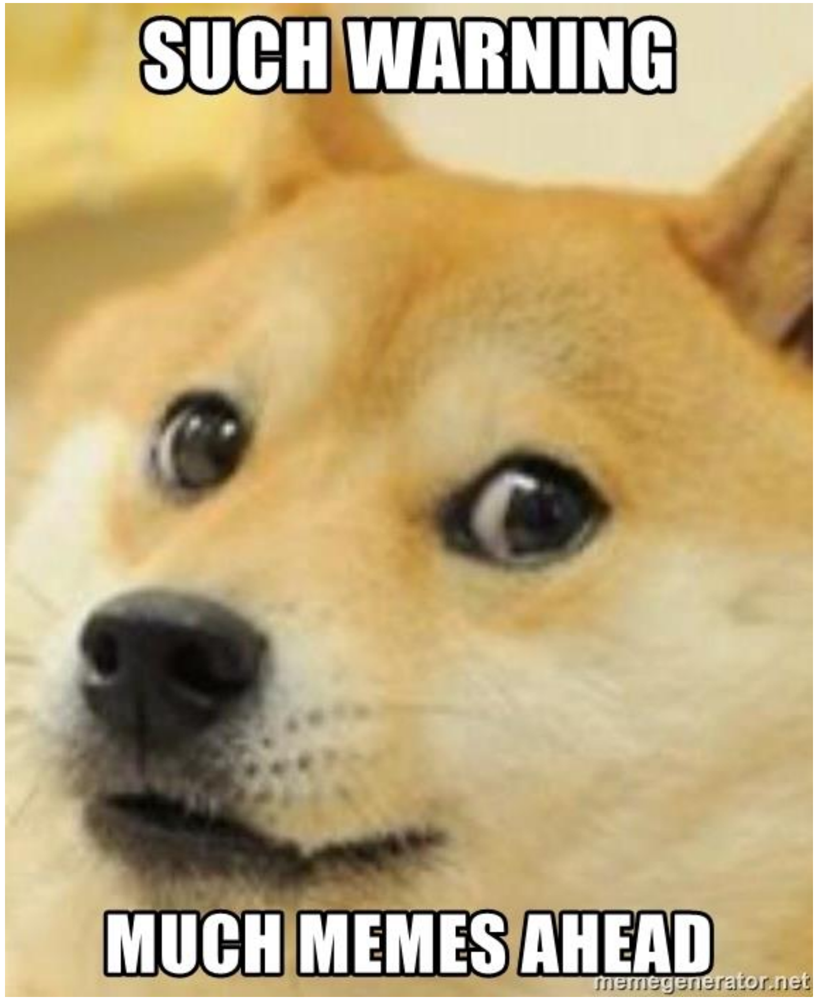
Tales from Failures …

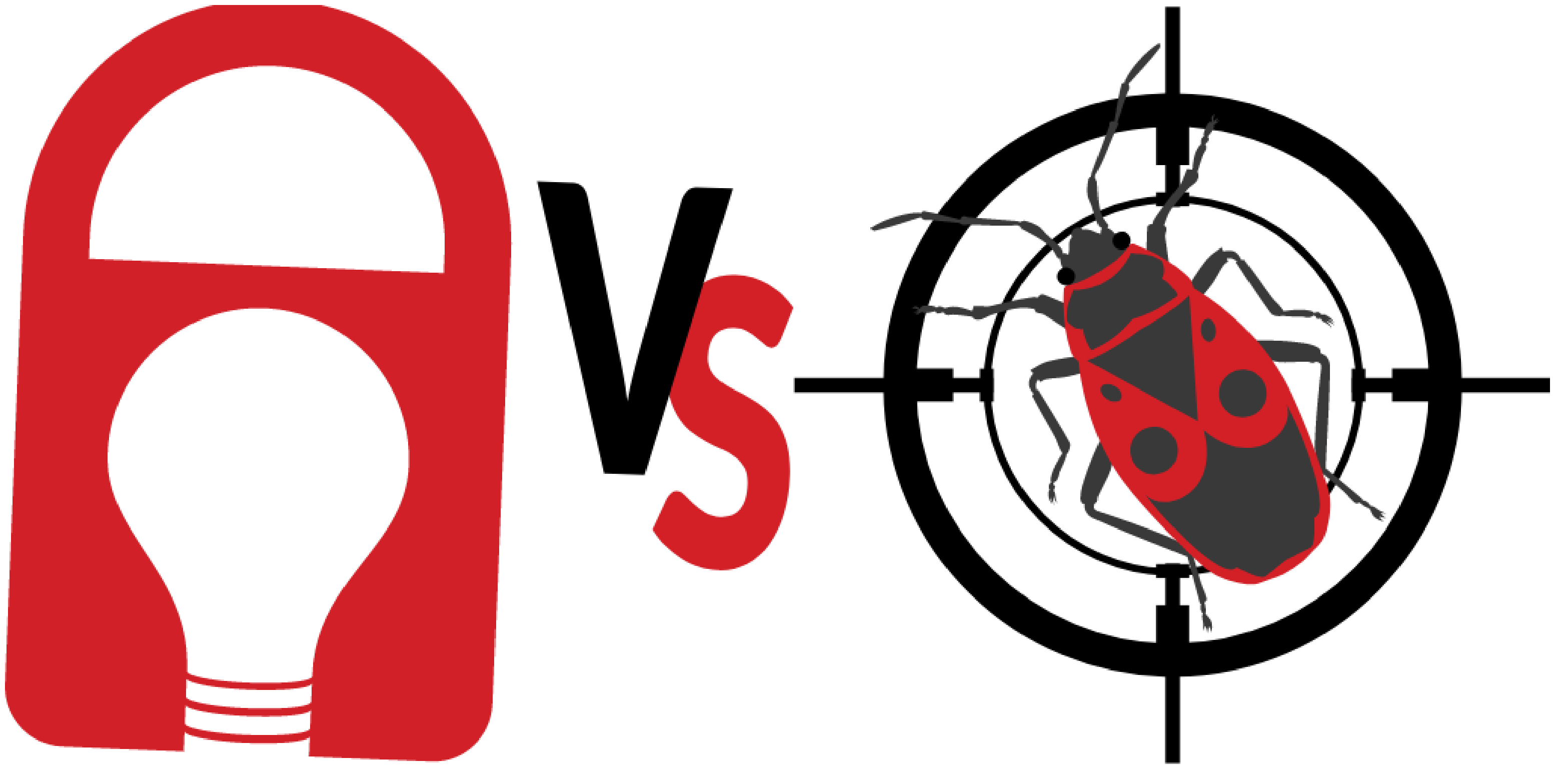
BeeFaauBee

Bug Bounty Hunter / Security Researcher

Important Public Warning !



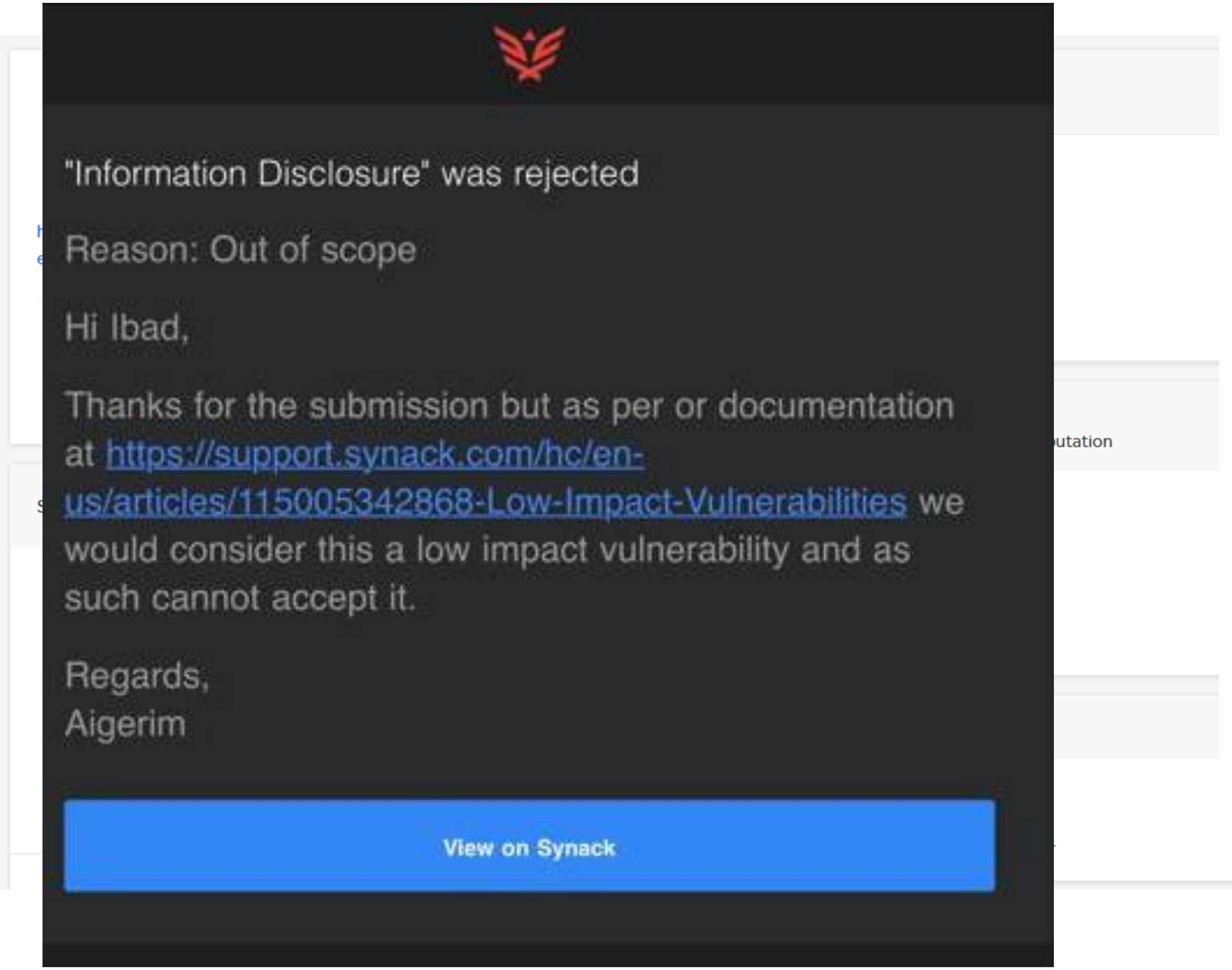
Pentest != Bug Bounties



Dude ! Who are you ?

- Head of Cyber Security at Banking Sector in Pakistan, Security Researcher, Developer
- Mobile, Web applications
- IoT and ARM
- Sometimes Speak at Public Forums

“There’s no short-cut to bug bounties,
You will always learn if you’re investing great amount of efforts and energy” - Stok



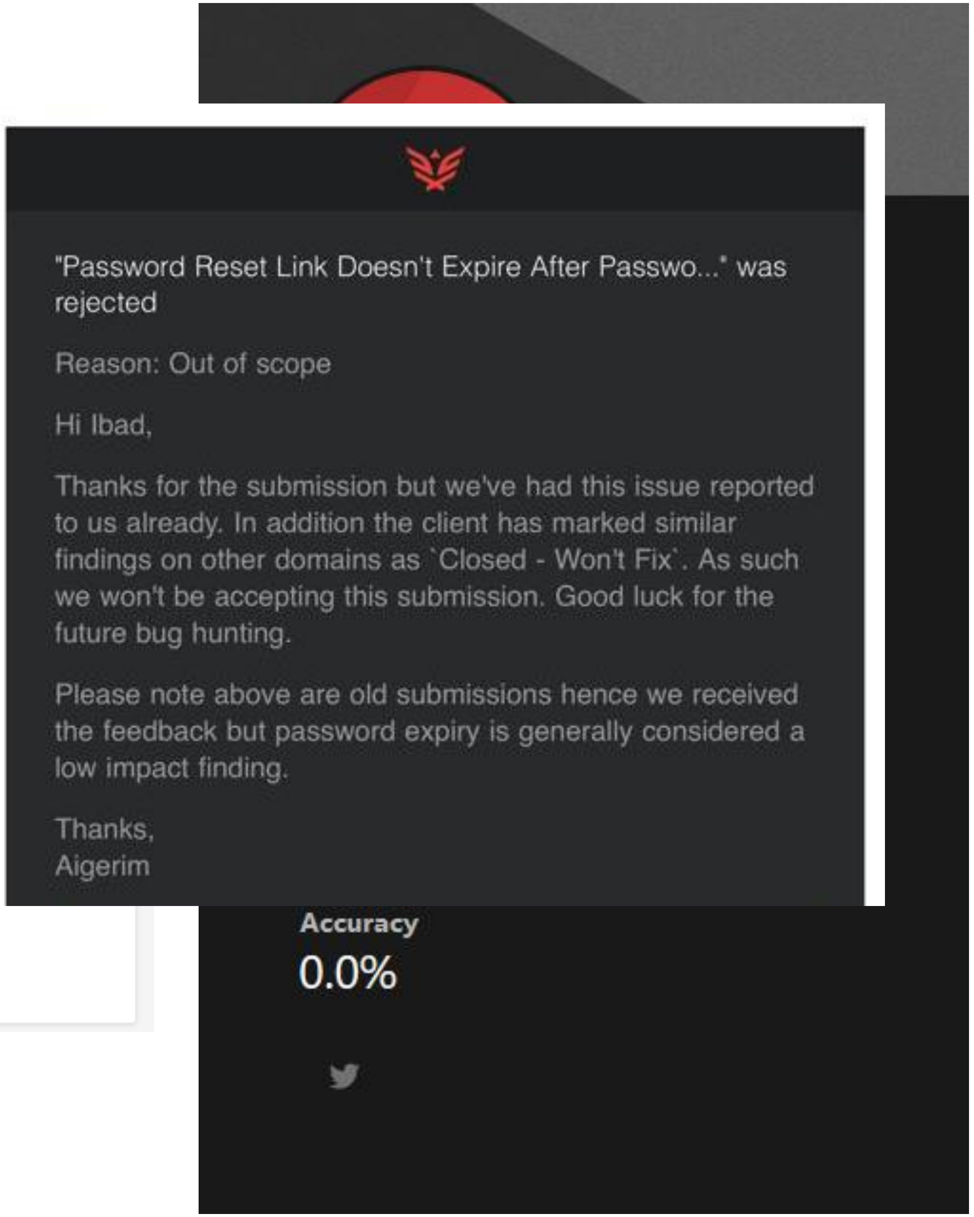
"Information Disclosure" was rejected

Reason: Out of scope

Hi Ibad,

Thanks for the submission but as per or documentation at https://support.synack.com/hc/en-us/articles/115005342868-Low-Impact-Vulnerabilities we would consider this a low impact vulnerability and as such cannot accept it.

Regards,
Aigerim



"Password Reset Link Doesn't Expire After Passwo..." was rejected

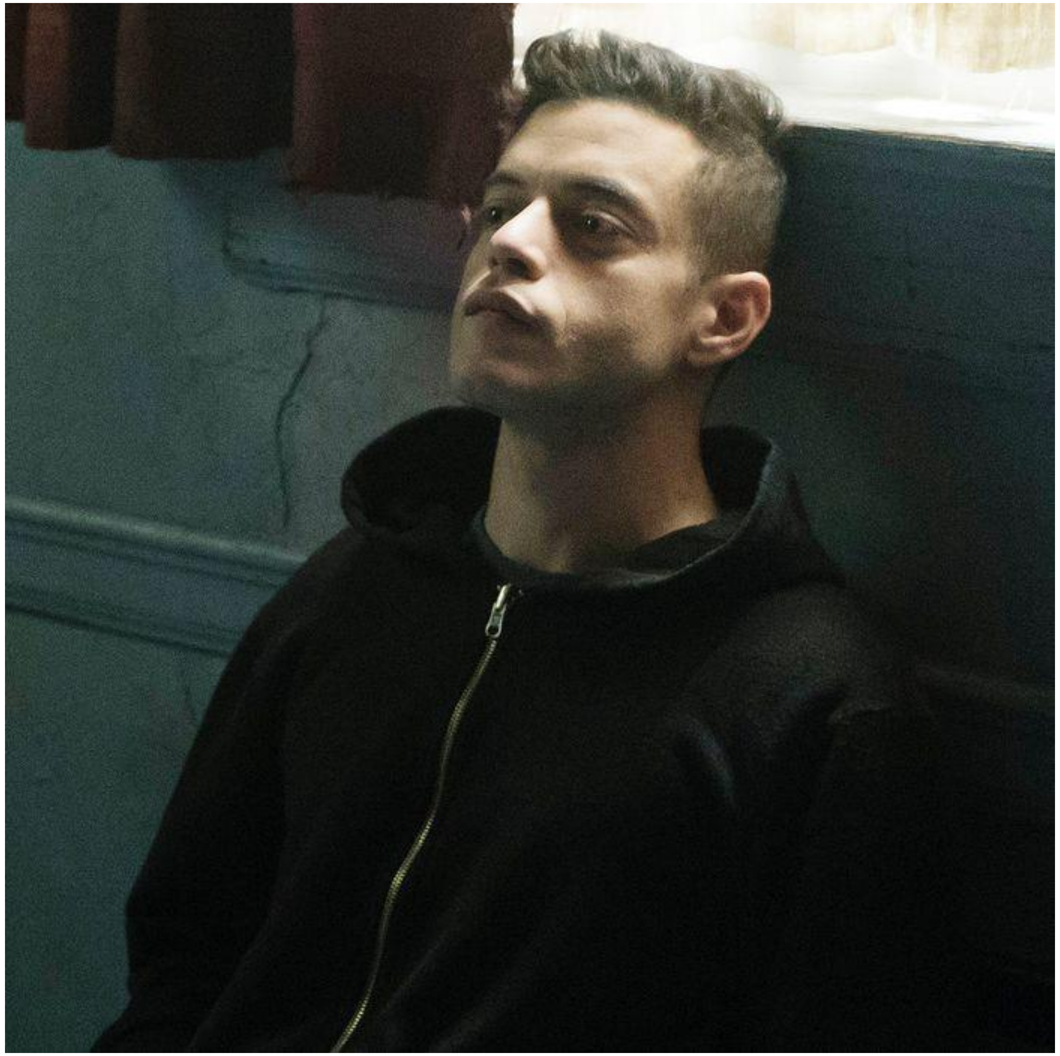
Reason: Out of scope

Hi Ibad,

Thanks for the submission but we've had this issue reported to us already. In addition the client has marked similar findings on other domains as `Closed - Won't Fix`. As such we won't be accepting this submission. Good luck for the future bug hunting.

Please note above are old submissions hence we received the feedback but password expiry is generally considered a low impact finding.

Thanks,
Aigerim



“Celebrate Your Failures” - Stok

Discovery To Disclosure

Journey from Discovering Vulnerabilities
Towards Disclosure

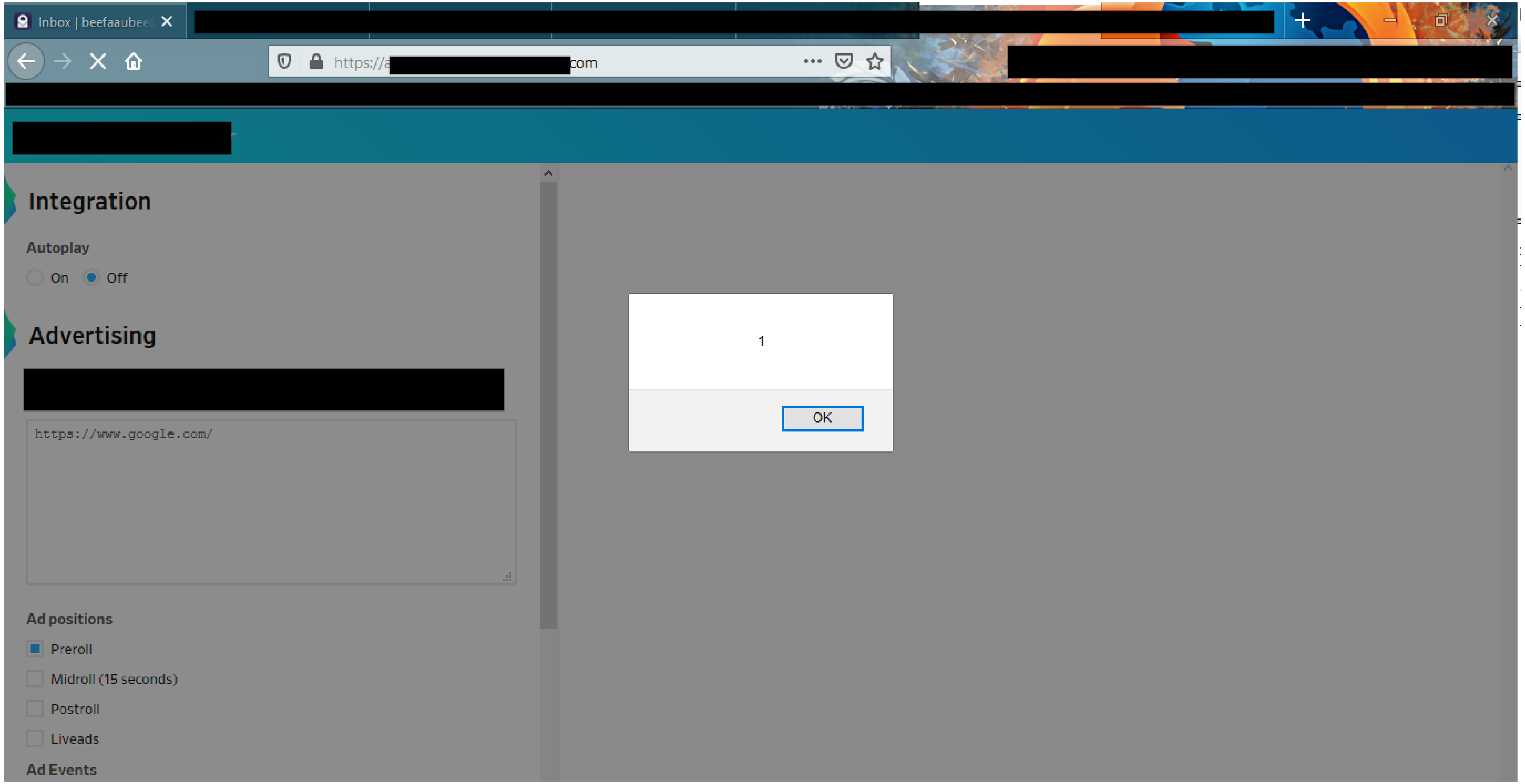
BeeFaauBee, Security Researcher
hello@beefaaubee.com
Twitter : @BeeFaauBee09

CorpApp.apk

Attack Scenario 3

- Marketing API inside APK
- Discovered other domains
- Access to Internal Portals

Lesson #1 : Know Impact



Integration

Autoplay

○ On ● Off

Advertising

[redacted]

```
https://www.google.com/
```

Ad positions

☑ Preroll

□ Midroll (15 seconds)

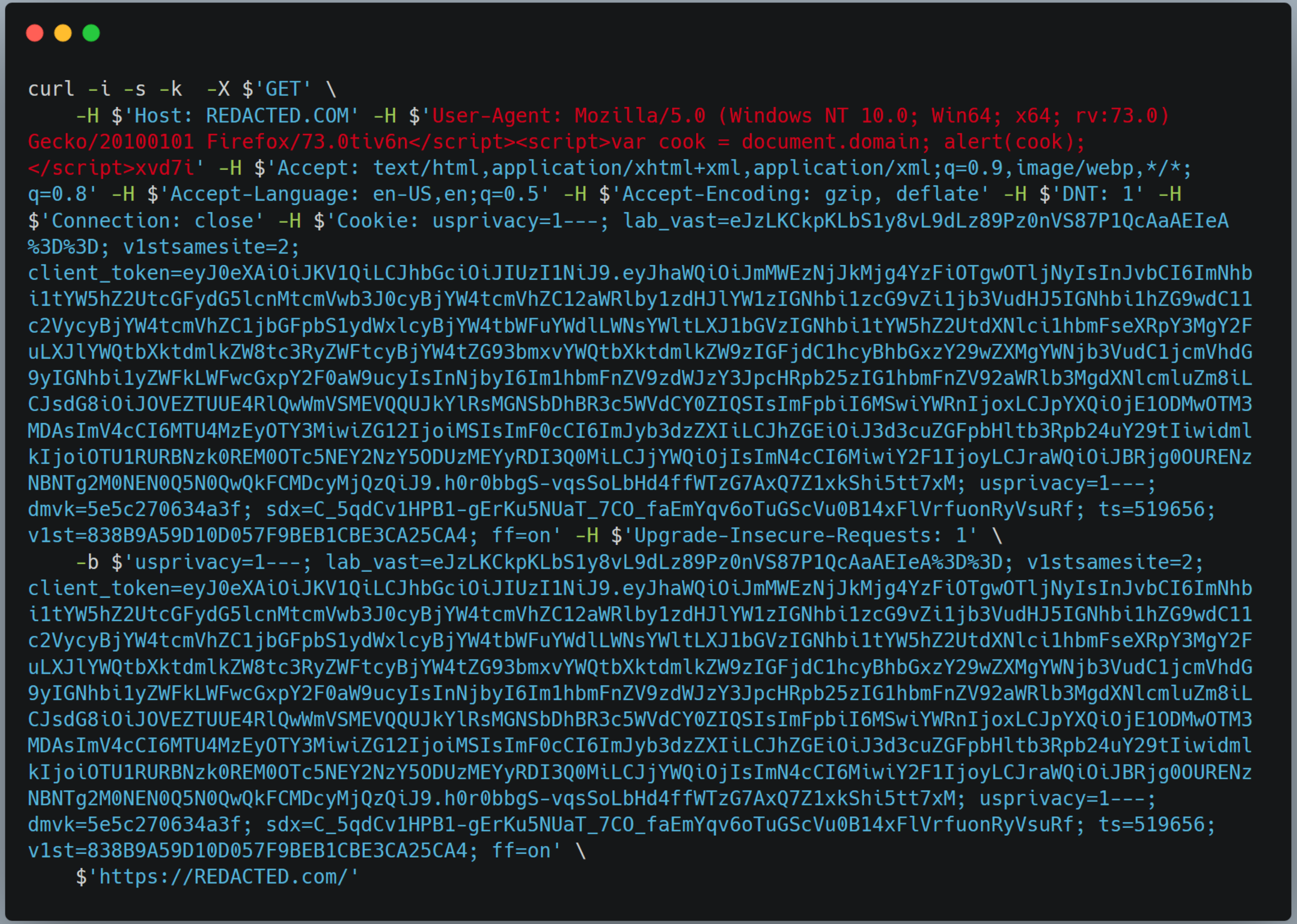
□ Postroll

□ Liveads

Ad Events

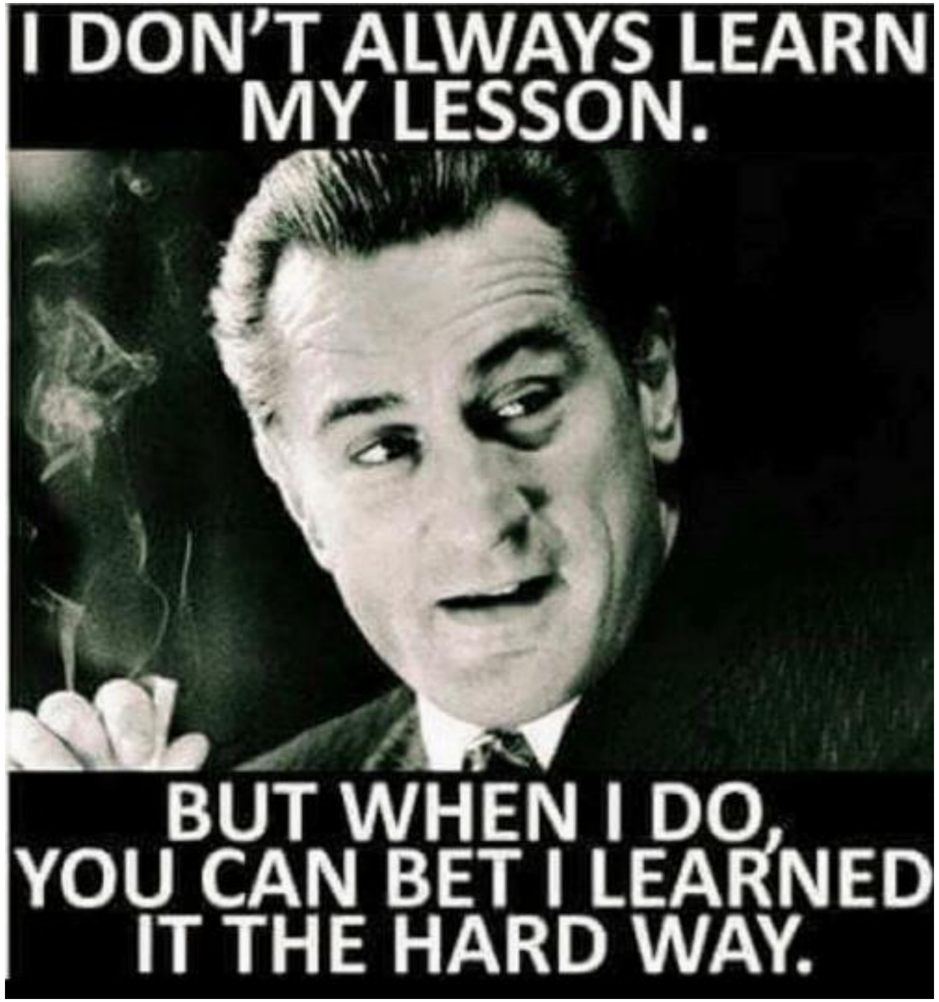
1

Lesson #1 : Know Impact



```
curl -i -s -k  -X $'GET' \
    -H $'Host: REDACTED.COM' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0)
Gecko/20100101 Firefox/73.0tiv6n</script><script>var cook = document.domain; alert(cook);
</script>xvd7i' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'DNT: 1' -H
$'Connection: close' -H $'Cookie: usprivacy=1---; lab_vast=eJzLKCkpKLbS1y8vL9dLz89Pz0nVS87P1QcAaAEIeA
%3D%3D; v1stsamesite=2;
client_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhaWQiOiJmMWEzNjJkMjg4YzFiOTgwOTljNyIsInJvbCI6ImNhb
i1tYW5hZ2UtcGFydG5lcnMtcmVwb3J0cyBjYW4tcmVhZC12aWRlby1zdHJlYW1zIGNhbi1zcG9vZi1jb3VudHJ5IGNhbi1hZG9wdC11
c2VycyBjYW4tcmVhZC1jbGFpbS1ydWxlcyBjYW4tbWFuYWdlLWNsYWltLXJ1bGVzIGNhbi1tYW5hZ2UtdXNlci1hbmFseXRpY3MgY2F
uLXJlYWQtbXktdmlkZW8tc3RyZWFtcyBjYW4tZG93bmxvYWQtbXktdmlkZW9zIGFjdC1hcyBhbGxzY29wZXMgYWNjb3VudC1jcmVhdG
9yIGNhbi1yZWFkLWFwcGxpY2F0aW9ucyIsInNjbyI6Im1hbmFnZV9zdWJzY3JpcHRpb25zIG1hbmFnZV92aWRlb3MgdXNlcmluZm8iL
CJsdG8iOiJOVEZTUUE4RlQwWmVSMEVQQUJkYlRsMGNSbDhBR3c5WVdCY0ZIQSIsImFpbiI6MSwiYWRnIjoxLCJpYXQiOjE1ODMwOTM3
MDAsImV4cCI6MTU4MzEyOTY3MiwiZG12IjoiMSIsImF0cCI6ImJyb3dzZXIiLCJhZGEiOiJ3d3cuZGFpbHltb3Rpb24uY29tIiwidml
kIjoiOTU1RURBNzk0REM0OTc5NEY2NzY5ODUzMEYyRDI3Q0MiLCJjYWQiOjIsImN4cCI6MiwiY2F1IjoyLCJraWQiOiJBRjg0OURENz
NBNTg2M0NEN0Q5N0QwQkFCMDcyMjQzQiJ9.h0r0bbgS-vqsSoLbHd4ffWTzG7AxQ7Z1xkShi5tt7xM; usprivacy=1---;
dmvk=5e5c270634a3f; sdx=C_5qdCv1HPB1-gErKu5NUaT_7CO_faEmYqv6oTuGScVu0B14xFlVrfuonRyVsuRf; ts=519656;
v1st=838B9A59D10D057F9BEB1CBE3CA25CA4; ff=on' -H $'Upgrade-Insecure-Requests: 1' \
    -b $'usprivacy=1---; lab_vast=eJzLKCkpKLbS1y8vL9dLz89Pz0nVS87P1QcAaAEIeA%3D%3D; v1stsamesite=2;
client_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhaWQiOiJmMWEzNjJkMjg4YzFiOTgwOTljNyIsInJvbCI6ImNhb
i1tYW5hZ2UtcGFydG5lcnMtcmVwb3J0cyBjYW4tcmVhZC12aWRlby1zdHJlYW1zIGNhbi1zcG9vZi1jb3VudHJ5IGNhbi1hZG9wdC11
c2VycyBjYW4tcmVhZC1jbGFpbS1ydWxlcyBjYW4tbWFuYWdlLWNsYWltLXJ1bGVzIGNhbi1tYW5hZ2UtdXNlci1hbmFseXRpY3MgY2F
uLXJlYWQtbXktdmlkZW8tc3RyZWFtcyBjYW4tZG93bmxvYWQtbXktdmlkZW9zIGFjdC1hcyBhbGxzY29wZXMgYWNjb3VudC1jcmVhdG
9yIGNhbi1yZWFkLWFwcGxpY2F0aW9ucyIsInNjbyI6Im1hbmFnZV9zdWJzY3JpcHRpb25zIG1hbmFnZV92aWRlb3MgdXNlcmluZm8iL
CJsdG8iOiJOVEZTUUE4RlQwWmVSMEVQQUJkYlRsMGNSbDhBR3c5WVdCY0ZIQSIsImFpbiI6MSwiYWRnIjoxLCJpYXQiOjE1ODMwOTM3
MDAsImV4cCI6MTU4MzEyOTY3MiwiZG12IjoiMSIsImF0cCI6ImJyb3dzZXIiLCJhZGEiOiJ3d3cuZGFpbHltb3Rpb24uY29tIiwidml
kIjoiOTU1RURBNzk0REM0OTc5NEY2NzY5ODUzMEYyRDI3Q0MiLCJjYWQiOjIsImN4cCI6MiwiY2F1IjoyLCJraWQiOiJBRjg0OURENz
NBNTg2M0NEN0Q5N0QwQkFCMDcyMjQzQiJ9.h0r0bbgS-vqsSoLbHd4ffWTzG7AxQ7Z1xkShi5tt7xM; usprivacy=1---;
dmvk=5e5c270634a3f; sdx=C_5qdCv1HPB1-gErKu5NUaT_7CO_faEmYqv6oTuGScVu0B14xFlVrfuonRyVsuRf; ts=519656;
v1st=838B9A59D10D057F9BEB1CBE3CA25CA4; ff=on' \
    $'https://REDACTED.com/'
```

Lesson #1 : Know Impact


I DON'T ALWAYS LEARN MY LESSON.
BUT WHEN I DO, YOU CAN BET I LEARNED IT THE HARD WAY.

- No Way of Exploiting User-Agents until its MITM
- Closed/Not Applicable

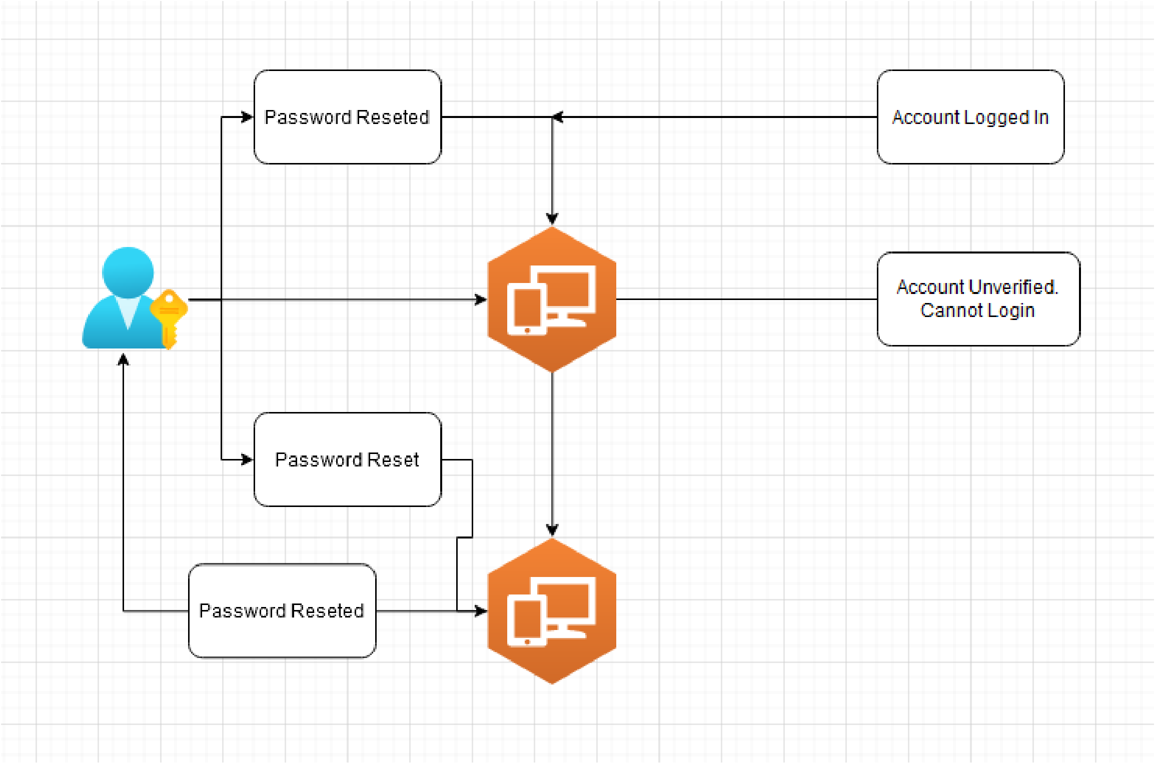
Lesson #2 : Never Give Up

Lesson #2 : Never Give Up

90 Reports Submitted
20 Validated

But Then ….

Scenario 1
Account Verification Bypass



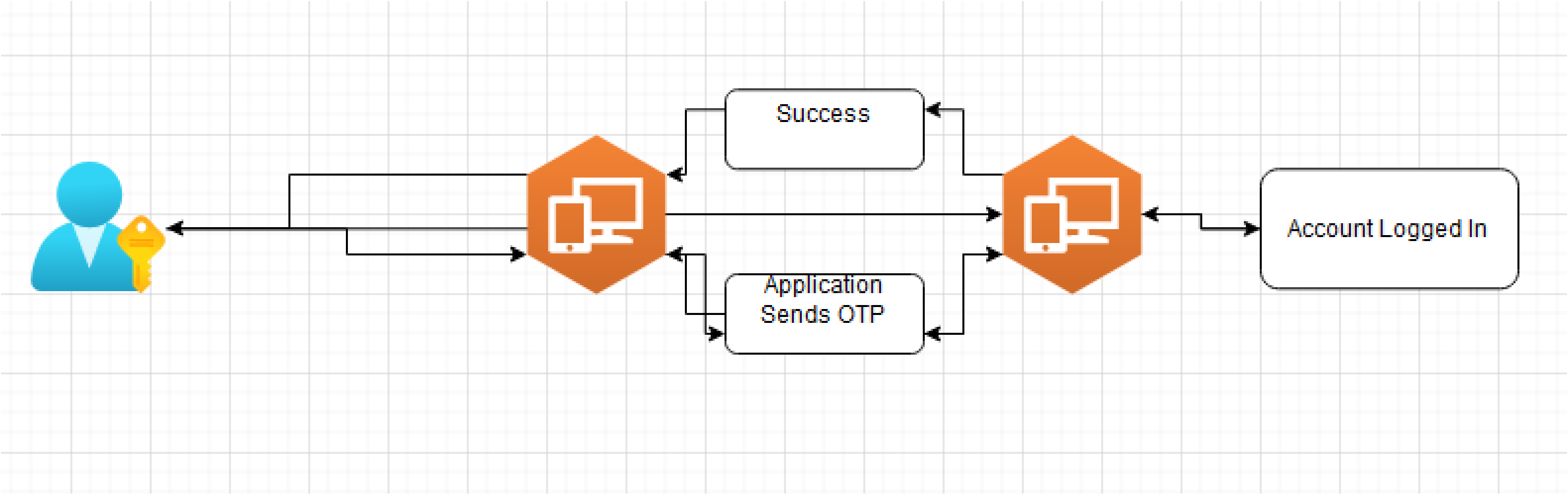
Lesson #2 : Never Give Up

90 Reports Submitted
20 Validated

But Then ….

Scenario 2

Old OTP
Reuse

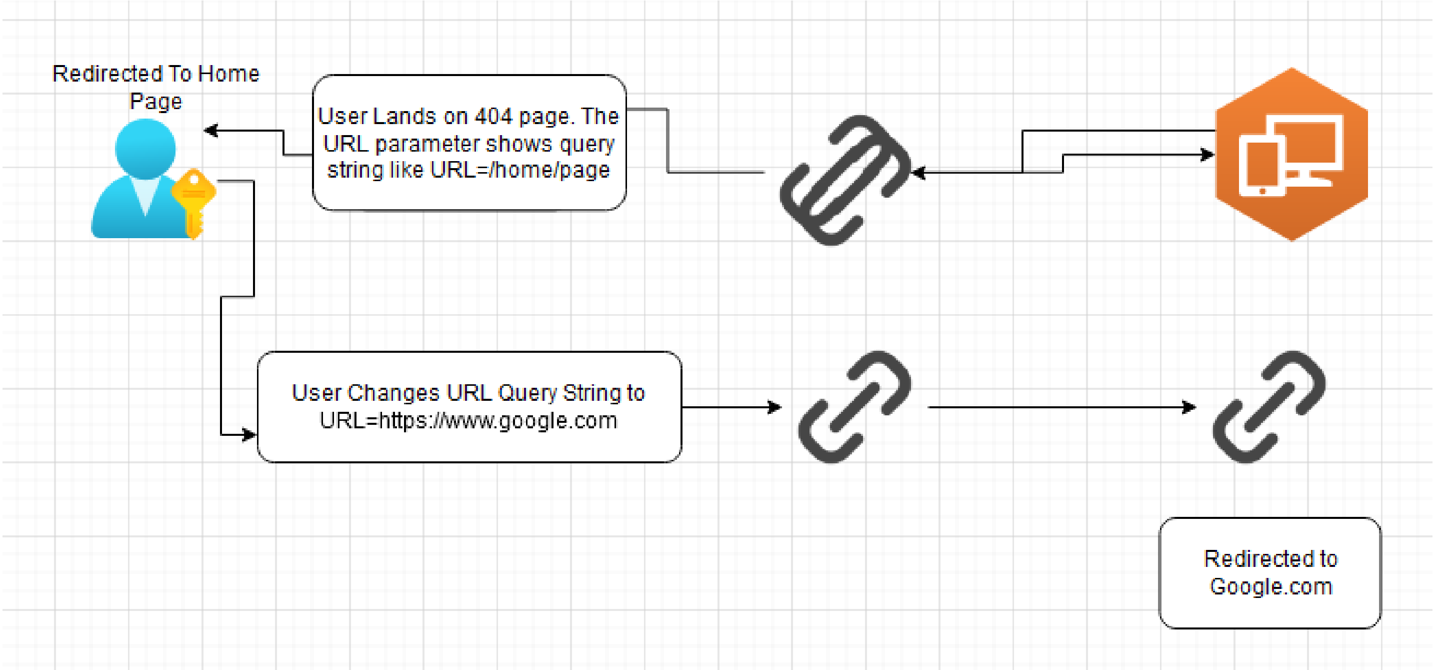


Lesson #2 : Never Give Up

90 Reports Submitted
20 Validated

But Then ....

Scenario 3
URL Redirection



Redirected To Home Page

User Lands on 404 page. The URL parameter shows query string like URL=/home/page

User Changes URL Query String to URL=https://www.google.com

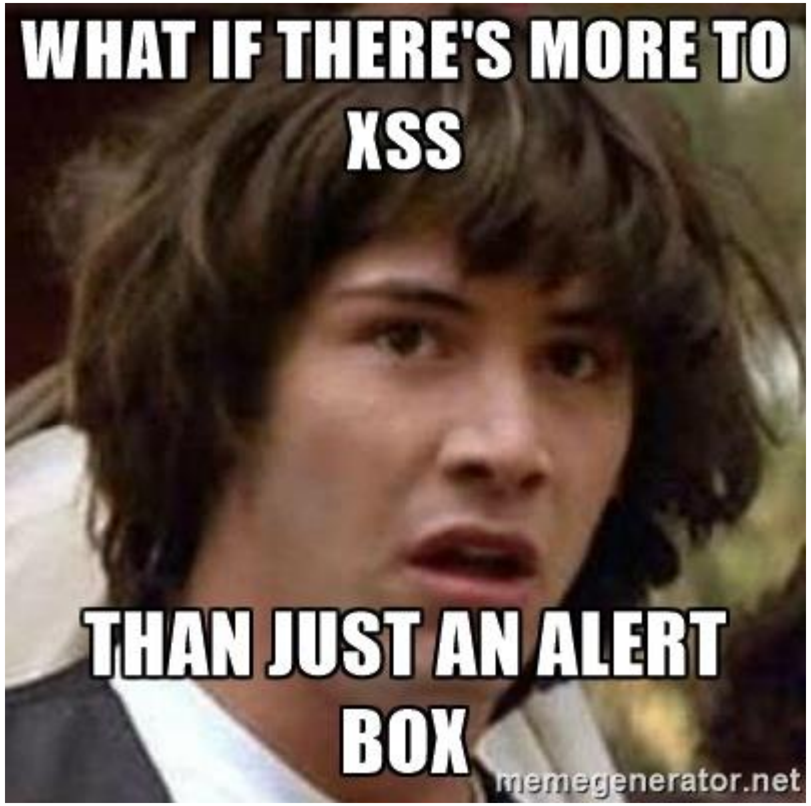
Redirected to Google.com

What we’ve got from all of this?

- Started Back in December 2019/January 2020.
- 17 Not Applicable/Duplicates/Won’t Fix.
- 24 Accepted/Valid Vulnerabilities.
- Only 1 Critical Vulnerability from all 24 Vulnerabilities

How did I Learn this?

- Less Relying on Low-hanging Fruits.
- Automation is the Key !
- Found a Vulnerability? What’s the Business Impact?
- Keep Notes.
- Patience.



Resources

- NahamSec Resources for Bug Bounties. https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters
- Resources about different tools, techniques, YT Videos etc. https://medium.com/@gguzelkokar.mdbf15/bug-bounty-resources-advices-2cc9cfb69f6
- Farah Hawa YT Channel Must Recommended for Beginners (https://www.youtube.com/channel/UCq9IyPMXiwD8yBFHkxmN8zg)
- Jason Haddix, STÖK, TomNomNom, Sandeep(Geekboy), Aditya Shende, Ifrah Iman, Neha Tariq, Harsh Bothra, etc. (List goes Long)

GOODBYE, FRIEND.