*Web Application Vulnerability Assessment*

* CyberFocus

The assessment was conducted on the following site:

<http://testphp.vulnweb.com>

Risk Levels:

Included: High, Medium, Low, Informational

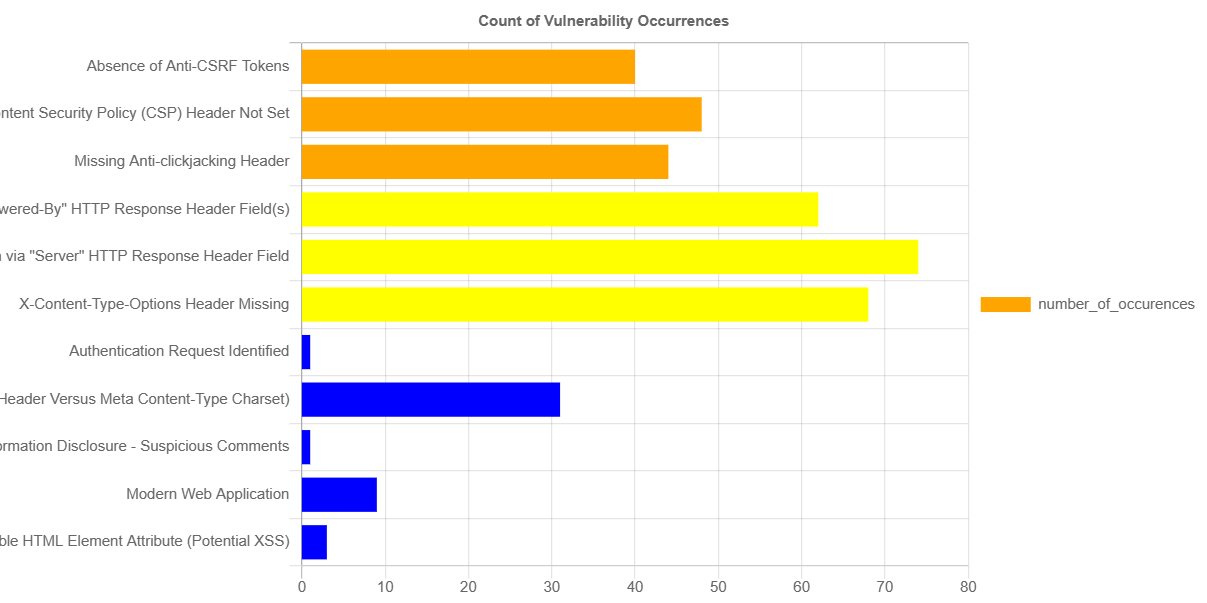
Excluded: None

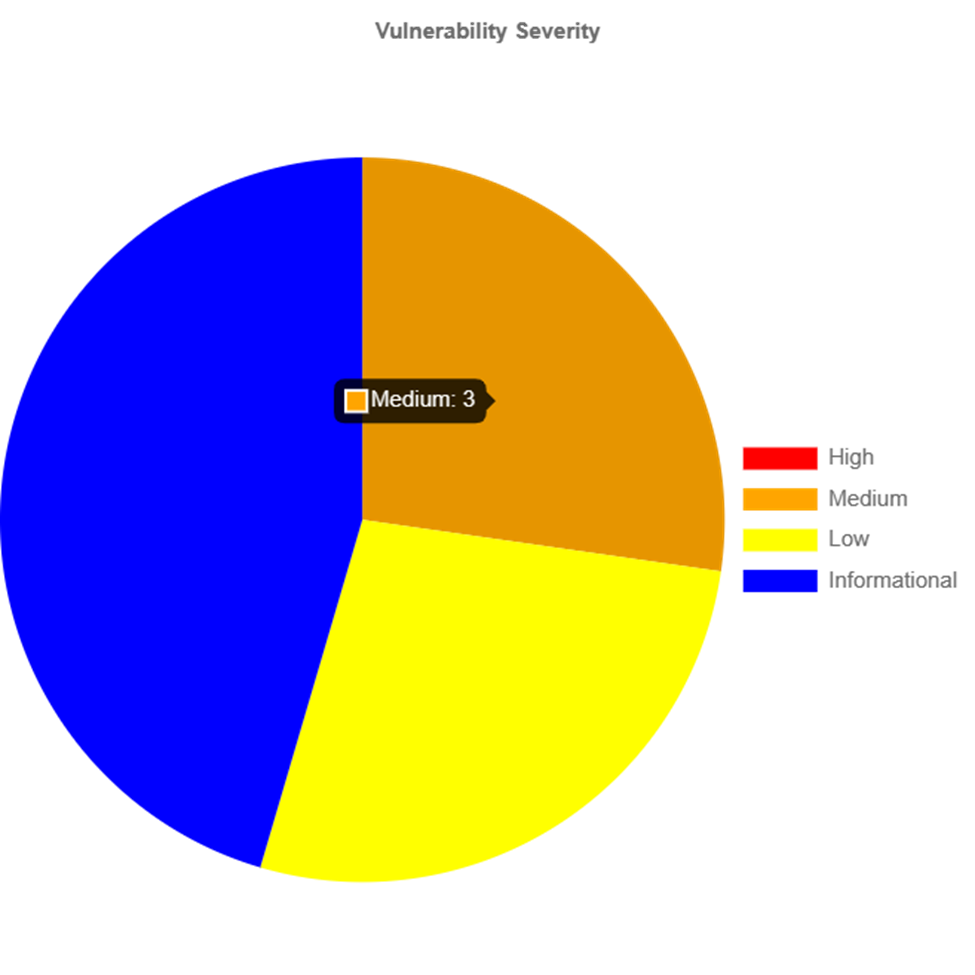
Confidence Levels:

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Severity: Medium

The most severe alert is ‘Medium’ level. 



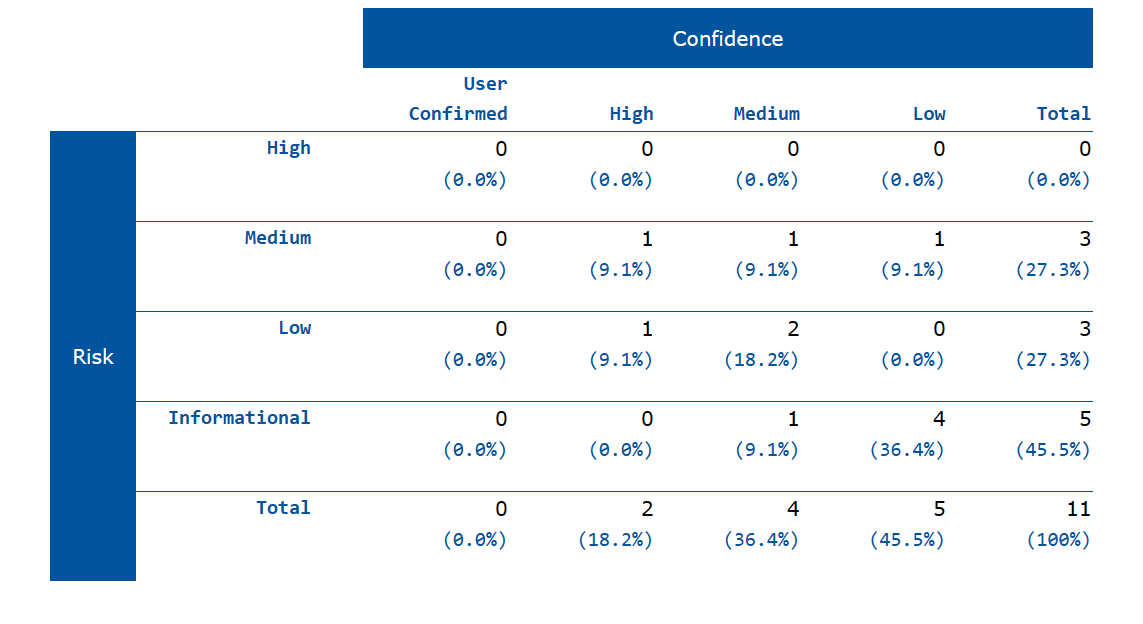
**Most Common Bug**  
Server Leaks Version Information via "Server" HTTP Response Header Field (74)

Vulnerability classification:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | Alert Type | Risk | Count | | |  | Absence of Anti-CSRF Tokens | Medium | 40 | | |  | Content Security Policy (CSP) Header Not Set | Medium | 48 | | |  | Missing Anti-clickjacking Header | Medium | 44 | | |  | Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) | Low | 62 | | |  | Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 74 | | |  | X-Content-Type-Options Header Missing | Low | 68 | | |  | Authentication Request Identified | Informational | 1 | | |  | Charset Mismatch (Header Versus Meta Content-Type Charset) | Informational | 31 | | |  | Information Disclosure - Suspicious Comments | Informational | 1 | | |  | Modern Web Application | Informational | 9 | | |  | User Controllable HTML Element Attribute (Potential XSS) | Informational | 3 | | |  | Total | 11 | | |

Summary:

Confidence v/s Risk



Reproducing the vulnerability:

Vulnerability Scanning:

- Use automated tools like Nessus, OpenVAS, or others to perform vulnerability scans on the target systems. These tools can help identify known vulnerabilities.

Issue Remediation:

1. Content Security Policy (CSP) Header Not Set(Confidence:High)

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

2. Missing Anti-clickjacking Header(Confidence:Medium)

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

3.Absence of Anti-CSRF Tokens(Confidence:Low)

Solution: Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

4. Server Leaks Version Information via "Server" HTTP Response Header Field(Confidence:High)

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

5. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (Confidence:Medium)

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

6. X-Content-Type-Options Header Missing (Confidence:Medium)

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

7. Modern Web Application(Confidence:Medium)

Solution: This is an informational alert and so no changes are required.

8. Authentication Request Identified(Confidence:Low)

Solution: This is an informational alert and so no changes are required.

9. Charset Mismatch (Header Versus Meta Content-Type Charset) (Confidence:Low)

Solution: Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.

10. Information Disclosure - Suspicious Comments (Confidence:Low)

Solution: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

11. User Controllable HTML Element Attribute (Potential XSS) (Confidence:Low)

Solution: Validate all input and sanitize output it before writing to any HTML attributes.

References:

1. Zaproxy
2. YouTube- <https://www.youtube.com/watch?v=alJLui61v2Y>
3. 
4. 