

CAK3BAB3
IMPLEMENTASI DAN
PENGUJIAN PERANGKAT LUNAK

WHITEBOX TESTING AND
BLACKBOX TESTING



ANGGOTA KELOMPOK:

- | | |
|-----------------------------|--------------|
| 1. Zahra Puspita Paramastri | (2211102081) |
| 2. Dewi Aminah Chan | (2211102089) |
| 3. Hana Setia Putri A.R | (2211102155) |
| 4. Gea Amarlinda Sassy M | (2211102301) |

DOSEN:

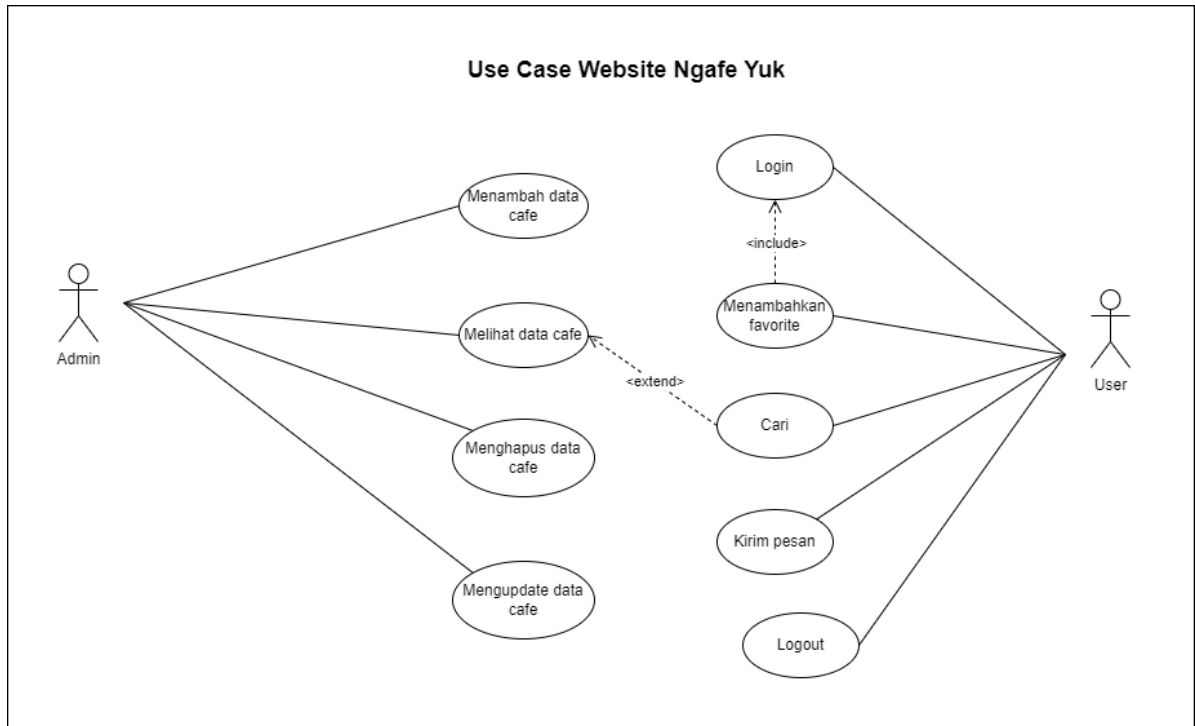
Muhamad Azrino Gustalika, S.Kom., M.Tr.T

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS TELKOM
PURWOKERTO
2024

WHITEBOX

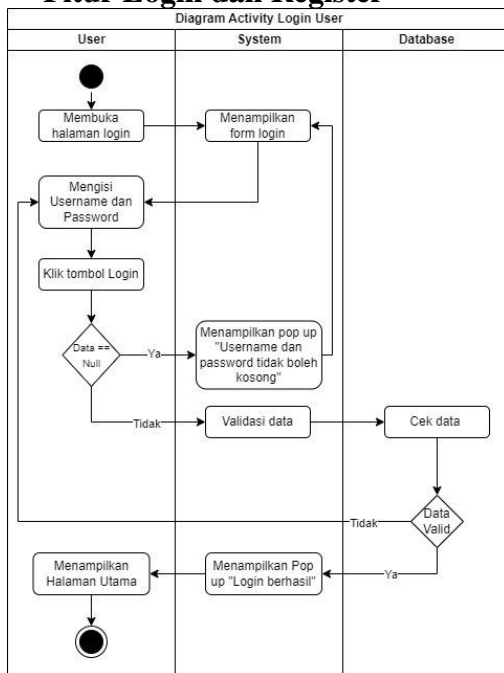
➤ Path Testing

• Use Case

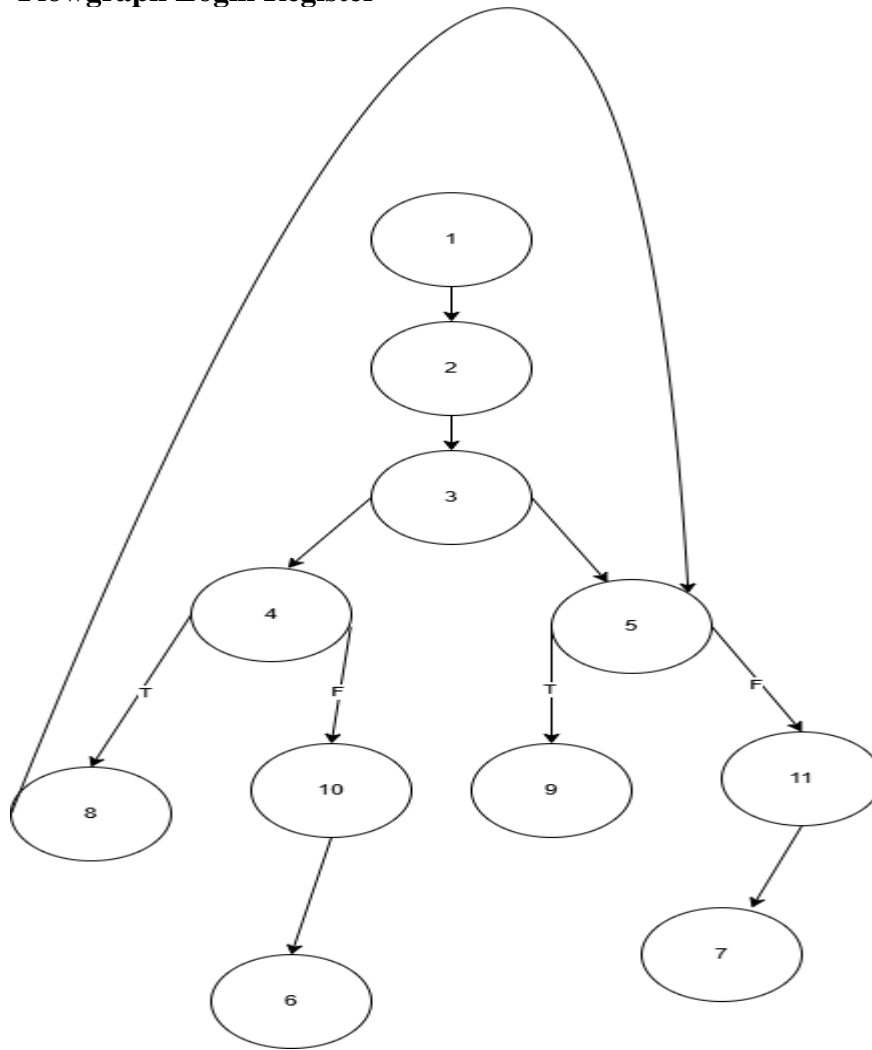


• Flowgraph

Fitur Login dan Register



Flowgraph Login Register



- Independent Path
 - 1-2-3-4-8
 - 1-2-3-4-10
 - 1-2-3-5-9
 - 1-2-3-11-7
 - 1-2-3-4-8-5-9
 - 1-2-3-4-6
 - 1-2-3-5-7

Sudah sesuai dari diagram awala dengan flowgraph.

➤ Security Testing

Vulnerability Testing

Menggunakan IP [192.168.18.253](#) sebagai target. dengan tools Nmap dan Nikto. Kita akan menggunakan nmap terlebih dahulu

```
mikemself@fedora:~$ nmap -p 22,80,3306 --script ssh2-enum-algos,http-methods,http-headers,http-enum,mysql-brute,mysql-info -sV 192.168.18.253
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-27 18:49 WIB
Nmap scan report for fedora (192.168.18.253)
Host is up (0.000083s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.8 (protocol 2.0)
| ssh2-enum-algos:
|   kex_algorithms: (11)
|     curve25519-sha256
|     curve25519-sha256@libssh.org
|     ecdh-sha2-nistp256
|     ecdh-sha2-nistp384
|     ecdh-sha2-nistp521
|     diffie-hellman-group-exchange-sha256
|     diffie-hellman-group14-sha256
|     diffie-hellman-group16-sha512
|     diffie-hellman-group18-sha512
|     ext-info-s
|     kex-strict-s-v00@openssh.com
|   server_host_key_algorithms: (4)
|     rsa-sha2-512
|     rsa-sha2-256
|     ecdsa-sha2-nistp256
|     ssh-ed25519
|   encryption_algorithms: (5)
|     aes256-gcm@openssh.com
|     chacha20-poly1305@openssh.com
|     aes256-ctr
|     aes128-gcm@openssh.com
|     aes128-ctr
|   mac_algorithms: (8)
|     hmac-sha2-256-etm@openssh.com
|     hmac-sha1-etm@openssh.com
|     umac-128-etm@openssh.com
|     hmac-sha2-512-etm@openssh.com
|     hmac-sha2-256
|     hmac-sha1
|     umac-128@openssh.com
|     hmac-sha2-512
```

```
mikrusek@fedora:~$
umac-128-etm@openssh.com
hmac-sha2-512-etm@openssh.com
hmac-sha2-256
hmac-sha1
umac-128@openssh.com
hmac-sha2-512
compression_algorithms: (2)
  none
  zlib@openssh.com
80/tcp open  http      Apache httpd 2.4.62 ((Fedora Linux))
http-enum:
  /phpmyadmin/: phpMyAdmin
  /phpMyAdmin/: phpMyAdmin
  /css/: Potentially interesting folder w/ directory listing
  /icons/: Potentially interesting folder w/ directory listing
  /img/: Potentially interesting folder w/ directory listing
  /js/: Potentially interesting folder w/ directory listing
  /src/: Potentially interesting folder w/ directory listing
http-headers:
  Date: Wed, 27 Nov 2024 11:49:17 GMT
  Server: Apache/2.4.62 (Fedora Linux)
  Last-Modified: Wed, 27 Nov 2024 10:19:27 GMT
  ETag: "17db-627e24cee42fc"
  Accept-Ranges: bytes
  Content-Length: 6107
  Connection: close
  Content-Type: text/html; charset=UTF-8
  (Request type: HEAD)
http-methods:
  Supported Methods: OPTIONS HEAD GET POST TRACE
  Potentially risky methods: TRACE
http-server-header: Apache/2.4.62 (Fedora Linux)
3306/tcp open  mysql      MariaDB (unauthorized)
mysql-brute:
  Accounts: No valid accounts found
  Statistics: Performed 50009 guesses in 3 seconds, average tps: 16669.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.85 seconds.
```

Perintah Utama:

```
nmap -p 22,80,3306 --script ssh2-enum-algos,http-methods,http-headers,http-enum,mysql-brute,mysql-info -sV 192.168.18.253
```

Perintah ini melakukan pemindaian mendalam terhadap port tertentu pada target IP

192.168.18.253 untuk mendeteksi layanan, versinya, dan potensi kerentanannya menggunakan skrip bawaan Nmap.

Detail Parameter:

1. `-p 22,80,3306`
 - Penjelasan: Menentukan port spesifik yang akan dipindai:
 - Port 22: Digunakan untuk protokol SSH (Secure Shell).
 - Port 80: Digunakan untuk layanan HTTP (web server).
 - Port 3306: Digunakan untuk protokol MySQL/MariaDB (database server).
 - Fungsi: Mempercepat proses pemindaian dengan hanya memeriksa port yang disebutkan, alih-alih memindai semua port secara default.
2. `--script ssh2-enum-algos,http-methods,http-headers,http-enum,mysql-brute,mysql-info`
 - Penjelasan: Menjalankan serangkaian skrip Nmap bawaan untuk memeriksa lebih dalam tentang konfigurasi dan potensi kerentanan di layanan yang terdeteksi. Berikut detail tiap skrip:
 - `ssh2-enum-algos`:
 - Mengidentifikasi algoritma enkripsi, autentikasi, dan pertukaran kunci yang didukung oleh server SSH.
 - Penting untuk mendeteksi apakah server menggunakan algoritma yang usang atau lemah.
 - `http-methods`:

- Memeriksa metode HTTP yang didukung oleh server (GET, POST, TRACE, dll).
 - Tujuan utamanya adalah menemukan metode berisiko seperti TRACE yang dapat digunakan untuk serangan.
 - **http-headers:**
 - Mengambil dan menganalisis header HTTP dari server.
 - Informasi seperti versi server, konfigurasi cache, atau header khusus dapat menunjukkan potensi kerentanan.
 - **http-enum:**
 - Mencoba menemukan direktori, file, atau aplikasi web yang bisa diakses pada server HTTP.
 - Berguna untuk mendeteksi struktur direktori yang terbuka atau file sensitif.
 - **mysql-brute:**
 - Melakukan brute force attack pada server MySQL untuk mencoba kredensial default atau lemah.
 - Digunakan untuk mengidentifikasi akun database yang rentan.
 - **mysql-info:**
 - Mengumpulkan informasi tentang server MySQL, seperti versi, mode autentikasi, dan fitur yang diaktifkan.
3. **-sV**

- Penjelasan: Mengaktifkan deteksi versi layanan (Service Version Detection).
- Fungsi: Memeriksa layanan yang berjalan di port tertentu dan menentukan versinya. Informasi ini berguna untuk mengidentifikasi kerentanan spesifik yang mungkin terkait dengan versi tersebut.

4. **192.168.18.253**

- Penjelasan: Alamat IP target yang akan dipindai.

- Fungsi: Mengarahkan Nmap untuk memfokuskan pemindaian pada host ini.
-

Fungsi Utama Perintah Ini

- Tujuan: Menganalisis keamanan tiga layanan utama yang berjalan pada server (SSH, HTTP, dan MySQL).
- Manfaat: Mendapatkan informasi mendetail tentang konfigurasi layanan, algoritma enkripsi, versi layanan, dan potensi kerentanan yang bisa dimanfaatkan.
- Penggunaan: Sangat cocok untuk tahap awal penilaian keamanan (vulnerability assessment) pada jaringan atau server.

Dokumentasi Penemuan

1. Hasil Pemindaian

Port yang Teridentifikasi Terbuka:

1. Port 22 (SSH)

- Layanan: OpenSSH 9.8
- Protokol yang Didukung: SSH 2.0
- Algoritma Pertukaran Kunci (Key Exchange Algorithms):
 - curve25519-sha256
 - ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
 - diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512
 - ext-info-s
- Algoritma Enkripsi:
 - aes256-gcm@openssh.com, aes128-gcm@openssh.com
 - chacha20-poly1305@openssh.com
 - aes256-ctr, aes128-ctr
- Fingerprint Host Key:
 - RSA-SHA2-512, RSA-SHA2-256
 - ECDSA-SHA2-NISTP256
 - SSH-ED25519
- Algoritma MAC (Message Authentication Code):
 - hmac-sha2-256, hmac-sha2-512
 - umac-128-etm@openssh.com

2. Port 80 (HTTP)

- Layanan: Apache HTTPD 2.4.62
- Direktori Terbuka:

- `/phpmyadmin/`
 - `/css/, /icons/, /img/, /js/, /src/`
 - Header Server HTTP:
 - Server: Apache/2.4.62 (Fedora Linux)
 - Last-Modified: Wed, 27 Nov 2024
 - ETag: "17db-627e24cee42fc"
 - Metode HTTP yang Didukung:
 - OPTIONS, HEAD, GET, POST, TRACE (TRACE terindikasi berisiko).
3. Port 3306 (MySQL/MariaDB)
- Layanan: MariaDB
 - Status: Unauthorized Access, tidak ada akun valid yang ditemukan.
 - Tes Brute Force:
 - Hasil: Tidak ada akun dengan kredensial default berhasil ditemukan.
-

2. Analisis Risiko

1. Port 22 (SSH)

- Kerentanan: Protokol SSH dapat dieksploitasi melalui brute force attack jika menggunakan kata sandi lemah. Algoritma yang tidak aman dapat digunakan untuk serangan downgrade.
- Dampak Potensial: Akses ke server melalui layanan shell aman ini bisa memberikan kontrol penuh kepada penyerang.
- Tingkat Risiko: Medium-High

2. Port 80 (HTTP)

- Kerentanan:
 - Directory listing aktif pada beberapa direktori penting, termasuk direktori phpMyAdmin yang sering menjadi target eksploitasi.
 - TRACE diizinkan, yang dapat digunakan untuk serangan XST (Cross-Site Tracing).

- Dampak Potensial: Potensi kebocoran data sensitif seperti konfigurasi file atau bahkan eksploitasi via phpMyAdmin.
- Tingkat Risiko: High

3. Port 3306 (MariaDB)

- Kerentanan: Akses terbuka ke port database dapat dimanfaatkan oleh penyerang untuk mencoba autentikasi brute force atau mengidentifikasi celah pada database itu sendiri.
- Dampak Potensial: Eksposur data sensitif atau kerentanan lainnya yang berpotensi merusak integritas sistem.
- Tingkat Risiko: High

3. Rekomendasi Mitigasi

1. Port 22 (SSH):

- Aktifkan autentikasi berbasis kunci publik dan nonaktifkan login berbasis kata sandi.
- Batasi akses SSH menggunakan firewall untuk IP tertentu.
- Terapkan mekanisme perlindungan brute force seperti Fail2Ban.

2. Port 80 (HTTP):

- Nonaktifkan directory listing dengan mengubah konfigurasi Apache:
Options -Indexes
- Nonaktifkan metode TRACE pada server HTTP untuk mencegah serangan XST.
- Amankan direktori phpMyAdmin dengan autentikasi tambahan atau firewall.

3. Port 3306 (MariaDB):

- Batasi akses port 3306 hanya untuk IP tertentu yang dipercaya.
- Gunakan kredensial yang kuat untuk akun database.
- Aktifkan logging dan analisis secara berkala untuk mendeteksi aktivitas mencurigakan.

4. Langkah Tindak Lanjut

- Lakukan audit ulang terhadap sistem setelah menerapkan mitigasi.
 - Gunakan IDS/IPS untuk memantau aktivitas mencurigakan secara real-time.
 - Pertimbangkan melakukan hardening tambahan pada konfigurasi server untuk mengurangi risiko eksploitasi di masa mendatang.
-

Kesimpulan

Hasil pemindaian mengungkapkan sejumlah kerentanan signifikan pada konfigurasi layanan yang sedang berjalan. Dengan fokus pada mitigasi yang cepat dan efektif, risiko terhadap integritas dan keamanan sistem dapat diminimalisir secara signifikan.

Selanjutnya kita akan mencoba menggunakan nikto

```
mikmself@fedora:~$ nikto -h 192.168.18.253 --port 80
- ***** RFIURL is not defined in nikto.conf--no RFI tests will run *****
- Nikto v2.5.0

+-----+
+ Target IP:      192.168.18.253
+ Target Hostname: 192.168.18.253
+ Target Port:    80
+ Start Time:     2024-11-27 19:08:51 (GMT7)
+-----+
+ Server: Apache/2.4.62 (Fedora Linux)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /zw8PlLNM.php: Retrieved x-powered-by header: PHP/8.3.14.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /src/: Directory indexing found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ 6440 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:      2024-11-27 19:08:59 (GMT7) (8 seconds)
+-----+
+ 1 host(s) tested
```

Analisis Temuan Keamanan Berdasarkan Pemindaian Nikto

1. Informasi Umum

- IP Target: 192.168.18.253
- Hostname Target: 192.168.18.253
- Port yang Dipindai: 80 (HTTP)
- Server Teridentifikasi: Apache/2.4.62 (Fedora Linux)
- Waktu Pemindaian: 27 November 2024, 19:08:51 (GMT+7)
- Durasi Pemindaian: 8 detik

2. Temuan Keamanan yang Terdeteksi

Nikto melaporkan beberapa kelemahan kritis dan non-kritis yang terdeteksi pada server target. Berikut adalah analisis mendalam:

1. Header HTTP Tidak Lengkap:

- X-Frame-Options Tidak Ditemukan:
 - Risiko: Membuka potensi serangan Clickjacking, di mana elemen berbahaya dapat ditempatkan di atas situs web target.
 - Referensi: [MDN Web Docs - X-Frame-Options](#).
 - X-Content-Type-Options Tidak Dikonfigurasi:
 - Risiko: Server dapat membiarkan browser merender konten yang tidak sesuai dengan tipe MIME yang diatur, memungkinkan serangan MIME Sniffing.
 - Referensi: [Netsparker - Missing Content-Type Header](#).
2. Metode HTTP yang Rentan:
- Metode TRACE Aktif:
 - Risiko: Rentan terhadap serangan Cross-Site Tracing (XST), yang dapat memungkinkan eksploitasi data cookie pengguna melalui skrip berbahaya.
 - Referensi: [OWASP - Cross Site Tracing](#).
3. Directory Indexing Aktif:
- Direktori seperti `/css/`, `/img/`, `/src/`, dan `/icons/` ditemukan memiliki directory listing yang aktif.
 - Risiko: Informasi terkait struktur direktori dapat dimanfaatkan oleh penyerang untuk mendapatkan akses file sensitif atau menavigasi direktori tanpa otorisasi.
4. File dan Direktori Sensitif:
- phpMyAdmin Directory Ditemukan:
 - Risiko: Direktori phpMyAdmin sering kali menjadi target serangan brute force atau eksploitasi jika tidak dilindungi dengan baik.
 - Header tambahan: `'x-ob_mode'` ditemukan dengan nilai `1`, menunjukkan kemungkinan pengaturan tertentu yang dapat dieksploitasi.

- Default File Apache ([icons/README](#)) Teridentifikasi:
 - Risiko: Menunjukkan server belum di-hardening dengan baik, berpotensi mengungkap informasi konfigurasi sensitif.
 - Referensi: [Restricting Access to icons/README](#).
 - 5. Pengungkapan Header Server:
 - Header X-Powered-By ditemukan dengan nilai [PHP/8.3.14](#). Informasi ini dapat membantu penyerang mengidentifikasi kerentanan spesifik pada versi PHP tersebut.
-

3. Penilaian Risiko

- Risiko Tinggi:
 1. Clickjacking (X-Frame-Options): Rentan terhadap eksploitasi visual yang dapat menipu pengguna.
 2. XST (HTTP TRACE): Eksposur TRACE membuka potensi serangan terhadap data autentikasi seperti cookie.
 - Risiko Sedang:
 1. Directory Indexing: Memberikan informasi tentang struktur file, membuka peluang eksploitasi file yang salah dikonfigurasi.
 2. phpMyAdmin Directory: Eksposur ke direktori admin database dapat menjadi vektor serangan signifikan.
 - Risiko Rendah:

Pengungkapan Versi PHP dan Apache: Informasi ini dapat digunakan dalam tahap reconnaissance oleh penyerang.
-

4. Rekomendasi Mitigasi

1. Header Keamanan HTTP:
 - Konfigurasi header **X-Frame-Options** dengan nilai SAMEORIGIN atau DENY.
 - Tambahkan header **X-Content-Type-Options: nosniff** untuk mencegah MIME sniffing.
 2. Nonaktifkan Metode TRACE:
 - Perbarui konfigurasi Apache untuk menonaktifkan metode HTTP TRACE: **TraceEnable off**
 3. Nonaktifkan Directory Indexing:
 - Modifikasi konfigurasi Apache dengan menambahkan: **Options -Indexes**
 4. Amankan Direktori phpMyAdmin:
 - Pindahkan direktori phpMyAdmin ke lokasi non-standar.
 - Terapkan autentikasi tambahan pada direktori tersebut.
 5. Sembunyikan Informasi Versi Server:
 - Ubah konfigurasi Apache dengan menambahkan: **ServerTokens Prod**
ServerSignature Off
 6. Pembaruan Perangkat Lunak:
 - Pastikan server Apache dan PHP diperbarui ke versi terbaru untuk menghindari eksploitasi kerentanan yang diketahui.
-

5. Kesimpulan

Hasil pemindaian menunjukkan kelemahan mendasar dalam konfigurasi keamanan server, termasuk header HTTP yang tidak lengkap, directory indexing yang aktif, dan metode TRACE yang diaktifkan. Implementasi langkah mitigasi yang disarankan dapat secara signifikan meningkatkan keamanan server dan mengurangi risiko serangan terhadap target.

Rate Limiting & Denial of Service (DoS)

Celah: Aplikasi ini tidak memiliki mekanisme untuk membatasi jumlah request yang diterima oleh endpoint `/api/send-message`.

Contoh Eksploitasi:

Penyerang dapat menggunakan alat seperti `curl` atau `burpsuite` untuk mengirimkan ribuan request dalam waktu singkat:

```
for i in {1..10000}; do curl -X POST -d  
'{"name":"test","email":"test@test.com","message":"spam"}' -H "Content-Type:  
application/json" http://localhost:3000/api/send-message; done
```

Ini dapat:

- Membebani server dan membuatnya tidak responsif.
- Mengisi database dengan data spam.

Solusi:

- Terapkan rate limiting menggunakan middleware seperti `express-rate-limit`.
- Validasi pengiriman berdasarkan IP atau autentikasi token.

CSRF (Cross-Site Request Forgery)

Celah: Endpoint tidak memeriksa apakah request berasal dari sumber yang sah.

Contoh Eksploitasi:

Jika ada sesi yang aktif, seorang penyerang dapat membuat halaman palsu dengan kode berikut:

```
<form action="http://localhost:3000/api/send-message" method="POST">
```



```
<input type="hidden" name="name" value="malicious">
```

```
<input type="hidden" name="email" value="hacker@evil.com">
```

```
<input type="hidden" name="phone" value="123456789">
```

```
<input type="hidden" name="message" value="CSRF Exploit">
```

```
<input type="submit" value="Submit">
```

```
</form>
```

Ketika korban membuka halaman tersebut, form akan terkirim ke server dengan kredensial aktif.

Solusi:

- Gunakan token CSRF untuk memastikan validitas pengiriman form.
- Validasi header referer/origin untuk memeriksa asal request.

Insecure Direct Object Reference (IDOR) & Missing Authentication and Authorization

Celah: Jika endpoint API tidak melakukan otorisasi dengan benar, penyerang dapat mengakses data atau melakukan operasi yang seharusnya tidak diizinkan.

Contoh Eksploitasi:

Jika endpoint `/api/send-message` tidak memvalidasi pengguna yang mengaksesnya, penyerang dapat mengirim request dengan data palsu tanpa autentikasi:

```
curl -X POST http://localhost:3000/api/send-message -d
```

```
'{"name":"Attacker","email":"attacker@evil.com","phone":"12345","message":"Hacked!"}' -H  
"Content-Type: application/json"
```

Solusi:

- Tambahkan autentikasi untuk semua endpoint, seperti JWT atau OAuth.

- Periksa izin pengguna sebelum memproses data.

Log Injection & XSS

Celah: Jika input dari pengguna disimpan langsung tanpa sanitasi, ini dapat memungkinkan penyerang menyisipkan kode berbahaya atau memanipulasi.

Contoh Eksploitasi:

Penyerang dapat mengirimkan input seperti berikut:

```
{  
"name": "<script>alert('LogInjection')</script>",  
"email": "attacker@evil.com",  
"phone": "12345",  
"message": "Injected"  
}
```

Jika log aplikasi mencatat input tanpa sanitasi, penyerang dapat memanfaatkan ini untuk:

- Membaca log sensitif & menyisipkan skrip berbahaya.

Solusi:

- Encode semua input sebelum disimpan ke log.

Bagian Penetration Testing dalam dokumen terutama meliputi:

1. Uji Kerentanan (menggunakan Nmap)

- Pemindaian mendetail pada IP 192.168.18.253
- Memindai port 22 (SSH), 80 (HTTP), dan 3306 (MySQL)
- Menganalisis versi layanan, konfigurasi, dan potensi kerentanan

2. Pemindaian Nikto

- Analisis keamanan web server pada port 80
- Mengidentifikasi kerentanan header HTTP
- Mendeteksi direktori yang terbuka dan risiko keamanan potensial

3. Analisis Kerentanan Keamanan Tambahan

- Risiko pembatasan laju & Denial of Service (DoS)
- Kerentanan CSRF (Cross-Site Request Forgery)
- Referensi Objek Langsung Tidak Aman (IDOR)
- Autentikasi dan Otorisasi yang Hilang
- Potensi eksploitasi Log Injection & XSS

Setiap bagian mengikuti metodologi penetration testing standar:

- Rekognisi (pemindaian)
- Identifikasi kerentanan
- Penilaian risiko
- Rekomendasi mitigasi

Dokumen menyediakan pendekatan komprehensif untuk mengidentifikasi dan mengatasi kelemahan keamanan potensial pada sistem target.

BLACKBOX

Black Box Testing: Sebuah Pendekatan Sistematis dalam Evaluasi Perangkat Lunak

Konsep black box testing merupakan metode pengujian yang sangat strategis dalam rekayasa perangkat lunak, di mana pengembang melakukan evaluasi fungsionalitas sistem secara menyeluruh tanpa melakukan intervensi atau analisis pada struktur internal kode program. Metode ini bukan sekadar pengujian akhir, melainkan pendekatan komprehensif yang mengungkap potensi kelemahan sistem dari perspektif fungsional.

Analisis Mendalam Teknik-Teknik Black Box Testing:

1. **All Pair Testing (Pairwise Testing)** Teknik ini lebih dari sekadar pengujian kombinasi sederhana. Ia merepresentasikan pendekatan matematis yang kompleks untuk memetakan seluruh kemungkinan interaksi antarparameter, dengan tujuan mengidentifikasi potensi kesalahan yang mungkin terjadi pada titik pertemuan antarvariabel.
2. **Boundary Value Analysis** Suatu metode pengujian yang tidak sekadar memeriksa batas-batas input, melainkan menyelidiki titik-titik kritis di mana sistem paling rentan mengalami kegagalan. Teknik ini memfokuskan analisis pada zona marginal di mana kesalahan paling mungkin terjadi.
3. **Cause-Effect Graph** Pendekatan yang menampilkan hubungan kausal antarfaktor dalam sistem secara visual. Bukan sekadar grafik sederhana, melainkan peta kompleksitas interaksi yang memungkinkan pengujian sistematis terhadap kondisi-kondisi kritis dalam perangkat lunak.
4. **Equivalence Partitioning** Metode yang melampaui pengujian input acak. Teknik ini menggunakan logika pembagian data yang cerdas untuk mengidentifikasi kelompok input yang berperilaku serupa, sehingga mengurangi jumlah test case tanpa mengurangi efektivitas pengujian.
5. **Fuzzing** Teknik pengujian yang revolusioner dalam mengungkap kerentanan keamanan. Dengan memasukkan data tidak terstruktur atau tidak sempurna, fuzzing memaksa sistem untuk bereaksi di luar skenario normal, mengekspos celah keamanan potensial.
6. **Orthogonal Array Testing** Metode sophisticated untuk pengujian dengan input terbatas. Teknik ini menggunakan prinsip matematika untuk merancang test case yang paling efisien, memaksimalkan cakupan pengujian dengan jumlah skenario minimal.
7. **State Transition** Pengujian yang mendalam terhadap dinamika sistem, khususnya pada antarmuka pengguna. Metode ini tidak sekadar menelusuri perpindahan status, melainkan menganalisis seluruh siklus perubahan dan potensi perilaku anomali dalam sistem.

Kesimpulan:

Black box testing bukanlah sekadar metodologi pengujian, melainkan filosofi komprehensif dalam memahami perilaku perangkat lunak. Setiap teknik menawarkan perspektif unik dalam mengungkap kompleksitas dan potensi kelemahan sistem, yang tidak dapat dicapai melalui pendekatan pengujian tunggal.

Pendekatan ini menuntut keahlian tinggi dari penguji untuk merancang skenario pengujian yang cerdas, mampu mengeksplorasi berbagai kemungkinan interaksi dan potensi kegagalan dalam sistem perangkat lunak.

Data Pengujian

Link spreadsheets

<https://docs.google.com/spreadsheets/d/1YXUDYqUOORnjwtMo4Nn-HoE2gkh7X4JEQk2UeUErGFBY/edit?usp=sharing>

	A	B	C	D	E	F
	Form_Responses1					
1	Timestamp	Nama	Umur	Jenis Kelamin	Jenis Pekerjaan	Apakah pengguna dapat melakukan login / re
2	11/12/2024 12:39:52	Rosa Nur Aliana Sawafi		18 Perempuan	Pelajar/Mahasiswa	Berhasil
3	11/12/2024 13:32:36	indy aurellia		19 Perempuan	Pelajar/Mahasiswa	Berhasil
4	11/12/2024 14:03:51	Rahma Setiani		21 Perempuan	Pelajar/Mahasiswa	Berhasil
5	11/12/2024 15:47:26	Rahayu Saskia Putri	27 th	Perempuan	Bekerja	Gagal
6	11/12/2024 15:50:45	FATIH LUTHFIAN ADANI		18 Laki-laki	Pelajar/Mahasiswa	Berhasil
7	11/12/2024 16:14:24	Dyah Rahayu Anggraeni		25 Perempuan	Ibu Rumah Tangga	Gagal
8	11/12/2024 16:23:58	Klara Maharani	15 tahun	Perempuan	Pelajar/Mahasiswa	Gagal
9	11/12/2024 17:41:43	Bunga hati tifani		19 Perempuan	Pelajar/Mahasiswa	Berhasil
10	11/12/2024 19:27:27	Fatimah Alex		15 Perempuan	Pelajar/Mahasiswa	Berhasil
11	11/12/2024 19:42:05	Anggun Dewanti		19 Perempuan	Pelajar/Mahasiswa	Berhasil
12	11/12/2024 19:54:59	Widya Abhipraya Paramastri		14 Perempuan	Pelajar/Mahasiswa	Berhasil

	G	H	I
1	Apakah pengguna dapat mencari website ngafe yuk melalui chrome/edge?	Apakah Pengguna dapat semua mencoba menu navigasi dengan baik?	Apakah pengguna dapat mencoba dari halaman Rekomendasi untuk melihat Rekomendasi Cafe beserta detailnya?
2	Berhasil	Berhasil	Berhasil
3	Berhasil	Berhasil	Berhasil
4	Berhasil	Berhasil	Berhasil
5	Berhasil	Berhasil	Berhasil
6	Berhasil	Berhasil	Berhasil
7	Berhasil	Berhasil	Berhasil
8	Berhasil	Berhasil	Berhasil
9	Berhasil	Berhasil	Berhasil
10	Berhasil	Berhasil	Berhasil
11	Berhasil	Berhasil	Berhasil
12	Berhasil	Berhasil	Berhasil

1	Apakah pengguna dapat mencoba fitur favorit dengan menambahkan dari menu rekomendasi cafe?	Apakah pengguna dapat menghapus cafe favorit yang sudah ditambahkan?	Apakah pengguna dapat menggunakan fitur searc cafe?	Apakah desain visual website ini menarik?
2	Berhasil	Berhasil	Gagal	Ya
3	Berhasil	Berhasil	Gagal	Ya
4	Berhasil	Berhasil	Berhasil	Ya
5	Gagal	Gagal	Gagal	Ya
6	Gagal	Gagal	Gagal	Ya
7	Gagal	Gagal	Gagal	Ya
8	Gagal	Gagal	Gagal	Ya
9	Berhasil	Berhasil	Berhasil	Ya
10	Berhasil	Berhasil	Gagal	Ya
11	Berhasil	Berhasil	Berhasil	Ya
12	Berhasil	Berhasil	Gagal	Ya

1	Apakah skema warna dan tata letak website nyaman di mata? ▾	Apakah Anda dapat menemukan informasi yang Anda butuhkan dengan mudah? ▾	Apakah ukuran teks dan gambar pada website mudah dibaca dan dilihat? ▾	Apakah kecepatan loading halaman website memadai? ▾
2	Ya	Ya	Ya	Ya
3	Ya	Ya	Ya	Ya
4	Ya	Ya	Ya	Ya
5	Ya	Ya	Ya	Ya
6	Ya	Tidak	Ya	Ya
7	Ya	Ya	Ya	Ya
8	Ya	Ya	Ya	Ya
9	Ya	Ya	Ya	Ya
10	Ya	Ya	Ya	Ya
11	Ya	Ya	Ya	Ya
12	Ya	Ya	Ya	Ya

1	Apakah Anda mengalami masalah teknis saat menggunakan website ini? ▾	Apakah Anda puas dengan website "ngafe yuk" secara keseluruhan? ▾	Apakah Anda akan merekomendasikan website ini kepada orang lain? ▾	Saran Kritik ▾
2	Tidak	Ya	Ya	-
3	Tidak	Ya	Ya	-
4	Tidak	Ya	Ya	Sudah baik
5	Ya	Tidak	Ya	Search dan favorit semoga bisa digunakan agar bisa berfungsi dengan baik
6	Ya	Ya	Ya	# kritik Masih banyak yang harus diperbaiki, salah satunya - Belum bisa registrasi - fitur favorit masih belum berfungsi - editan masih belum bagus
7	Ya	Ya	Ya	Beberapa fitur belum bisa digunakan sesuai dengan fungsinya
8	Tidak	Ya	Ya	User belum bisa login dan belum bisa menambahkan cafe ke dalam fitur favo
9	Tidak	Ya	Ya	rekomendasi cafe nya diperbanyak, dan ditambah profil user
10	Ya	Ya	Ya	tingkatkan fiturnya
11	Tidak	Ya	Ya	Keren, lanjutkan 🍷
12	Ya	Ya	Ya	Website sudah bagus dan menarik, fitur search bisa diperbaiki lagi dan kedep

Presentase Keberhasilannya 85 %

Dokumentasi



