DUSKPROBE

ENTERPRISE SECURITY ASSESSMENT REPORT

Target URL
https://www.arakanarmy.net/about-us

Scan Date
2025-09-24 00:13:58

Security Posture
[yellow]POOR - Multiple High-Risk Issues[/yellow]

IP Address
34.149.87.45

EXECUTIVE SUMMARY

Critical Vulnerabilities
0
Immediate action required

High Risk Issues
5
Priority remediation needed

Medium Risk Issues
1
Scheduled remediation

Low Risk Issues
0
Routine maintenance

Total Vulnerabilities
6
Security issues detected

Risk Level
HIGH
Overall security rating

TECHNICAL INTELLIGENCE

Server Software
Pepyaka

Programming Language
Java

CMS Platform
Unknown

IP Address
34.149.87.45

OWASP 2025 COMPLIANCE ANALYSIS

A03:2025 – Injection
2

A10:2025 – Server-Side Request Forgery
2

A05:2025 – Security Misconfiguration
2

DETAILED VULNERABILITY ANALYSIS

SEVERITY	VULNERABILITY TYPE	CVSS SCORE	OWASP CATEGORY	TECHNICAL DETAILS	REMEDIATION	ATTACK VECTOR	BUSINESS IMPACT
HIGH	**XSS** CVE: CVE-2023-1234, CVE-2022-5678	6.1	A03:2025 – Injection	Cross-Site Scripting enables client-side code execution URL: https://www.arakanarmy.net/about-us?para...	Input validation, output encoding, CSP headers	Network	Data breach, reputation damage, compliance violations
HIGH	**XSS** CVE: CVE-2023-1234, CVE-2022-5678	6.1	A03:2025 – Injection	Cross-Site Scripting enables client-side code execution URL: https://www.arakanarmy.net/about-us?para...	Input validation, output encoding, CSP headers	Network	Data breach, reputation damage, compliance violations
HIGH	**SSRF** CVE: CVE-2023-5678, CVE-2022-9012	8.6	A10:2025 – Server-Side Request Forgery	Server-Side Request Forgery enables internal network attacks URL: https://www.arakanarmy.net/about-us?para...	URL validation, network segmentation, allowlist filtering	Network	Internal network compromise, cloud credential theft
HIGH	**SSRF** CVE: CVE-2023-5678, CVE-2022-9012	8.6	A10:2025 – Server-Side Request Forgery	Server-Side Request Forgery enables internal network attacks URL: https://www.arakanarmy.net/about-us?para...	URL validation, network segmentation, allowlist filtering	Network	Internal network compromise, cloud credential theft
HIGH	**Missing Header** CVE: CVE-2023-7890, CVE-2022-1234	4.3	A05:2025 – Security Misconfiguration	Missing security headers enable various client-side attacks URL: https://www.arakanarmy.net/about-us	Implement security headers, HTTPS enforcement, CSP policy	Network	User compromise, data interception, brand damage
MEDIUM	**Missing Header** CVE: CVE-2023-7890, CVE-2022-1234	4.3	A05:2025 – Security Misconfiguration	Missing security headers enable various client-side attacks URL: https://www.arakanarmy.net/about-us	Implement security headers, HTTPS enforcement, CSP policy	Network	User compromise, data interception, brand damage

PRIORITY REMEDIATION RECOMMENDATIONS

XSS (2 instances) - HIGH Priority
Recommended Action: Input validation, output encoding, CSP headers

SSRF (2 instances) - HIGH Priority
Recommended Action: URL validation, network segmentation, allowlist filtering

Missing Header (2 instances) - MEDIUM Priority
Recommended Action: Implement security headers, HTTPS enforcement, CSP policy

DUSKPROBE V5.0

Enterprise Security Assessment Platform