Possible CSRF (Cross-site request forgery)

Description

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form which seems vulnerable to CSRF. Consult the 'Attack details' section for more information about the affected HTML form.

Remediation

Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.

The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes.

- The anti-CSRF token should be unique for each user session
- The session should automatically expire after a suitable amount of time
- The anti-CSRF token should be a cryptographically random value of significant length
- The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm
- The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent)
- The server should reject the requested action if the anti-CSRF token fails validation

When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.

References

What is Cross Site Reference Forgery (CSRF)? (https://www.acunetix.com/websitesecurity/csrf-attacks/)

Cross-Site Request Forgery (CSRF) Prevention Cheatsheet (https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html)

The Cross-Site Request Forgery (CSRF/XSRF) FAQ (https://www.cgisecurity.com/csrf-faq.html)

Cross-site Request Forgery (https://en.wikipedia.org/wiki/Cross-site_request_forgery)

Related Vulnerabilities

WordPress Plugin WP Database Backup Cross-Site Request Forgery (4.3.5) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-wp-database-backup-cross-site-request-forgery-4-3-5/)

WordPress Plugin Login Block IPs Cross-Site Request Forgery (1.0.0) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-login-block-ips-cross-site-request-forgery-1-0-0/)

WordPress Plugin WatchMan-Site7 Cross-Site Request Forgery (3.0.2) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-watchman-site7-cross-site-request-forgery-3-0-2/)

WordPress Plugin Pricing Table by Supsystic Cross-Site Request Forgery (1.8.0) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-pricing-table-by-supsystic-cross-site-request-forgery-1-8-0/)

WordPress Plugin WooCommerce Checkout For Digital Goods Cross-Site Request Forgery (2.2) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-woocommerce-checkout-for-digital-goods-cross-site-request-forgery-2-2/)

Severity

LOW

Classification

CWE-352 (https://cwe.mitre.org/data/definitions/352.html)

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
(https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)

Tags

CSRF (https://www.acunetix.com/vulnerabilities/web/tag/csrf/)

Get a demo (https://www.acunetix.com/web-vulnerability-scanner/demo/)






PRODUCT INFORMATION

AcuSensor Technology (https://www.acunetix.com/vulnerability-scanner/acusensor-technology/)

AcuMonitor Technology (https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/)

Acunetix Integrations (https://www.acunetix.com/vulnerability-scanner/acunetix-integrations/)

Vulnerability Scanner (/vulnerability-scanner/)

Support Plans (https://www.acunetix.com/support-plans/)

USE CASES

Penetration Testing Software (https://www.acunetix.com/vulnerability-scanner/penetration-testing-software/)

Website Security Scanner (https://www.acunetix.com/vulnerability-scanner/website-security-scanner/)

External Vulnerability Scanner (https://www.acunetix.com/vulnerability-scanner/external-vulnerability-scanner/)

Web Application Security (https://www.acunetix.com/vulnerability-scanner/web-application-security/)

Vulnerability Management Software (https://www.acunetix.com/vulnerability-scanner/vulnerability-management-software/)

WEBSITE SECURITY

Cross-site Scripting (https://www.acunetix.com/websitesecurity site-scripting/)

SQL Injection (https://www.acunetix.com/websitesecurity injection/)

Reflected XSS (https://www.acunetix.com/websitesecurity

CSRF Attacks (https://www.acunetix.com/websitesecurity attacks/)

Directory Traversal (https://www.acunetix.com/websitesecurity traversal/)

LEARN MORE

White Papers (https://www.acunetix.com/white-papers/)

TLS Security (https://www.acunetix.com/blog/articles/tls-security-what-is-tls-ssl-part-1/)

WordPress Security (https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/)

Web Service Security (https://www.acunetix.com/websitesecurity/web-services-wp/)

COMPANY

About Us (https://www.acunetix.com/about/)

Customers (https://www.acunetix.com/vulnerability-scanner/customers/)

Become a Partner (https://www.acunetix.com/partners/)

Careers (https://www.acunetix.com/careers/)

Contact (https://www.acunetix.com/contact/)

DOCUMENTATION

Case Studies (https://www.acunetix.com/case-studies/)

Support (https://www.acunetix.com/support/)

Videos (https://www.acunetix.com/support/videos

Vulnerability Index (/vulnerabilities)

Webinars (https://www.acunetix.com/webinars/)

Prevent SQL Injection (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)