Vulnerability Assessment Report

By: Surya Sriram Karumuri

Generated by: ZAP

Version: 2.15.0
Date: Tue 11 Jun 2024, at 11:56:24
Supported by: Crash Override Open Source Fellowship

Report Parameters

Included Sites:

- http://testphp.vulnweb.com

Risk Levels Included: High, Medium, Low, Informational
Confidence Levels Included: User Confirmed, High, Medium, Low

---

Alert Counts by Risk and Confidence

Risk	User Confirmed	High	Medium	Low	Total
High	0	0	0	0	0
Medium	0	1	1	1	3
Low	0	1	2	0	3
Informational	0	0	1	4	5
Total	0	2	4	5	11

Alert Counts by Site and Risk

Site	High	Medium	Low	Informational	Total
http://testphp.vulnweb.com	0	3	3	5	11

Alerts

Medium Risk, High Confidence

- **Content Security Policy (CSP) Header Not Set**
  - URL: http://testphp.vulnweb.com/robots.txt

Medium Risk, Medium Confidence

- **Missing Anti-clickjacking Header**
  - URL: http://testphp.vulnweb.com/login.php

Medium Risk, Low Confidence

- **Absence of Anti-CSRF Tokens**
  - URL: http://testphp.vulnweb.com/login.php

Low Risk, High Confidence

- **Server Leaks Version Information via "Server" HTTP Response Header Field**
  - URL: http://testphp.vulnweb.com/robots.txt

Low Risk, Medium Confidence

- **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
  - URL: http://testphp.vulnweb.com/login.php
- **X-Content-Type-Options Header Missing**
  - URL: http://testphp.vulnweb.com/login.php

Informational, Medium Confidence

- **Modern Web Application**
  - URL: http://testphp.vulnweb.com/artists.php

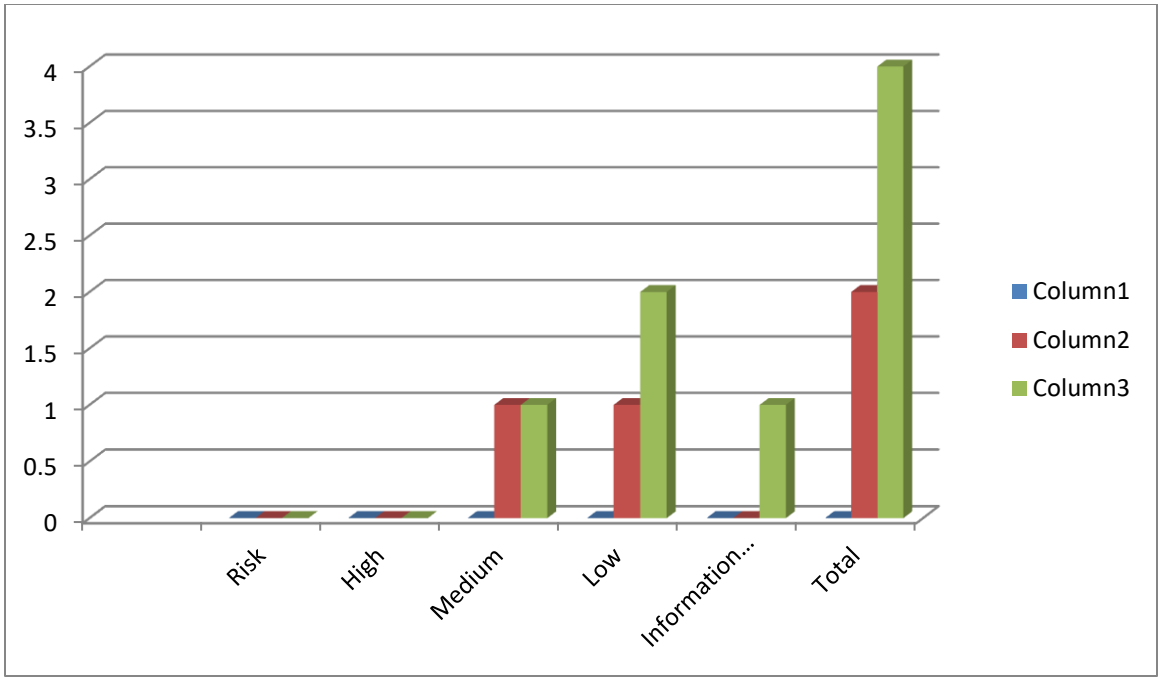
Informational, Low Confidence

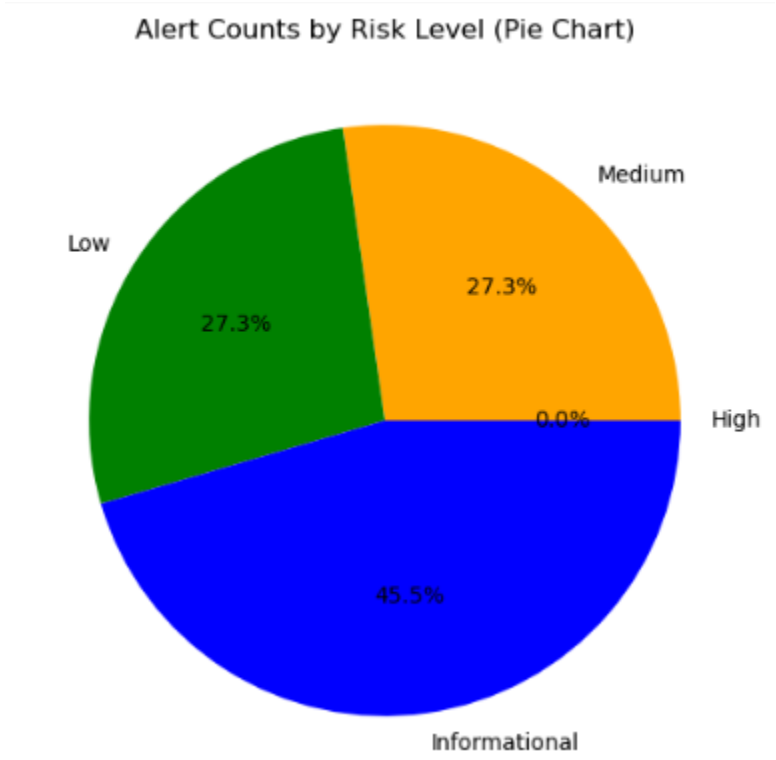
- **Authentication Request Identified**
  - URL: POST http://testphp.vulnweb.com/secured/newuser.php
- **Charset Mismatch (Header Versus Meta Content-Type Charset)**
  - URL: GET http://testphp.vulnweb.com/login.php
- **Information Disclosure - Suspicious Comments**
  - URL: GET http://testphp.vulnweb.com/AJAX/index.php
- **User Controllable HTML Element Attribute (Potential XSS)**
  - URL: POST http://testphp.vulnweb.com/search.php?test=query

---

Visual Representation

Bar Graph of Alert Counts by Risk and Confidence





Summary

The vulnerability assessment report generated by ZAP reveals a total of 11 alerts across various risk levels for the site http://testphp.vulnweb.com. The findings include three medium-risk issues, three low-risk issues, and five informational alerts. Notably, medium-risk vulnerabilities involve the absence of anti-CSRF tokens, missing anti-clickjacking headers, and the lack of a Content Security Policy (CSP) header. Low-risk issues are

primarily related to server information disclosure via HTTP response headers. The informational alerts highlight minor issues such as charset mismatches and potential XSS vectors in user-controllable HTML elements. The report underscores the need for implementing robust security headers and enhancing input validation mechanisms to mitigate the identified risks effectively.