

Vulnerability Assessment Test Report

Prepared by
Mulearn circle : **Zyberbee**

Content

- Summary

Vulnerabilities :

1. SQL Injection
2. Cross site scripting
3. Conclusion

Summary

This Vulnerability Assessment report presented by muLean Circle **Zyberbee** contains reports of various vulnerabilities findings present in the website <http://testphp.vulnweb.com> . The various assessments were conducted using manual and automated methods and tools. With more time we are confident to present more issues with more proof. Several minor vulnerabilities are also mentioned.

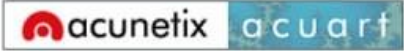
1.SQL Injection

> Authentication bypassed using SQL injection ' or '1'='1

Sol:

The problem of SQL injection, as exemplified by the malicious input ' or '1'='1, can be effectively addressed by implementing stringent input validation and adopting secure coding practices. By thoroughly validating and sanitizing user inputs, and utilizing parameterized SQL queries, organizations can prevent SQL injection attacks, including authentication bypass attempts. This ensures the security and integrity of their databases and web applications, safeguarding sensitive information and maintaining user trust.

Request :



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](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

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

Username :

Password :

login

You can also signup here.

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

Response :



The screenshot shows the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes links for home, categories, artists, disclaimer, your cart, guestbook, AJAX Demo, and Logout test. The left sidebar contains a search bar, a list of categories (Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo), and a Links section (Security art, PHP scanner, PHP vuln help, Fractal Explorer). The main content area is titled 'John Smith (test)' and contains a form for user information. The form fields are: Name (John Smith), Credit card number (1234-5678-2300-9000), E-Mail (email@email.com), Phone number (2323345), and Address (../etc/passwd). An 'update' button is at the bottom right of the form. Below the form, it says 'You have 7 items in your cart. You visualize you cart here.'

2.Cross site scripting

> we managed to display browser cookies using crose site scripting

```
<script>alert(document.cookie);</script>
```

Sol:

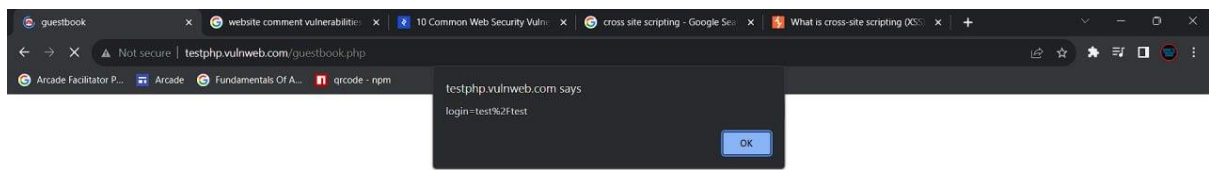
Cross-site scripting (XSS) is a serious security issue that allows attackers to execute malicious scripts in the context of a user's browser. To mitigate this problem and prevent the display of sensitive information like browser cookies, it is essential to employ various security measures. These include input validation and output encoding, which ensure that user inputs are sanitized and that any data rendered in the browser is properly encoded. Additionally, implementing security headers like Content Security Policy (CSP) can help prevent the execution of unauthorized scripts, making it much more difficult for attackers to exploit XSS vulnerabilities. The provided malicious script '`<script>alert(document.cookie);</script>`' should never be allowed to execute, and with proper security practices in place, the risk of XSS attacks can be significantly reduced.

Request :



The screenshot shows the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes links for home, categories, artists, disclaimer, your cart, guestbook, AJAX Demo, and Logout test. The left sidebar contains a search bar, a list of categories (Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo, Logout), and a Links section (Security art, PHP scanner, PHP vuln help, Fractal Explorer). The main content area is titled 'Our guestbook' and shows a message from 'test' dated '11.07.2023, 5:31 pm'. The message content is '`<script>alert(document.cookie);</script>`'. An 'add message' button is at the bottom left of the message box.

Response :



Conclusion

In conducting this comprehensive vulnerability assessment, we have systematically identified and evaluated potential security risks within the system. The analysis encompassed various aspects, including network vulnerabilities, application weaknesses, and potential exposure of sensitive information. Our findings underscore the importance of a proactive approach to cybersecurity. Addressing the identified vulnerabilities is crucial to fortify the system against potential exploits, unauthorized access, and data breaches. The recommended remediation measures, outlined in the assessment, provide a strategic roadmap for enhancing the overall security posture. It is imperative for stakeholders to prioritize the implementation of these remedial actions promptly. Additionally, ongoing vigilance and regular assessments are vital components of a robust security strategy to adapt to evolving threats and vulnerabilities. By addressing the identified issues and fostering a culture of continuous improvement in cybersecurity practices, the organization can significantly reduce the risk landscape and bolster its resilience against potential security threats.