Vulnerability Assessment Report

For : TechXen Company

Prepared by

Mr. Herco

Assessment Type : Web Application | **Date :** 12/03/2026

Target :

Overall Website	https://techxen.com

Total Vulnerabilities Identified : 4

High : 1 | Medium : 2 | Low : 3

Overall Risk : High

Summary : This assessment identified multiple security vulnerabilities within the target website . One high - risk vulnerability could lead to serious security impact if exploited . Immediate remediation is recommended for high risk finding to reduce overall exposure.

Scope of Assessment

In-Scope:

- Public-facing website (https://techxen.com)
- Login and authentication modules
- Input forms and user interaction pages

Out of Scope:

- Internal network infrastructure
- Physical security
- Third-party services

Methodology

The assessment was performed using a combination of:

- Automated vulnerability scanning
- Manual testing
- OWASP Top 10 security testing framework

Testing included:

- Information gathering
- Vulnerability identification
- Exploitation attempts (non-destructive)
- Risk analysis and reporting

Risk Rating Criteria

Risk Level	Description
High	Critical vulnerabilities that can lead to full system compromise, data breach, or service disruption. Immediate action required.
Medium	Vulnerabilities that could be exploited with some effort and may impact system security. Should be addressed soon.
Low	Minor issues with limited impact but should be fixed as part of security best practices.

Summary of Findings

ID	Vulnerability	Risk Level	Status
VAPT-01	SQL Injection in Login Form	High	Open
VAPT-02	Cross-Site Scripting (XSS) in Contact Form	Medium	Open
VAPT-03	Insecure Password Policy	Medium	Open
VAPT-04	Missing Security Headers	Low	Open
VAPT-05	Directory Listing Enabled	Low	Open

Detailed Findings

VAPT-01: SQL Injection in Login Form

Risk Level: High
Description: The login form is vulnerable to SQL Injection, allowing attackers to manipulate database queries. This can lead to unauthorized access, data extraction, or complete database compromise.

Impact:

- Unauthorized access to user accounts
- Exposure of sensitive data
- Potential full system compromise

Evidence (Sample):

```
' OR '1'='1
```

Recommendation:

- Use parameterized queries (prepared statements)
- Implement server-side input validation
- Employ a Web Application Firewall (WAF)

VAPT-02: Cross-Site Scripting (XSS) in Contact Form

Risk Level: Medium
Description: The contact form does not properly sanitize user input, allowing attackers to inject malicious scripts.

Impact:

- Session hijacking
- Defacement
- Redirection to malicious websites

Recommendation:

- Sanitize and encode all user inputs
- Implement Content Security Policy (CSP)

VAPT-03: Insecure Password Policy

Risk Level: Medium
Description: The application allows weak passwords without enforcing complexity or length requirements.

Impact:

- Increased risk of brute-force and credential stuffing attacks

Recommendation:

- Enforce strong password policies (minimum length, complexity)
- Implement account lockout after multiple failed attempts

VAPT-04: Missing Security Headers

Risk Level: Low
Description: The website is missing important HTTP security headers such as `X-Frame-Options`, `X-Content-Type-Options`, and `Content-Security-Policy`.

Impact:

- Increased risk of clickjacking and MIME-type attacks

Recommendation:

- Configure web server to include standard security headers

VAPT-05: Directory Listing Enabled

Risk Level: Low
Description: Directory listing is enabled on certain paths, allowing attackers to view file structures.

Impact:

- Information disclosure

Recommendation:

- Disable directory listing in the web server configuration

Remediation Plan

Priority	Action	Timeline
High	Fix SQL Injection vulnerability	Immediate (0–3 days)
Medium	Patch XSS and update password policy	1–2 weeks
Low	Add security headers and disable directory listing	2–4 weeks

Conclusion

The assessment identified one critical high-risk vulnerability that poses a serious threat to the website's security. Addressing this issue should be the top priority. By following the recommended remediation steps, the overall security posture of the website can be significantly improved.