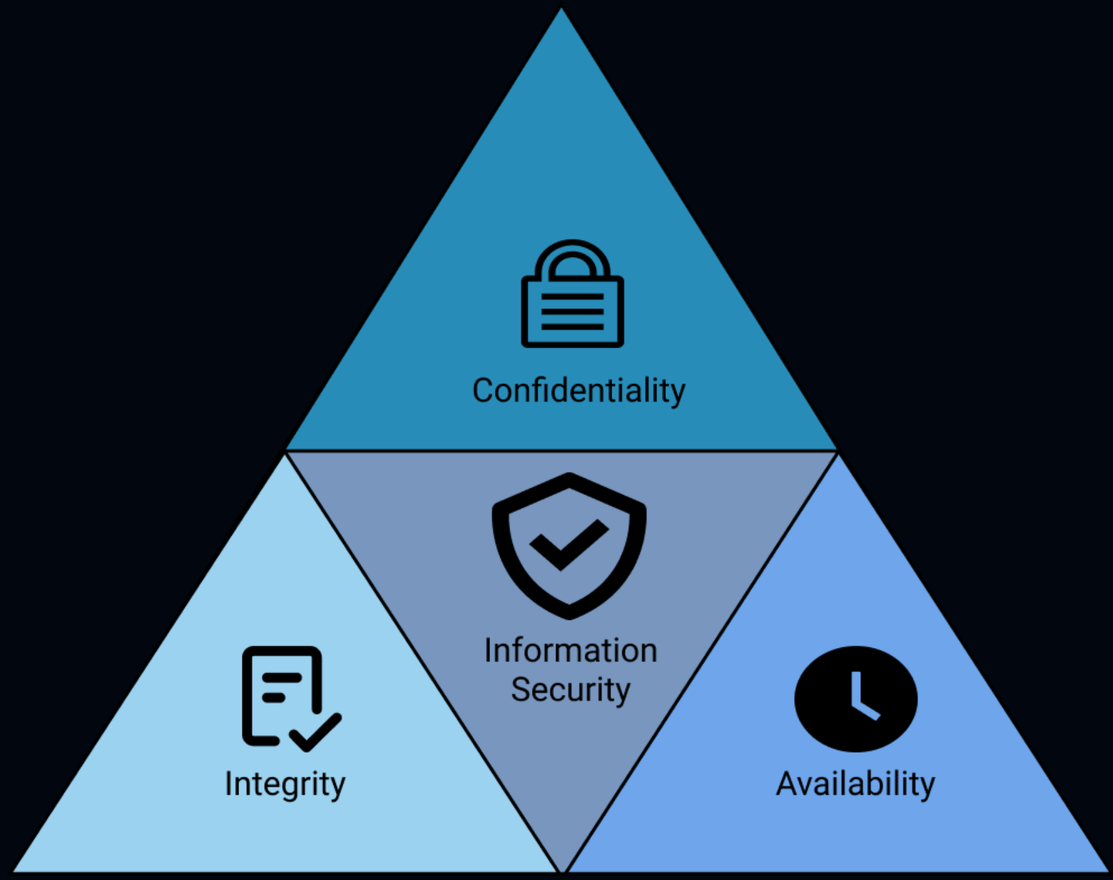
Pentester shutdown server

VULNERABILITY 1

Insecure File Upload

Analisis Dampak

- **Confidentiality (Kerahasiaan):** Kebocoran total database pengguna (email & password).
- **Availability (Ketersediaan):** Risiko Server Shutdown (DoS) yang mengganggu layanan bisnis.
- **Integrity (Integritas):** Penyerang dapat memodifikasi sistem atau menanamkan backdoor.
- **Severity:** CRITICAL.



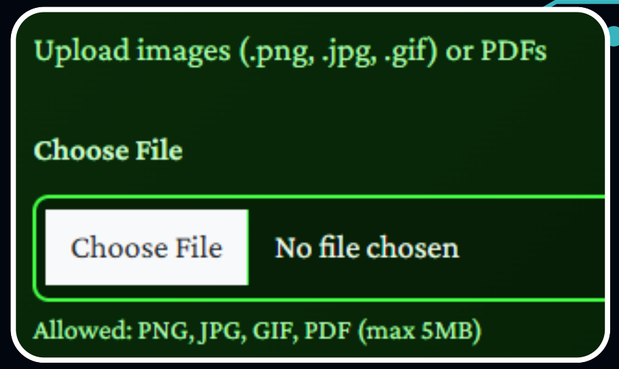
Segitiga Ilustrasi CIA Triad

VULNERABILITY 1

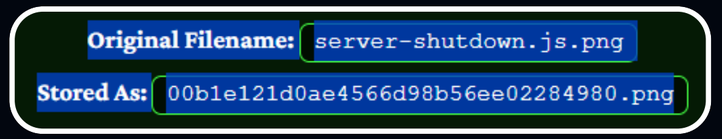
Insecure File Upload

Remediasi & Mitigasi

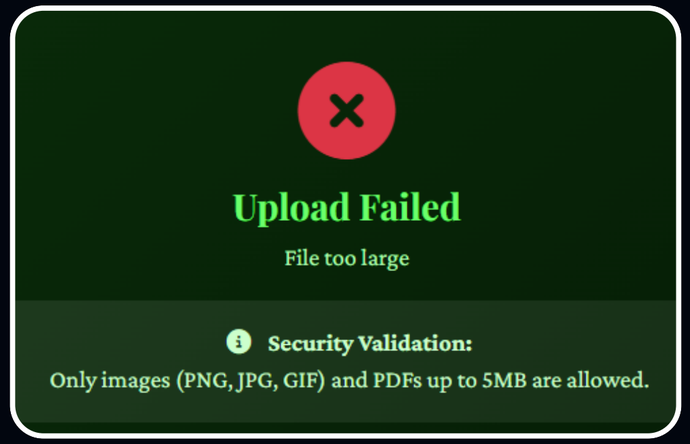
- **Whitelist Extensions:** Hanya mengizinkan .jpg, .png, .pdf. File .js atau .exe ditolak.
- **MIME Type Validation:** Memastikan isi file sesuai ekstensinya (mencegah renaming file berbahaya).
- **File Size Limit:** Maksimal 5MB untuk mencegah DoS via disk filling.
- **Randomized Filename:** Menggunakan crypto.randomBytes untuk nama file agar tidak bisa ditebak/ditimpa.
- **Static Serving:** File disimpan di direktori statis yang tidak memiliki izin eksekusi (non-executable).



Pengecekan ekstensi file sebelum upload



Penyimpanan file dengan nama acak



Gagal upload file jika size terlalu beaar

VULNERABILITY 2

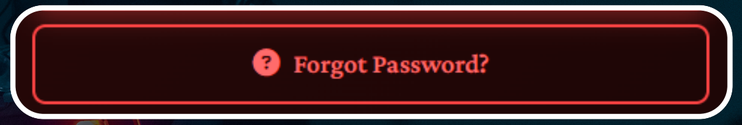
Insecure Change Password (OTP)

Deskripsi

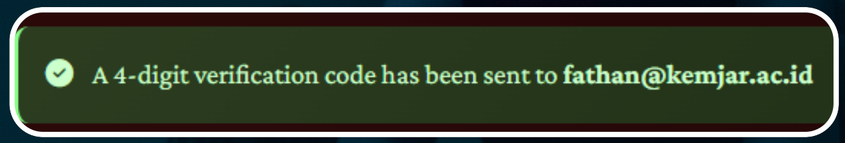
Fitur reset password menggunakan OTP 4 digit tanpa pembatasan percobaan (rate limiting).

Temuan Enumerasi

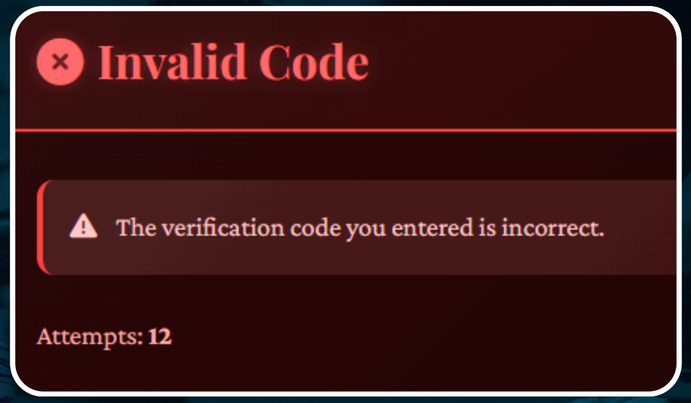
- OTP hanya terdiri dari angka 0000-9999 (10.000 kemungkinan).
- Tidak ada mekanisme lockout setelah input salah berulang kali.
- HTML pattern="[0-9]{4}" mengkonfirmasi format input.



Pentester menklik tombol “Forgot Password” seolah-olah dia user aslinya



Pentester menemukan bahwa kode OTP hanya 4 karakter dan terdiri dari angka 0-9 saja



Pentester menyadari bahwa tidak ada rate-limiting dari menginput kode OTP-nya

VULNERABILITY 2

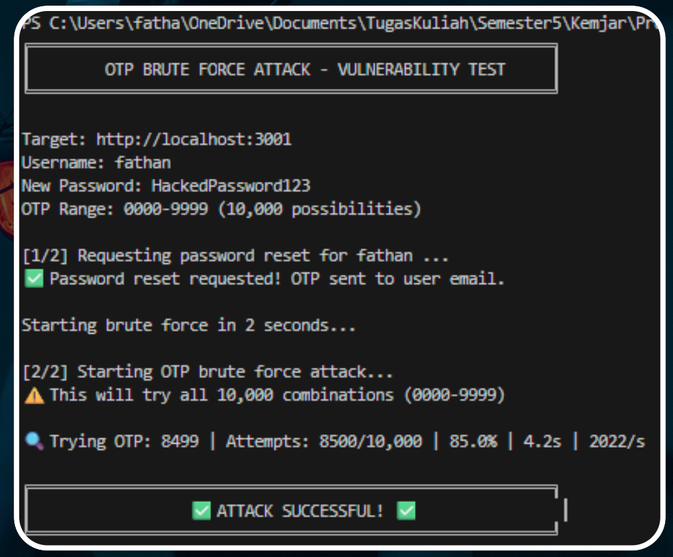
Insecure Change Password (OTP)

Skenario Serangan:

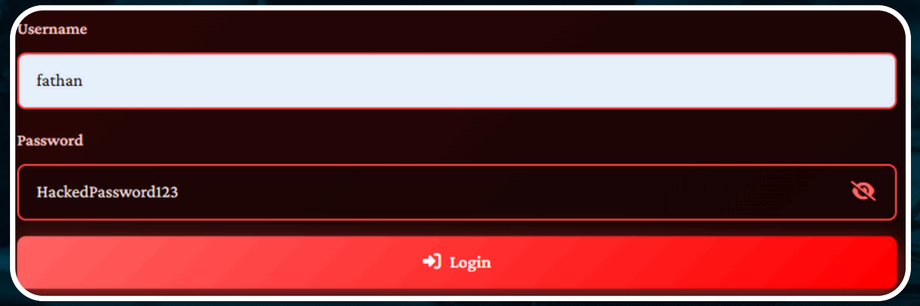
- Penyerang me-request OTP untuk target (misal: user fathan).
- Menjalankan script (**otp-bruteforce.js**) menggunakan node-fetch.

Hasil:

- Waktu serangan: < 10 detik.
- OTP ditemukan (misal: 3847).
- Password berhasil diubah dan Account Takeover berhasil.



Pentester menjalankan script untuk brute-force kode OTP



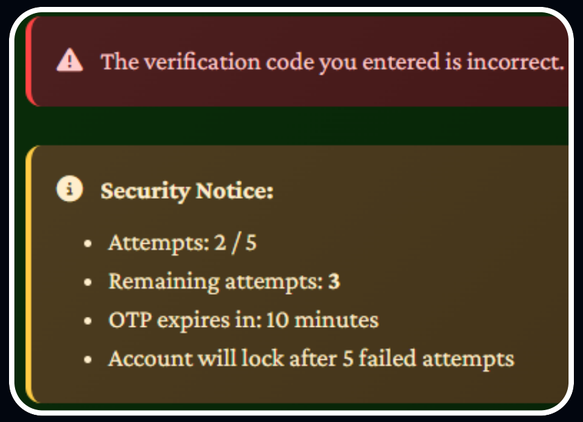
Pentester dapat login dengan password baru yang ia ganti

VULNERABILITY 2

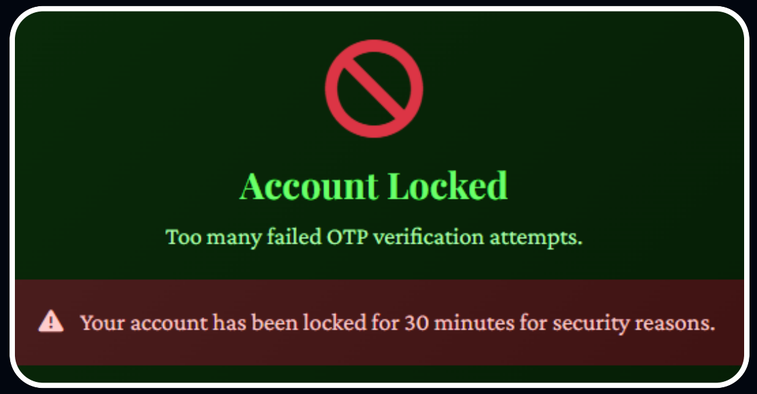
Insecure Change Password (OTP)

Remediasi & Mitigasi

- **Kompleksitas OTP:** Menggunakan 6 digit (1 juta kemungkinan vs 10 ribu).
- **Rate Limiting:** Maksimal 5 kali percobaan salah.
- Account Lockout: Akun terkunci selama 30 menit jika batas percobaan terlampaui.
- **Expiration Time:** OTP expired dalam 10 menit.
- **Password Policy:** Password baru wajib kombinasi Huruf Besar, Kecil, Angka, dan Simbol.



Pentester menyadari bahwa kali ini terdapat maskimum percobaan sehingga tidak bisa brute-force



Pentester menyadari bahwa setelah 5 percobaan tidak bisa mengirim kode OTP ulang hingga waktu tertentu


netlab
THANK YOU