OWASP Top 10 Vulnerability Report (Reorganized from ZAP Scan)

A01: Broken Access Control

Finding	Severity
Absence of Anti-CSRF Tokens	Medium
Directory Browsing	Medium
Hidden File Found (phpinfo.php)	Medium

A02: Cryptographic Failures

Finding	Severity
Cookie without SameSite Attribute	Low
Cookie No HttpOnly Flag	Low

A03: Injection

Finding	Severity
Remote Code Execution – CVE-2012-1823	High
Source Code Disclosure – CVE-2012-1823	High

A04: Insecure Design

Finding	Severity
Default admin credentials in DVWA	High
No account lockout after failed logins	Medium

A05: Security Misconfiguration

Finding	Severity
Missing Anti-clickjacking Header	Medium
Content Security Policy (CSP) Header Not Set	Medium
X-Content-Type-Options Header Missing	Low
Server Leaks Information via X-Powered-By Header	Low
Server Leaks Version Information via Server Header	Low

A06: Vulnerable and Outdated Components

Finding	Severity
Outdated PHP version with known CVEs	High
Outdated Apache server (identified in headers)	Medium

A07: Identification and Authentication Failures

Finding	Severity
Authentication Request Identified	Informational
Session Management Response Identified	Informational
Weak password handling in DVWA login	Medium

A08: Software and Data Integrity Failures

Finding	Severity
Remote Code Execution may allow malicious payload injection	High

A09: Security Logging and Monitoring Failures

Finding	Severity
User Agent Fuzzer – No detection of abnormal traffic	Informational

A10: Server-Side Request Forgery (SSRF)

Finding	Severity
File Inclusion + File Upload module abuse to fetch remote resources	High (Simulated)