ZAP Scanning Report

Site: http://testphp.vulnweb.com

Generated on Thu, 18 May 2023 10:09:3s

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	3
Low	2
Informational	2

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (DOM Based)	High	17
Cross Site Scripting (Reflected)	High	16
SQL Injection	High	8
.htaccess Information Leak	Medium	7
Absence of Anti-CSRF Tokens	Medium	41
Missing Anti-clickjacking Header	Medium	45
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	63
X-Content-Type-Options Header Missing	Low	68
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	32
Information Disclosure - Suspicious Comments	Informational	1

Alert Detail

High	Cross Site Scripting (DOM Based)
	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML /JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.