

#BugBounty @ LinkedIn-How I was able to bypass Open Redirection Protection



Avinash Jain (@logicbomb_1)

Follow

Jan 24, 2018 · 3 min read

Hi Guys,

Here I'll be talking about a nice vulnerability that I found couple of months ago in LinkedIn. Before jumping into the vulnerability, let me quickly brief you about Open Redirection-

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain. An example of a vulnerable website link could look something like this: <http://xyz.com/login.html?vulparam=https://xyz.com/next>

In this example, “vulparam” parameter indicates where to send user upon successful login. If website doesn’t validate the “vulparam” parameter value to make sure that target web page is legitimate and intended, attacker could manipulate that parameter to send a victim to a fake page crafted by attacker:
<https://xyzcom/login.html?vulparam=http://evil.com>

But bypassing LinkedIn open redirection was not that easy. The vulnerable URL was —

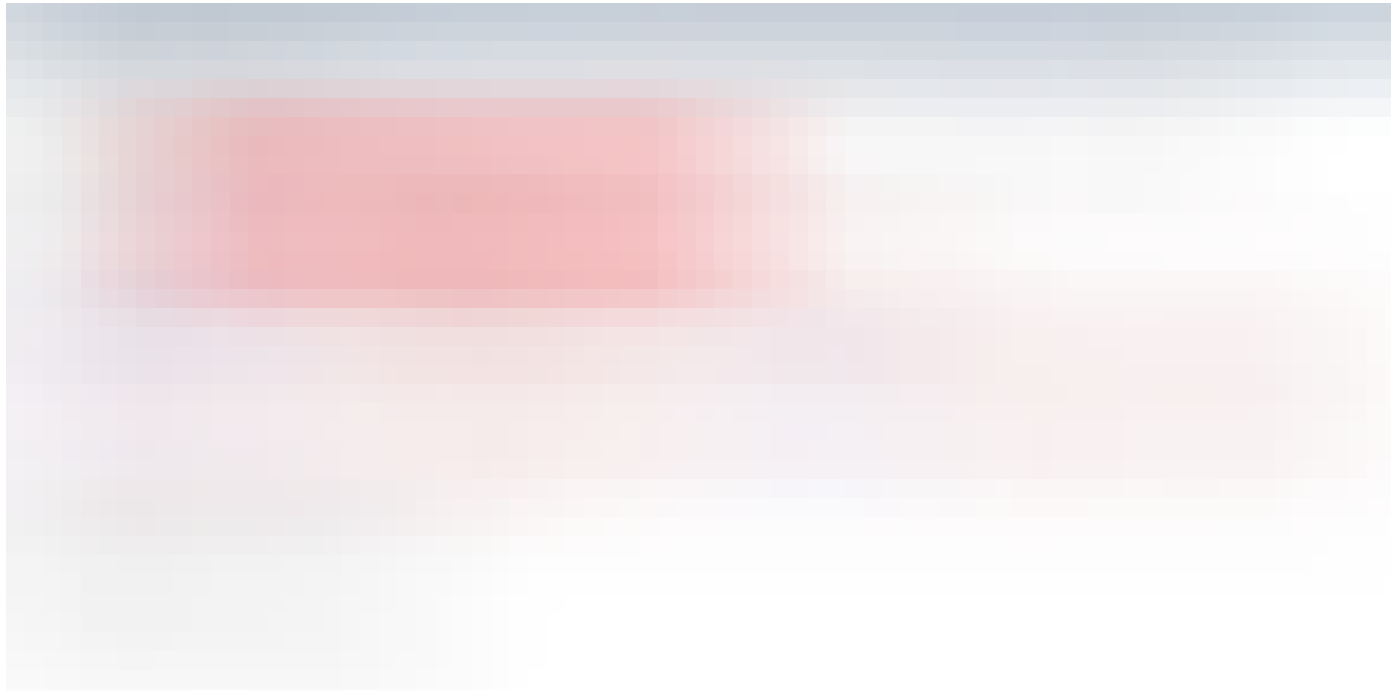
<https://www.linkedin.com/lite/external-redirect?url=http://evilzone.org&urlHash=YKI5>

LinkedIn has indeed some good protection against open redirection since I was not able to bypass using some common techniques like

url=../evilzone.org , url= ///evilzone.org , url= ///www.linkedin.com@www.evilzone.org/%2f%2e%2e

Now simply changing the “url” value to any malicious site won’t work here. As you can see there is an extra parameter “urlHash” which looks like some hash

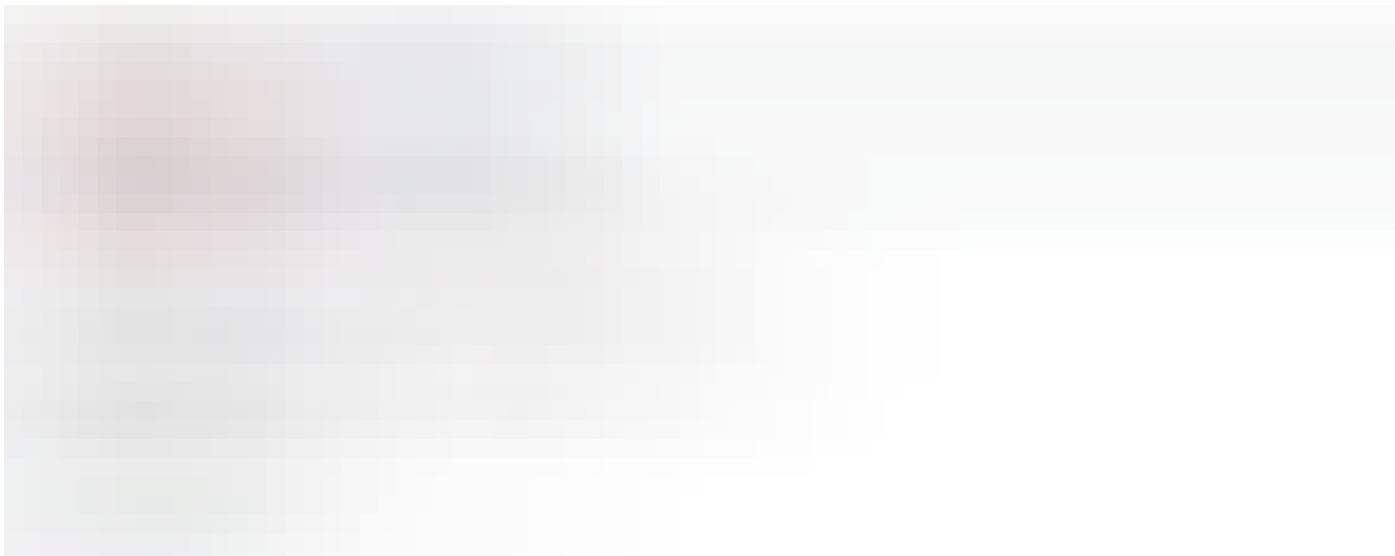
value for the URL to which the user getting redirected so if “urlHash” value is the actual valid hash value for the “url” then only successful redirection will take place. One thing was clear till now basic techniques were not going to do anything good and then I went back to the raw request to find some help —



Open Redirection Raw Request

The request includes the “referrer” field, which indicates the last page the user was on (the one where they clicked the link) and here something struck my mind- “How about changing the referrer header value and see whether the validation working there?” . So I quickly jumped into it and changed the header value to some other domains and [face palm] still no luck. :/ .

Let’s give one more try , I searched for LinkedIn android app referrer and found the following link- <https://github.com/snowplow/referer-parser/issues/131> and there came across LinkedIn android referrer value as “*android-app://com.linkedin.android*” . I used the referrer value in the “referrer” header field and the rest is as below :D —





Successful redirection and yeah finally I managed to bypass the Open redirection protection of LinkedIn :)

Report details-

11-Nov-2017—Bug reported to the concerned company.

07-Dec-2017—Bug was marked fixed.

21-Dec-2017—Re-tested and confirmed the fix.

Thanks for reading!

~Logicbomb (https://twitter.com/logicbomb_1)

[Vulnerability](#)[Bug Bounty](#)[LinkedIn](#)[Hacking](#)[Information Security](#)

449 claps



5



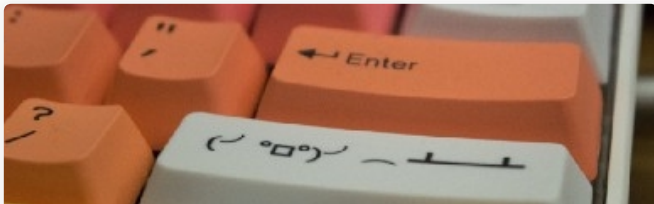
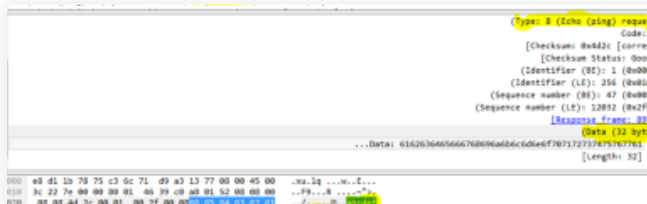
...

**Avinash Jain**
(@logicbomb_1)[Follow](#)

Lead Infrastructure
Security Engineer
@groferseng | DevSecops
| Part time BugBounty
Hunter | Acknowledged
by Google, NASA, Yahoo,
United Nations, BBC etc.

**InfoSec Write-ups**[Follow](#)

A collection of write-ups
from the best hackers in
the world on topics
ranging from bug
bounties and CTFs to
vulnhub machines,
hardware challenges and
real life encounters. In a
nutshell, we are the
largest InfoSec
publication on Medium.
#sharingiscaring

[More from InfoSec Write-ups](#)**Writing a Password Protected Bind
Shell (Linux/x64)**[More from InfoSec Write-ups](#)**Ping Power—ICMP Tunnel**[More from InfoSec Write-ups](#)**How to Make a Captive Portal of
Death**



0x0FFB347

Mar 8 · 5 min read

246



Nir Chako

Dec 17, 2018 · 8 min read

488




Trevor Phillips

Dec 18, 2018 · 6 min read

280



Responses

 Write a response...

Conversation with Avinash Jain (@logicbomb_1).



Apurve Jain

Jan 27, 2018

LinkedIn android referer value as “ android-app://com.linkedin.android

Didnt understood one thing u used android app link as refer value and in get parameter u used evil.com url ?am i right ?

1

1 response 



Avinash Jain (@logicbomb_1)

Jan 27, 2018

Didnt understood one thing u used android app link as refer value and in get parameter u used evil.com url ?am i right ?

Yes, you are right. Whenever user was visiting their page from that specific header, they were not verifying it for the redirection. May be they have some whitelisting of domains.

52



Conversation with Avinash Jain (@logicbomb_1).



Sarthak Tanwani

Feb 5, 2018

The request includes the “referrer” field, which indicates the last page the user was on (the one where they clicked the link) and here something striked my mind- “How about changing ...

What were you expecting to happen by changing the referer header?

1

1 response





Avinash Jain (@logicbomb_1)

Feb 5, 2018

To check whether the open direction protection based on referer header. They might have some whitelisting of domains.



Conversation with Avinash Jain (@logicbomb_1).



Federico R

Mar 26, 2018

If you are writing a report of your finding and then we all have to guess what exactly was placed in Burp to bypass the open redirection It is not really detailed. You should update this article with an exact screen capture showing what was sent as well.

1 response



Avinash Jain (@logicbomb_1)

Mar 26, 2018

Sure will do it. 😊



Show all responses