

Sublist3r

Coded By Ahmed About-Elia - @aboul3la

```
-] Enumerating subdomains now for tesla.com
-] Searching now in Baidu...
-] Searching now in Yahoo...
-] Searching now in Google...
-] Searching now in Bing...
-] Searching now in Ask...
-] Searching now in Netcraft...
-] Searching now in DNSdumpster...
-] Searching now in Virustotal...
-] Searching now in ThreatCrowd...
-] Searching now in SSL Certificates...
-] Searching now in PassiveDNS...
[!] Error: Google probably now is blocking our requests
-] Finished now the Google Enumeration ...
-] Total Unique Subdomains Found: 36
```

```
now.tesla.com
nuth.tesla.com
autodiscover.tesla.com
log.tesla.com
comparison.tesla.com
dev.tesla.com
uaa-origin.tesla.com
forums.tesla.com
map.tesla.com
r.tesla.com
yncdiscover.tesla.com
odel3.tesla.com
y.tesla.com
aa-origin.tesla.com
as-origin.tesla.com
ew.tesla.com
ew-dev.tesla.com
partners.tesla.com
op.tesla.com
owerwall.tesla.com
esources.tesla.com
hop.tesla.com
ling.tesla.com
atn.tesla.com
```

What Makes a Good Submission



Bugcrowd University

bugcrowd.com

Module Trainer

- JP Villanueva - [@swagnetow](#)
- Trust & Security Engineer [@Bugcrowd](#)
- Programmer, hacker, speaker, gamer!



Module Outline

1. Introduction
2. Selecting the Correct VRT Category
3. Using Styling to Write Effective Reports
4. POC||GTFO
5. Best Practices



bugcrowd.com

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our request
[*] Finished now the Google Enumeration ..
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Introduction



The Golden Rule

- Treat others the way you want to be treated.
- Consider how it would feel to be on the receiving end of your bug report.
- Respect is key.
- Write to a developer audience, not a security person.



**KEEP
CALM
AND
RESPECT
OTHERS**

Why does it matter?

Submissions that are written well:

- Get paid faster.
- Program owners remember who you are.
- Repeatability allows you to not waste time.



```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in 3rd-Party..
[*] Searching now in 3rd-Party..
[!] Error: Google probably doesn't accept our requests
[*] Finished now.
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Selecting the Correct VRT Category

Selecting the Correct VRT Category



- Understand what your bug actually is
- Understand the impact of your bug finding
- Read the program brief and which categories are excluded from bounty

Selecting the Correct VRT Category

- Researcher Documentation:
<https://researchdocs.bugcrowd.com/>
- Check out the Bugcrowd Forum and ask for help:
<https://forum.bugcrowd.com/>
- Take part in the discussions about the VRT on GitHub:
<https://github.com/bugcrowd/vulnerability-rating-taxonomy>



VRT

Categories

If a bug class is not represented you can always chose a top level category for your submission.

VRT				DOWNLOAD PDF
Bugcrowd's Vulnerability Rating Taxonomy				
Bugcrowd's Vulnerability Rating Taxonomy is a resource outlining Bugcrowd's baseline priority rating, including certain edge cases, for common vulnerabilities. Have a suggestion to improve the VRT? Join the conversation on GitHub .				
Taxonomy				
Methodology				
Usage guide				
Version history				
Vulnerability Rating Taxonomy				
Version 1.4 (current) last updated on 04/13/18				
Search table				
Technical Severity▼	VRT Category	Specific Vulnerability Name	Variant / Affected Function	
P1	Server Security Misconfiguration	Using Default Credentials		
P1	Server-Side Injection	File Inclusion	Local	
P1	Server-Side Injection	Remote Code Execution (RCE)		
P1	Server-Side Injection	SQL Injection		
P1	Server-Side Injection	XML External Entity Injection (XXE)		
P1	Broken Authentication and Session Management	Authentication Bypass		
P1	Sensitive Data Exposure	Critically Sensitive Data	Password Disclosure	
P1	Sensitive Data Exposure	Critically Sensitive Data	Private API Keys	
P1	Insecure OS/Firmware	Command Injection		
P1	Insecure OS/Firmware	Hardcoded Password	Privileged User	
P1	Broken Cryptography	Cryptographic Flaw	Incorrect Usage	

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in Shodan..
[*] Searching now in PassiveDNS..
[!] Error: Google probably blocked our requests
[*] Finished now. Subdomains found: 36
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Using Styling to Write Effective Reports

Expectations vs. Reality

What you think your submission looks like vs. what it actually looks like:



Using Markdown



Great **looking** submissions make it easier to triage. Remember, developers are going to read your submissions to fix the bug you found. Can they understand your bug? Its impact?

Markdown is a researchers **best friend**.

<https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet>

<https://guides.github.com/pdfs/markdown-cheatsheet-online.pdf>

The Final Product

Description

WRITE

PREVIEW

Issue

The application contains a vulnerability that allows an attacker to view account data of other users. This class of vulnerability is called an insecure direct object reference.

The vulnerability is exploited on this resource:

- <http://umbrella.com/accounts/id?=465246>

The **id** parameter can be iterated to a different number like **465245** which will give an attacker access to another users private data.

Steps to Reproduce

1. Log into the Umbrella Bank as your @bugcrowdninja.com username.
2. Navigate to the Account details page.
3. Notice that there is an id parameter in the query string.
4. Attach this id parameter into the query string of any page that you would like to access as a different user.
5. Change id parameter into a different number other than your own account on the checking account page.
6. You will now be looking at another Iron Bank user's account details and see another user's gold, bitcoin, and ethereum holdings.

Impact

Exploiting this vulnerability to it's fullest, an attacker could automate and download through all six digit **id** numbers from 1 to 465246. This would be a complete breach of all user account details for the application. He/She could then use this information to gain trade advantages, or blackmail the business.

📄

 Markdown supported

Markdown

Issue

The application contains a vulnerability that allows an attacker to view account data of other users. This class of vulnerability is called an insecure direct object reference.

The vulnerability is exploited on this resource:

* <http://umbrella.com/accounts/id?=465246>

The ****id**** parameter can be iterated to a different number like ****465245**** which will give an attacker access to another users private data.

Steps to Reproduce

1. Log into the Umbrella Bank as your @bugcrowdninja.com username.
2. Navigate to the Account details page.
Notice that there is an id parameter in the query string.
3. Attach this id parameter into the query string of any page that you would like to access as a different user.
4. Change id parameter into a different number other than your own account on the checking account page.
5. You will now be looking at another Iron Bank user's account details and see another user's gold, bitcoin, and ethereum holdings.

<snip>


```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ..
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

POC || GTFO



Building a Proof of Concept

Write a descriptive title.

- Avoid “CRITICAL or PLZ READ NOW” as they dont help legitimize your submission

Example Titles:

XSS in Search function - [hostname] (search parameter)

or

Insecure Direct Object Reference on [hostname, parameter] - Allows complete compromise of all user account data

Remember to choose the correct target and the correct VRT category

Info

Help us get an idea of what this vulnerability is about.

A summary of your submission

Target

Select the vulnerable target

Targets that are not explicitly in scope may not be eligible for a reward

Select target...

Technical severity

The [Vulnerability Rating Taxonomy](#) is the baseline guide used for classifying technical severity.

A severity rating does not match a specific reward amount, and the approved rating will be unique based on each vulnerability's context after it is reviewed.

Select a vulnerability type (e.g., XSS, SQLi)

Building a Proof of Concept - Continued

- Put the actual URL of where the vulnerability is
- Use Markdown
- Always use screenshots and videos for your POC!
 - You never know when a fix might come and you may need to prove your bug was there at time of submission

Vulnerability details
Describe the vulnerability, and provide a proof of concept. How would you fix it?

URL / Location of vulnerability

https://secure.server.com/some/path/file.php

Description

WRITE

PREVIEW

What is the vulnerability?

What is security impact?

Replication Steps:

1. Press the button
2. Enter `xxx` into the input
3. Boom

Proof of Concept:

MD

 Markdown supported

+ Add attachment

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

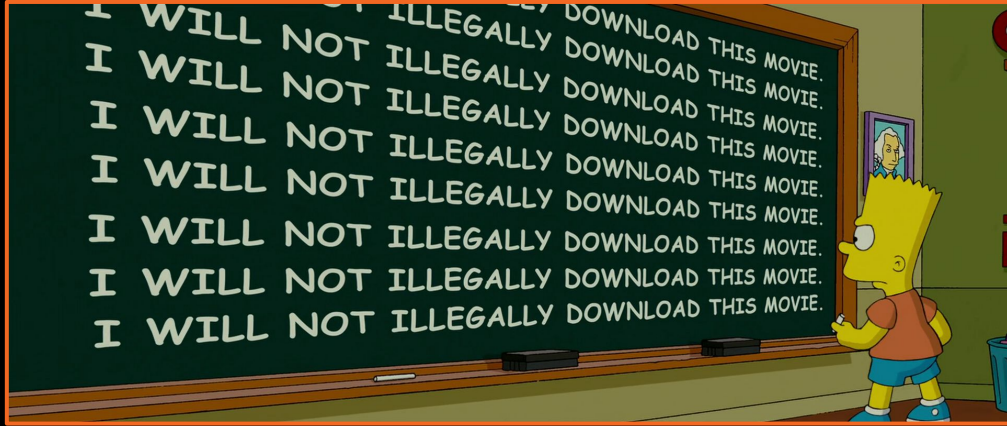
```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking your request.
[*] Finished now the Google Enumerate..
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Best Practices



Best Practices



For all of the above it is incredibly important to use **reporting templates**.

Also:

- Use tools and automation
- Be as verbose in your reports as possible