WEBSITE VULNERABILITY TEST

EXOTION INFOTECH PROJECT-2

Gudipati Rohith Kumar Reddy
Project-2

Table of Contents

Project Overview:

The project aims to conduct a comprehensive assessment of the infrastructure of [testphp.vulnweb] to identify and mitigate potential vulnerabilities. The assessment 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:
   o Define scope and objectives.
   o Obtain necessary permissions and approvals.
   o Set up scanning tools and resources.

2. Vulnerability Scanning:

o Conduct external and internal network scans using appropriate vulnerability scanning tools (e.g., Nessus, OpenVAS, and Nmap).

o Analyse scan results to identify vulnerabilities.

3. Risk Assessment:

o Prioritize identified vulnerabilities based on severity (e.g., CVSS scores).

o Assess potential impact on network security and operations.

4. Mitigation Strategy:

o Develop a plan to address identified vulnerabilities.

o Prioritize mitigation efforts based on risk assessment.

5. Implementation:

o Implement recommended changes and security patches.

o Verify effectiveness of mitigation measures.

6. Documentation and Reporting:

o Compile assessment findings into a comprehensive report.

o Create an executive summary and presentation for stakeholders.

Resources Required:

- Vulnerability Scanning Tools: Nessus, Pen-Test tools
- Documentation Tools: Microsoft Office Suite, reporting templates.
- Communication Tools: Email, Mobiles, WhatsApp.

Tools used in the prroject:

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: testphp.vulnweb

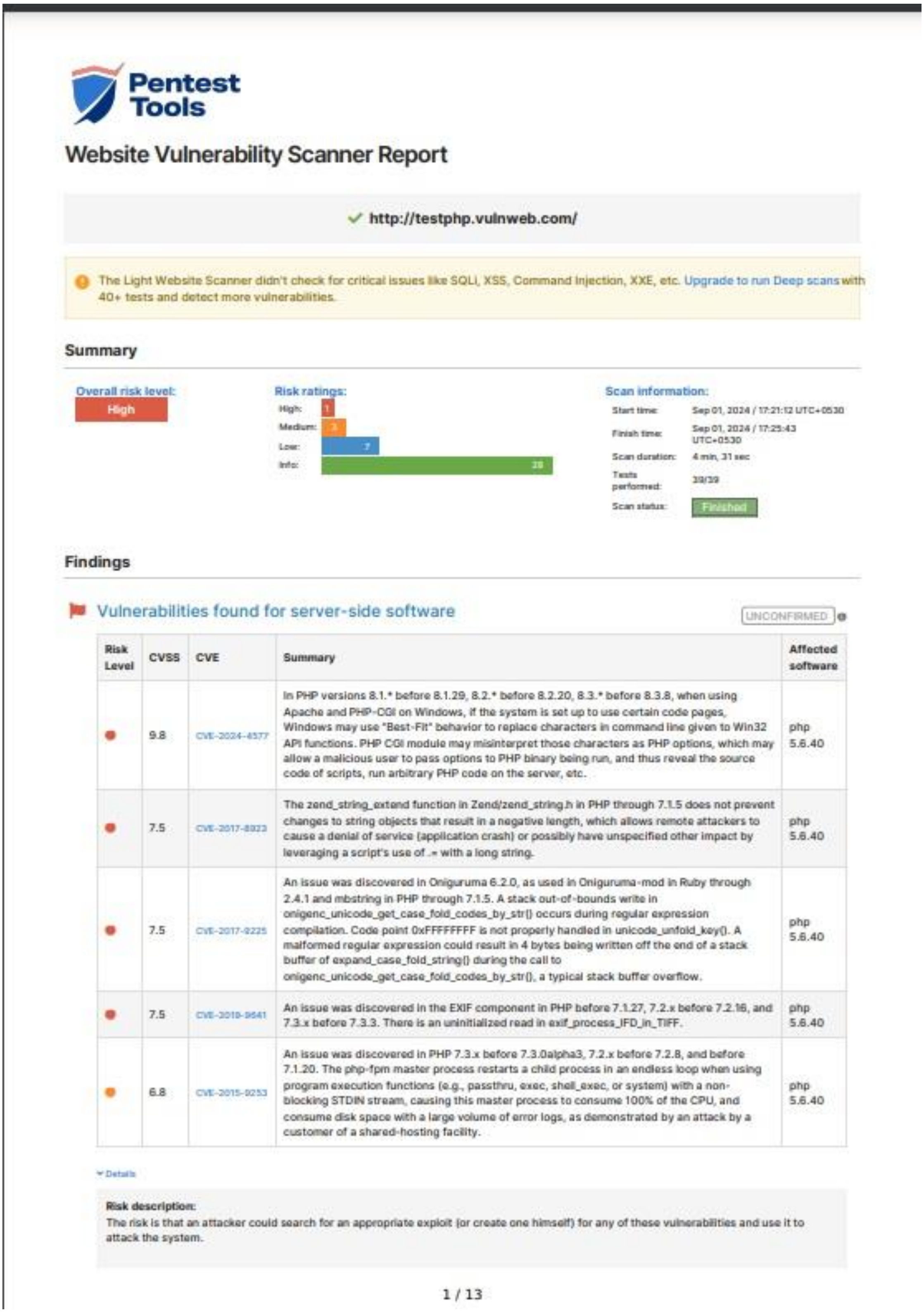
Website URL: http://testphp.vulnweb.com/

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

2. The Harvester (Email info about Websites): -
   Using this tool to know what technologies are used to build this website and any vulnerabilities/bugs available in these technologies (Outdated software's) are used.
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.
4. Scanning Reports



Pentest Tools

Website Vulnerability Scanner Report

✓ http://testphp.vulnweb.com/

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:
High

Risk ratings:

High:	1
Medium:	3
Low:	7
Info:	28

Scan information:

Start time:	Sep 01, 2024 / 17:21:12 UTC+0530
Finish time:	Sep 01, 2024 / 17:25:43 UTC+0530
Scan duration:	4 min, 31 sec
Tests performed:	39/39
Scan status:	Finished

Findings

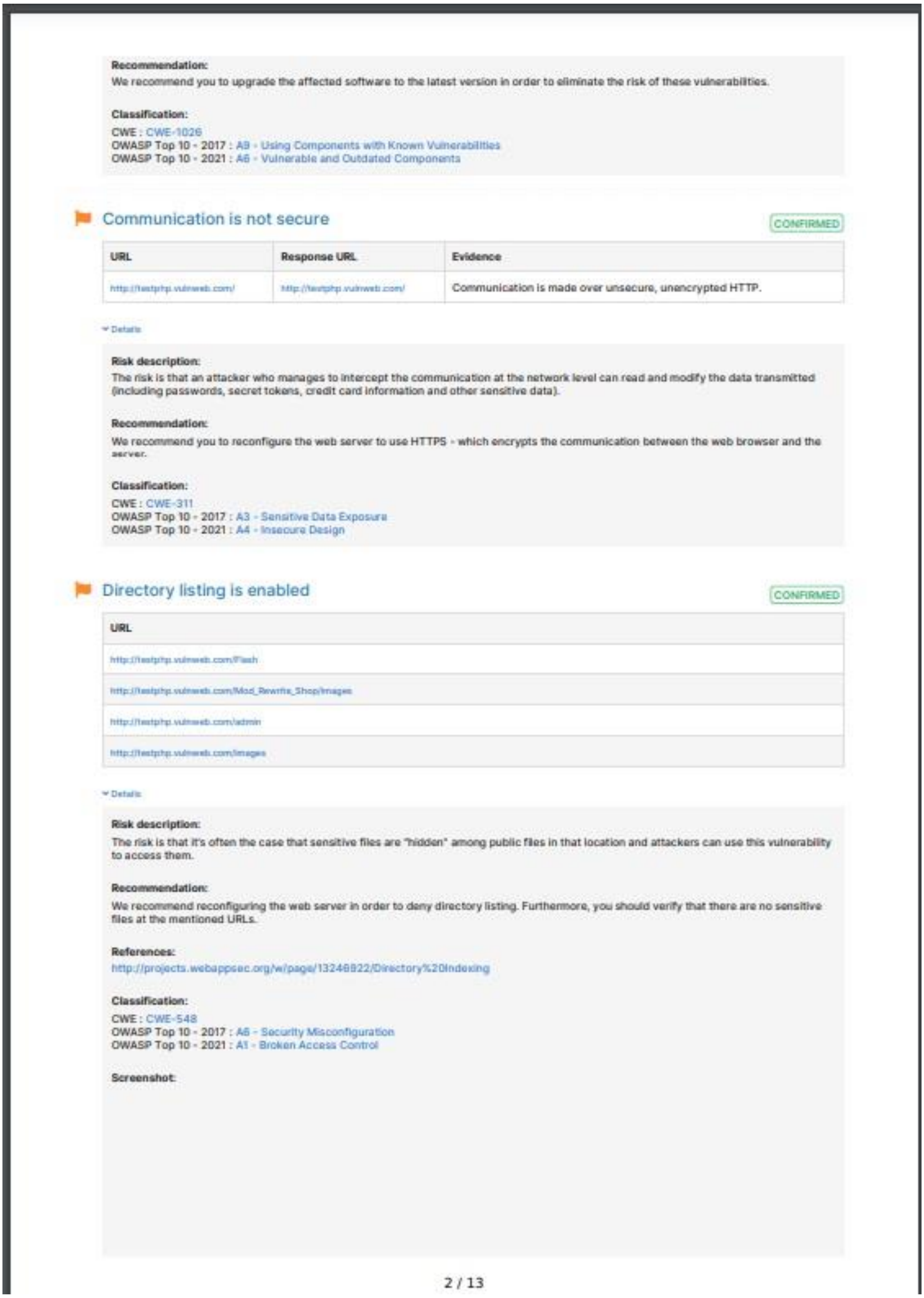
Vulnerabilities found for server-side software

UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Affected software
●	9.8	CVE-2024-4577	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.	php 5.6.40
●	7.5	CVE-2017-8923	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	php 5.6.40
●	7.5	CVE-2017-9225	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds write in onigenc_unicode_get_case_fold_codes_by_str() occurs during regular expression compilation. Code point 0xFFFFFFFF is not properly handled in unicode_unfold_key(). A malformed regular expression could result in 4 bytes being written off the end of a stack buffer of expand_case_fold_string() during the call to onigenc_unicode_get_case_fold_codes_by_str(), a typical stack buffer overflow.	php 5.6.40
●	7.5	CVE-2019-9641	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.	php 5.6.40
●	6.8	CVE-2015-9253	An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.	php 5.6.40

▾ Details

Risk description:
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.



Recommendation:

We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Classification:

CWE : CWE-1026
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

Communication is not secure

CONFIRMED

URL	Response URL	Evidence
http://testphp.vulnweb.com/	http://testphp.vulnweb.com/	Communication is made over unsecure, unencrypted HTTP.

▾ Details

Risk description:

The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:

CWE : CWE-311
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure
OWASP Top 10 - 2021 : A4 - Insecure Design

Directory listing is enabled

CONFIRMED

URL
http://testphp.vulnweb.com/Flash
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
http://testphp.vulnweb.com/admin
http://testphp.vulnweb.com/images

▾ Details

Risk description:

The risk is that it's often the case that sensitive files are "hidden" among public files in that location and attackers can use this vulnerability to access them.

Recommendation:

We recommend reconfiguring the web server in order to deny directory listing. Furthermore, you should verify that there are no sensitive files at the mentioned URLs.

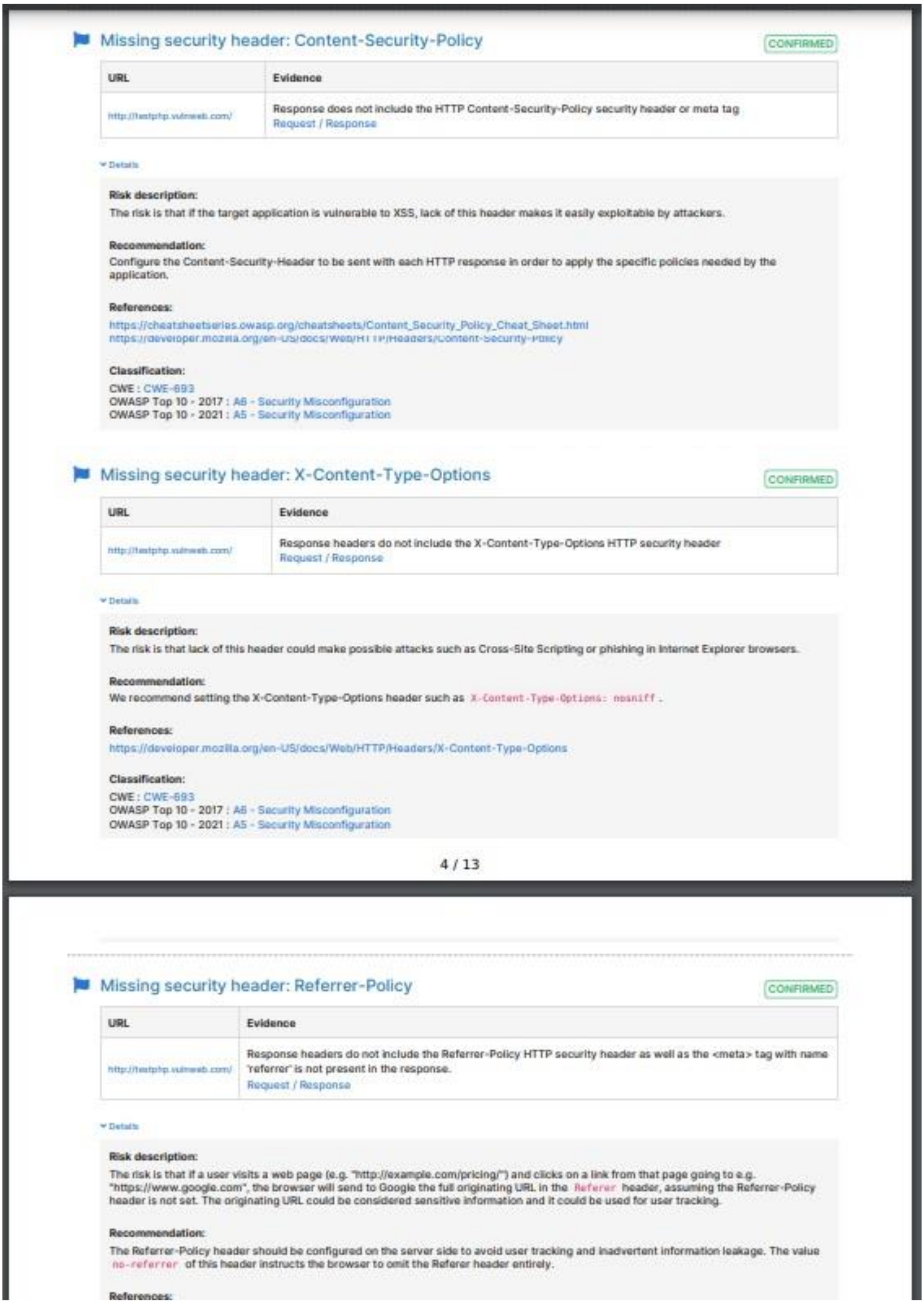
References:

http://projects.webappsec.org/w/page/13246922/Directory%20Indexing

Classification:

CWE : CWE-548
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A1 - Broken Access Control

Screenshot:



Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
http://testphp.vulnweb.com/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

▾ Details

Risk description:

The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:

Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:

CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
http://testphp.vulnweb.com/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

▾ Details

Risk description:

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:

We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

References:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:

CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
http://testphp.vulnweb.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

▾ Details

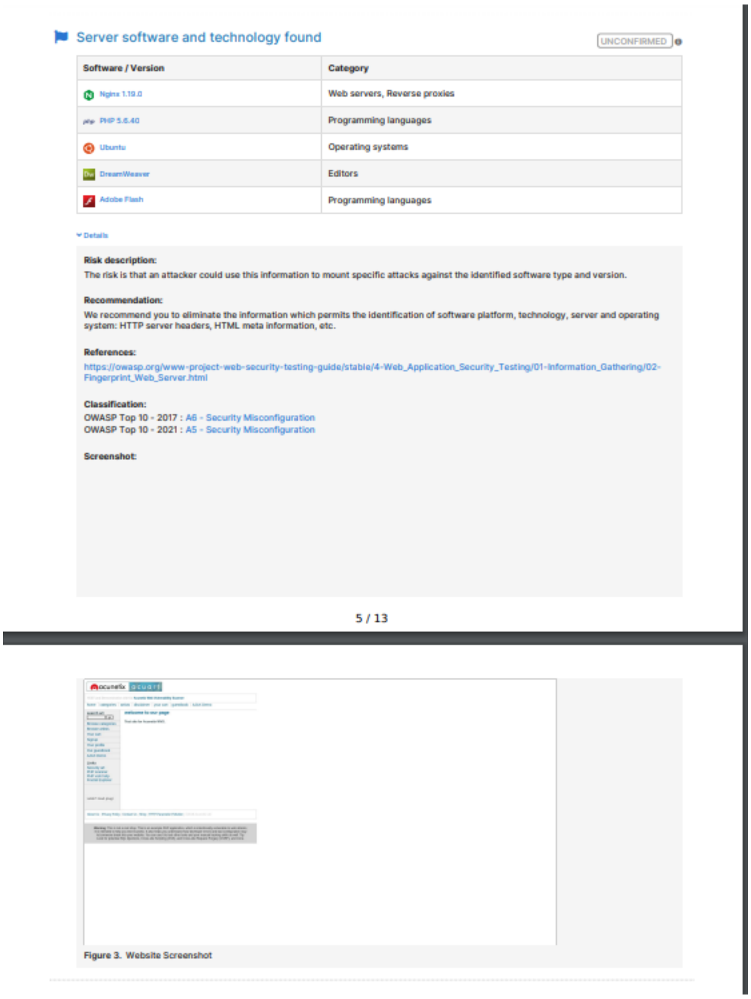
Risk description:

The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:



Server software and technology found

Software / Version	Category
Nginx 1.19.0	Web servers, Reverse proxies
PHP 5.6.40	Programming languages
Ubuntu	Operating systems
DreamWeaver	Editors
Adobe Flash	Programming languages

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:

Figure 3. Website Screenshot

Conclusion:

In conclusion, penetration testing plays a crucial role in Strengthening an organization's security posture. By simulating real world attacks, pen testing helps identify vulnerabilities before malicious actors can exploit them, allowing for timely remediation. This proactive approach not only enhances the security of systems and data but also builds resilience against 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 pen testing, 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 pen testing, organizations can better safeguard their assets, protect sensitive information, and maintain trust with clients and stakeholders.