#BugBounty — Exploiting CRLF Injection can lands into a nice bounty

Avinash Jain (@logicbomb_1) Follow
Feb 17, 2018 · 2 min read

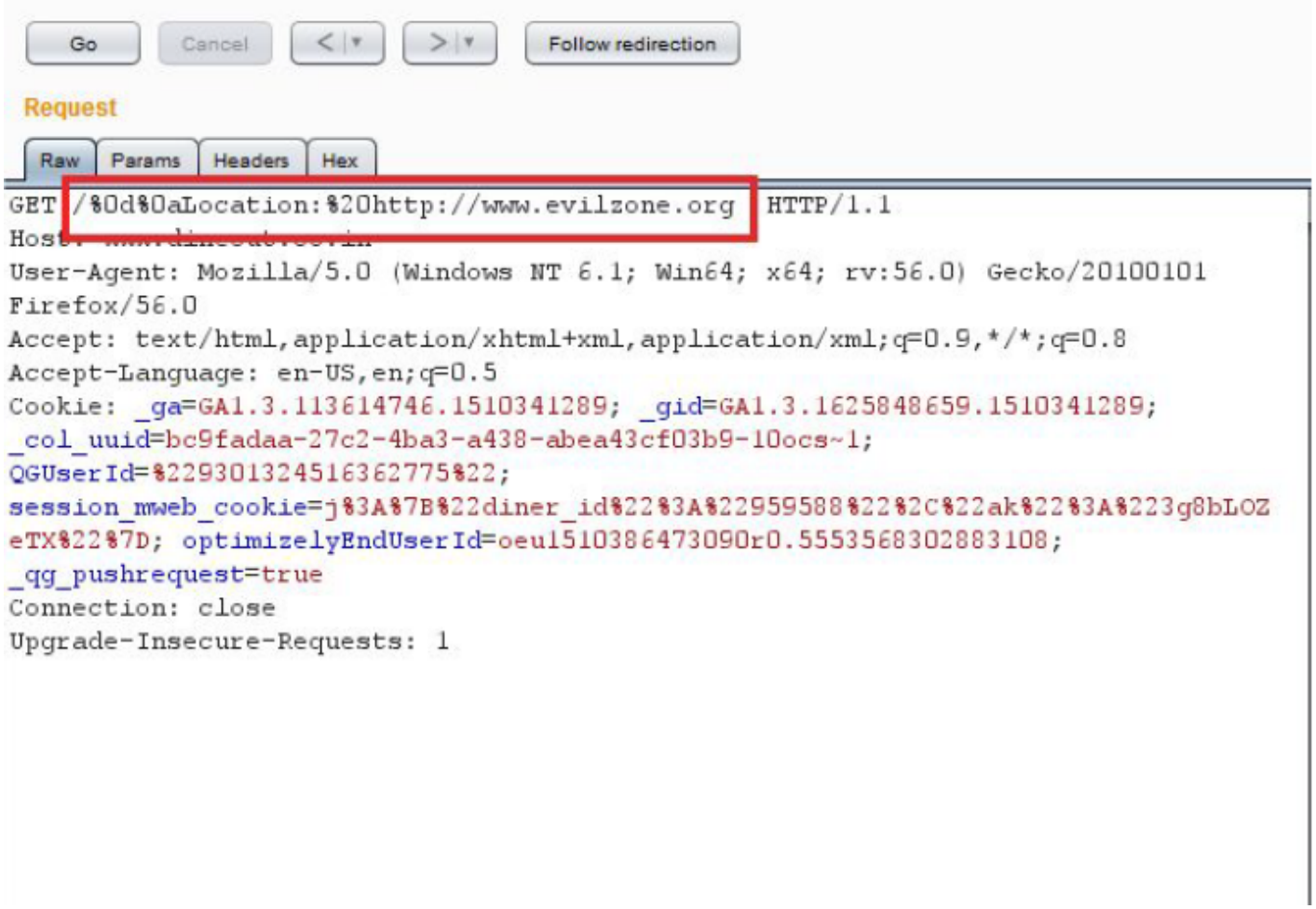
Hi Guys,

Back with one more blog and this time I would be sharing my experience of exploiting CRLF injection and how it lands me to a good bounty.

> *CRLF Injection Vulnerability is a web application vulnerability happens due to direct passing of user entered data to the response header fields like (Location, Set-Cookie and etc) without proper sanitsation, which can result in various forms of security exploits.Security exploits range from XSS, Cache-Poisoning, Cache-based defacement,page injection and etc.*

So this comes in an Online Food Delivery company of India while searching for some security loophole in their website. In their home page, there are a

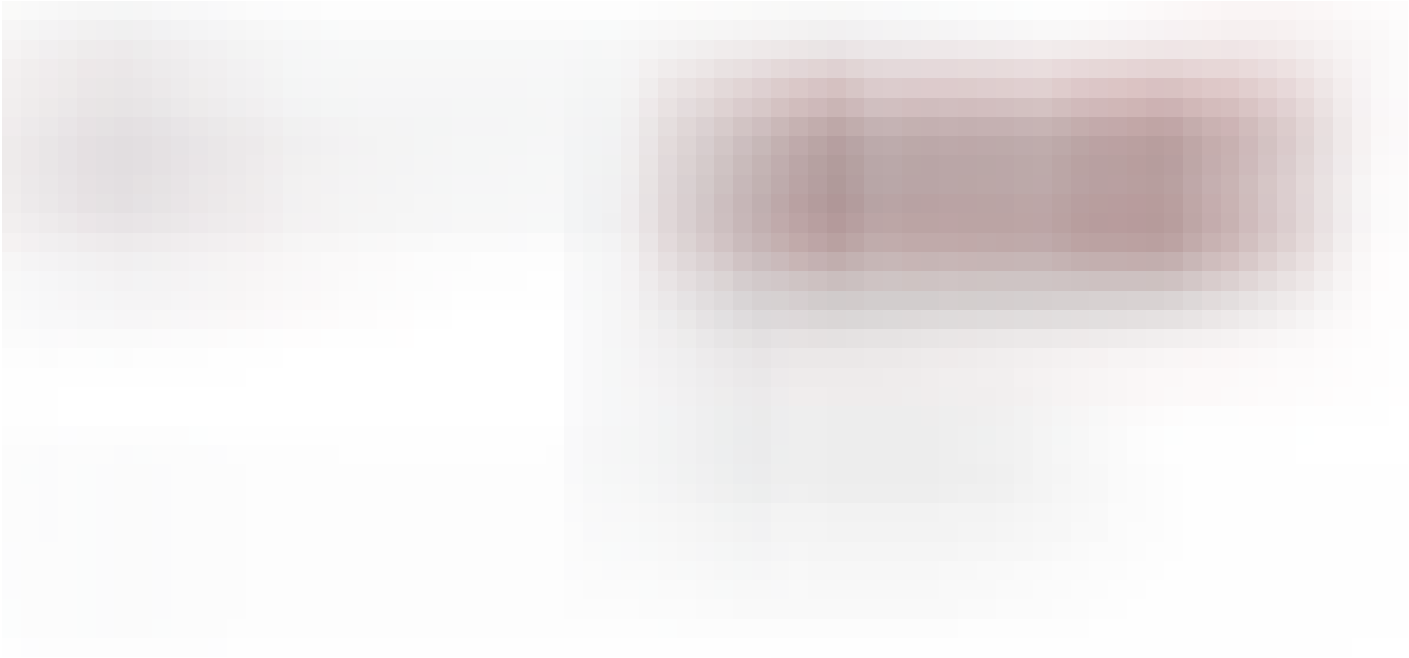
couple of inputs being reflected into the HTTP Headers . After a bit of fiddling, I discovered that non-printable control characters were not encoded which they should be, which took me to try for CRLF and I tried to add “Location” header to see whether it was getting redirected. Below is the POC —



Now the Server responds to this request by injecting the CRLF characters in the response , you will find “Location” http header has been set in the http response with the value “http://www.evilzone.org” as injected via the CRLF payload in the below screesnshot—

CRLF Injection

and the successful redirection was taking place to the attacker site -”evilzone.org”.



Successful Redirection via CRLF Injection

Impact of CRLF Injection vary and also include all the impacts of Cross-site Scripting to information disclosure. It can also deactivate certain security restrictions like XSS Filters and the Same Origin Policy in the victim's browsers, leaving them susceptible to malicious attacks.

Mitigation Techniques-

A simple solution for CRLF Injection is to sanitise the CRLF characters before passing into the header or to encode the data which will prevent the CRLF sequences entering the header.

Report details-

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

06-Dec-2017—Bug was marked fixed.

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

20-Dec-2017—Awarded by company (USD 250).

Thanks for reading!

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

Hacking | Ethical Hacking | Bug Bounty | Penetration Testing | Vulnerability

Avinash Jain (@logicbomb_1) Follow

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

More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)

0x0FFB347
Mar 8 · 5 min read
246

More from InfoSec Write-ups

Ping Power—ICMP Tunnel

Nir Chako
Dec 17, 2018 · 8 min read
488

More from InfoSec Write-ups

How to Make a Captive Portal of Death

Trevor Phillips
Dec 18, 2018 · 6 min read
280

Responses

Write a response...

Applause from Avinash Jain (@logicbomb_1) (author)

Ak1T4
Feb 17, 2018

nice write, you could try too cookies injection manipulation

6

Applause from Avinash Jain (@logicbomb_1) (author)

crhua
Apr 20, 2018

it's good job.

3

Conversation with Avinash Jain (@logicbomb_1).

Dipanjan Das

Jul 8, 2018

Unless you have a time-machine, the last two dates in the “Report Details” timeline seem to be in the future!

1 response

Avinash Jain (@logicbomb_1)
Jul 8, 2018

lol. Corrected it! Thanks :)

Show all responses