Application Security Alert Report

Chrome Web Store

Anti-CSRF Tokens Check

Description

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

* The victim has an active session on the target site.
* The victim is authenticated via HTTP auth on the target site.
* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Risk

High

Reliability

Medium

URLs

1-https://bugs.chromium.org/g/test-corp-mode@google.com/
Evidence: <form method="POST" action="edit.do">

2-https://bugs.chromium.org/p/monorail/adminComponents
Evidence: <form action="adminComponents.do" id="adminComponents" method="POST">

3-https://bugs.chromium.org/p/monorail/adminLabels
Evidence: <form action="adminLabels.do" id="adminLabels" method="POST">

4-https://bugs.chromium.org/p/monorail/adminStatuses
Evidence: <form action="adminStatuses.do" id="adminStatuses" method="POST">

5-https://bugs.chromium.org/p/monorail/adminViews
Evidence: <form action="adminViews.do" id="adminViews" method="POST">

6-https://bugs.chromium.org/p/monorail/components/detail?component=Wizard
Evidence: <form action="detail.do" method="POST">

7-https://bugs.chromium.org/p/monorail/fields/detail?field=sz
Evidence: <form action="detail.do" method="POST">

8-https://bugs.chromium.org/p/monorail/templates/detail?template=Federated+Reference+Setup
Evidence: <form action="detail.do" method="POST">

9-https://bugs.chromium.org/u/60425923/hotlists/andrew-new-hotlist
Evidence: <form>

10-https://bugs.chromium.org/u/60425923/hotlists/hotlist-anti-meta
Evidence: <form>

11-https://bugs.chromium.org/u/60425923/hotlists/andrew-new-hotlist
Evidence: <form id="colspecform" action="andrew-new-hotlist" method="GET" autocomplete="off"
style="display:inline; margin-left:1em">

12-https://bugs.chromium.org/u/60425923/hotlists/hotlist-anti-meta
Evidence: <form id="colspecform" action="hotlist-anti-meta" method="GET" autocomplete="off"
style="display:inline; margin-left:1em">

13-https://bugs.chromium.org/u/60425923/hotlists/hotlist-meta
Evidence: <form>

14-https://bugs.chromium.org/u/60425923/hotlists/hotlist-meta
Evidence: <form id="colspecform" action="hotlist-meta" method="GET" autocomplete="off"
style="display:inline; margin-left:1em">

15-https://bugs.chromium.org/u/60425923/hotlists/workflow-sre
Evidence: <form>

16-https://bugs.chromium.org/u/60425923/hotlists/workflow-sre
Evidence: <form id="colspecform" action="workflow-sre" method="GET" autocomplete="off"
style="display:inline; margin-left:1em">

17-https://bugs.chromium.org/u/dtu@google.com/hotlists/Goose-Hotlist
Evidence: <form>

18-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Hotlist-1
Evidence: <form>

19-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Hotlist-1
Evidence: <form id="colspecform" action="Hotlist-1" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

20-https://bugs.chromium.org/u/dtu@google.com/hotlists/Goose-Hotlist
Evidence: <form id="colspecform" action="Goose-Hotlist" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

21-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Monocharts-LauchBlockers
Evidence: <form>

22-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Monocharts-v2
Evidence: <form>

23-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Monocharts-LauchBlockers
Evidence: <form id="colspecform" action="Monocharts-LauchBlockers" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

24-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Monocharts-v2
Evidence: <form id="colspecform" action="Monocharts-v2" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

25-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Monoperf-Q3
Evidence: <form>

26-https://bugs.chromium.org/u/jeffcarp@chromium.org/hotlists/Monoperf-Q3
Evidence: <form id="colspecform" action="Monoperf-Q3" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

27-https://bugs.chromium.org/u/jojwang@chromium.org/hotlists/v3-API-dogfood
Evidence: <form>

28-https://bugs.chromium.org/u/jojwang@chromium.org/hotlists/v3-API-dogfood
Evidence: <form id="colspecform" action="v3-API-dogfood" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

29-https://bugs.chromium.org/u/pawalls@google.com/hotlists/Monorail-Debt
Evidence: <form>

30-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Bugdroid-GCP-Internship-Rampup
Evidence: <form>

31-https://bugs.chromium.org/u/pawalls@google.com/hotlists/Monorail-Debt
Evidence: <form id="colspecform" action="Monorail-Debt" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

32-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Bugdroid-GCP-Internship-Rampup
Evidence: <form id="colspecform" action="Bugdroid-GCP-Internship-Rampup" method="GET"
autocomplete="off"
 style="display:inline; margin-left:1em">

33-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-Comment-Renovations
Evidence: <form>

34-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-FE-Testing
Evidence: <form>

35-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-Comment-Renovations
Evidence: <form id="colspecform" action="Monorail-Comment-Renovations" method="GET"
autocomplete="off"
 style="display:inline; margin-left:1em">

36-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-FE-Testing
Evidence: <form id="colspecform" action="Monorail-FE-Testing" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

37-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-Git-Integration
Evidence: <form>

38-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-ProductExcellence
Evidence: <form>

39-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-Git-Integration
Evidence: <form id="colspecform" action="Monorail-Git-Integration" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

40-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-ProductExcellence
Evidence: <form id="colspecform" action="Monorail-ProductExcellence" method="GET" autocomplete="off"
 style="display:inline; margin-left:1em">

41-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Tiffs-Monorail-Backlog
Evidence: <form>

42-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-SPA-Rewrite-Starter-Bugs
Evidence: <form>

43-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Tiffs-Monorail-Backlog
Evidence: <form id="colspecform" action="Tiffs-Monorail-Backlog" method="GET" autocomplete="off"
style="display:inline; margin-left:1em">

44-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/Monorail-SPA-Rewrite-Starter-Bugs
Evidence: <form id="colspecform" action="Monorail-SPA-Rewrite-Starter-Bugs" method="GET"
autocomplete="off"
style="display:inline; margin-left:1em">

45-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/zhangtiff-impact
Evidence: <form>

46-https://bugs.chromium.org/u/zhangtiff@chromium.org/hotlists/zhangtiff-impact
Evidence: <form id="colspecform" action="zhangtiff-impact" method="GET" autocomplete="off"
style="display:inline; margin-left:1em">

Solution

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation
Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design
Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).
Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.
This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation
Check the HTTP Referer header to see if the request originated from an expected page. This could break

legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

References

http://projects.webappsec.org/Cross-Site-Request-Forgery
http://cwe.mitre.org/data/definitions/352.html