

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Aplikasi Pemandu Wisata



OUR TEAM



Fitrah Habibullah
(team Lead)



Hamdani Arif, S.Pd.,
M.Sc.
(Manager Project)



Ageng Kurnia Muhammad



Dzakiy Naofal Akbar



Muhamad Iqbal
Ramadhon Alhabsyi



M.Kelvin Prayoga

PROJECT DESCRIPTION



This project is designed to train students in system security techniques through a series of tasks such as network scanning, application vulnerability testing, and general security evaluation. Students will conduct penetration tests on a client website called **SENSOR** using the latest tools and methodologies, identify and assess any vulnerabilities found, and develop appropriate mitigation strategies. They will also prepare a testing report detailing the actions taken, recommended solutions, and outcomes achieved. Through this project, students are expected to enhance their understanding of the importance of information security and gain practical skills in application security testing in real-world environments.

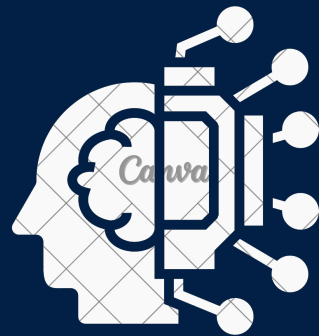


PROJECT METHOD

GRAY BOX

a method of security penetration testing (pentesting) in which the tester has some information about the target system, such as the credentials of a typical user, a network diagram, or API documentation.

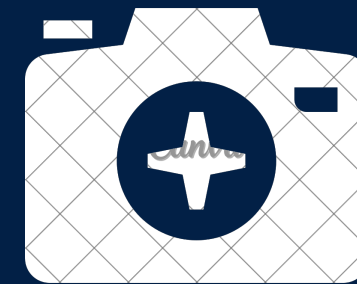
OBJECTIVE



Detect vulnerabilities
and provide security
recommendations



Prevent possible
attacks



Protect sensitive data
and the organization's
reputation.

PENTEST STAGES

pentesting involves four stages: Planning and Preparation to define the scope and objectives, Reconnaissance to gather information about the target, Exploitation to actively exploit identified vulnerabilities, and Reporting to document findings and recommend solutions.



01

**Planning
and
Preparation**

02

Reconnaissance


03

Exploitation

04

Reporting

PROJECT RESULTS

€  .com

Security Pentest Document Reports (SPDR) – Uji Keamanan Sistem Aplikasi Pemandu Wisata

Reports Findings SENSOR.com

1. [DoS] Denial-of-Service

Affected Host	SENSOR
CVSS Score	7.5 AV:N/AC:L/PR:N/UI:N/S:U/A:H
Severity	High
Environment	Production
Type	Domain

Summary

During the penetration testing process on the GuideMe website, it was found that the web service became unresponsive (down) when a parallel directory scan was performed using 3 dirb tabs. This indicates that the server has no overload protection and is highly vulnerable to Denial of Service (DoS) attacks, even with minimal resources.

Step to Reproduce

1. Open kali linux and download tool dirb, use dirb for searching hidden directory

```
(jukii@DESKTOP-PB526P6)~$ dirb https://SENSOR
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Apr 8 20:01:53 2025
URL_BASE: https://SENSOR/
WORDLIST_FILES: sts/common.txt
-----

GENERATED WORDS: 4612
```

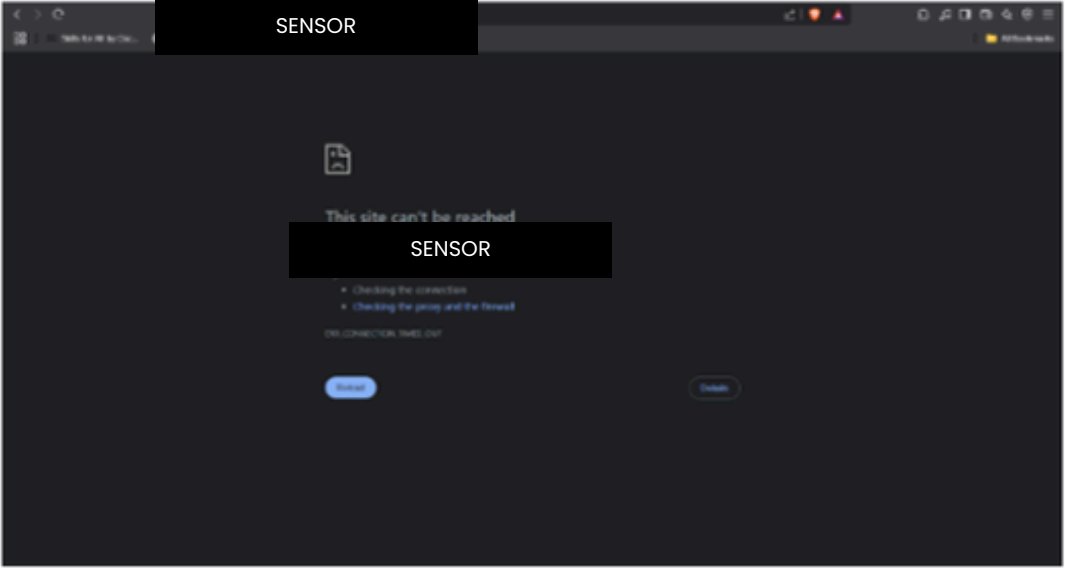
2. when we test using 3 dirb simultaneously the website become down

```
----- Entering directory: https://SENSOR.com/cgi-sys/ -----
+ https://SENSOR.com/c (CODE:403|SIZE:318)
+ https://SENSOR.com/cgi-sys/.ntpasswd (CODE:403|SIZE:318)
+ https://SENSOR.com/cgi-sys/error_log (CODE:403|SIZE:318)
+ https://SENSOR.com/cgi-sys/index.html (CODE:500|SIZE:675)
+ https://SENSOR.com/cgi-sys/php.ini (CODE:403|SIZE:318)

(!) FATAL: Too many errors connecting to host
(Possible cause: OPERATION TIMEOUT)

-----
END_TIME: Tue Mar 25 02:00:58 2025
DOWNLOADED: 13683 - FOUND: 22
```

Response



Impact

A DoS attack makes a site inaccessible to legitimate users for a period of time, which can be detrimental to reputation and user experience. Given that the site is public and used by potential travelers, downtime can potentially reduce trust in the services provided.

Mitigation

1. Use rate limiting for any IP that makes repeated HTTP requests in a short period of time.
2. Implement a Web Application Firewall (WAF) such as Cloudflare or ModSecurity to detect and block brute force request patterns.
3. Use a load balancer or reverse proxy that can filter malicious traffic before it reaches the main server.

References

CWE-400: Uncontrolled Resource Consumption

2. Directory Listing Enabled

Affected Host	https://[REDACTED]/des/
CVSS Score	5.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Severity	Medium
Environment	Production
Type	Endpoint

3. [ID] Information Disclosure

Affected Host	[REDACTED]
CVSS Score	None
Severity	Information
Environment	Production
Type	Port

PROJECT RESULTS

 SENSOR .com - admin

1) Improper Restriction of Excessive Authentication Attempts

Affected Host	https://[REDACTED]/admin/index.php
CVSS Score	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Severity	Medium
Environment	Production
Type	Domain

2. Cleartext Transmission of Sensitive Information

Affected Host	https://[REDACTED]/admin/index.php
CVSS Score	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Severity	High
Environment	Production
Type	Domain

3. Stored XSS (Cross-Site Scripting)

Affected Host	https://[REDACTED]/admin/index.php
CVSS Score	3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:L
Severity	Medium
Environment	Production
Type	Domain

4. file upload vulnerability

Affected Host	https://[REDACTED]/admin/index.php
CVSS Score	6.1 (AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:H)
Severity	Medium
Environment	Production
Type	Domain

LOGBOOK

ID	Tahapan	Detail Pengerjaan	Ouput	Mulai	Selesai	Progress
1	Kick Off PBM(L) dan Pertemuan dengan Manpro	Penentuan anggota, Pembahasan tentang Judul PBL seperti mencari client, lalu batas penyelesain PBL , dan untuk minggu pertama Pembuatan RPP dahulu.	RPP	2025-02-24	2025-03-02	0%
2	Pertemuan dengan Client dan Pembuatan NDA	Membahas link Web yang akan di Pentest, dll. Lalu tim kami lanjut membuat NDA antara Client, Manpro, KPS, dan Tim PBL.	NDA	2025-03-10	2025-03-14	15%
3	Scanning/Information Gathering and Pentest	Pada saat ini kami sedang fokus melakukan Scanning atau Information Gathering terhadap Website yang akan kami lakukan Pengujian, Selanjutnya kami melakukan Pentest pada Website tersebut dan menemukan beberapa Vuln.	Vulnerability	2025-03-17	2025-04-04	30%
4	Pembuatan Report Pentest	Membuat Report yang berisi Temuan Vulnerability seperti [DOS] Denial-of-Service, Directory Listing Enabled, dan Information Disclosure. Lalu juga berapa severity, step to reproduce, impact dan mitigasi dari Vulnerability yang didapat.	Report Pentest	2025-04-07	2025-04-11	35%
5	Pertemuan dengan Client	Membahas Keberlanjutan Pentest Web pada bagian admin dan Mendapat Akses ke Admin, Seperti URL, Username dan Password.	Akses Web Admin	2025-04-14	2025-04-18	40%
6	Penetration Testing	Disini kami Mendapatkan Vulnerability Improper Restriction of Excessive Authentication Attempts, Cleartext Transmission of Sensitive Information, Stored XSS (Cross-Site-Scripting), dan Unrestricted Upload of File with Dangerous Type pada Bagian Web Admin	Vulnerability	2025-04-21	2025-04-25	45%
7	Pembuatan Report Pentest, Poster dan PPT	Disini kami Telah membuat Poster, PPT dan Report Pentest yang berisi Vulnerability dari Web Admin yaitu Improper Restriction of Excessive Authentication Attempts, Cleartext Transmission of Sensitive Information, Stored XSS (Cross-Site-Scripting), dan Unrestricted Upload of File with Dangerous Type.	Report Pentest, Poster dan PPT	2025-04-28	2025-05-02	50%

**THANK YOU FOR
YOUR ATTENTION**