Vulnerability Report on VulnWeb

muLearn Circle: Team Samosa

Code: **SACYBMUT**

Summary

The comprehensive Vulnerability Assessment report by muLean Circle Cyber Security unveils various findings within the website http://testphp.vulnweb.com. Conducted through a combination of manual and automated methods using tools like Burp Suite, the report delineates vulnerabilities along with their severity, details, background, and proof of concept (POC). It's essential to note that the report covers a subset of issues that could be verified manually within the allocated time. With additional time, more issues are expected to be identified and substantiated.

The risk analysis, integral to organizational security, is meticulously presented, encompassing both public and private portals of services provided by testphp.vulnweb.com. The assessment, inclusive of authenticated and unauthenticated penetration testing, delves into backend infrastructure scanning for potential vulnerabilities such as brute force attacks, unauthorized access, data leakage, and exploitation.

The evaluation of the "Vulnweb" website underscores numerous vulnerabilities, posing a significant threat to client data security. The absence of database encryption exposes critical information like passwords, usernames, email addresses, and phone numbers to potential unauthorized access. In essence, user inputs are vulnerable on this site, necessitating immediate attention and remediation measures.

Throughout the assessment, tools like Burp Suite and others were employed to ensure a thorough examination of the website's security posture. The findings presented in this report aim to guide remediation efforts and enhance the overall security resilience of the tested web application.

LFI (LOCAL FILE INCLUSION)

`Summary: LFI is possible due to lack of validation`

`Vulnerable Endpoint:` http://testphp.vulnweb.com/showimage.php

`Severity:` **High**

Details

The URL http://testphp.vulnweb.com/showimage.php is vulnerable to a PHP Local File Inclusion (LFI) exploit. LFI is a security vulnerability that occurs when a web application includes files based on user input without proper validation. In this case, the "showimage.php" script is likely to include files using user-controlled input, making it susceptible to directory traversal attacks, where an attacker could manipulate input parameters to access and display sensitive files on the server. This vulnerability poses a significant risk as it could potentially expose confidential information and compromise the security of the web application. Mitigation strategies should involve implementing proper input validation, using absolute file paths, and ensuring that user input is not directly used in file inclusion functions.

POC

```
GET /showimage.php?file=%2e%2e%2f%2e%2e%2fetc%2fpasswd HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4324.150 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://testphp.vulnweb.com/listproducts.php?cat=1
```

Mitigation

- Use Include Functions Securely
- File Path Verification
- Directory Whitelisting

Cross Site Scripting

Summary: XSS is possible due to lack of validation

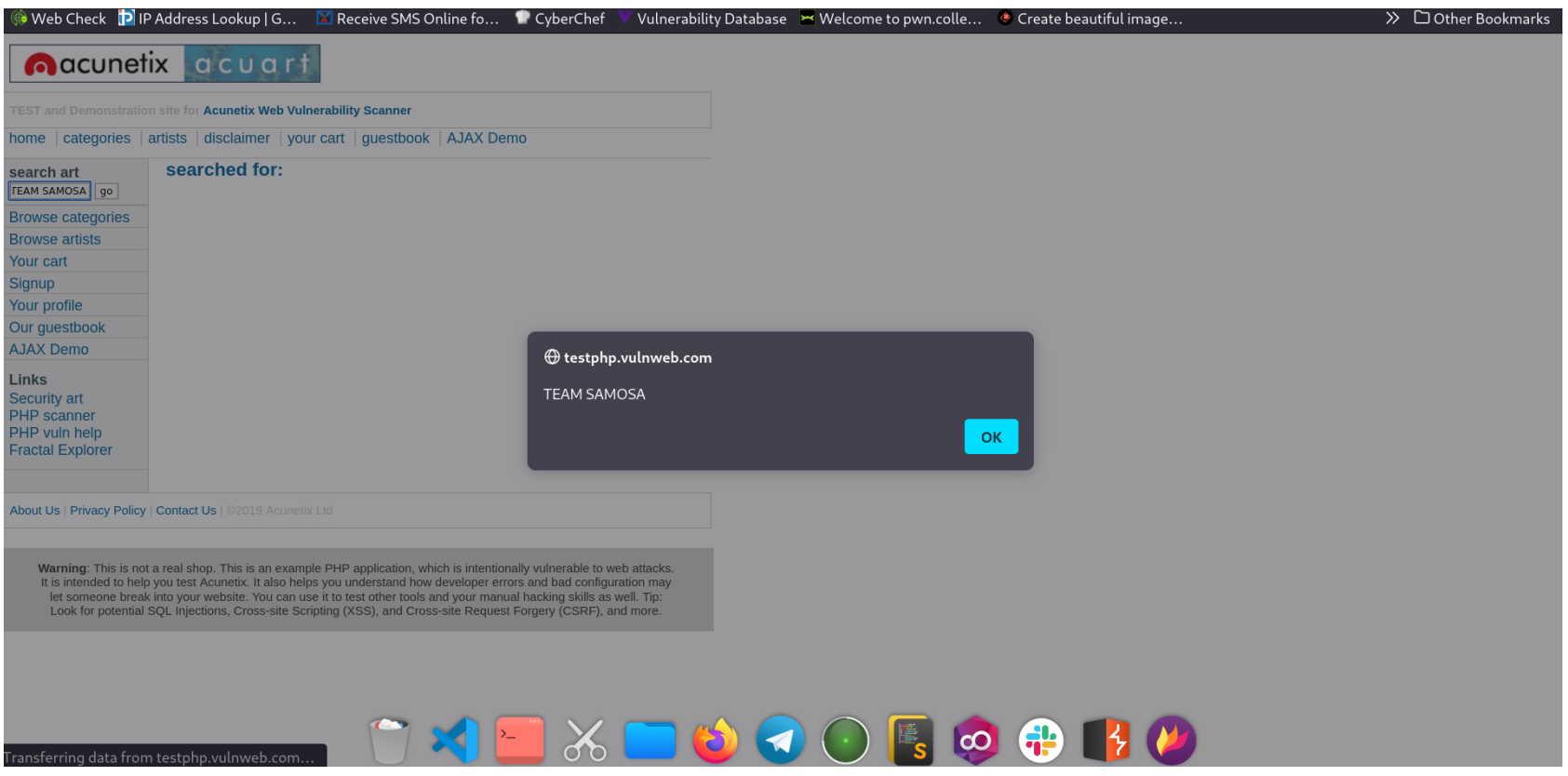
Vulnerable Endpoint: http://testphp.vulnweb.com/search.php?test=query

Severity: **MEDIUM**

Details

The application displays an HTML document where the name from an arbitrarily supplied URL parameter is directly inserted as plain text between `<pre>` tags. A submitted payload, `<script>alert("TEAM+SAMOSA")</script>` in the name of the URL parameter remained unaltered in the application's response. This behavior illustrates a vulnerability, indicating the potential for injecting new HTML tags into the returned document.

POC



Mitigation

- Validate input rigorously based on expected content
- Reject, rather than sanitize, input that fails validation criteria.
- HTML-encode user input whenever it is incorporated into application responses.
- Replace HTML metacharacters (< > " ' =) with corresponding HTML entities to prevent XSS attacks.

Sensitive Information Disclosure

Summary: Lack of access controls leads to sensitive information disclosure

Vulnerable Endpoint:

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

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

Severity: **LOW**

Details

The system is vulnerable to sensitive files disclosure, which could allow an unauthorized user to gain access to confidential information. This poses a significant risk to the privacy and security of the system's data, as well as the individuals whose information may be exposed.

POC

PHP Logo

PHP Version 5.1.6

System	FreeBSD svn.local 6.2-RELEASE FreeBSD 6.2-RELEASE #0: Fri Jan 12 10:40:27 UTC 2007 root@dessler.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386
Build Date	Jul 30 2007 12:20:01
Configure Command	'./configure' '--enable-versioning' '--enable-memory-limit' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--with-libxml-dir=/usr/local' '--enable-reflection' '--enable-spl' '--program-prefix=' '--enable-fastcgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--disable-ipv6' '--prefix=/usr/local' 'i386-portbld-freebsd6.2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
additional .ini files parsed	/usr/local/etc/php/extensions.ini
PHP API	20041225
PHP Extension	20050922

Mitigation

- Implement strict access controls to restrict access to sensitive information based on the principle of least privilege.
- Regularly review and update user permissions, ensuring that individuals only have access to the data necessary for their roles.
- Employ multi-factor authentication to add an additional layer of security, particularly for accounts with access to sensitive data.

SACYBMUT - Muthoot Institute Of Technology And Science
Learning circle name : Samosa

Name : Advaith Narayanan

Muid : advaithnarayanan@mulearn

Name : Adithi Asok

Muid : adithiasok@mulearn

Name : Athul Prakash NJ

Muid: athulprakashnj@mulearn

Name : V Vishnu Jyothi

Muid : vvishnujyothi@mulearn

Name:Jerit Joshy

Muid: jeritjoshy@mulearn