Cross-Origin Resource Sharing (CORS) Vulnerability

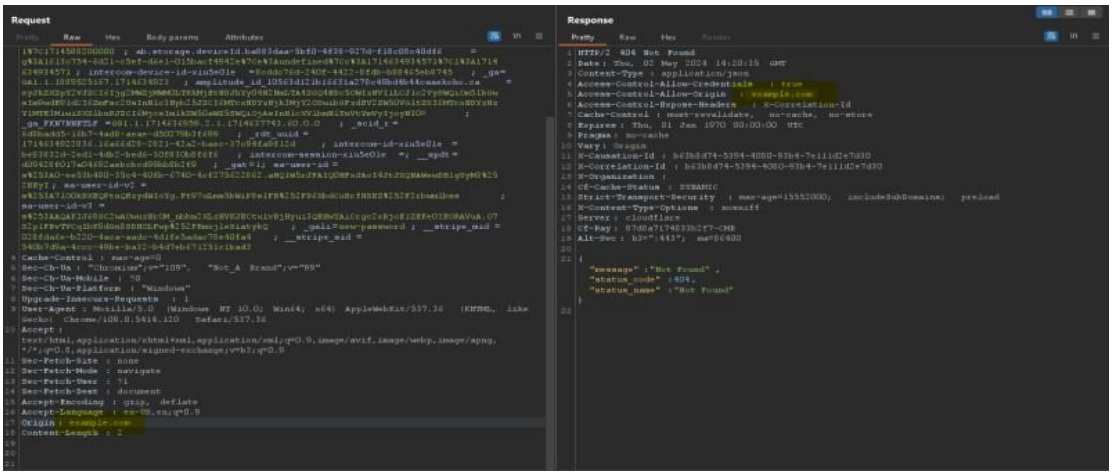
Description:

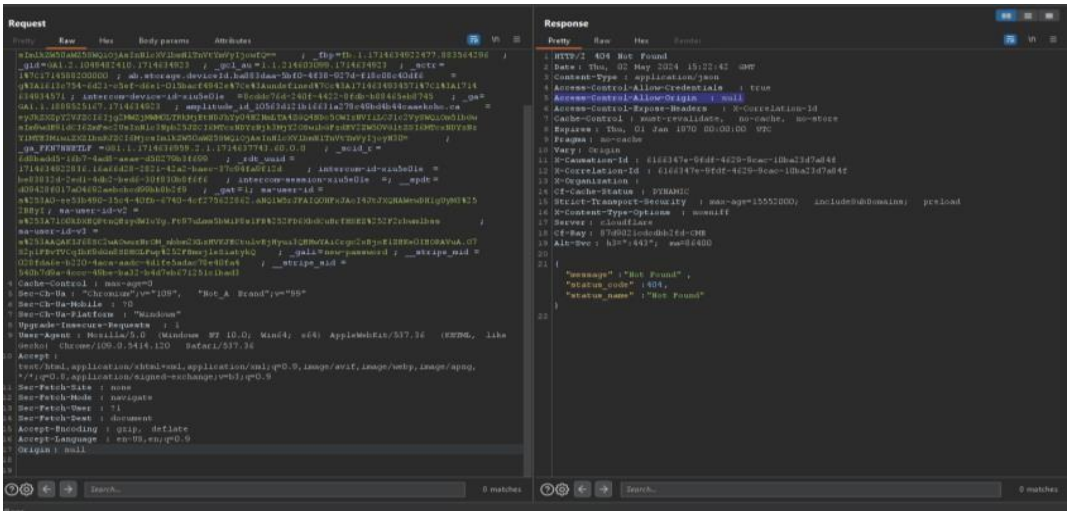
The application's CORS policy allows access from any domain, including the requested origin api.koho.ca/1.0 .The site passing 404 code error but that origin header is allowing untrusted HTTPs.

Affected Components:

The CORS policy of the application.

Proof of Concept:





Proposed Solution:

Whitelisting Origins: Create a whitelist of trusted origins using the Access-Control-Allow-Origin header. Only allow access from domains explicitly permitted to access resources. Avoid setting the header to NULL, as it could expose the application to exploitation by malicious actors.

Method Validation: Specify the HTTP methods allowed for approved origins using the Access-Control-Allow-Methods header. Different domains may need different levels of access. By defining permitted methods, the risk of unauthorized actions can be reduced.

Continuous Monitoring: Regularly check the CORS headers in the application's responses to ensure they align with security policies. Validate these headers to identify any misconfigurations or vulnerabilities. Consider using open-source scanners to automate this process and find potential security issues.

Impact:

Accessing Sensitive Data: Retrieve confidential information from other origins.

Executing CSRF Attacks: Perform unauthorized actions on behalf of authenticated users.

Information Leakage: Disclose sensitive details about the target system.

Session Hijacking: Steal session tokens to impersonate legitimate users.

XSS Exploitation: Facilitate data theft by sending stolen data to remote domains.

Data Manipulation: Modify or delete critical resources on vulnerable servers.

Conclusion:

Securing web applications against CORS-based attacks requires careful configuration and continuous monitoring. By implementing a whitelist-based approach, validating permitted methods, and regularly reviewing CORS headers, organizations can reduce the risk of unauthorized access and protect sensitive data from exploitation.

Response Form HackerOne

scott_brown KOHO staff posted a comment. 6 days ago

Hi @pradhap_r ,

Thank you for submitting this report. It is being triaged now.

Warm regards,

KOHO Security Team