Assignment-1(Footprinting & Reconnaissance)

# **Testphp\_vulns**

# Overview:

The provided information outlines various vulnerabilities and sensitive points within the http://testphp.vulnweb.com/ website. Here's an overview of the identified issues:

## Testphp\_vulns

Collect all vulns and informations in http://testphp.vulnweb.com/

Sensitive Files:

Several sensitive files and directories are accessible, potentially exposing critical information or configuration details to unauthorised users.

http://testphp.vulnweb.com/index.zip

http://testphp.vulnweb.com/.idea/workspace.xml

http://testphp.vulnweb.com/admin/

http://testphp.vulnweb.com/Mod\_Rewrite\_Shop/.htaccess

http://testphp.vulnweb.com/crossdomain.xml

http://testphp.vulnweb.com/CVS/Root

http://testphp.vulnweb.com/secured/phpinfo.php

http://testphp.vulnweb.com/\_mmServerScripts/mysql.php

Directory Index:

The presence of directory index listings could reveal directory structures and sensitive files, aiding attackers in their reconnaissance efforts.

http://testphp.vulnweb.com/Flash/

http://testphp.vulnweb.com/CVS/

http://testphp.vulnweb.com/.idea/

Information Disclosure:

Email addresses (`wvs@acunetix.com`, `test@gmail.com`, `wasp@acunetix.com`) and a local IP address (`http://127.0.0.1`) are disclosed, which could be leveraged for social engineering or targeted attacks.

wvs@acunetix.com

test@gmail.com

http://127.0.0.1

wasp@acunetix.com

XSS (Cross-Site Scripting):

Multiple endpoints are vulnerable to XSS attacks, allowing attackers to inject malicious scripts into web pages viewed by other users, potentially leading to session hijacking or data theft.

POST http://testphp.vulnweb.com/search.php 'searchFor'

POST http://testphp.vulnweb.com/guestbook.php 'name'

POST http://testphp.vulnweb.com/secured/newuser.php 'uuname'

GET http://testphp.vulnweb.com/listproducts.php?cat=<IMG sRC=X onerror=jaVaScRipT:alert`xss`>

GET http://testphp.vulnweb.com/listproducts.php?artist=<IMG sRC=X onerror=jaVaScRipT:alert`xss`>

GET http://testphp.vulnweb.com/hpp/?pp=%22%3E%3CIMG%20sRC=X%20onerror=jaVaScRipT:alert`xss`%3E

GET http://testphp.vulnweb.com/hpp/params.php?p=<IMG sRC=X onerror=jaVaScRipT:alert`xss`>

SQL Injection:

Several URLs are susceptible to SQL injection attacks, enabling attackers to manipulate databases, extract data, or execute arbitrary SQL commands.

POST http://testphp.vulnweb.com/secured/newuser.php 'uuname' error SQLi vulnerable

POST http://testphp.vulnweb.com/userinfo.php 'uname' blind SQLi vulnerable

GET http://testphp.vulnweb.com/artists.php 'artist' error SQLi vulnerable

GET http://testphp.vulnweb.com/listproducts.php 'cat' error SQLi vulnerable

GET http://testphp.vulnweb.com/listproducts.php 'artist' error SQLi vulnerable

GET http://testphp.vulnweb.com/product.php 'pic' error SQLi vulnerable

GET http://testphp.vulnweb.com/Mod\_Rewrite\_Shop/details.php 'id' SQLi vulnerable

GET http://testphp.vulnweb.com/AJAX/infocateg.php 'id' SQLi vulnerable

File Inclusion:

The `showimage.php` script allows for arbitrary file inclusion, potentially leading to remote code execution or unauthorised access to system files.

http://testphp.vulnweb.com/showimage.php?file=showimage.php

http://testphp.vulnweb.com/showimage.php?file=php://filter/convert.base64-encode/resource=showimage.php

SSRF (Server-Side Request Forgery):

The `showimage.php` script is vulnerable to SSRF attacks, allowing attackers to make unauthorised requests to internal or external resources, potentially bypassing security measures.

http://testphp.vulnweb.com/showimage.php?file=http://127.0.0.1:22

Weak Password:

The presence of a weak password (`test/test`) poses a security risk, potentially allowing unauthorised access to restricted areas or sensitive information.

CRLF (Carriage Return Line Feed):

Although listed, there is no specific information provided about CRLF vulnerabilities in the overview.

Overall, the website exhibits multiple security vulnerabilities ranging from information disclosure to critical vulnerabilities like XSS, SQL injection, and SSRF. Immediate action should be taken to address these issues to prevent potential exploitation and data breaches.