🔐 Web Application Security Assessment Report

Website: https://www.kmctemergingtechnology.org/
Assessment Type: Manual Web Security Review
Test Scope: Public-facing web application & exposed endpoints
Test Date: December 2025
Performed By: QA / Security Review

---

1. Executive Summary

A security assessment was conducted on the KMCT Emerging Technology website to identify potential vulnerabilities, misconfigurations, and code quality issues. The review focused on exposed paths, form security, and basic application hardening.

The assessment identified **critical security gaps**, particularly related to **CSRF protection**, **control panel exposure**, and **code quality issues**. While some sensitive administrative paths are properly restricted, other weaknesses could allow exploitation if not addressed promptly.

---

2. Scope of Testing

✔ In Scope

- Public website pages
- Contact and newsletter forms
- Common administrative and control paths
- Client-side code inspection
- Basic server exposure checks

❌ Out of Scope

- Authenticated admin dashboard testing
- Infrastructure-level penetration testing
- Automated vulnerability scanning
- Source code repository review

---

3. Critical Findings

🔴 1. Missing CSRF Protection (High Risk)

Affected Components:

- Contact Form (`/contact`)
- Newsletter Subscription Form (Footer)

Observation:

- No CSRF (Cross-Site Request Forgery) tokens are present in form submissions.
- Forms rely solely on client-side submission without request validation tokens.

Impact:

- Attackers can trick authenticated users or visitors into submitting malicious requests unknowingly.
- Can lead to spam submissions, data pollution, or backend misuse.

Risk Level: High

Recommendation:

- Implement server-side CSRF tokens for all forms.
- Validate CSRF tokens on every POST request.
- Consider same-site cookies (`SameSite=Strict`) for additional protection.

🔴 2. Exposed Hosting Control Panel (High Risk)

Affected Path:

- `/cpanel`

Observation:

- Directly redirects to HostGator cPanel login page.
- Uses a common and predictable path.

Impact:

- Makes the application a target for brute-force attacks.
- Reveals hosting environment details.
- Increases attack surface unnecessarily.

Risk Level: High

Recommendation:

- Restrict `/cpanel` access by IP whitelist.
- Move control panel access to a non-standard port or path.
- Enable 2FA on cPanel.
- Consider disabling public access entirely.

🟠 3. Code Quality Issues (Medium Risk)

a) JavaScript Typo

Issue:

```
javascripr:void(0);
```

Expected:

```
javascript:void(0);
```

Impact:

- Button functionality may break.
- Indicates lack of proper QA/code review.

---

b) Missing Resource (404 Error)

Affected Path:

```
/images/slider/
```

Impact:

- Broken UI elements.

- Poor user experience.
- Potential indicator of incomplete deployments.

Risk Level: Medium

Recommendation:

- Fix JavaScript typos.
- Remove unused resource references or restore missing files.
- Enforce code review and pre-release validation.

---

4. Tested Paths Summary

Path	Status	Result
`/admin`	✅ Secure	Returns 404 (Not exposed)
`/cpanel`	❌ Exposed	Redirects to cPanel login
`/phpmyadmin`	✅ Secure	Returns 404

---

5. Forms Security Analysis

📋 Contact Form (`/contact`)

Fields:

- Name
- Email
- Phone
- Subject
- Message

Findings:

- ❌ No CSRF token
- ❌ No visible server-side validation
- ❌ No sanitization evidence

📋 Newsletter Subscription Form

Findings:

- ❌ No CSRF token
- ❌ No rate limiting
- ❌ No validation feedback

---

6. Security Risks Summary

Category	Risk Level
CSRF Vulnerabilities	🔴 High
Control Panel Exposure	🔴 High
Input Validation	🟠 Medium
Code Quality	🟠 Medium
Admin Path Exposure	🟢 Low (Well handled)

---

7. Recommendations

✅ Immediate Actions (High Priority)

1. Implement CSRF protection on all forms
2. Restrict or hide `/cpanel` access
3. Fix JavaScript typo issues
4. Resolve missing static resources

🔍 Further Security Testing Recommended

- XSS testing on all form inputs
- SQL Injection testing on backend form handlers

- Rate limiting & CAPTCHA for public forms
- Server-side input validation review
- Security headers audit (CSP, HSTS, X-Frame-Options)
- File upload testing (if applicable)

---

8. Conclusion

While the application shows some good security practices (admin paths not exposed), **critical vulnerabilities remain** that could be exploited with minimal effort. Addressing CSRF protection and control panel exposure should be treated as **urgent**.

A follow-up security review is strongly recommended after fixes are applied.