



PENETRATION TESTING



Proyek Akhir Praktikum Keamanan Jaringan

Oleh Kelompok 15



ANGGOTA KELompok 15



Ryan Adidaru E. B.

2306266994



Fathan Yazid S.

2306250560

netlab

PENDAHULUAN

RUANG LINGKUP

TOPIK - TOPIK

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).



INSECURE FILE UPLOAD

Menguji validasi server terhadap berkas yang diunggah.



INSECURE CHANGE PASSWORD

Menguji mekanisme reset password berbasis OTP.



METODOLOGI PENETRATION TESTING

Target Creation

Pembuatan sistem vulnerable (tanpa DVWA/source code jadi).

Enumeration

Pengumpulan informasi (Port scanning, tech stack analysis).

Exploitation

Eksekusi serangan dan pembuktian akses.

Remediation

Penerapan patch keamanan dan best practices.

Proof

Validasi ulang bahwa celah telah tertutup.

VULNERABILITY 1

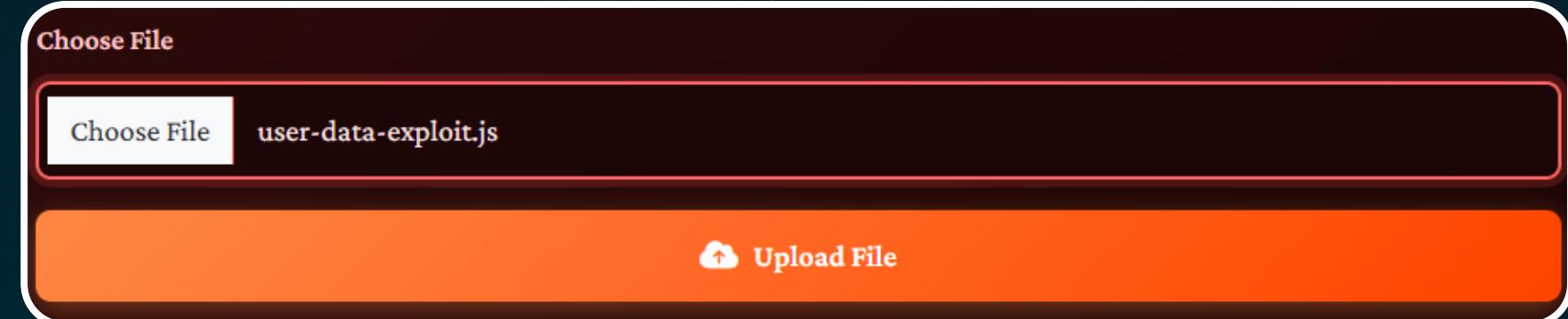
Insecure File Upload

Deskripsi

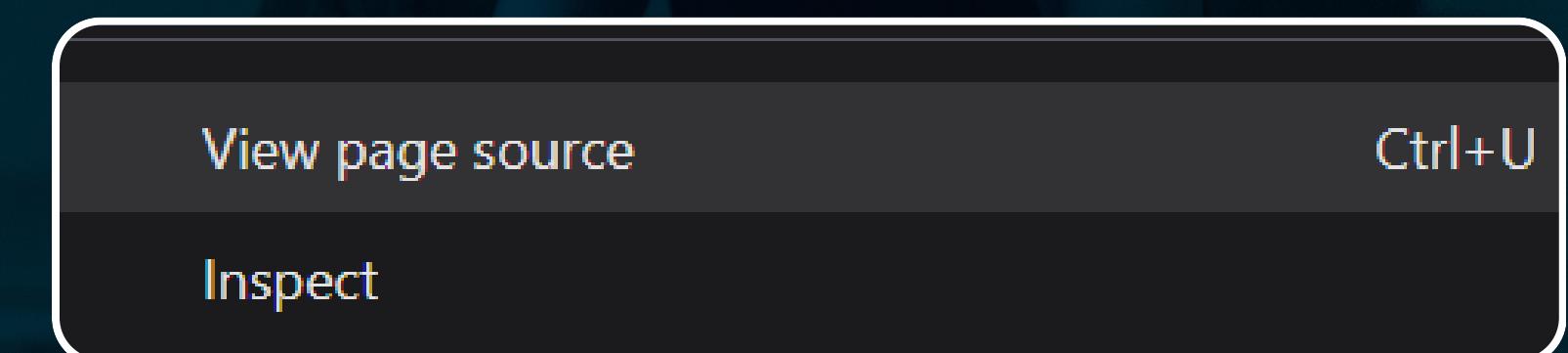
Server mengizinkan pengunggahan berkas tanpa validasi tipe, ekstensi, atau isi yang memadai.

Temuan Enumeration

- 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 tersenit dari page source



Pentester menemukan endpoint untuk mendapatkan informasi users

VULNERABILITY 1

Insecure File Upload

Metode 1: Data Extraction

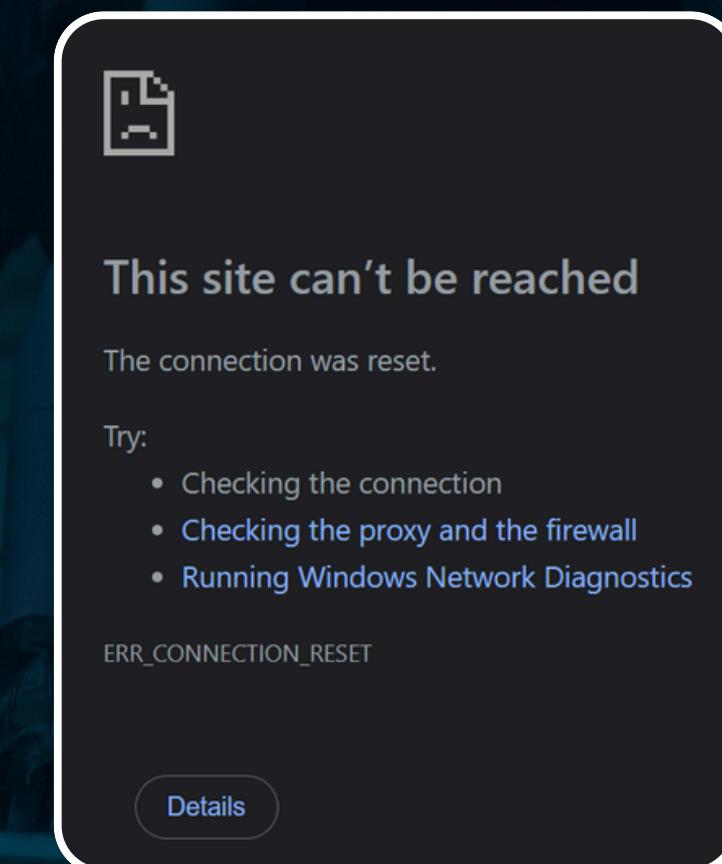
- Upload ***user-data-exploit.js***.
- **Hasil:** Server mengeksekusi script dan menampilkan database dump (Username, Email, Password Hash & Plaintext).

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\$FjgEsic087tAV2EL.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



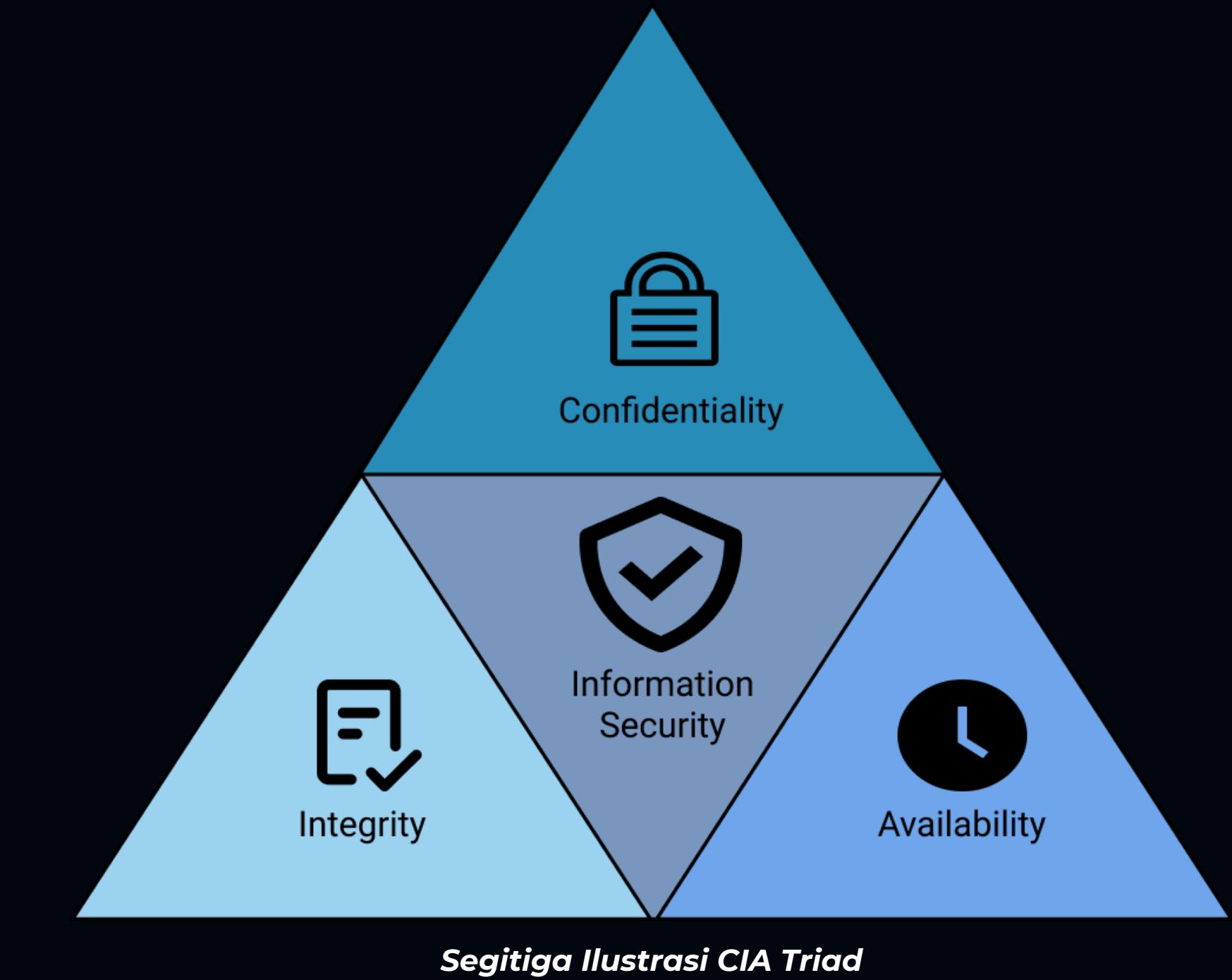
Pentester shutdown server

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.



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/ditimpas.
- Static Serving:** File disimpan di direktori statis yang tidak memiliki izin eksekusi (non-executable).

Upload images (.png, .jpg, .gif) or PDFs

Choose File

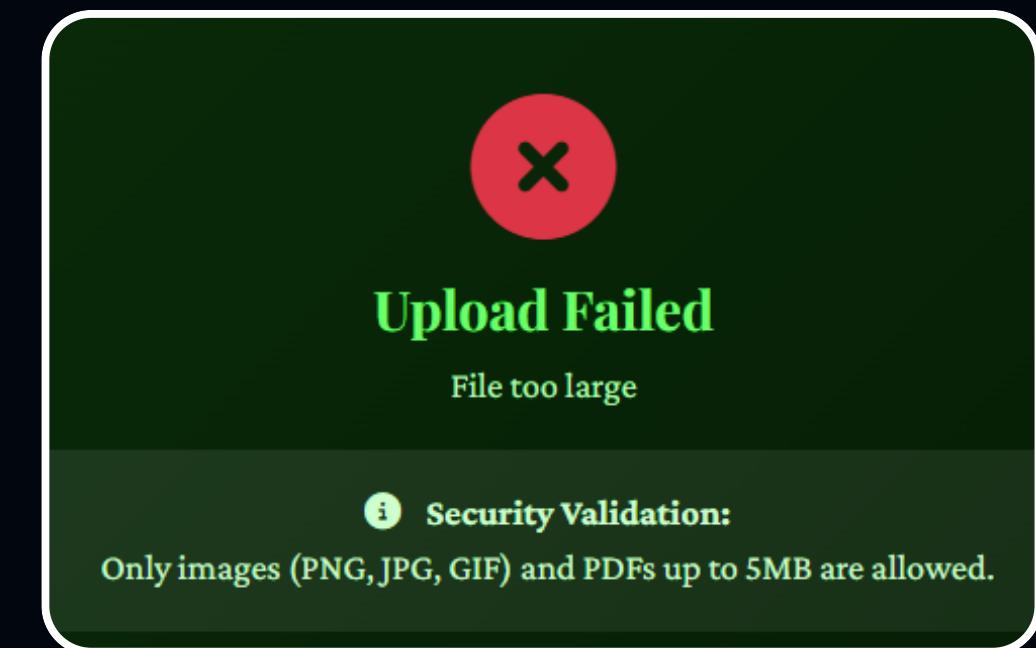
No file chosen

Allowed: PNG, JPG, GIF, PDF (max 5MB)

Pengecekan ekstensi file sebelum upload

Original Filename: `server-shutdown.js.png`
Stored As: `00b1e121d0ae4566d98b56ee02284980.png`

Penyimpanan file dengan nama acak



Gagal upload file jika size terlalu besar

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.

A 4-digit verification code has been sent to **fathan@kemjar.ac.id**

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

Invalid Code

The verification code you entered is incorrect.

Attempts: 12

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

pentester menklik tombol "Forgot Password"
seolah-olah dia user aslinya

VULNERABILITY 2

Insecure Change Password (OTP)

Skenario Serangan:

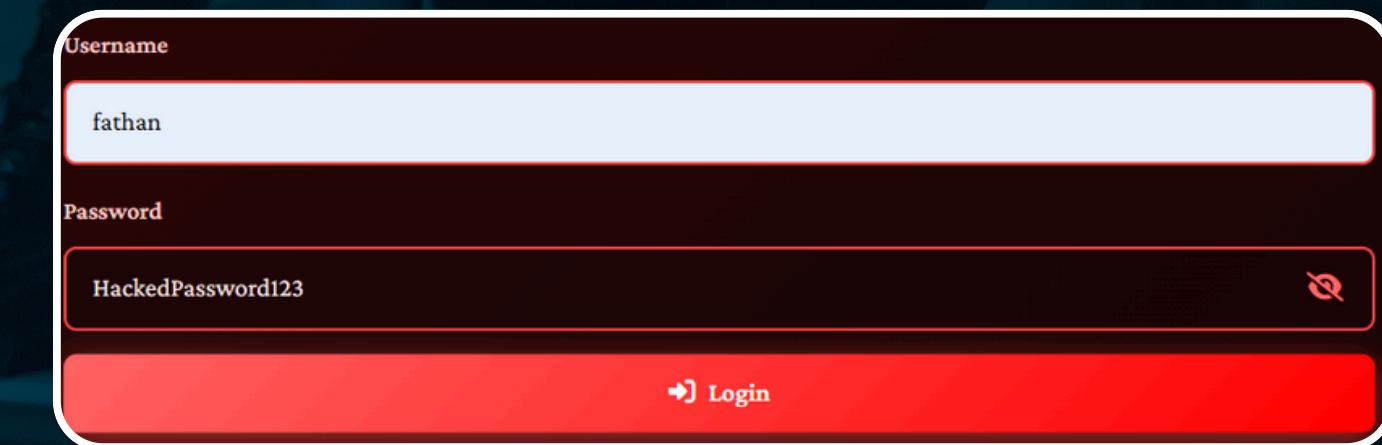
- Penyerang me-request OTP untuk target (misal: user fathan).
- Menjalankan script (**otp-bruteforce.js**) menggunakan node-fetch.

Hasil:

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

```
PS C:\Users\fatha\OneDrive\Documents\TugasKuliah\Semester5\Kemjar\Pr  
OTP BRUTE FORCE ATTACK - VULNERABILITY TEST  
  
Target: http://localhost:3001  
Username: fathan  
New Password: HackedPassword123  
OTP Range: 0000-9999 (10,000 possibilities)  
  
[1/2] Requesting password reset for fathan ...  
✓ Password reset requested! OTP sent to user email.  
  
Starting brute force in 2 seconds...  
  
[2/2] Starting OTP brute force attack...  
⚠ This will try all 10,000 combinations (0000-9999)  
  
● Trying OTP: 8499 | Attempts: 8500/10,000 | 85.0% | 4.2s | 2022/s  
  
ATTACK SUCCESSFUL!
```

Pentester menjalankan script untuk brute-force kode OTP



A screenshot of a web browser showing a login form. The form has two fields: 'Username' containing 'fathan' and 'Password' containing 'HackedPassword123'. Below the form is a large red button labeled 'Login' with a key icon.

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.

 The verification code you entered is incorrect.

Security Notice:

- Attempts: 2 / 5
- Remaining attempts: 3
- OTP expires in: 10 minutes
- Account will lock after 5 failed attempts

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



Account Locked

Too many failed OTP verification attempts.

 Your account has been locked for 30 minutes for security reasons.

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



THANK YOU