WEB APPLICATION SECURITY ASSESSMENT REPORT

Web Application Security Assessment

Abstract

This project demonstrates web application security testing using a black box approach to identify common vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS).

Rushikesh Pawar

Rushikeshpawar977@gmail.com

WEB APPLICATION SECURITY ASSESSMENT REPORT

Target: testphp.vulnweb.com

Author : Rushikesh Pawar

Date : 07-01-2026

INDEX

INTRODUCTION

Web application security is an important part of cybersecurity. Many applications are vulnerable due to improper input validation and insecure configurations.

In this project, a security assessment was performed on an intentionally vulnerable web application (testphp.vulnweb.com) to understand common web vulnerabilities and attack techniques.

SCOPE OF TESTING

Target Application: testphp.vulnweb.com

Testing Type: Black Box Testing

Environment: Kali Linux

Authorization: Public vulnerable test application

TOOLS USED

Kali Linux	-	Penetration testing OS
Nmap	-	Network scanning
Burp Suite	-	Proxy and web testing
Firefox	-	Browser testing

METHODOLOGY

The testing methodology followed these steps:

1. Network reconnaissance using Nmap
2. Application mapping using Burp Suite proxy
3. Identification of input points
4. Manual vulnerability testing
5. Analysis and documentation

RISK RATING SCALE

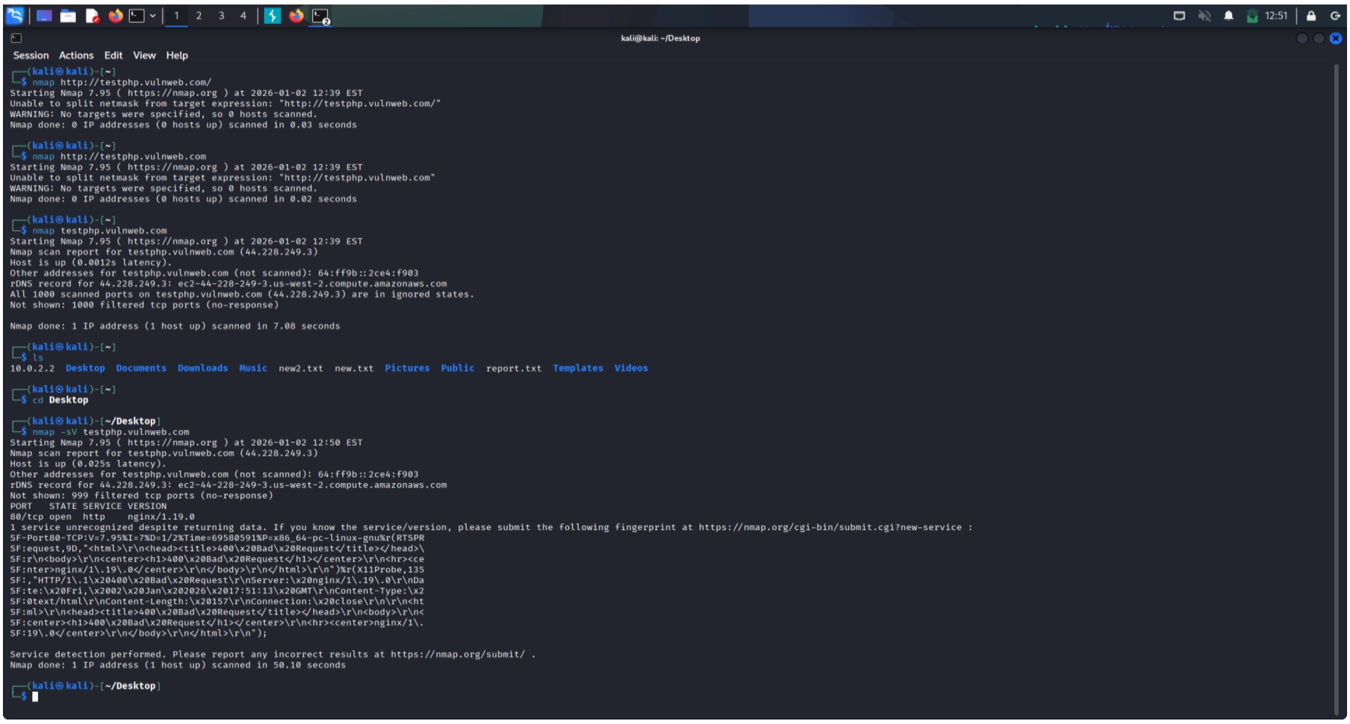
Risk Rating is calculated based on the potential impact and likelihood of exploitation.

High – Critical security risk with serious impact
Medium – Moderate risk that can be exploited
Low – Minor security issue with limited impact

RECONNAISSANCE (NMAP)

Nmap was used to scan the target application to identify open ports and running services.

Port **80** was found **open** running an **Nginx** web server.



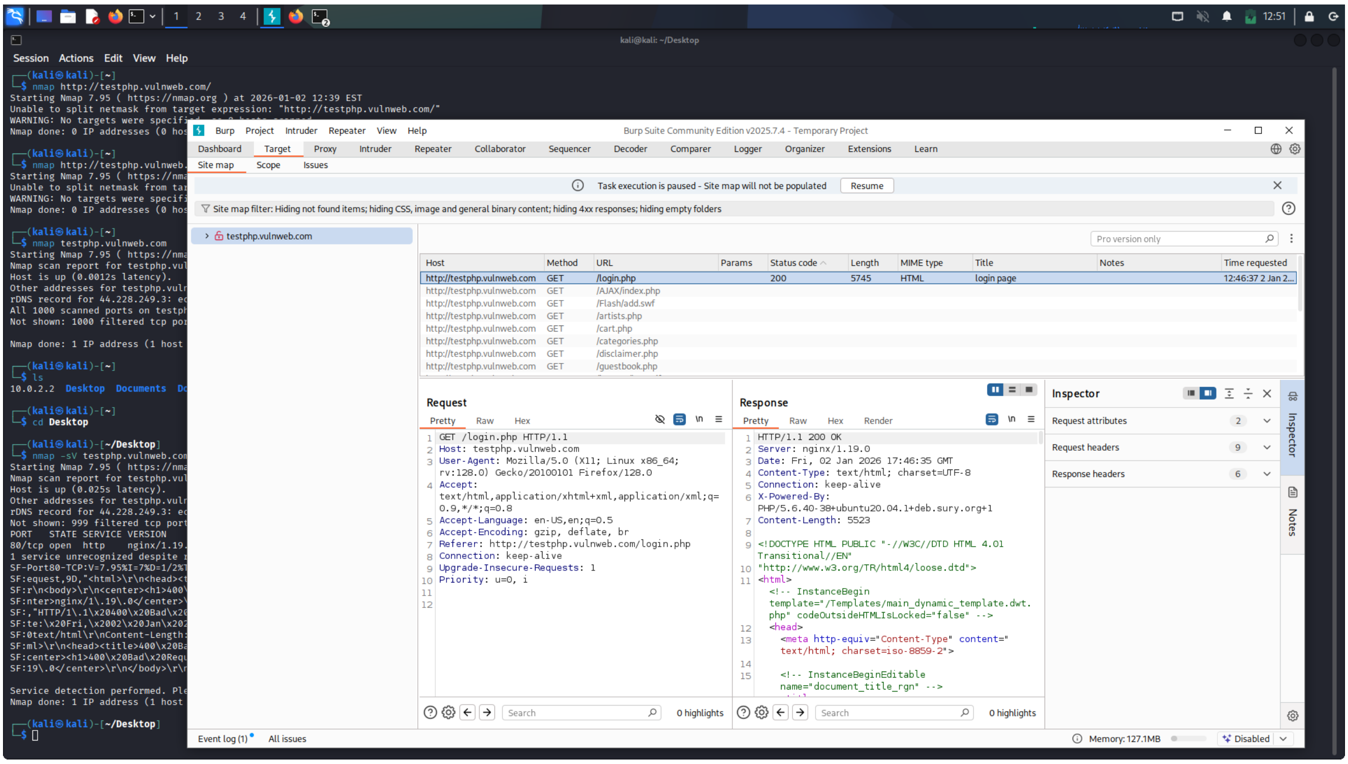
```
┌──(kali㉿kali)-[~]
└─$ nmap http://testphp.vulnweb.com/
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 12:39 EST
Unable to split netmask from target expression: "http://testphp.vulnweb.com/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap http://testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 12:39 EST
Unable to split netmask from target expression: "http://testphp.vulnweb.com"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

┌──(kali㉿kali)-[~]
└─$ nmap testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 12:39 EST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0012s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
All 1000 scanned ports on testphp.vulnweb.com (44.228.249.3) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 7.08 seconds

┌──(kali㉿kali)-[~]
└─$ ls
10.0.2.2  Desktop  Documents  Downloads  Music  new2.txt  new.txt  Pictures  Public  report.txt  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 12:50 EST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.025s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx/1.19.0
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.95%I=7%D=1/2%Time=69580591%P=x86_64-pc-linux-gnu%r(RTSPR
SF:equest,9D,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head>\
SF:r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><ce
SF:nter>nginx/1\.19\.0</center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,135
SF:,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20nginx/1\.19\.0\r\nDa
SF:te:\x20Fri,\x2002\x20Jan\x202026\x2017:51:13\x20GMT\r\nContent-Type:\x2
SF:0text/html\r\nContent-Length:\x20157\r\nConnection:\x20close\r\n\r\n<ht
SF:ml>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<
SF:center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><center>nginx/1\.
SF:19\.0</center>\r\n</body>\r\n</html>\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.10 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

BURP SUITE TESTING

Burp Suite proxy was configured to intercept HTTP requests.

The site map feature was used to identify application endpoints

such as login, search, and product pages.



kali@kali: ~/Desktop
Session Actions Edit View Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Site map Scope Issues
Resume
testphp.vulnweb.com
Pro version only
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights
Inspector
Event log (1) All issues
Memory: 127.1MB
Disabled

```
┌──(kali㉿kali)-[~]
└─$ nmap http://testphp.vulnweb.com/
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 12:39 EST
Unable to split netmask from target expression: "http://testphp.vulnweb.com/"
WARNING: No targets were specifi
Nmap done: 0 IP addresses (0 hos

┌──(kali㉿kali)-[~]
└─$ nmap http://testphp.vulnweb.
Starting Nmap 7.95 ( https://nma
Unable to split netmask from tar
WARNING: No targets were specifi
Nmap done: 0 IP addresses (0 hos

┌──(kali㉿kali)-[~]
└─$ nmap testphp.vulnweb.com
Starting Nmap 7.95 ( https://nma
Nmap scan report for testphp.vul
Host is up (0.0012s latency).
Other addresses for testphp.vulr
rDNS record for 44.228.249.3: ec
All 1000 scanned ports on testph
Not shown: 1000 filtered tcp por

Nmap done: 1 IP address (1 host

┌──(kali㉿kali)-[~]
└─$ ls
10.0.2.2  Desktop  Documents  Do

┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV testphp.vulnweb.com
Starting Nmap 7.95 ( https://nma
Nmap scan report for testphp.vul
Host is up (0.025s latency).
Other addresses for testphp.vulr
rDNS record for 44.228.249.3: ec
Not shown: 999 filtered tcp port
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx/1.19.
1 service unrecognized despite r
SF-Port80-TCP:V=7.95%I=7%D=1/2%T
SF:equest,9D,"<html>\r\n<head><t
SF:r\n<body>\r\n<center><h1>400\
SF:nter>nginx/1\.19\.0</center>\
SF:,"HTTP/1\.1\x20400\x20Bad\x20
SF:te:\x20Fri,\x2002\x20Jan\x202
SF:0text/html\r\nContent-Length:
SF:ml>\r\n<head><title>400\x20Ba
SF:center><h1>400\x20Bad\x20Requ
SF:19\.0</center>\r\n</body>\r\r

Service detection performed. Ple
Nmap done: 1 IP address (1 host

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Task execution is paused - Site map will not be populated

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://testphp.vulnweb.com	GET	/login.php		200	5745	HTML	login page		12:46:37 2 Jan 2...
http://testphp.vulnweb.com	GET	/AJAX/index.php							
http://testphp.vulnweb.com	GET	/Flash/add.swf							
http://testphp.vulnweb.com	GET	/artists.php							
http://testphp.vulnweb.com	GET	/cart.php							
http://testphp.vulnweb.com	GET	/categories.php							
http://testphp.vulnweb.com	GET	/disclaimer.php							
http://testphp.vulnweb.com	GET	/guestbook.php							

Request

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 02 Jan 2026 17:46:35 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By:
PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 5523

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <!-- InstanceBegin
  template="/Templates/main_dynamic_template.dwt.
  php" codeOutsideHTMLIsLocked="false" -->
  <head>
    <meta http-equiv="Content-Type" content="
    text/html; charset=iso-8859-2">

    <!-- InstanceBeginEditable
    name="document_title_rgn" -->
```

Request attributes	2
Request headers	9
Response headers	6

VULNERABILITY 1: SQL INJECTION

Vulnerability Name: SQL Injection

Severity: **Critical**

Risk Rating: **High**

Location: /listproducts.php?cat=

Description:

Improper input validation allows SQL queries to be manipulated by the user.

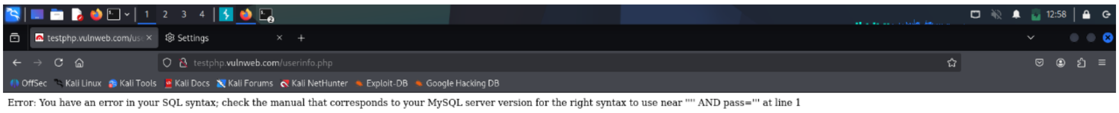
Impact:

- Unauthorized database access
- Data leakage

Recommendation:

Use prepared statements and input validation.

Disable detailed SQL error messages.



```
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "'' AND pass=''' at line 1
```

VULNERABILITY 2: XSS

Vulnerability Name: Cross-Site Scripting (XSS)

Severity: **Medium**

Risk Rating: **Medium**

Location: Search Input Field

Description:

User input is reflected in the response without proper sanitization, allowing script execution in the victim's browser.

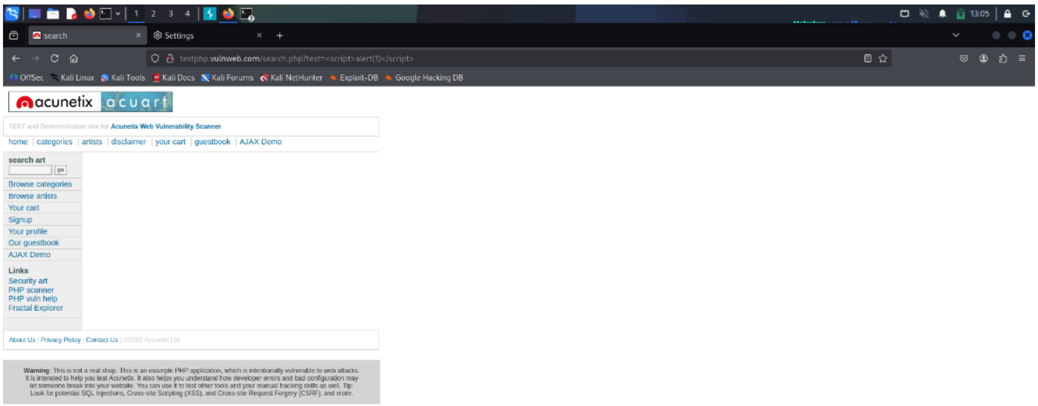
Impact:

- Session hijacking
- Execution of malicious scripts
- User data compromise

Recommendation:

Implement output encoding and input sanitization.

Use Content Security Policy (CSP).



testphp.vulnweb.com/search.php?test=<script>alert(1)</script>

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

SENSITIVE INFORMATION DISCLOSURE

Vulnerability Name: Sensitive Information Disclosure

Severity: **Low**

Risk Rating: **Low**

Location: HTTP Response Headers

Description:

The application discloses sensitive information
such as web server and scripting language versions
in HTTP response headers.

Impact:

- System fingerprinting
- Helps attackers plan targeted attacks

Recommendation:

Disable server version disclosure.

Configure web server security headers

CONCLUSION

This project helped in understanding real-world
web application vulnerabilities.
Manual testing techniques provided hands-on
experience with ethical hacking tools.