

Vulnerability Scan Report

Vulnerability	Status	Severity	Recommendation
Open Redirect	Not Vulnerable	N/A	N/A
Security Headers	Not Vulnerable	N/A	N/A
SQL Injection	Vulnerable	High	Sanitize and parameterize all user inputs.
Brute Force Login	Vulnerable	High	Implement account lockout mechanisms and CAPTCHAs.
Open Ports	Vulnerable	High	Close unused ports and use firewalls.
XSS	Not Vulnerable	N/A	N/A
Phishing	Vulnerable	High	Verify domain legitimacy and educate users.
Ransomware	Not Vulnerable	N/A	N/A
Weak Passwords	Vulnerable	High	Enforce strong password policies.
DNS Tunneling	Not Vulnerable	N/A	N/A
Session Hijacking	Not Vulnerable	N/A	N/A
Cryptojacking	Not Vulnerable	N/A	N/A
Drive-By Attack	Vulnerable	High	Use up-to-date security patches and scan for malicious scripts.
Malware	Not Vulnerable	N/A	N/A
CSRF	Vulnerable	High	Implement CSRF tokens in forms.
Directory Traversal	Not Vulnerable	N/A	N/A
Trojans	Not Vulnerable	N/A	N/A
Spyware	Not Vulnerable	N/A	N/A
Code Injection	Not Vulnerable	N/A	N/A
URL Manipulation	Vulnerable	High	Implement input validation and authorization checks.
XXE	Vulnerable	High	Disable XML external entity processing.