EXTION INFOTEC PROJECT 2

WEBSITE VULNERABILITY ASSESSMENTS

MYCHARLA MADHAVKUMAR

27/08/2024

Table of Contents

Project Overview:

The project aims to conduct a comprehensive assessment of the infrastructure of [**RIVAN SMART**] to identify and mitigate potential vulnerabilities. Theassessment will external Website components to ensure a thorough evaluation.

Project Objectives:

1. **Identify Vulnerabilities:** Conduct a thorough scan and analysis of the network to identify potential vulnerabilities.
2. **Assess Risk Levels:** Evaluate the severity and potential impact of identified vulnerabilities on the network.
3. **Recommend Mitigation Strategies:** Propose effective strategies and countermeasures to mitigate identified vulnerabilities.
4. **Enhance Security Posture:** Improve overall network security by implementing recommended changes and best practices.

Project Scope:

1. **Network Components:** Assess all critical network components including routers, switches, firewalls, servers, and endpoints.
2. **Network Protocols:** Evaluate vulnerabilities related to TCP/IP protocols, DNS, DHCP, etc.
3. **External Assessment:** Perform external scans to identify vulnerabilities accessible from outside the organization’s network.
4. **Web Applications:** Scan web applications hosted on the network for security vulnerabilities.

Project Methodology:

1. **Preparation:**
   - Define scope and objectives.
   - Obtain necessary permissions and approvals.
   - Set up scanning tools and resources.
2. **Vulnerability Scanning:**
   - Conduct external and internal network scans using appropriate vulnerability scanning tools (e.g., Nessus, The harvest).
   - Analyze scan results to identify vulnerabilities.
3. **Risk Assessment:**
   - Prioritize identified vulnerabilities based on severity.
   - Assess potential impact on network security and operations.
4. **Mitigation Strategy:**
   - Develop a plan to address identified vulnerabilities.
   - Prioritize mitigation efforts based on risk assessment.
5. **Implementation:**
   - Implement recommended changes and security patches.
   - Verify effectiveness of mitigation measures.
6. **Documentation and Reporting:**
   - Compile assessment findings into a comprehensive report.
   - Create an executive summary and presentation for stakeholders.

Resources Required:

- **Vulnerability Scanning Tools:** Nessus, Penetration Tools
- **Information Gathering:** Google Dorks, Metadata, Reverse image.
- **Documentation Tools:** Microsoft Office Suite, reporting templates.
- **Communication Tools:** Email, Mobiles, WhatsApp.

Personally Used Tools in this Project:

1. Censys Web Scanner

- A search engine that scans and indexes internet-connected devices, helping cybersecurity professionals identify vulnerabilities and monitor networks.

2. The Harvester

- An OSINT tool used to gather emails, subdomains, and IPs from various public sources during the reconnaissance phase of penetration testing.

3. Pen Tools

- A collective term for tools used in penetration testing to assess the security of systems by simulating attacks and finding vulnerabilities.

4. Napalm FTP Server

- A lightweight FTP server often used in penetration testing labs for serving files or interacting with FTP clients in a controlled environment.

5. Meta Data

- Data that provides information about other data, often extracted from files to gather additional intelligence during penetration testing or forensic analysis.

6. Tor Browser

- A browser that enables anonymous internet browsing by routing traffic through the Tor network, helping users protect their privacy and evade tracking.

7. Parrot & Kali Linux Operating Systems

- Security-focused Linux distributions preloaded with tools for penetration testing, digital forensics, and security research.

8. Windows 2019 Server

- A server operating system by Microsoft used for managing enterprise applications, services, and networks, often tested in security assessments.

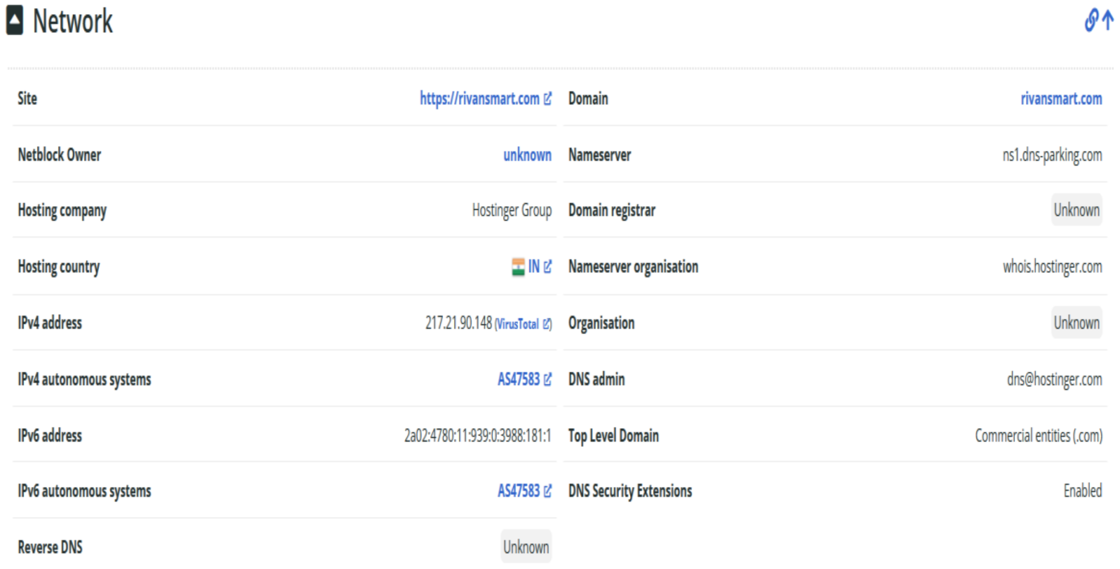
9. WordPress Scanner

- A tool that scans WordPress websites for vulnerabilities, outdated plugins, and security weaknesses to help protect against potential attacks.

Purpose of the Network Vulnerability Assessment:

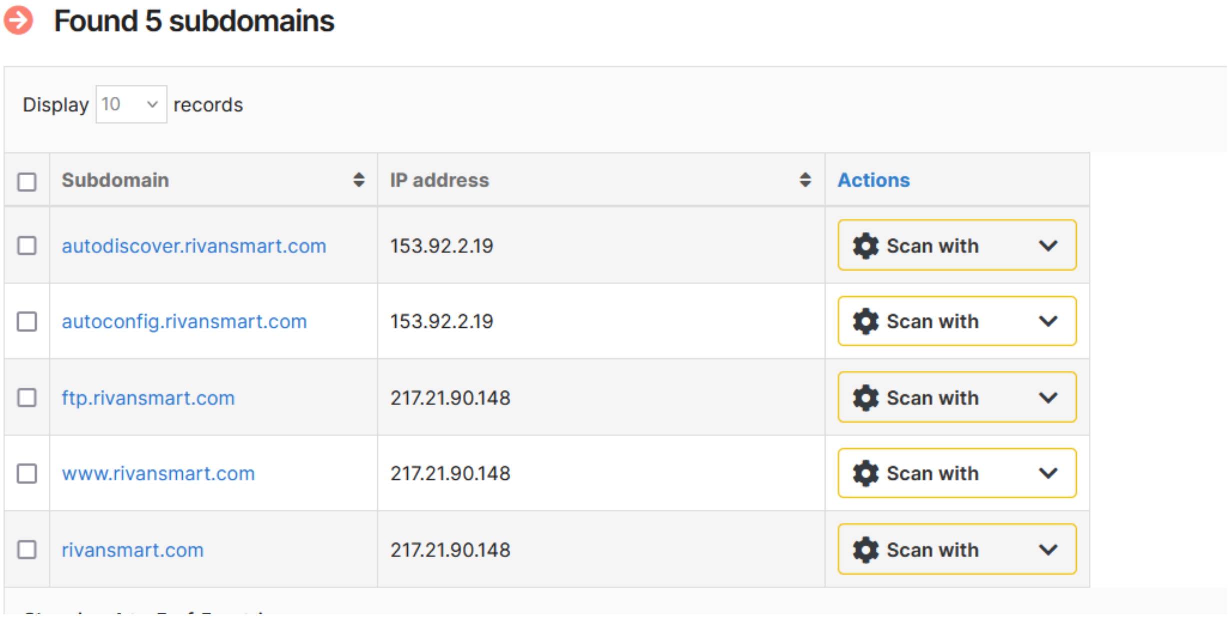
The main Aim of Website Vulnerability test has to identify the vulnerabilities in network and Websites Using the Above tools.

Target Network:	Rivan Smart Pvt Limited
Website URL:	https://rivansmart.com/



Network

Site	https://rivansmart.com	Domain	rivansmart.com
Netblock Owner	unknown	Nameserver	ns1.dns-parking.com
Hosting company	Hostinger Group	Domain registrar	Unknown
Hosting country	IN	Nameserver organisation	whois.hostinger.com
IPv4 address	217.21.90.148 (VirusTotal)	Organisation	Unknown
IPv4 autonomous systems	AS47583	DNS admin	dns@hostinger.com
IPv6 address	2a02:4780:11:939:0:3988:181:1	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS47583	DNS Security Extensions	Enabled
Reverse DNS	Unknown		



Found 5 subdomains

Display 10 records

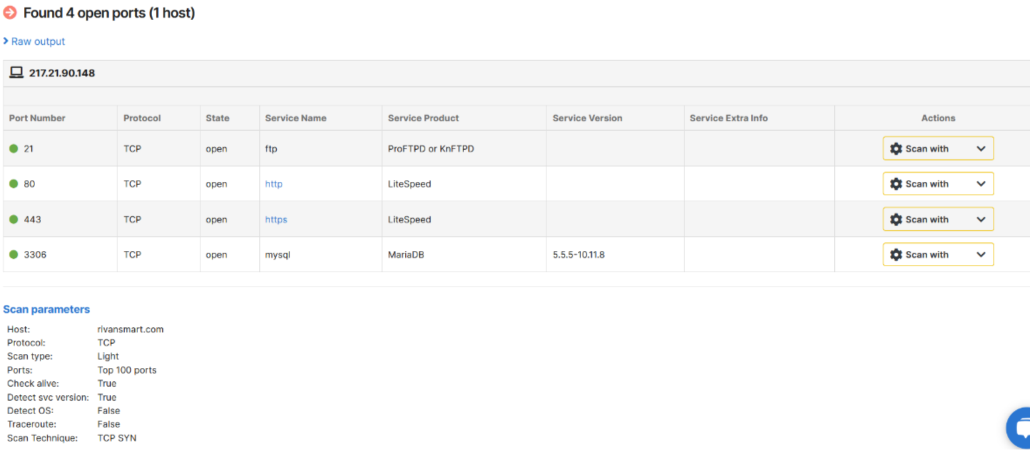
□	Subdomain	IP address	Actions
□	autodiscover.rivansmart.com	153.92.2.19	Scan with
□	autoconfig.rivansmart.com	153.92.2.19	Scan with
□	ftp.rivansmart.com	217.21.90.148	Scan with
□	www.rivansmart.com	217.21.90.148	Scan with
□	rivansmart.com	217.21.90.148	Scan with

USAGE OF THE TOOLS IN THIS PROJECT

1. (Port Scanner):-

I Performed port scanning on this website, there some open ports

21/Tcp	ftp
80/Tcp	http
443/tcp	https
3306/tcp	MySQL



Found 4 open ports (1 host)

Raw output

217.21.90.148

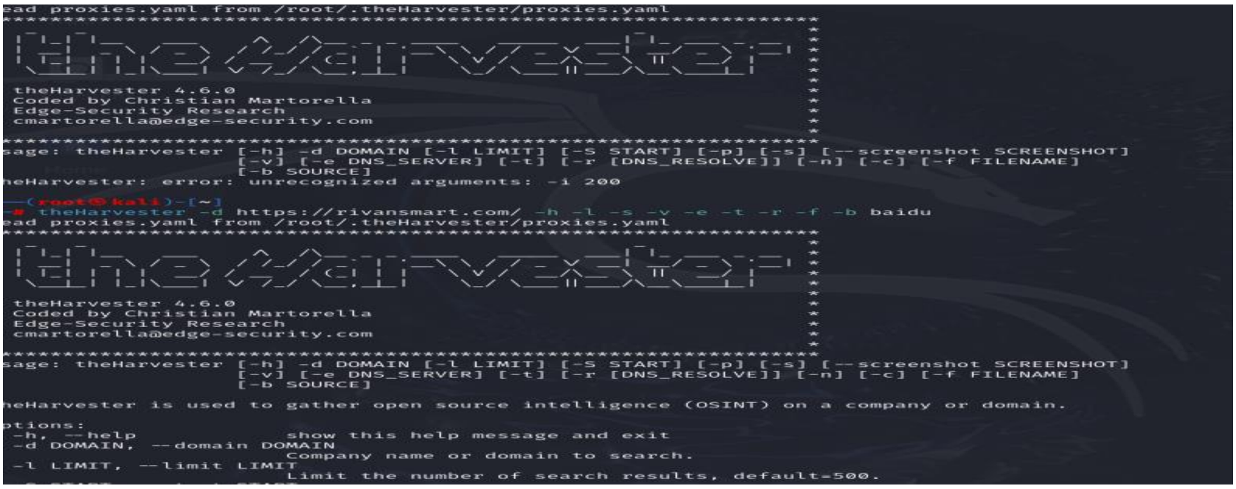
Port Number	Protocol	State	Service Name	Service Product	Service Version	Service Extra Info	Actions
21	TCP	open	ftp	ProFTPD or KnFTPD			Scan with
80	TCP	open	http	LiteSpeed			Scan with
443	TCP	open	https	LiteSpeed			Scan with
3306	TCP	open	mysql	MariaDB	5.5.5-10.11.8		Scan with

Scan parameters

Host:	rivansmart.com
Protocol:	TCP
Scan type:	Light
Ports:	Top 100 ports
Check alive:	True
Detect svc version:	True
Detect OS:	False
Traceroute:	False
Scan Technique:	TCP SYN

2. The Harvester (Email info about Websites):-

Using this tool to know what are technologies are used to build this website and any vulnerabilities/bugs available in this technologies (Outdated software's) are used.



```
ead proxies.yaml from /root/.theHarvester/proxies.yaml
*******************************************************************
 theHarvester 4.6.0                                               *
 Coded by Christian Martorella                                    *
 Edge-Security Research                                           *
 cmartorella@edge-security.com                                    *
*******************************************************************
sage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT]
                   [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME]
                   [-b SOURCE]
heHarvester: error: unrecognized arguments: -i 200

—(root㉿kali)-[~]
-# theHarvester -d https://rivansmart.com/ -h -l -s -v -e -t -r -f -b baidu
ead proxies.yaml from /root/.theHarvester/proxies.yaml
*******************************************************************
 theHarvester 4.6.0                                               *
 Coded by Christian Martorella                                    *
 Edge-Security Research                                           *
 cmartorella@edge-security.com                                    *
*******************************************************************
sage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT]
                   [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME]
                   [-b SOURCE]

heHarvester is used to gather open source intelligence (OSINT) on a company or domain.

ptions:
 -h, --help            show this help message and exit
 -d DOMAIN, --domain DOMAIN
                       Company name or domain to search.
 -l LIMIT, --limit LIMIT
                       Limit the number of search results, default=500.
```

3. Google Dorks (Some Info Leaked in Web):-

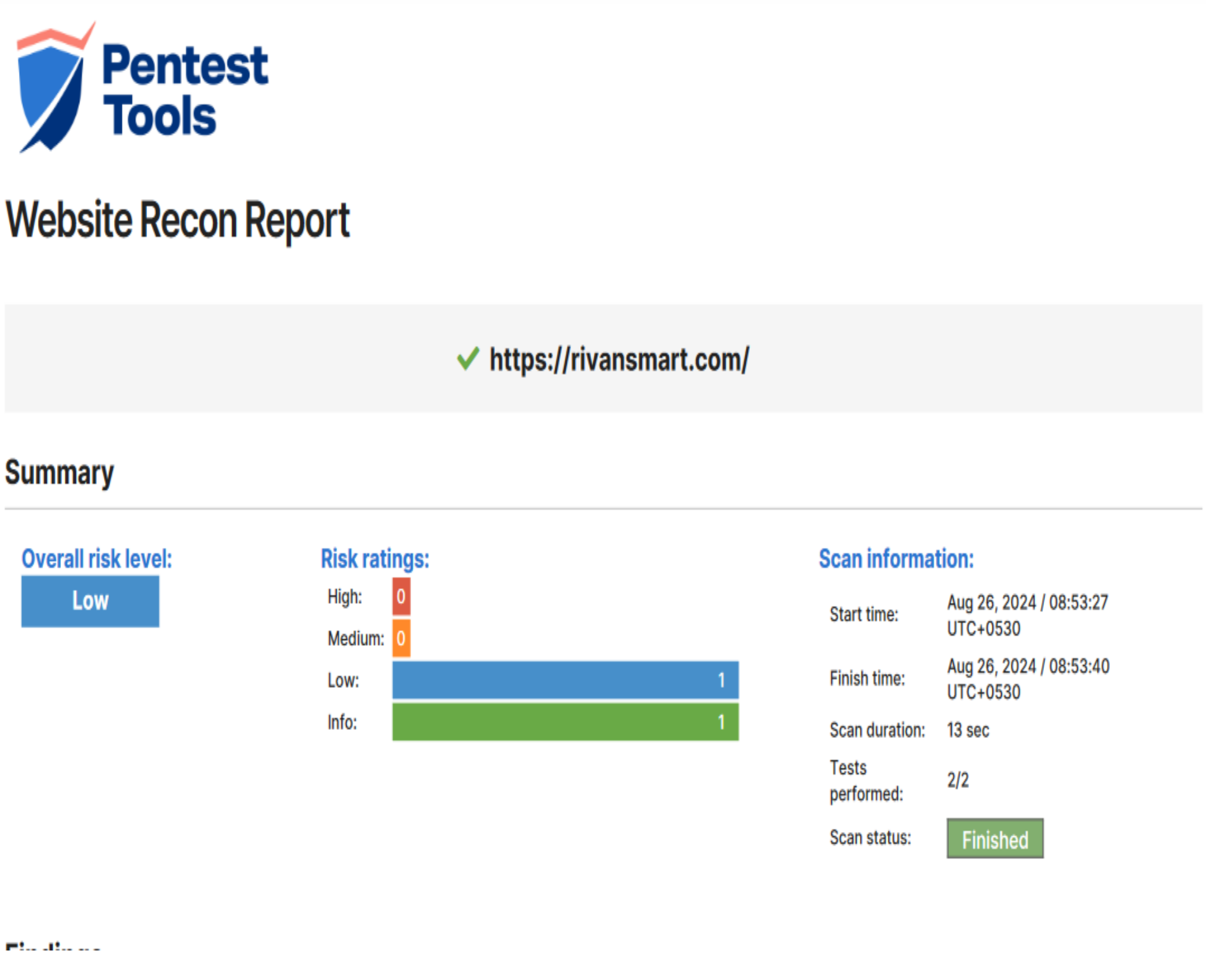
Google Dorks is mainly used for deep report about Website, which is Dns address, Document snapshots, domains, any data is leaked in web like PDFs, Sub Domains, Email ids, Phone Numbers …etc.

Leaked Pdfs:

Q-File CNC Turning Programmer.pdf_.pdf

QF-Reverse Engineering and Additive Manufacturing QA Supervisor.pdf_.pdf

4. Scanning Reports:



Pentest Tools

Website Recon Report

✓ https://rivansmart.com/

Summary

Overall risk level:

Low

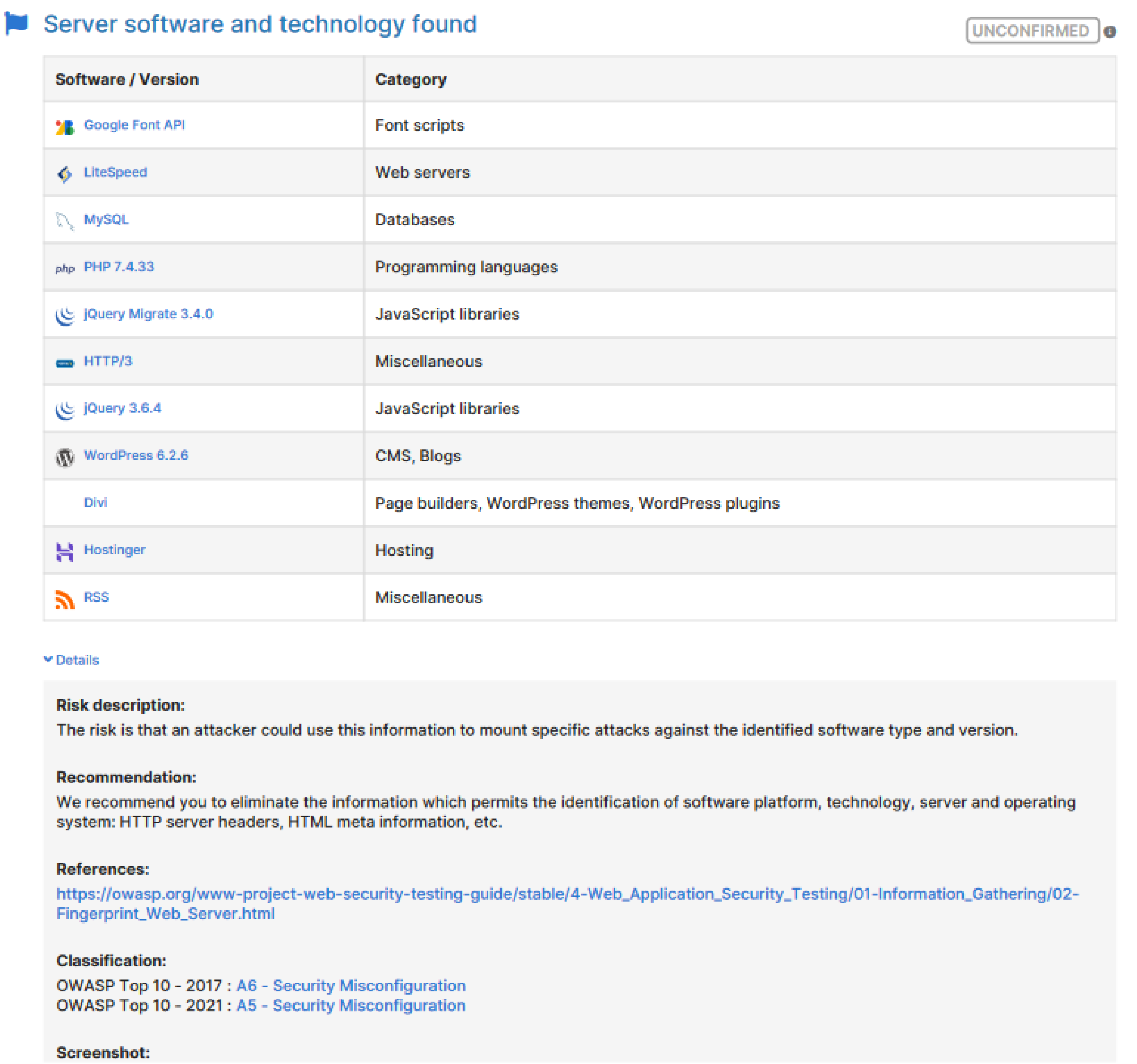
Risk ratings:

High:	0
Medium:	0
Low:	1
Info:	1

Scan information:

Start time:	Aug 26, 2024 / 08:53:27 UTC+0530
Finish time:	Aug 26, 2024 / 08:53:40 UTC+0530
Scan duration:	13 sec
Tests performed:	2/2
Scan status:	Finished

Findings



Server software and technology found

UNCONFIRMED

Software / Version	Category
Google Font API	Font scripts
LiteSpeed	Web servers
MySQL	Databases
PHP 7.4.33	Programming languages
jQuery Migrate 3.4.0	JavaScript libraries
HTTP/3	Miscellaneous
jQuery 3.6.4	JavaScript libraries
WordPress 6.2.6	CMS, Blogs
Divi	Page builders, WordPress themes, WordPress plugins
Hostinger	Hosting
RSS	Miscellaneous

Details

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Screenshot:

-

Web scanning Reports:

- https://drive.google.com/file/d/1a0XLz1sqfPabvT5TXXU1oEK0kqKm6paj/view?usp=sharing
- https://drive.google.com/file/d/1AfflFMUpEhfsEL9cuthvrzwYnuvilHfJ/view?usp=sharing
- https://drive.google.com/file/d/1qTHbnQWBxrjJ-mdezoR2rk2e7IJ55GPw/view?usp=sharing
- https://drive.google.com/file/d/1kKRH22gOR1oTmN2rs4jvXOq9WZrQFSRr/view?usp=sharing
- https://drive.google.com/file/d/1QzMecChP3MmijHc4wVUgsTz87jR1D-LB/view?usp=sharing

Conclusion:

In conclusion, penetration testing plays a crucial role in Strengthening an organization's security posture. By simulating real-world attacks, pentesting helps identify vulnerabilities before malicious actors can exploit them, allowing for timely remediation. This proactive approachnot only enhances the security of systems and data but also builds resilienceagainst potential breaches.

Effective penetration testing involves a thorough assessment of an organization’s IT infrastructure, applications, and network configurations. The insights gained from these tests provide valuable feedback for improving security policies, practices, and technologies. Regular pentesting, combined with continuous monitoring and updates, ensures that security measures evolve alongside emerging threats.

Ultimately, the benefits of penetration testing extend beyond merely addressing weaknesses; they foster a culture of security awareness and preparedness within the organization. By prioritizing and investing in pentesting, organizations can better safeguard their assets, protect sensitive information, and maintain trust with clients and stakeholders.

_______________END__________________