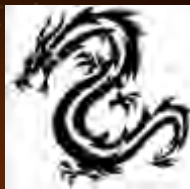


How I Hacked Yahoo, Twitter & Google!



Speaker: **Ebrahim Hegazy (@Zigoo0)**

Over 8 years in information security field that included, WebApps Pentesting, Client Side Attacks, Linux Systems Administration, Training & Instructing, Network Security and lately a Systems Security Engineer.

Agenda

- 1- About me
- 2- What are bug Bounty Programs & Why we need it?
- 3- What are the Bug Bounty Platforms?
- 4- Bug Hunting Methodology
- 5- My findings in different bug bounty programs.
- 6- Questions.



Not this type of bugs!



2- What are bug Bounty Programs & Why we need it?

When a company starts to offer rewards for security researchers to research/find vulnerabilities in their infrastructure, applications and so on under their rules, this is so called “Bug Bounty Program”.

- Yahoo pays a minimum of \$50 and up to \$15,000
- Google pays a minimum of \$100 and up to \$20,000
- Facebook pays a minimum of \$500 and no max payout
- Github Pays a minimum of \$500

Who Has a Bug Bounty Program?



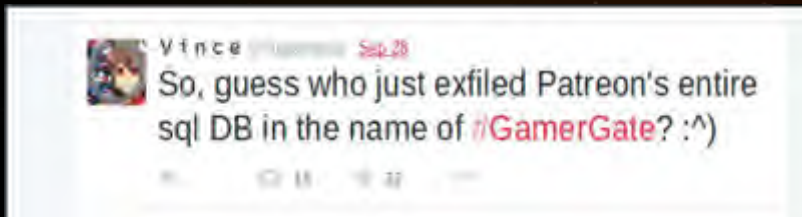
Why we need Bug Bounty Programs?

As a researcher :

- 1- Possibility of getting a job in the industry
- 2- Good opportunity to make \$\$\$
- 3- Better Experience

As a company:

- 1- Less Security Breaches!
- 2- Better and more secure Apps, Networks etc...
- 3- More researchers from across the world.



3- What are the Bug Bounty Platforms?

BBP Platforms are companies that coordinate between security researchers and the companies that offers the bug bounty programs.

Hackerone

BugCrowd

Vulnbox

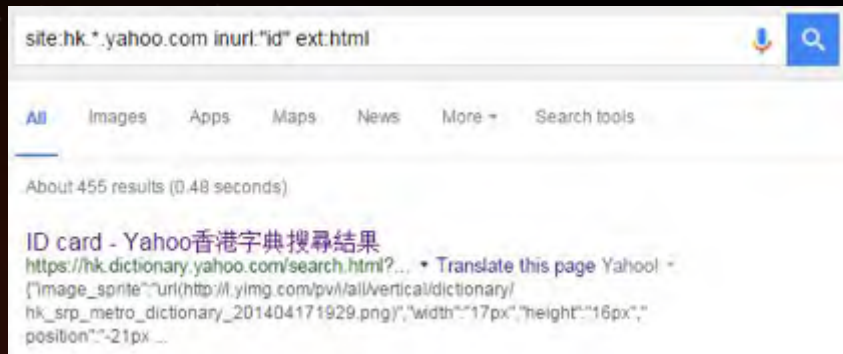
SynAck

CrowdCurity



4- Bug Hunting Methodology

- Pick a target
- Enumerate its sub-domains (e.g -> [SubList3r](#))
- Focus on a Vulnerability type (e.g SQL Injection)
- GHDB! (`site:hk.*.yahoo.com inurl:"id" ext:html`)
- Choosing a potentially vulnerable application!



5- My findings in different bug bounty programs.

Since 2012 I've found and reported over 1000+ vulnerabilities in different applications, websites & bug bounty programs.

Yahoo!

RCE
Bug!

YAHOO!

Google

SSRF
Bug

Google

Twitter!

UFU
Bug.



Yahoo! Remote Code/Command Execution

Remote code execution could happen when the developers pass the user input to the php “eval” function without any validation, which evaluates/execute the normal strings as a php code!



Yahoo! Remote Code/Command Execution - (Demo video)

Demo Time: <https://www.youtube.com/watch?v=V3CHd6ePICo>

```
1 <html>
2 </br>
3 <h1>Hello and welcome to our RCE testing page.</h1></br>
4 <?php
5 error_reporting(0);
6 $fake = $_GET['page'];
7 $sid = $_GET['sid'];
8 if(isset($_GET['sid'])) {
9
10     eval($_GET['sid'].");");
11 #echo "</br><font color='Blue'>Page SID = ".$sid." & page Number = ".$fake."</font>";
12 }
13 ?>
14 <h1>Hope you enjoy your stay :-)</h1></br>
15 <center><font size="3">@Zigoo0</center></font>
16 </html>
```

Twitter Un-restricted File Upload Vulnerability.

Un-restricted file upload vulnerabilities occurs due to the lack of validating the uploaded files!

Video Demo: <https://www.youtube.com/watch?v=enpDJ8MfiC8>



Google SSRF(Server Side Request Forgery)

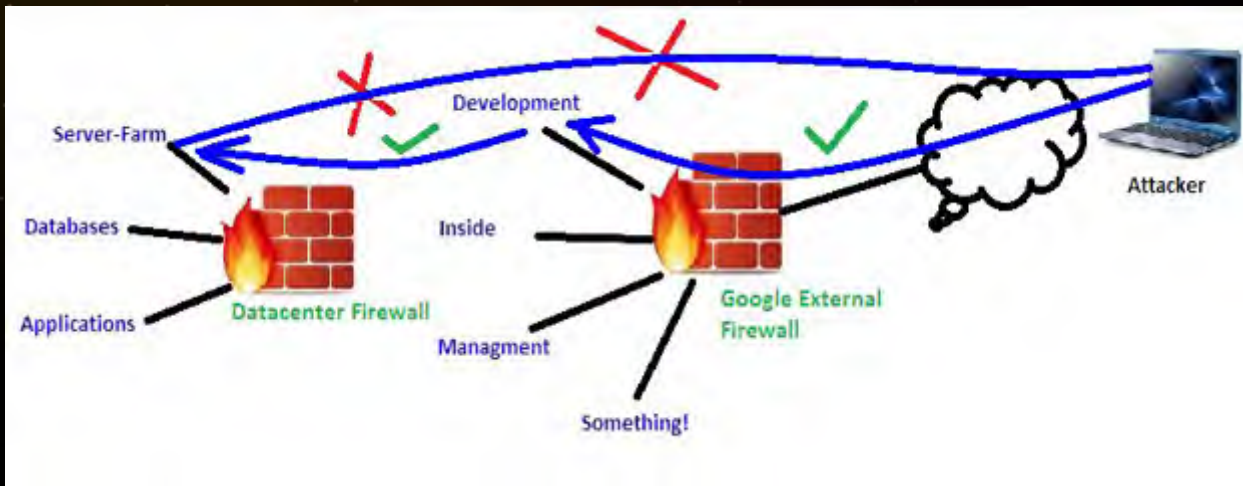
Server Side Request Forgery (SSRF) is a vulnerability that occurs when an attacker has the ability to initiate requests from the vulnerable server to the Intranet/Internet.

Demo Google.com



Google SSRF(Server Side Request Forgery)

How it works?



ANY
QUESTIONS
?

Contact Me

www.sec-down.com

[Twitter.com/Zigooo](https://twitter.com/Zigooo)

[Zigoo.eg\[@\]gmail.co
m](mailto:Zigoo.eg[@]gmail.com)

