Referer-based access control in an E-commerce webapp

Ref: CVE-2021-21745

Executive Summary

This report summarized the results of a security test conducted on an application's administrative role management system. A Referer-based access control flaw was discovered, allowing a low-privileged user to promote themselves to administrator by manipulating request headers. This vulnerability demonstrates a weak and easily bypassable access control mechanism and poses a **high risk** to the integrity and security of the system.

Introduction

The assessment aimed to evaluate the security of access controls within the administrative functionality of the target web application. Special attention was given to how role changes were authorized and restricted to trusted users.

Methodology

1. Logged in with admin credentials to study admin-only functionality.

2. Intercepted the role promotion request using Burp Suite and examined the HTTP headers.

3. Opened a new incognito window, logged in as a regular user.

4. Used Burp Repeater to replay the admin role promotion request with the non-admin user's session cookie.

5. Manually inserted the Referer header into the request to bypass the access control check.

Vulnerability Findings

- **Type**: Referer-based Access Control Bypass

- **Location**: `/admin-roles?username=<user>&action=upgrade`

- **Severity**: High

Description

The application controlled access to role modification functionality using the Referer HTTP header rather than enforcing proper authentication and authorization on the server side. This allows an attacker to forge the Referer header and escalate privileges by mimicking requests from the admin panel.

Proof of Concept (PoC)

1. As `user`, accessed the admin role endpoint directly:

   pgsql

   CopyEdit

   `GET /admin-roles?username=user&action=upgrade`

   Response: Unauthorized

2. Replayed the request via Burp Repeater using `user`'s session cookie and added:

   arduino

   CopyEdit

   `Referer: https://vulnerable-site.com/admin`

   Response: **Success – Role upgraded to administrator**

Impact Assessment

This vulnerability allowed unauthorized role escalation, granting administrative privileges to a regular user. Attackers could delete users, manipulate data, or access restricted areas. The risk to application integrity and user safety is severe.

Recommendations

1. Never rely on client-supplied headers like Referer for enforcing access control.

2. Implement robust server-side authorization checks to verify user roles before processing privileged actions.

3. Regularly audit access controls to identify logic flaws and enforce the principle of least privilege.

4. Use session-based role verification mechanisms rather than URL or header-dependent logic.

Conclusion

The access control flaw stemming from reliance on the Referer header exposed the application to privilege escalation attacks. Addressing this issue requires reinforcing role verification logic on the server and avoiding trust in user-controllable headers.