BUG BOUNTY ~~WORKSHOP~~ FUNSHOP

AGENDA

- ➔ Intro
- ➔ Bug Bounty Definition
- ➔ How to select a target
- ➔ Passive Recon Techniques
- ➔ Hacking with Burp Suite
- ➔ Importance of understanding an application flow
- ➔ Better Bug Bounty Report
- ➔ Keep up with all the new trends
- ➔ Live Burp Suite Session
- ➔ Recap | Wrapping up

Intro

#whoami

- Prateek Tiwari - @prateek_0490
- Security Lead @ Zomato
- Security Consultant, Occasional Bug Bounty Hunter
- Email: prateek0490@gmail.com

Hey you! What’s Bug Bounty?

What’s Bug Bounty?

- Bug Bounty is a reward offered to individuals who identifies and report bugs or security vulnerabilities in a computer program/system or software.
- The reward could be in any form - from goodies to hard cash or just acknowledgement.

How to select a target?

How to select a target?

Assets in scope:

- Priority to wildcard {*.example.com}
- Mobile Apps

Paying attention to out of scope / exclusions list:

- XSS
- CSRF
- Subdomain Takeovers

Meh “really? Do you even care about Security □”

Diving deep into the target, Passive..sh Recon

Diving deep into the target using passive..sh Recon

Find all the **__ASSETS__** that belongs to that organisation. Assets?

- Domains?
- Subdomains?
- 3rd Party Services used by Organisation (GitHub, Jira, Trello, Jenkins, GitLab, etc...)
- IP Ranges?
- iOS / Android Apps?
- Doesn’t ends [n number of assets] ……

Subdomains | Asset(s) Identification

- Subfinder [https://github.com/subfinder/subfinder]
- VirusTotal [https://www.virustotal.com/#/domain/domain.com]
- Certificate Transparency [https://crt.sh/?q=%.domain.com]
- Censys [https://www.censys.io]
- Google - site:example.com -www [Other Search Engines - Bing, DuckDuckGo, Yahoo]
- Google Certificate Transparency [https://transparencyreport.google.com/https/certificates?hl=en]
- Facebook Certificate Transparency Monitoring [https://developers.facebook.com/tools/ct]
- CSP Headers? Anyone? That's interesting isn't it? Well that has given me couple of criticals and a nice payouts. Never miss!
- GitHub, Gist, Gitlab, Trello, Jira, etc…

CSP Headers

```
Content-Security-Policy: frame-ancestors https://*.nearbuystag.in https://*.nearbuy.com 'self'; default-src *;
font-src * data:; img-src * data:; media-src * blob:; script-src 'self' 'unsafe-inline' 'unsafe-eval' *.jwpcdn.com
*.cloudflare.com *.twitter.com *.recruiterbox.com *.zdev.net *.zdev.net:8080 *.zomato.com *.tinymce.com
*.gstatic.com *.googleapis.com *.google.com *.google.co.in *.facebook.com sdk.accountkit.com *.doubleclick.net
*.googlesyndication.com *.nr-data.net *.newrelic.com *.google-analytics.com *.akamaihd.net *.zmtcdn.com
*.googletagmanager.com *.facebook.net *.googleadservices.com *.cdninstagram.com *.googlesyndication.com
*.inspectlet.com *.spreedly.com *.instagram.com *.twimg.com *.mouseflow.com *.usersnap.com
d3mvnvhjmkxpjz.cloudfront.net *.serving-sys.com *.sushissl.com *.pubnub.com tsgw.tataelxsi.co.in *.branch.io
app.link cdn.poll-maker.com *.ampproject.org *.smartlook.com *.hotjar.com dashboard.hypertrack.io zba.se
*.googletagmanager.com *.eff.org cdn.plot.ly *.zedo.com *.bing.com *.criteo.net *.criteo.com mddigital.in;
style-src * 'unsafe-inline';
```

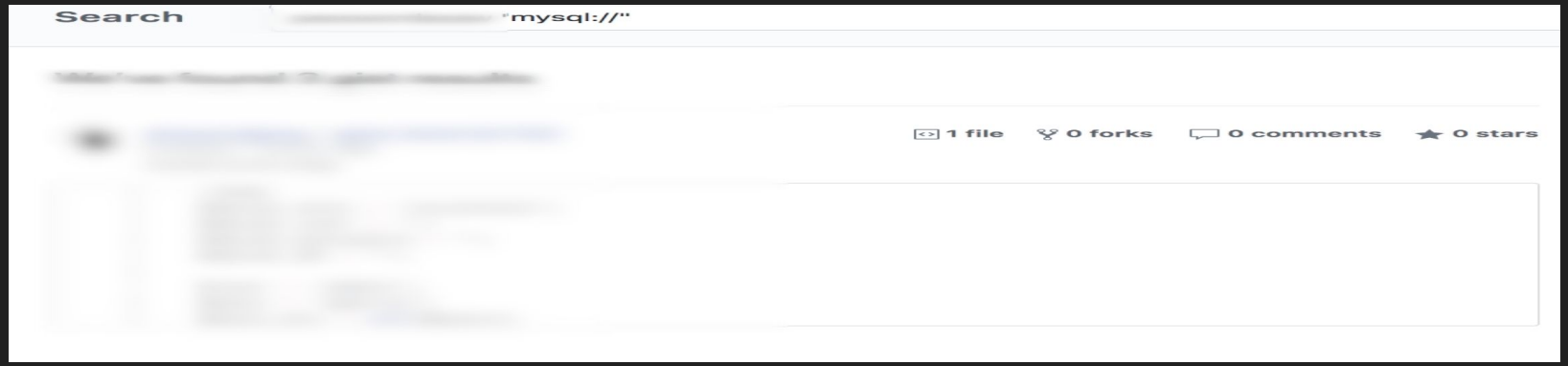
#XXXXXX **Admin Access to a domain used for development and admin access to internal dashboards on that domain**

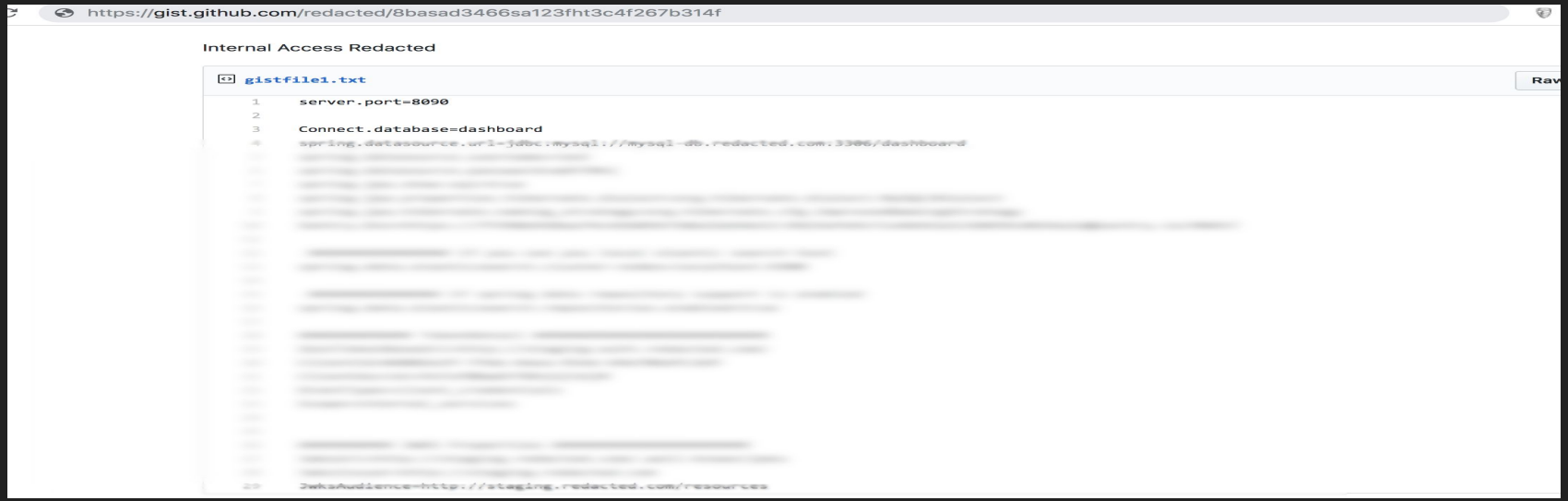
Share:

State	Resolved (Closed)	Severity	No Rating (---)
Disclosed publicly	December 28, 2017 6:42pm +0530	Participants	
Reported To	Redacted	Visibility	Public (Limited)
Asset	*.redacted.com (Domain)		
Weakness	Improper Access Control - Generic		
Bounty	XXXX		

Collapse

gist.github.com

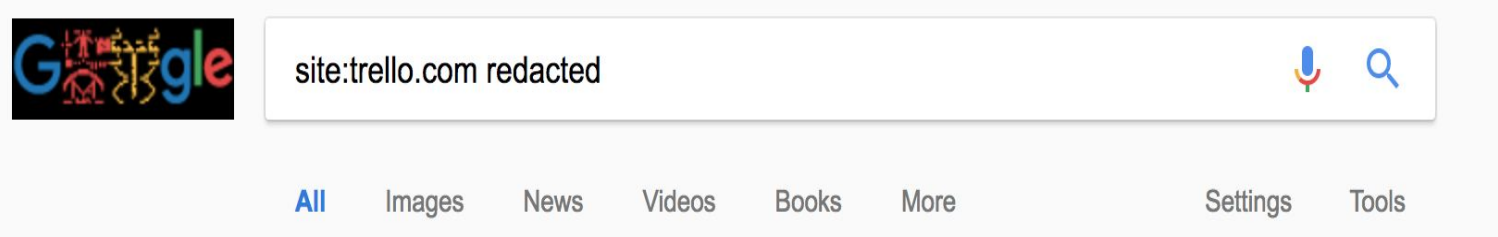




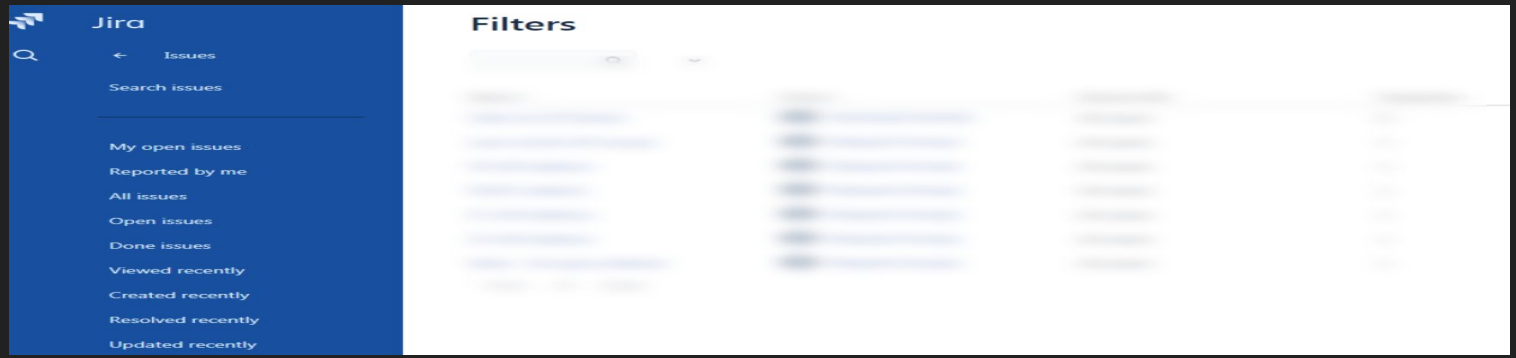
gist.github.com

Cost of Human Errors :(

Trello, Jira, Gitlab ...

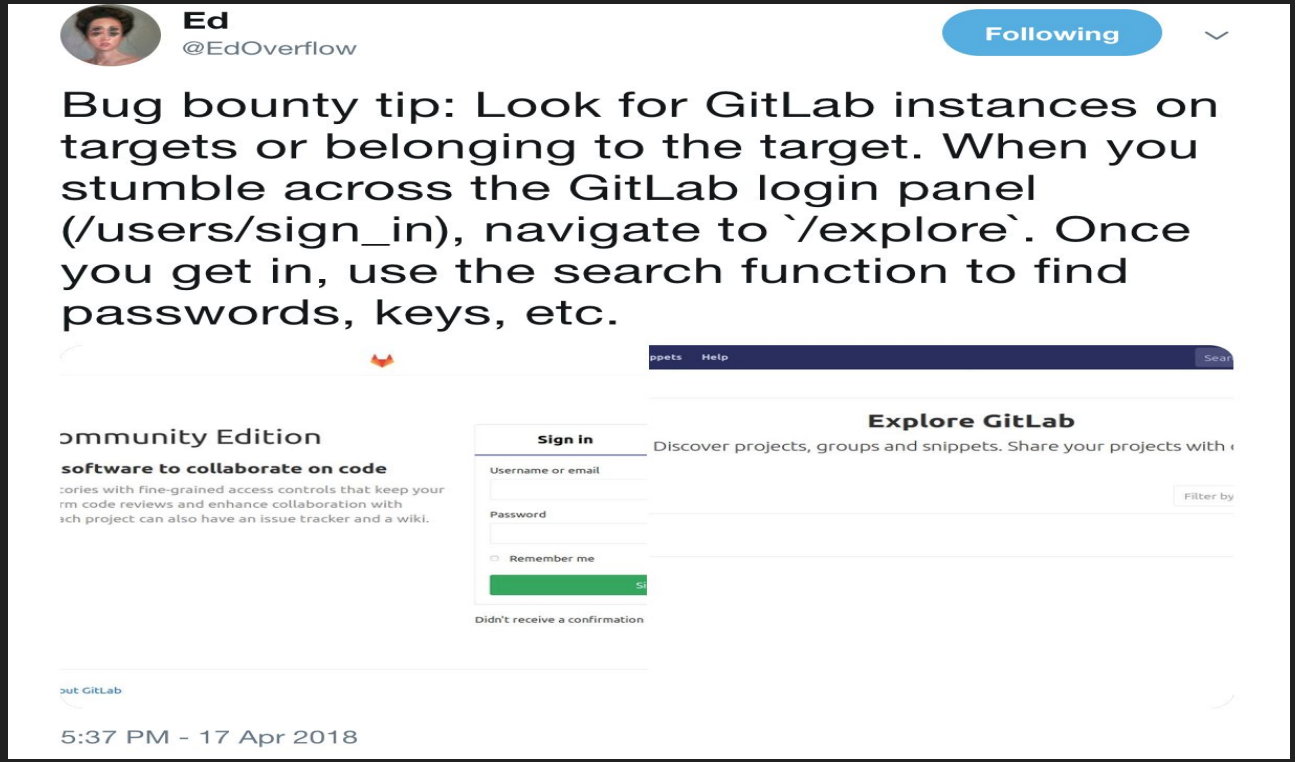


Even though if an organization's Jira instance has an auth, administrators set up "public" projects, they forget “public” means public for everyone. This could sometime give you keys to kingdom.

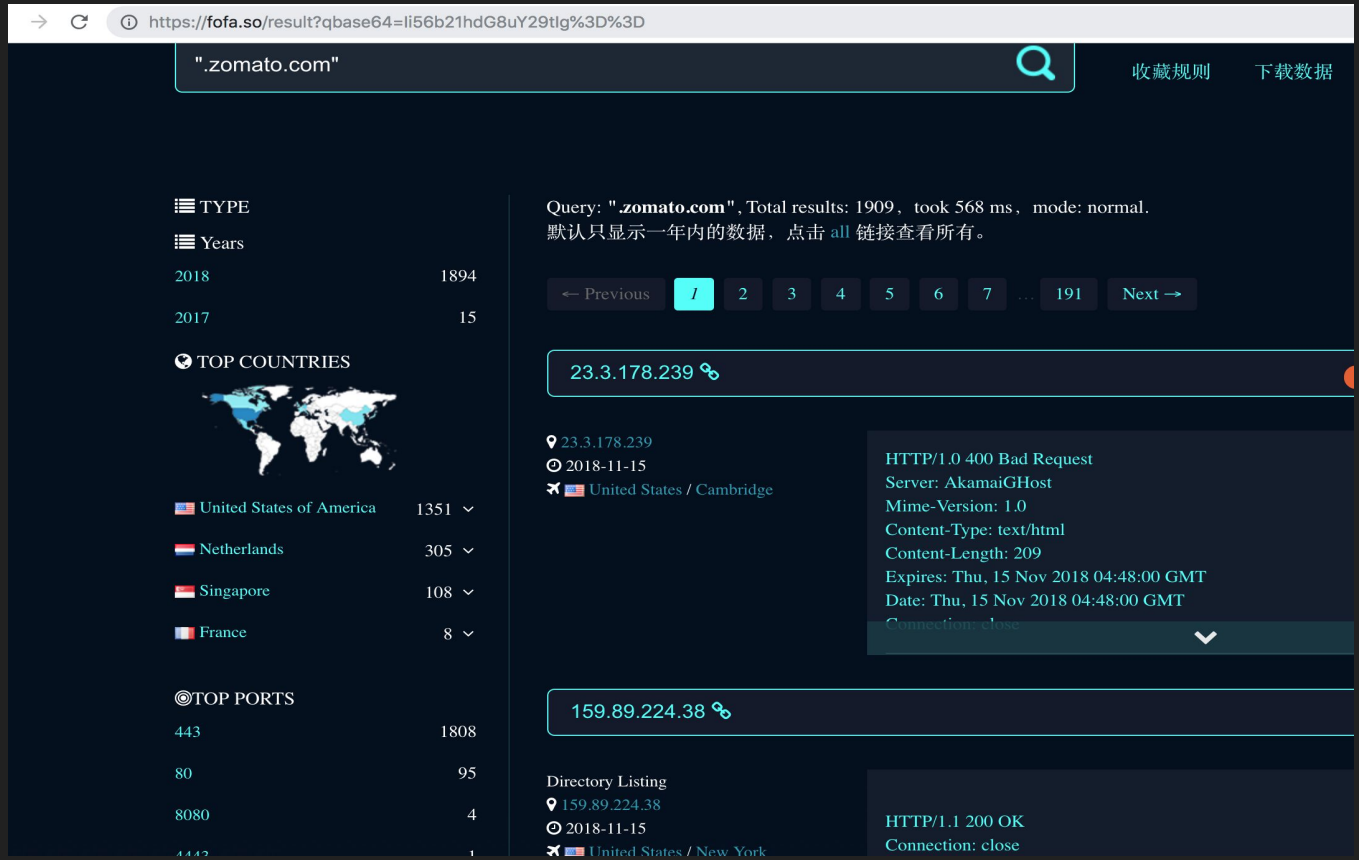


Trello, Jira, Gitlab ...

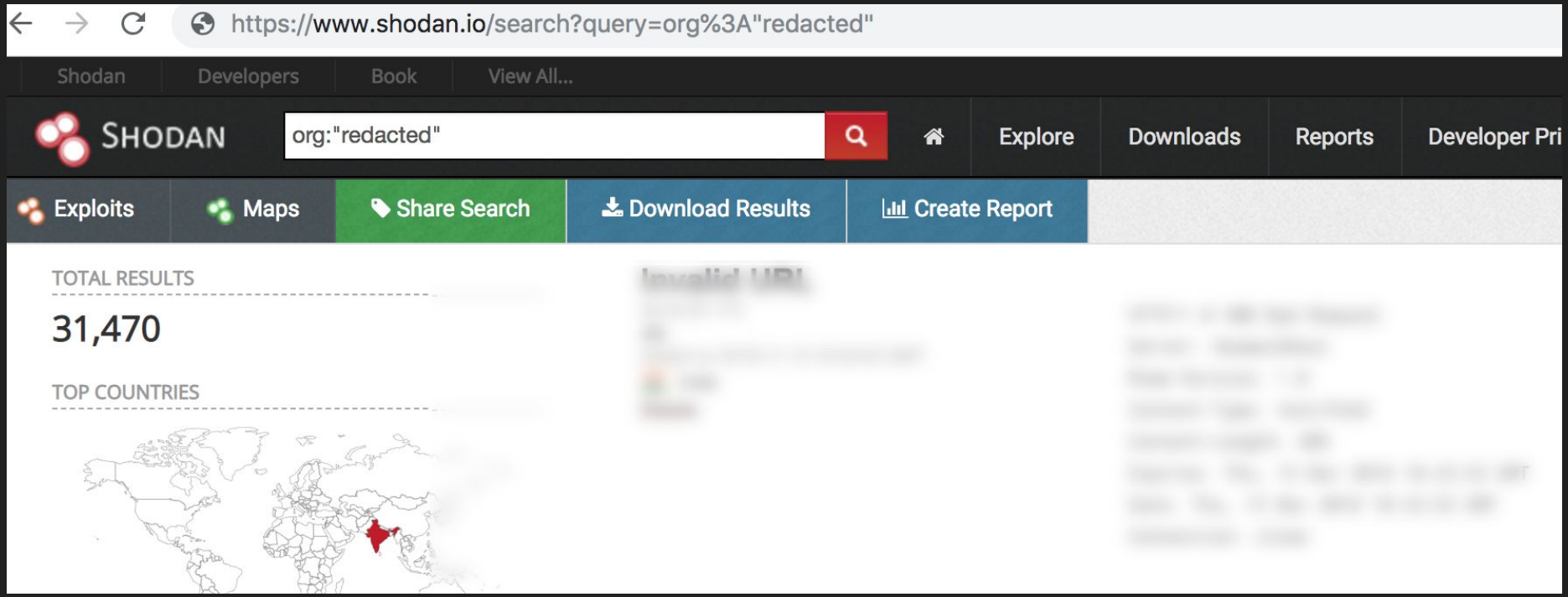
Thanks Ed :)



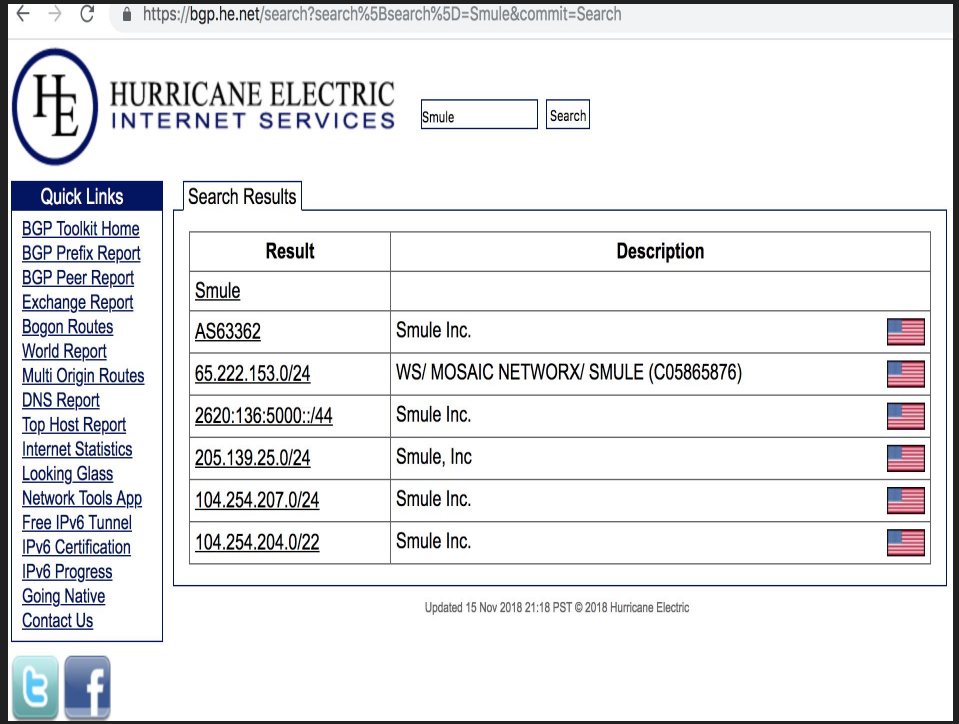
fofa.so - chinese version of shodan



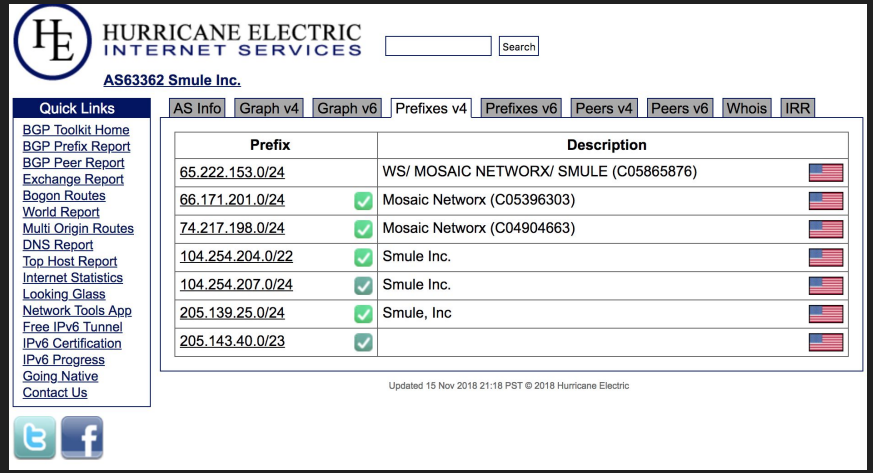
shodan.io


https://www.shodan.io/search?query=org%3A"redacted"
Shodan
Developers
Book
View All...
SHODAN
org:"redacted"
Explore
Downloads
Reports
Developer Pri
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
31,470
TOP COUNTRIES

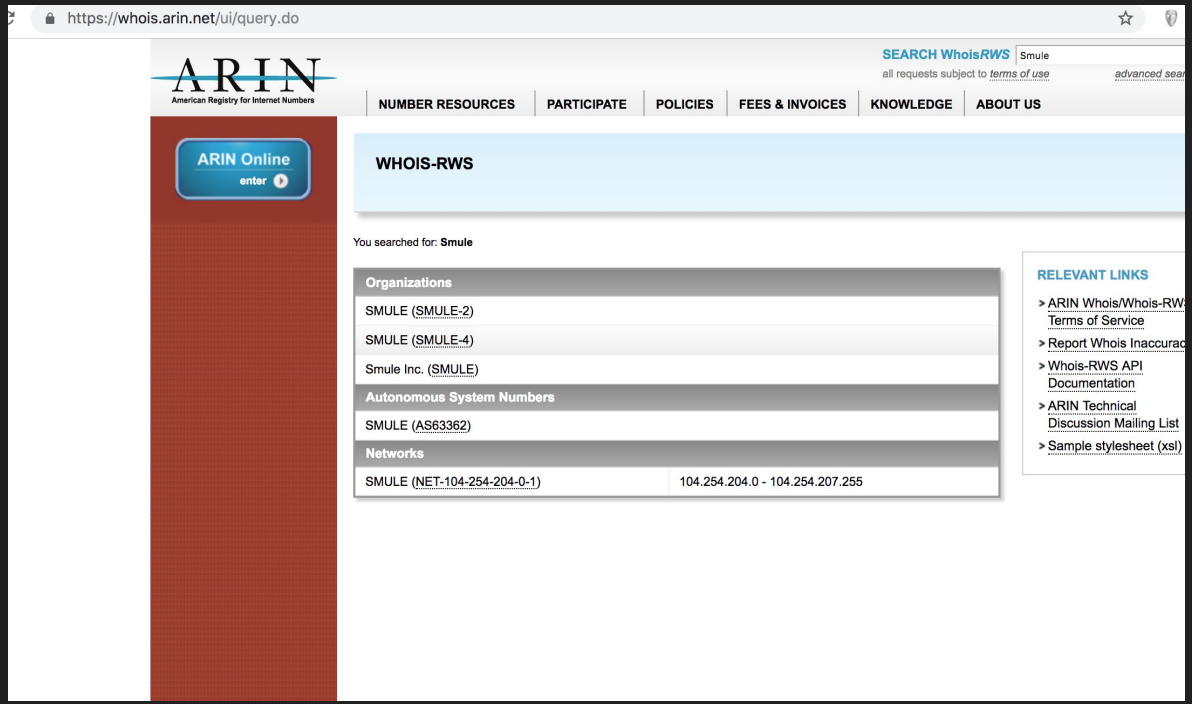
IP Ranges



https://bgp.he.net/search?search%5Bsearch%5D=Smule&commit=Search



IP Ranges



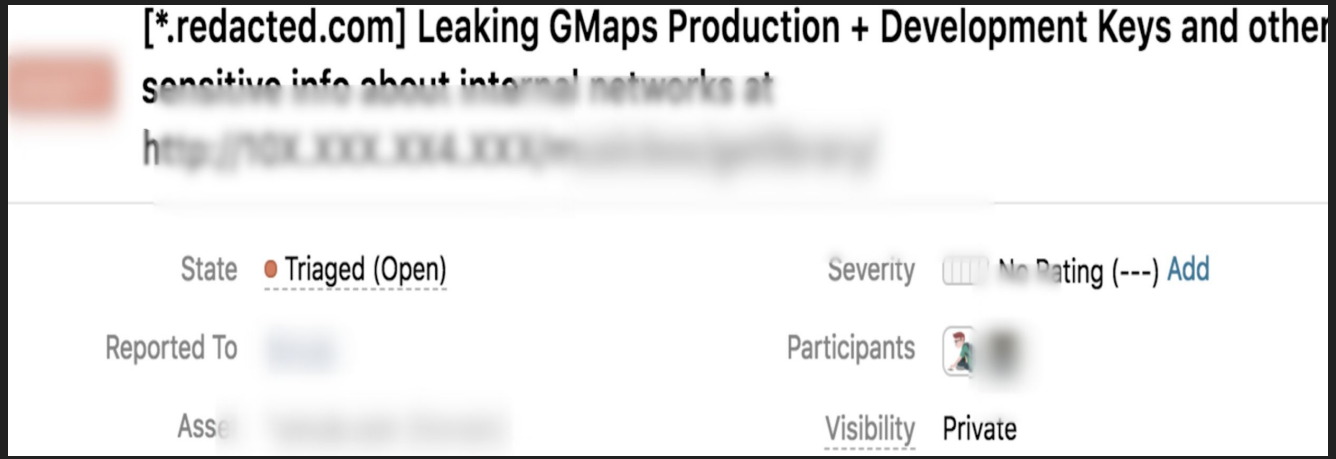
https://whois.arin.net/ui/query.do

IP Ranges

Sir, I’ve found the IP Space now what?

IP Range - now what?

- Fire NMap and run NSE Scripts on those discovered IP Ranges
- Perform content discovery (file/folder bruteforcing) on every discovered asset
  - BurpSuite
  - Dirsearch, Dirbuster
  - Wfuzz

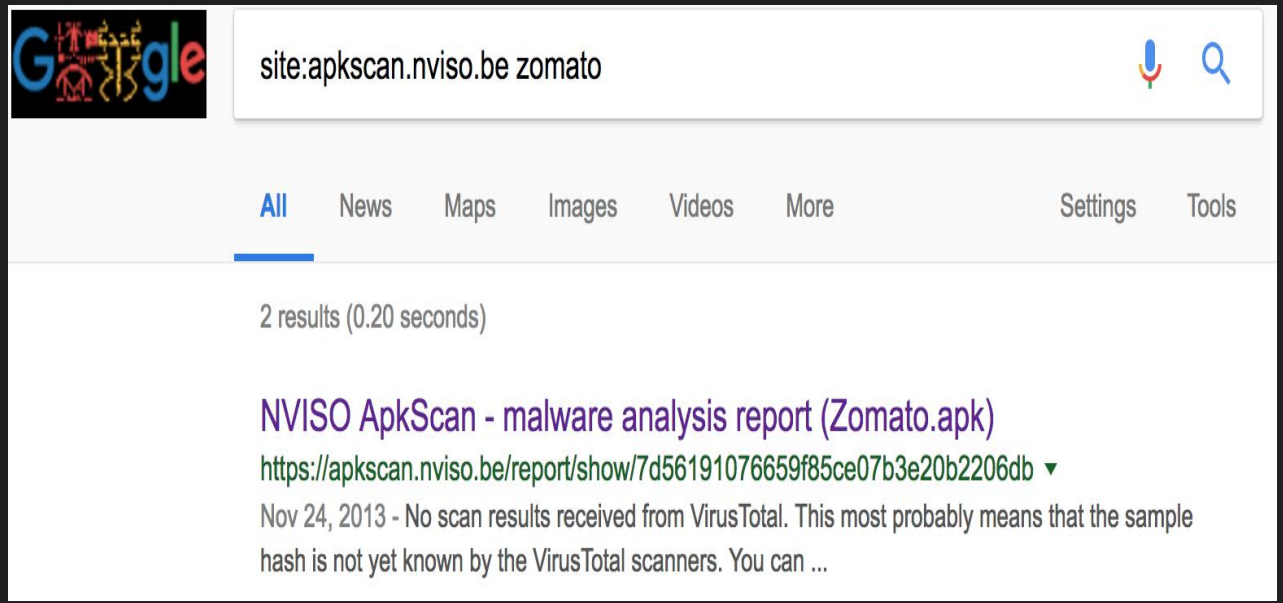


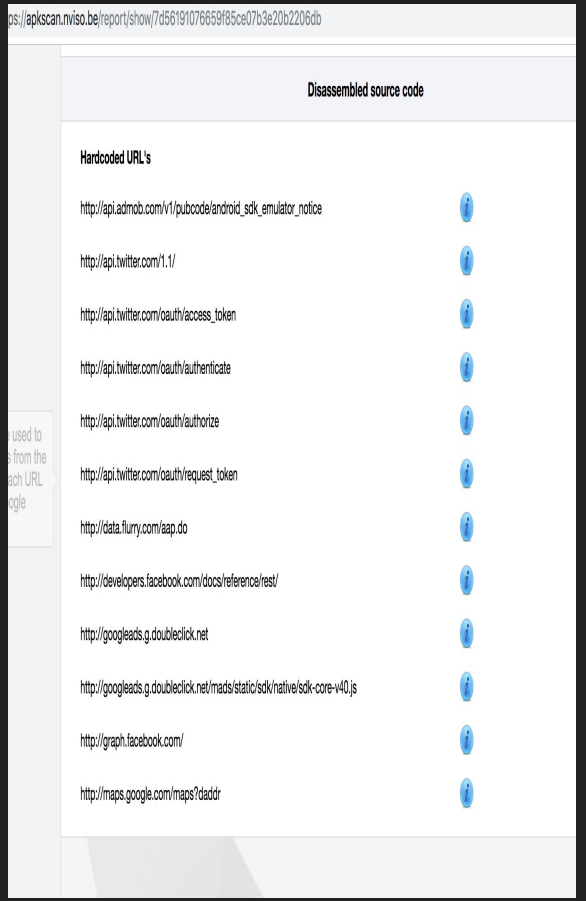
Oh the mobile apps are in scope, what should I look for?

Did you know? You can find leakage of sensitive data in mobile apps without even installing them on your phone. Howwww?

Oh the mobile apps are in scope, what should I look for?

Short Cut:





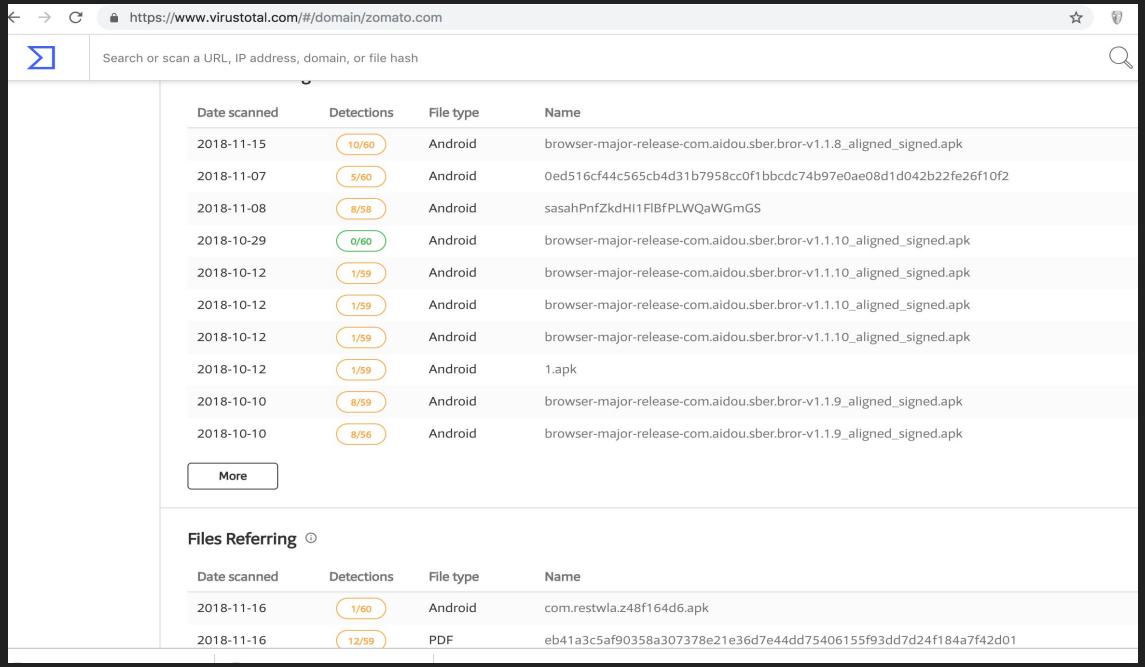
Oh the mobile apps are in scope, what should I look for?

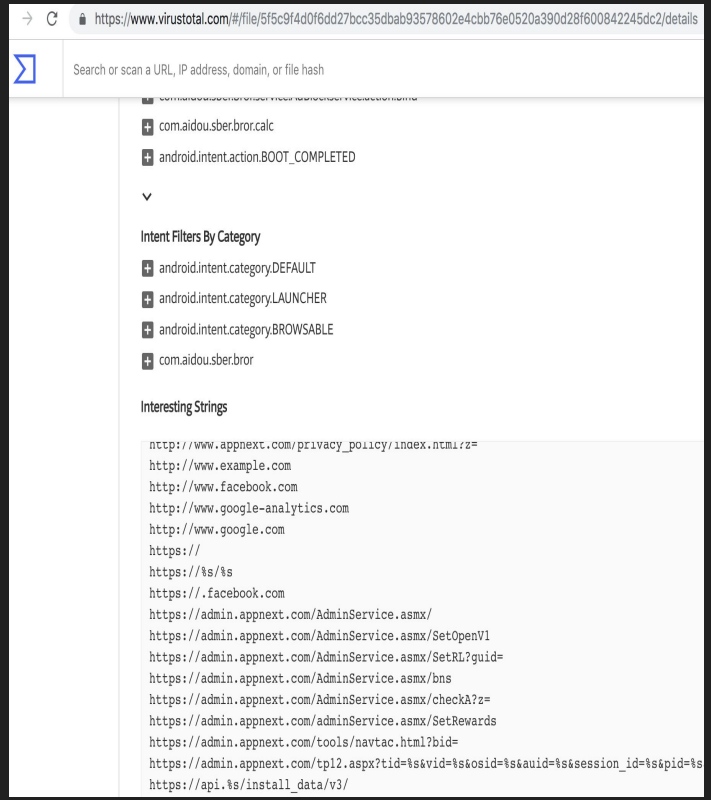
Long Route:

- Download the apk, you can do it from https://apkpure.com/
- Upload the apk at https://apkscan.nviso.be/, run the Scan and wait for the results.

Oh the mobile apps are in scope, what should I look for?

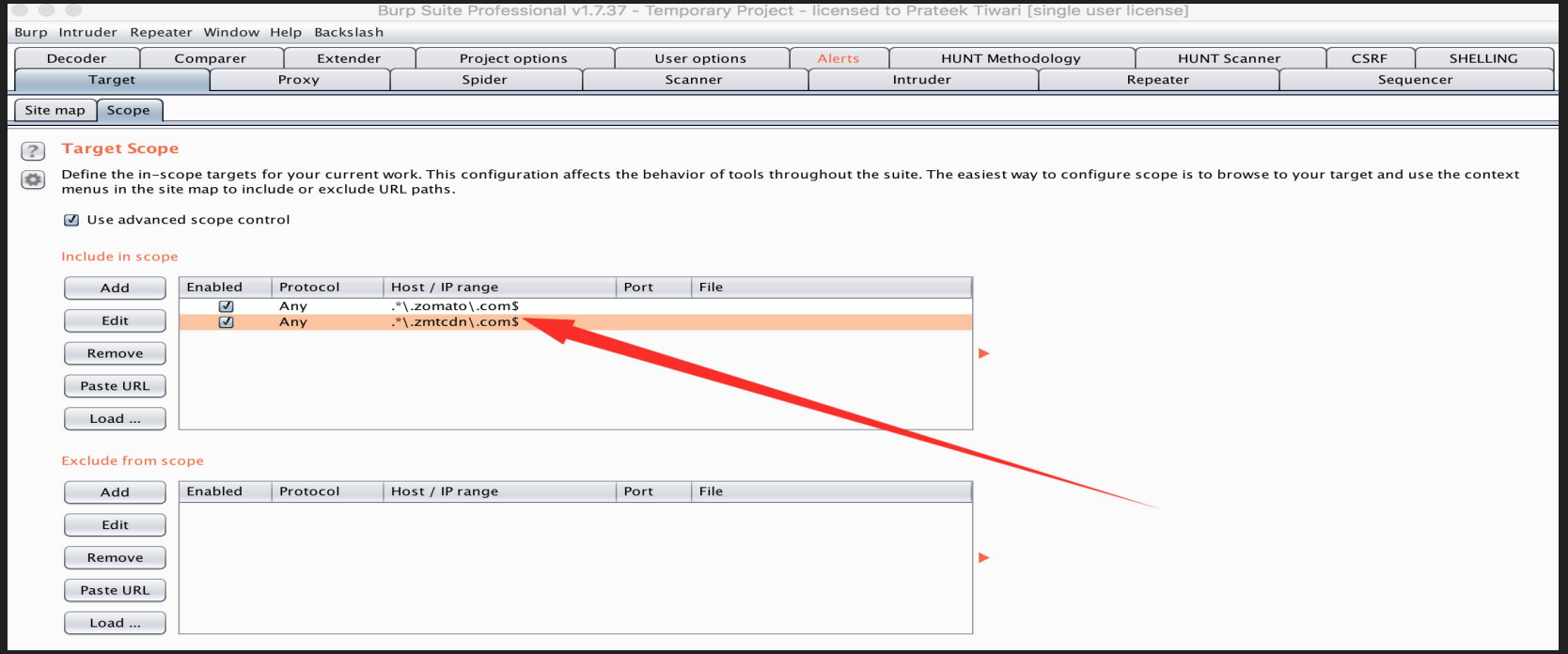
VIRUSTOTAL



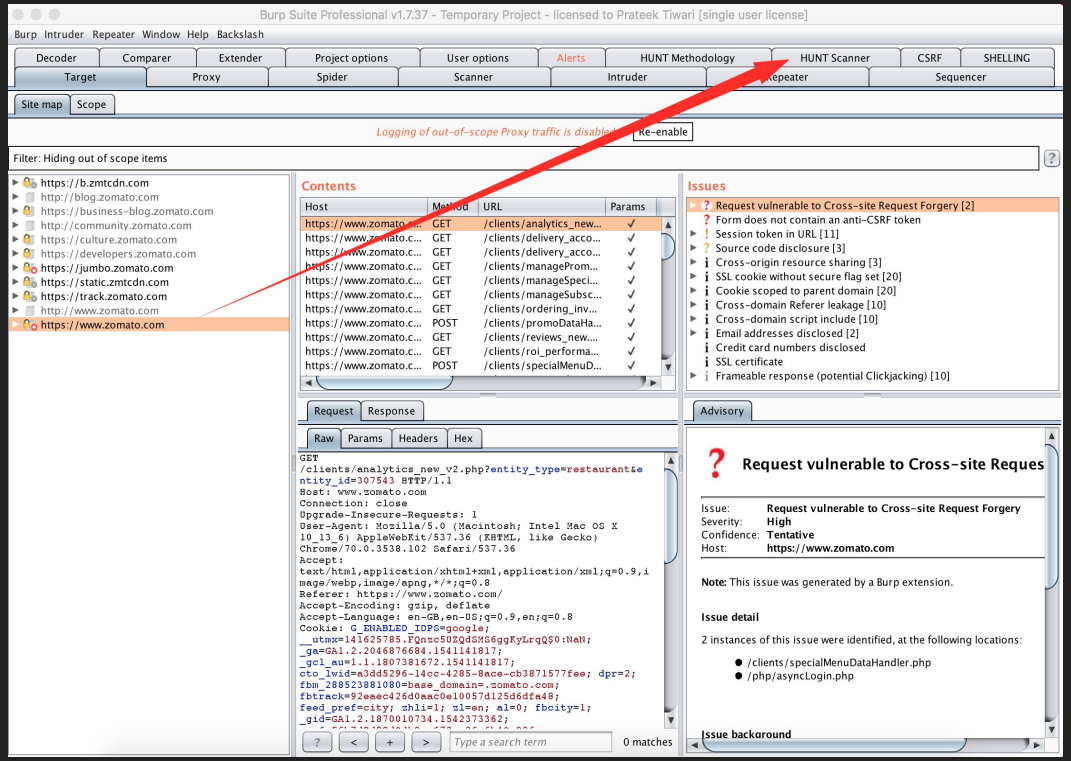


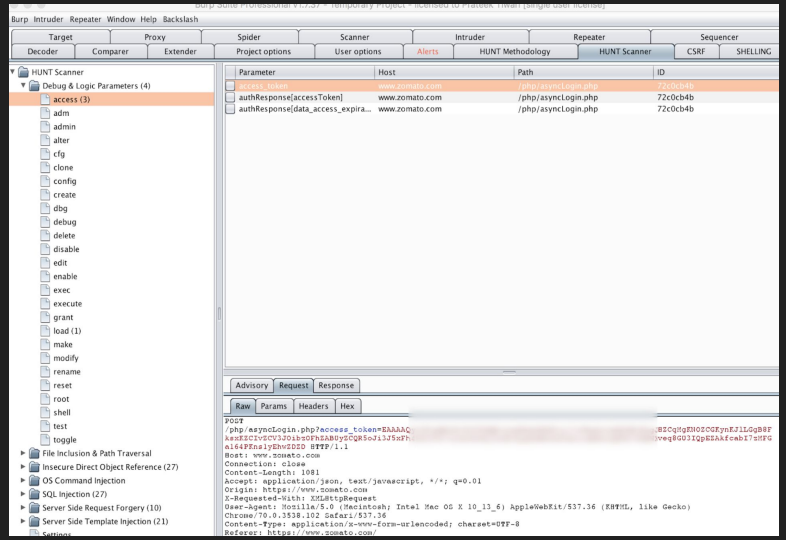
Hacking with BurpSuite

Setting the right Scope

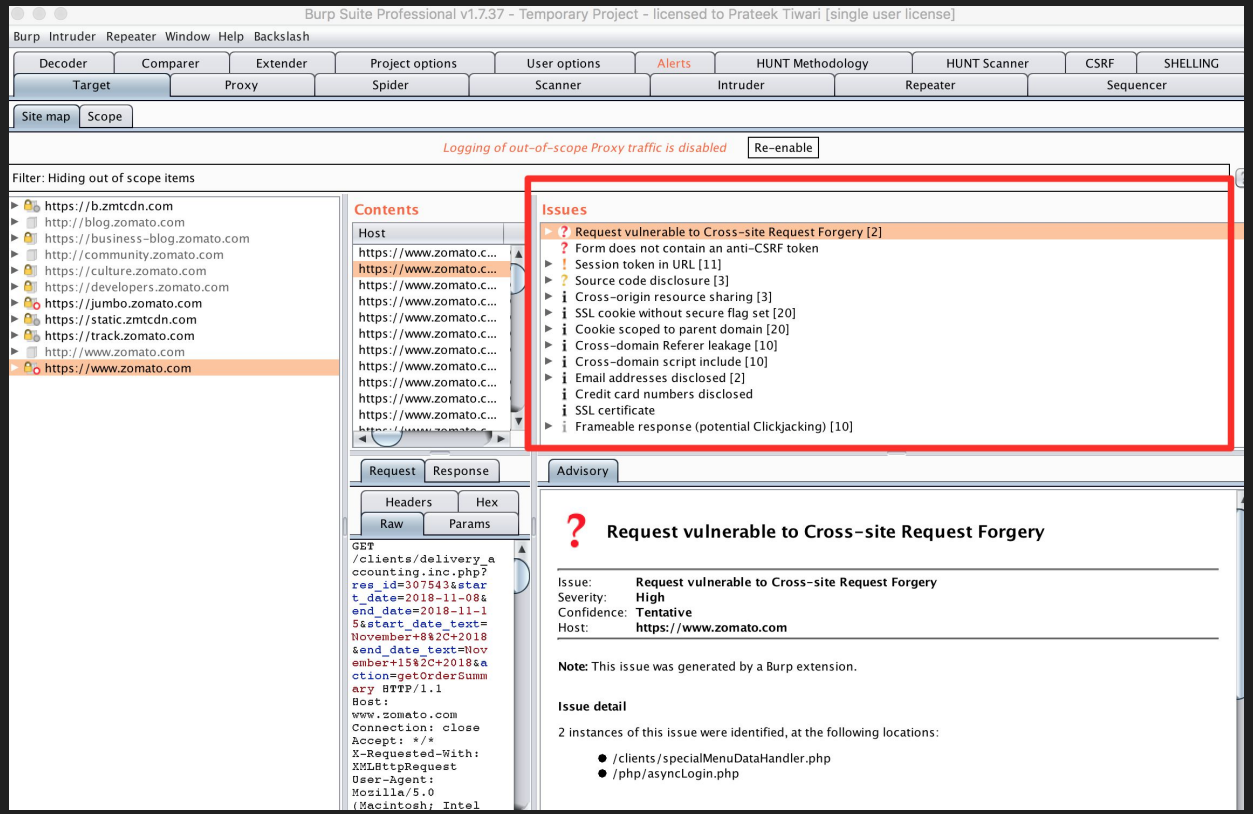


Hacking with BurpSuite





Hacking with BurpSuite



Keeping an eye on these issues list, always handy and helps a lot!

Hacking with BurpSuite

BURP SPIDER

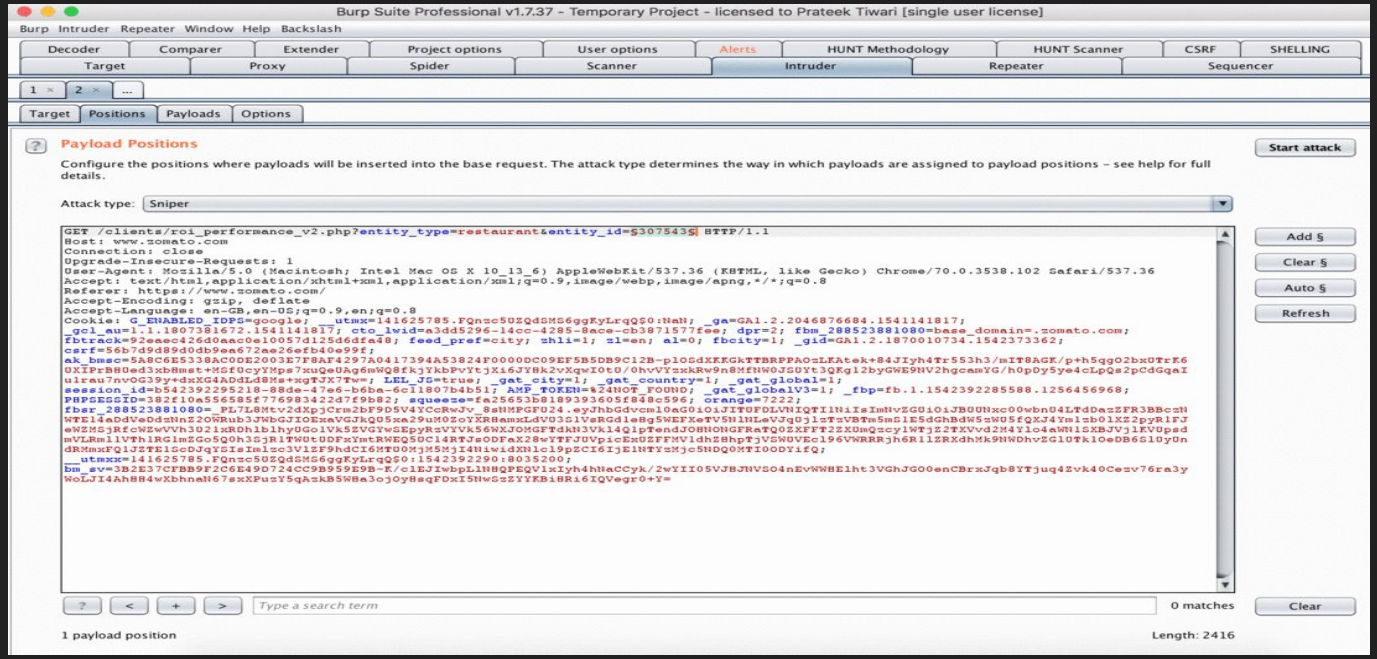
- Turn off Passive Scanning
- Set Forms to auto submit
- Set scope to advanced control and use a target name instead of regex (something like zomato instead of .zomato.com or .*\.zomato\.com$), you will be surprised to see the results and after effects of it
- Browse all URLs, make all requests POST/GET/PUT whatever, then spider all hosts recursively
- Profit (More Targets)!

Will cover up in Live Session

Hacking with BurpSuite

Did you know? You don't always need an automated Script to demonstrate the impact of any data leak [PIIs].

Intruder for the win!



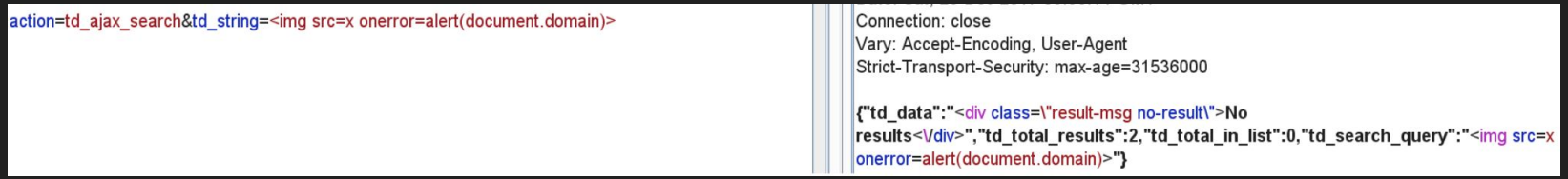
Hacking with BurpSuite

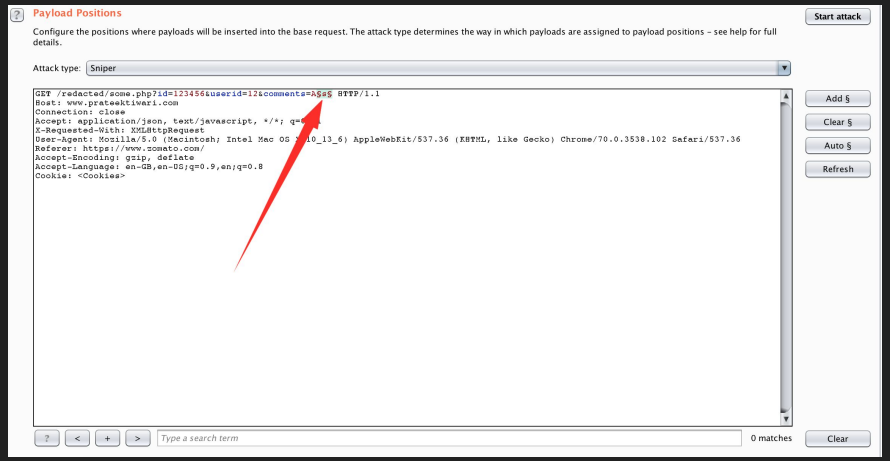
Using “Repeater tab” to find:

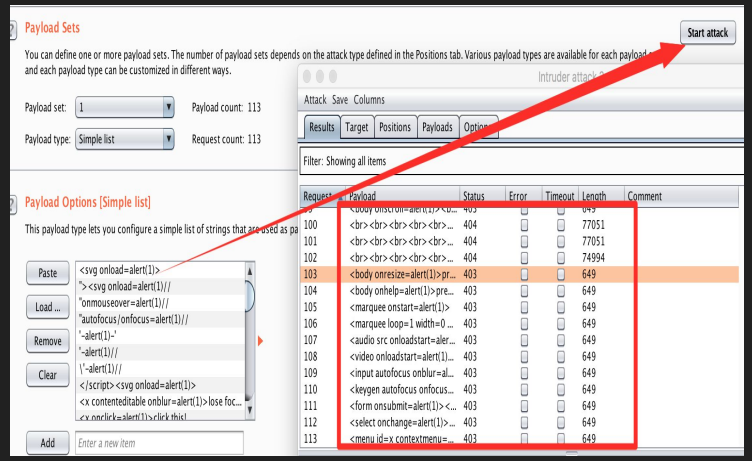
- XSS
- SQLi
- Privilege Escalation
- IDOR(s)
- More Bugs

Hacking with BurpSuite

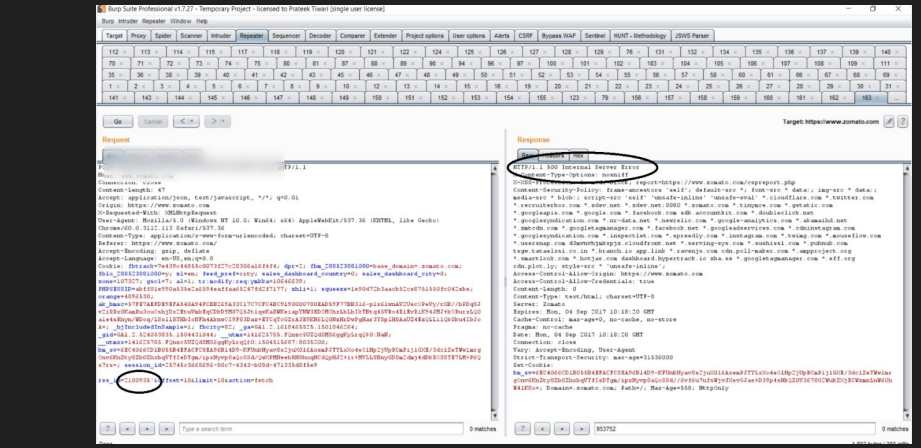
- Using “Repeater tab” to find XSS, SQLi, IDOR(s), Privilege Escalation
- Catch a Request which accepts user input and throw it into a repeater tab.
- Start Fuzzing the parameters.

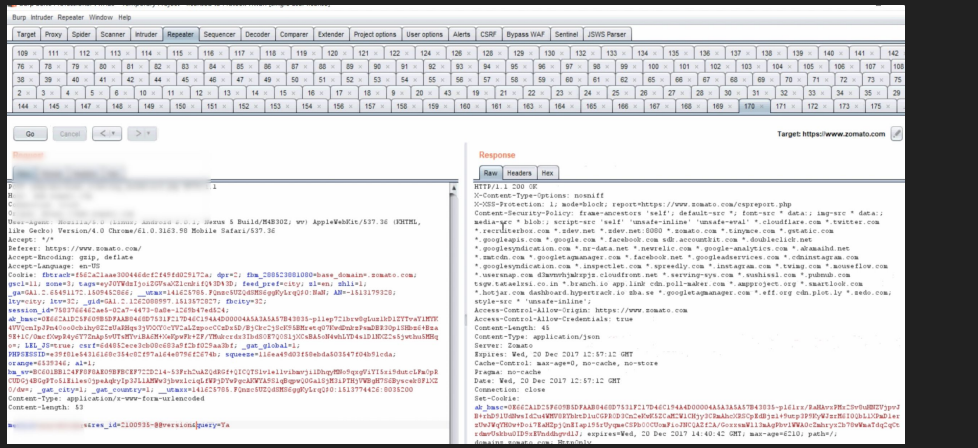




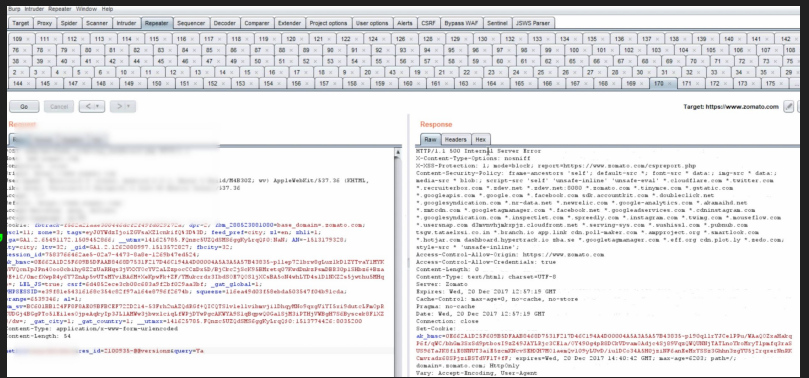


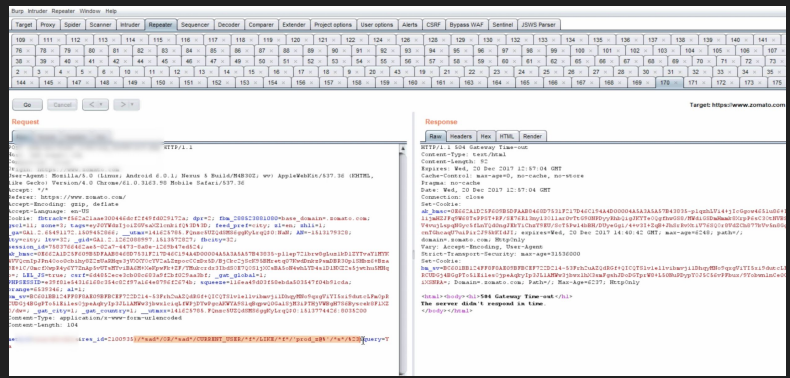
Hacking with BurpSuite





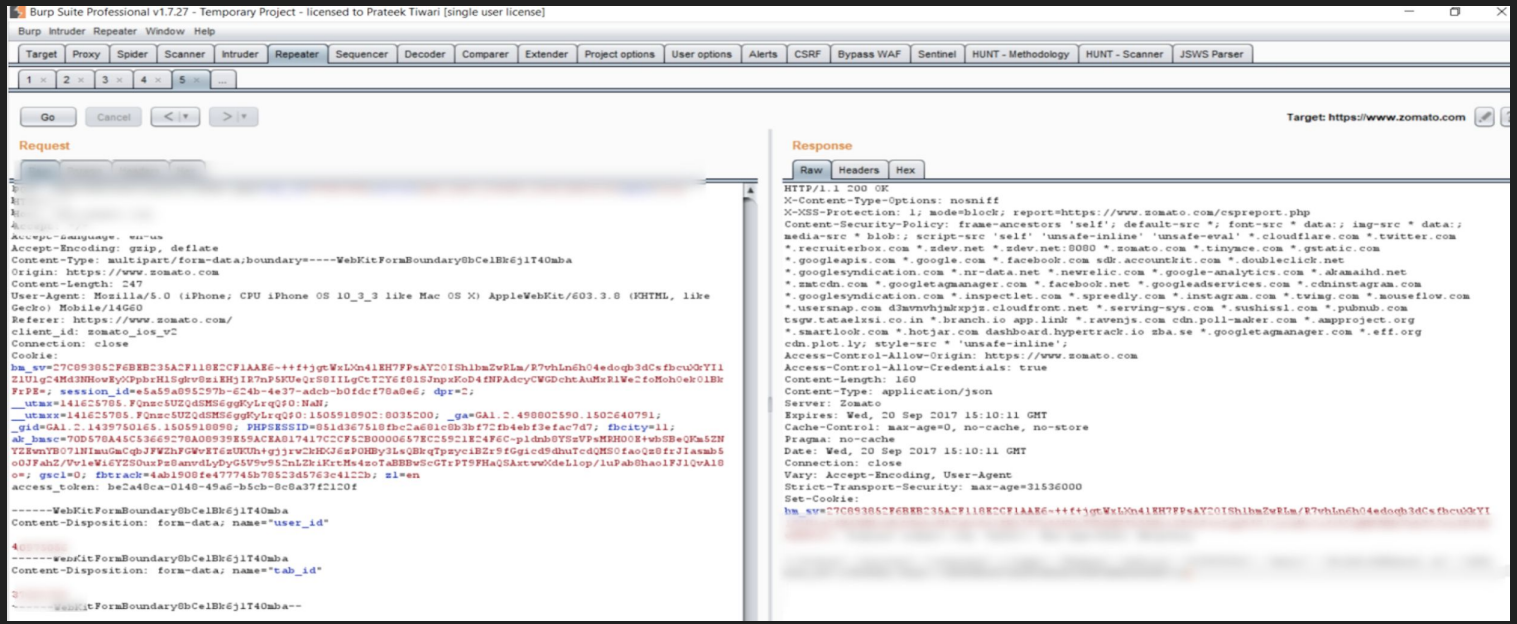
SQLi(s)
id=1’
id=1‘’
id=1’-sleep(10)-’
id=1"
id=1"“
id=1"-sleep(10)-”"
id=1/sleep(10)





Hacking with BurpSuite

- IDOR(s) are always easy, playing with the id parameters. Manipulate the create requests.
- id=1 > id=2 > Easy Money



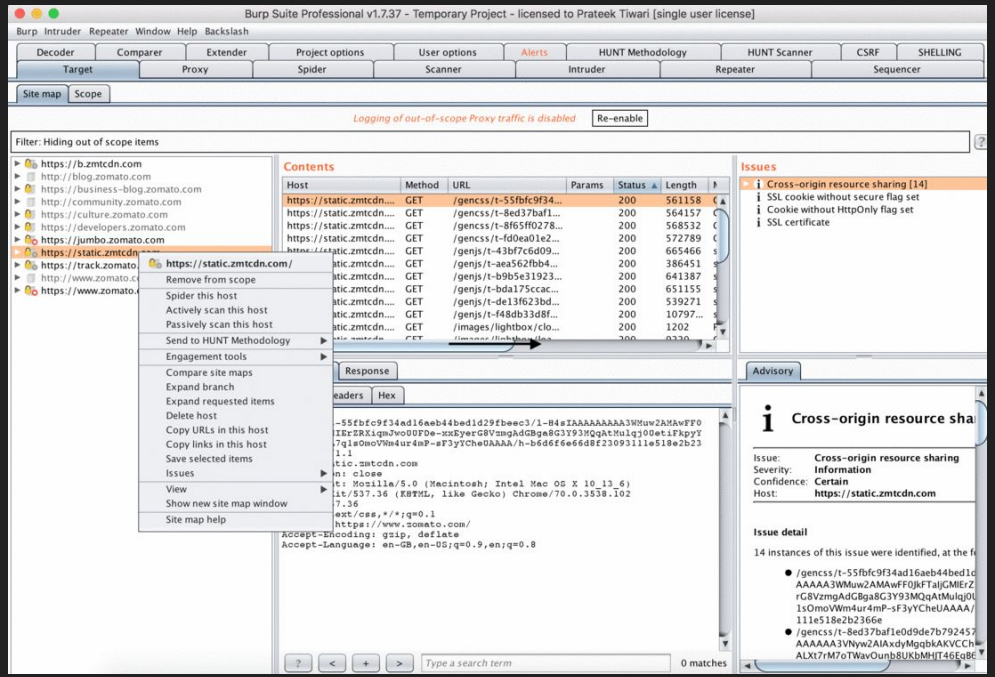
Hacking with BurpSuite

Easy Privilege Escalation with Repeater

- Have 2 different user accounts, one low privileged user and other one with some level of permissions.
- Catch the request in **BURPSUITE**, throw them into a “Repeater tab” replace the cookies of a high level privileged user with low level privileged user, see if it’s a success!

Hacking with BurpSuite

JS for the WIN



Feeding these in tools:

https://github.com/GerbenJavado/LinkFinder

Feeding these in tool

python linkfinder.py -i /Desktop/z.burp -b -o cli

```
[https://static.zmtcdn.com/images/lightbox/prev.png                                          ]
[https://static.zmtcdn.com/images/lightbox/close.png                                         ]
https://static.zmtcdn.com/images/lightbox/next.png
https://static.zmtcdn.com/images/lightbox/loading.gif
//www.youtube.com/embed/{id}
//player.vimeo.com/video/{id}
php/zfb/dashboard/dashboard_update.php
php/generate_ordering_invoices.php
php/client_permission.php?action=
php/client_permission.php?action=remove&amp;entity_id=
php/newShareWidget.php?etype=
php/client_permission.php?action=add&amp;entity_id=
php/delivery_menu_handler.php?case=confirm_drop_res&amp;res_id=
php/send_salt_link_via_email.php
promo-form-template.php?entity_id=
php/generate_new_o2_invoices.php
/{$tab}
restaurants-offer-preview.php?res_id=
clients/promoDataHandler.php
//www.youtube.com/embed/{id}
php/zfb/dashboard/dashboard_update.php
php/generate_ordering_invoices.php
php/client_permission.php?action=
php/client_permission.php?action=remove&amp;entity_id=
//player.vimeo.com/video/{id}
php/client_permission.php?action=add&amp;entity_id=
php/delivery_menu_handler.php?case=confirm_drop_res&amp;res_id=
php/send_salt_link_via_email.php
php/generate_new_o2_invoices.php
/{$tab}
php/delivery_menu_handler.php
//www.youtube.com/embed/{id}
php/zfb/dashboard/dashboard_update.php
php/generate_ordering_invoices.php
php/client_permission.php?action=
php/client_permission.php?action=remove&amp;entity_id=
images/star-line.png
images/star-fill.png
php/getDashboardSortedData.php?res_id=
php/client_permission.php?action=add&amp;entity_id=
php/delivery_menu_handler.php?case=confirm_drop_res&amp;res_id=
php/send_salt_link_via_email.php
clients/reviews.php?res_id=
php/generate_new_o2_invoices.php
/{$tab}
php/review_helpful_handler.php
```

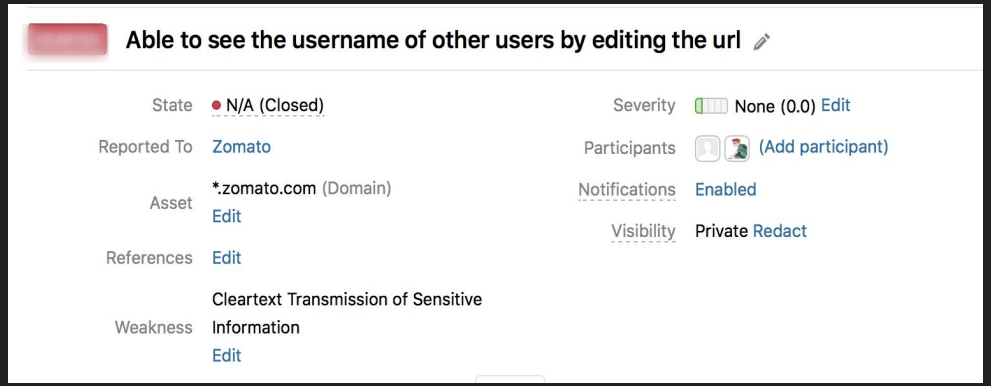
Shooting in Dark? Understand the application flow to find bugs

Shooting in Dark? Understand the application flow to find more bugs

You’re doing it wrong -

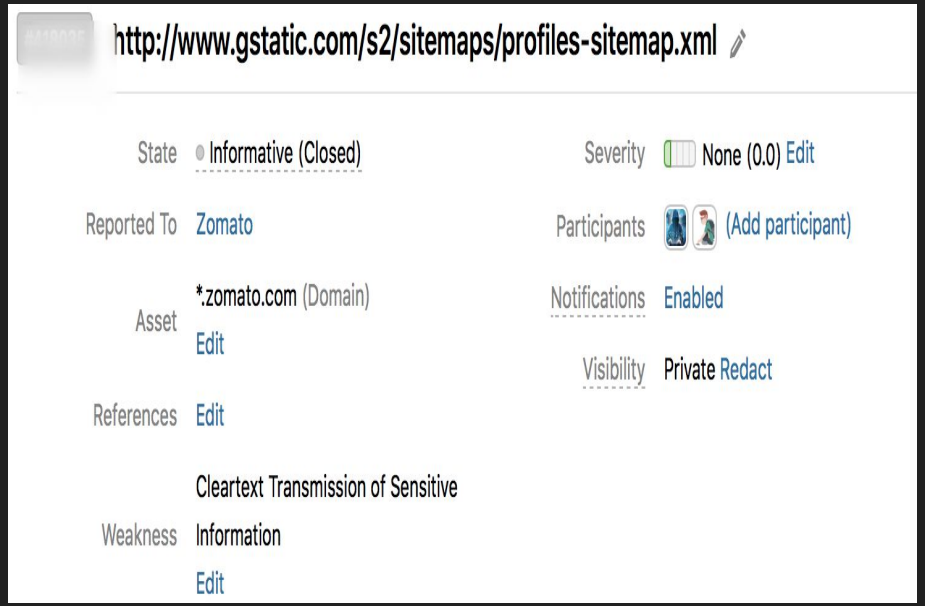
- If you haven’t spent good amount of time to study the target.
- If you haven’t understood the privileges and functionalities of a user.
- If you haven’t checked their available docs, neither gathered all the information about the target.

What happens next if you haven’t done your homework?



Shooting in Dark? Understand the application flow to find more bugs

What happens next if you haven't done your homework?

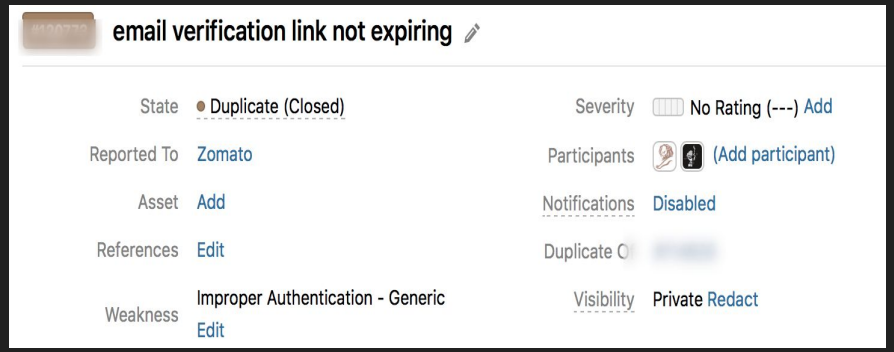


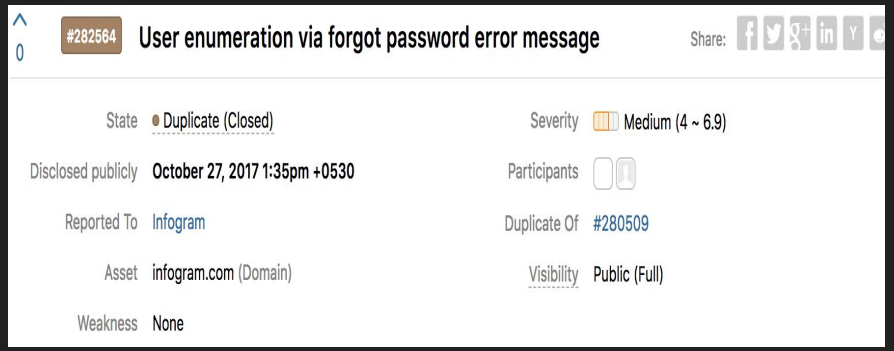
Shooting in Dark? Understand the application flow to find more bugs

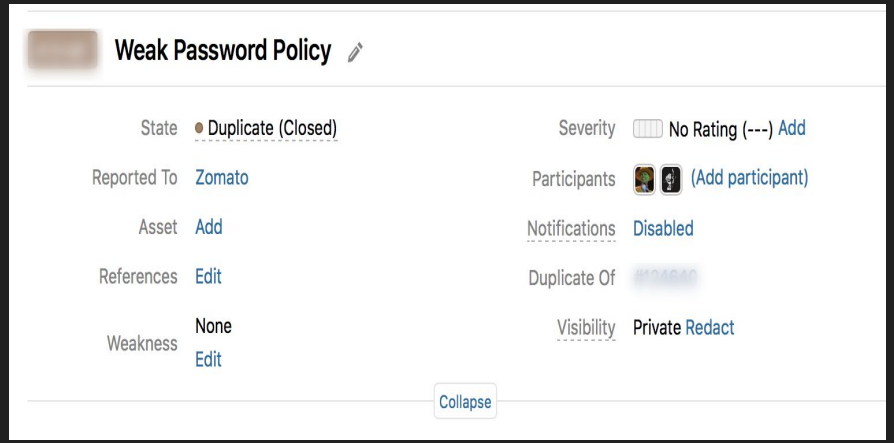
Researchers have a tendency to jump on the target application and start attacking them. What happens then?

YOU END UP GETTING DUPE

Shooting in Dark? Understand the application flow to find more bugs



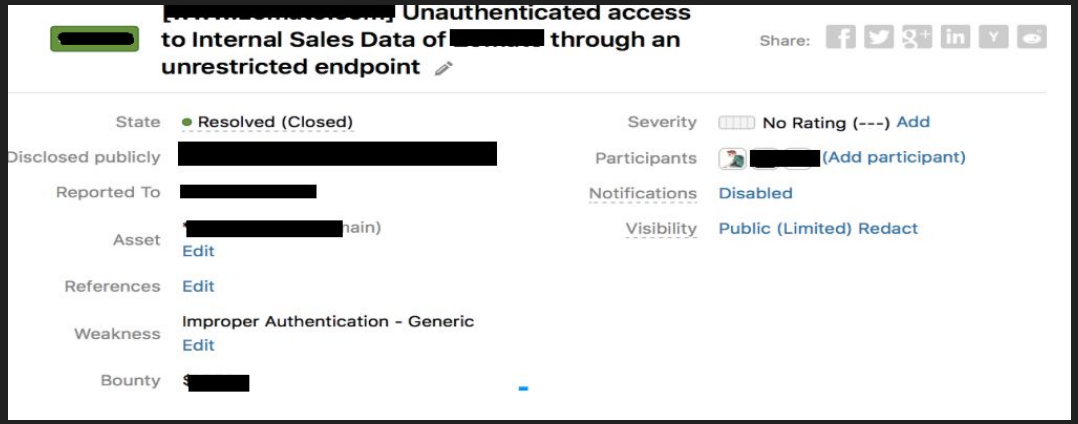




Shooting in Dark? Understand the application flow to find more bugs

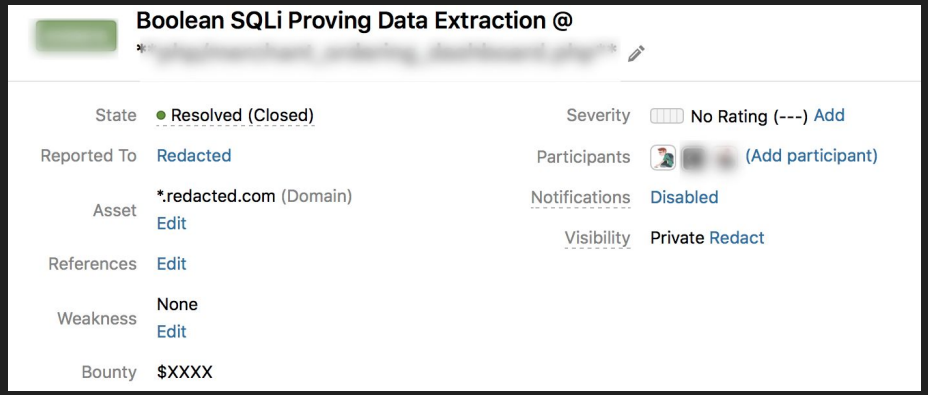
If you've invested good amount of time on a target, you will:

- Get better understanding about how the target app works.
- Know what parameters are usually being used by the target app.
- Understand the functionalities & privileges of the user's in target app.
- Be able to identify what parameters to use when you discover tons of endpoints in JS files.



Found an internal endpoint in JS and immediately knew what parameters to use based on my past research

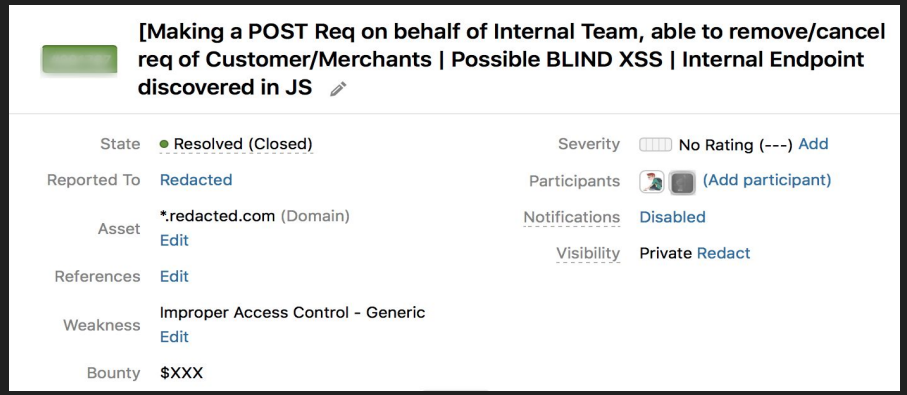
Shooting in Dark? Understand the application flow to find more bugs



Boolean SQLi Proving Data Extraction @

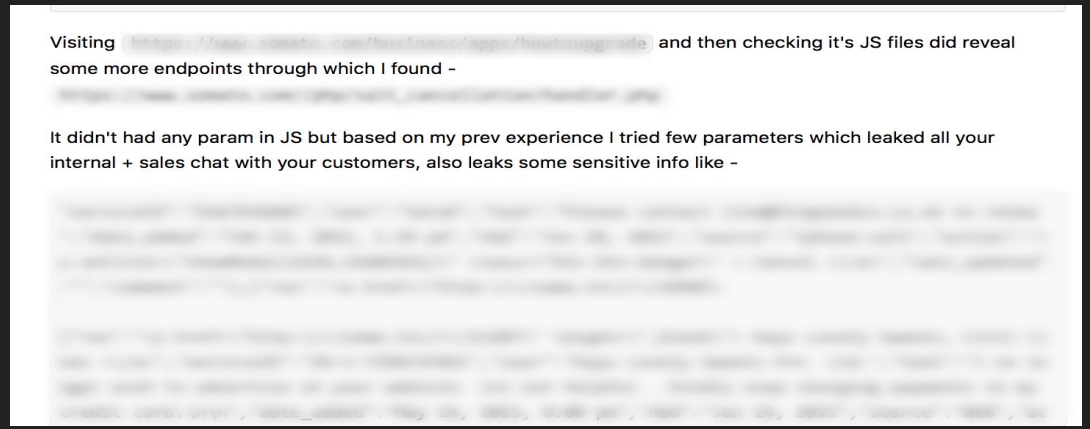
*[redacted]

State	Resolved (Closed)	Severity	No Rating (---) Add
Reported To	Redacted	Participants	(Add participant)
Asset	*.redacted.com (Domain) Edit	Notifications	Disabled
References	Edit	Visibility	Private Redact
Weakness	None Edit		
Bounty	$XXXX		



[Making a POST Req on behalf of Internal Team, able to remove/cancel req of Customer/Merchants | Possible BLIND XSS | Internal Endpoint discovered in JS

State	Resolved (Closed)	Severity	No Rating (---) Add
Reported To	Redacted	Participants	(Add participant)
Asset	*.redacted.com (Domain) Edit	Notifications	Disabled
References	Edit	Visibility	Private Redact
Weakness	Improper Access Control - Generic Edit		
Bounty	$XXX		



Visiting [redacted] and then checking it's JS files did reveal some more endpoints through which I found -

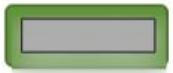
[redacted]

It didn't had any param in JS but based on my prev experience I tried few parameters which leaked all your internal + sales chat with your customers, also leaks some sensitive info like -

[redacted]

Shooting in Dark? Understand the application flow to find more bugs

Read the Docs = Get a BUG?



Sensitive Information like Email Address of Admin (Project Owner/Creator) being disclosed through an endpoint

"/api/v1/workspaces"

I was quite hesitant to report this at first place but after contacting your Support Team and reading through your Privacy Legal documentation I am pretty much sure this is a legitimate issue considering the fact that you guys give a lot of importance to users email address.

Details –

When an invited user (it should be with any invited user), here we are talking about very low privileged user [redacted] who only has an access to see their own items can actually find out an email address of an Admin (Project Owner), this shouldn't happen as per your current privacy policies if I'm correct.

Actually when I found the issue, I wanted to be sure about your privacy policy and after going through [redacted], I figured it out that [redacted] doesn't discloses the email addresses of anyone to any other users, specially not for the admins anyway. To confirm this I also contacted your support team and I got a response which states –

Shooting in Dark? Understand the application flow to find more bugs

Few Nice Reads:

- Static Analysis of Client-Side JavaScript for pen testers and bug bounty hunters - https://blog.appsecco.com/static-analysis-of-client-side-javascript-for-pen-testers-and-bug-bounty-hunters-f1cb1a5d5288
- Discovering hidden endpoints using LinkFinder - https://gerbenjavado.com/discovering-hidden-content-using-linkfinder/
- Getting started in Bug Bounty - https://medium.com/@ehsahil/getting-started-in-bug-bounty-7052da28445a

Better Bug Bounty Report

better bug reports

Better Bug Bounty Report

better bug reports

better relationship

Better Bug Bounty Report

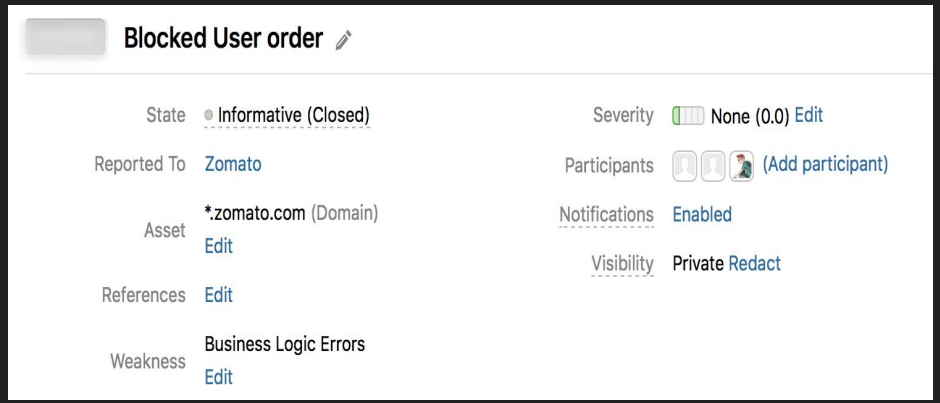
better bug reports

better relationship

better bounties

Sharing from other side of the fence

What you shouldn't do?



Sharing from other side of the fence

- What you shouldn’t do?
- Follow up after 5 mins of report submission
- Bounty Plz!
- Contacting someone from Security Team on Twitter asking for an update.

Sharing from other side of the fence

The Wrong Way,

How not to submit a report?

Affected Link:- https://www.zomato.com/restaurants" onmouseover=prompt(/XSS/) very bad

steps to reproduce

1.open vulnerable url

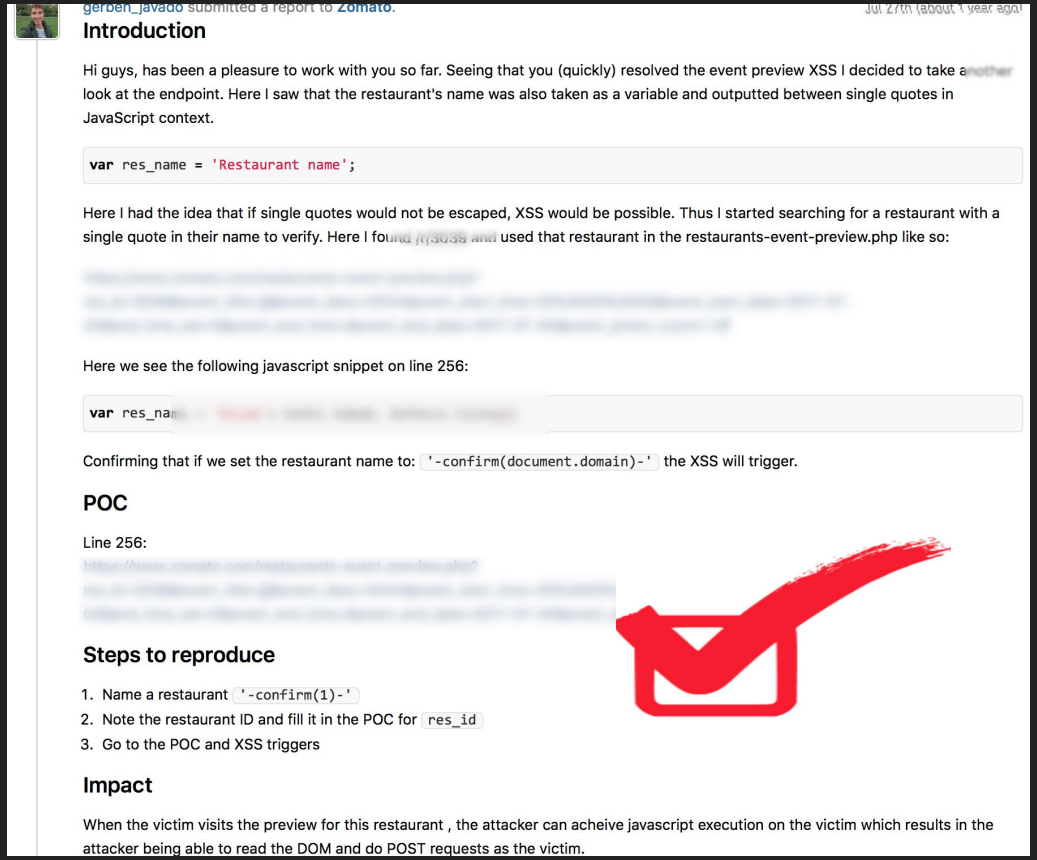
2.Hover mouse the XSS pop up will be work.

Bounty pls rward

Sharing from other side of the fence

The Right Way -

- Introduction
- Details
- Steps to reproduce (POC)
- Impact



gerben_javado submitted a report to Zomato. Jul 27th (about 1 year ago)

Introduction

Hi guys, has been a pleasure to work with you so far. Seeing that you (quickly) resolved the event preview XSS I decided to take another look at the endpoint. Here I saw that the restaurant's name was also taken as a variable and outputted between single quotes in JavaScript context.

```
var res_name = 'Restaurant name';
```

Here I had the idea that if single quotes would not be escaped, XSS would be possible. Thus I started searching for a restaurant with a single quote in their name to verify. Here I found [redacted] and used that restaurant in the restaurants-event-preview.php like so:

[redacted]

Here we see the following javascript snippet on line 256:

```
var res_na[redacted]
```

Confirming that if we set the restaurant name to: `'-confirm(document.domain)-'` the XSS will trigger.

POC

Line 256:

[redacted]

Steps to reproduce

1. Name a restaurant `'-confirm(1)-'`
2. Note the restaurant ID and fill it in the POC for `res_id`
3. Go to the POC and XSS triggers

Impact

When the victim visits the preview for this restaurant , the attacker can acheive javascript execution on the victim which results in the attacker being able to read the DOM and do POST requests as the victim.

Sharing from other side of the fence

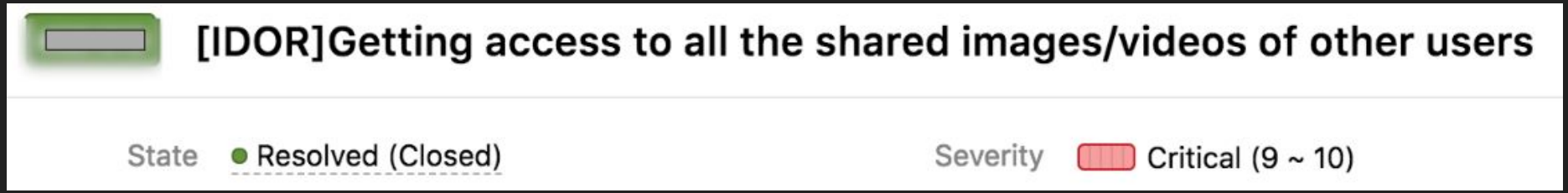
Before reporting, always think from organization's point of view and think from the other side -

Understand companies nature of business

Seeing an image of other users on a company like Zomato? Seriously are you kidding me? That's not sensitive at all - Closing it as N/A

VS

Viewing others uploaded images on an Image Sharing Site



Sharing from other side of the fence

Mantra to build a strong relationship with Security team

- Be Professional with your communication
- While Submitting a report, provide detailed report with clear steps to reproduce
- Don’t bug or spam them, prepare a schedule for follow up’s
- Don’t do this - send a LinkedIn invite, or DM on Twitter asking for an update

Keeping up with new trends

….Staying on top of new hacking trends can help you earn more bounties.

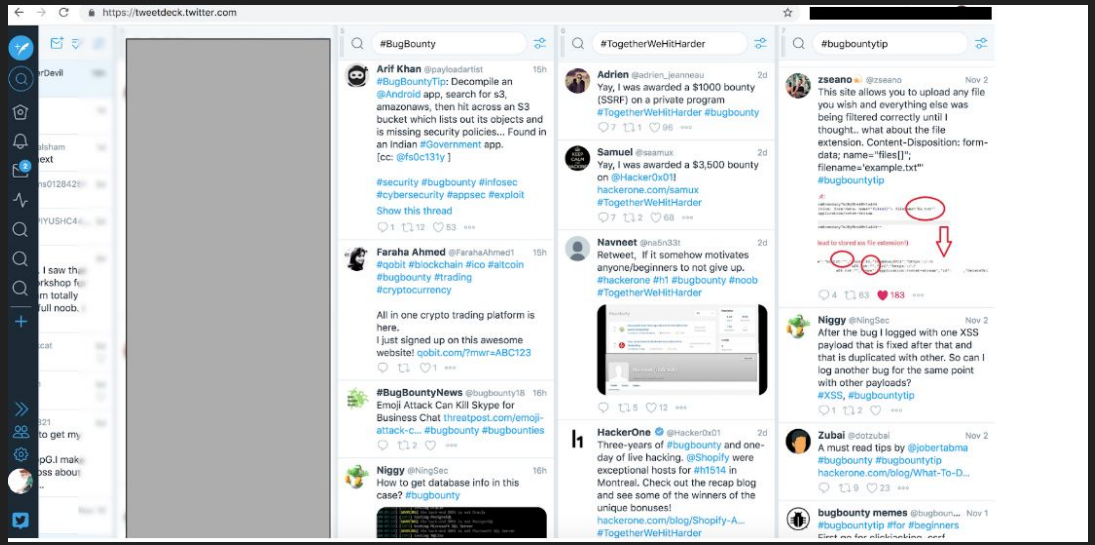
Keeping up with new trends

Sir, what should we do to keep up with all the new trends?

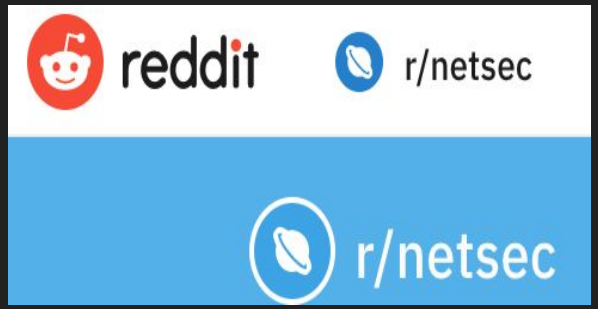
#BugBounty #BugBountyTip #TogetherWeHitHarder

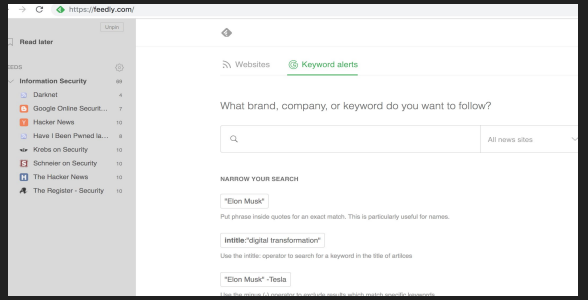
Medium

Subscribe to topics like Information Security, Bug Bounty, Infosec, etc..



Keeping up with new trends



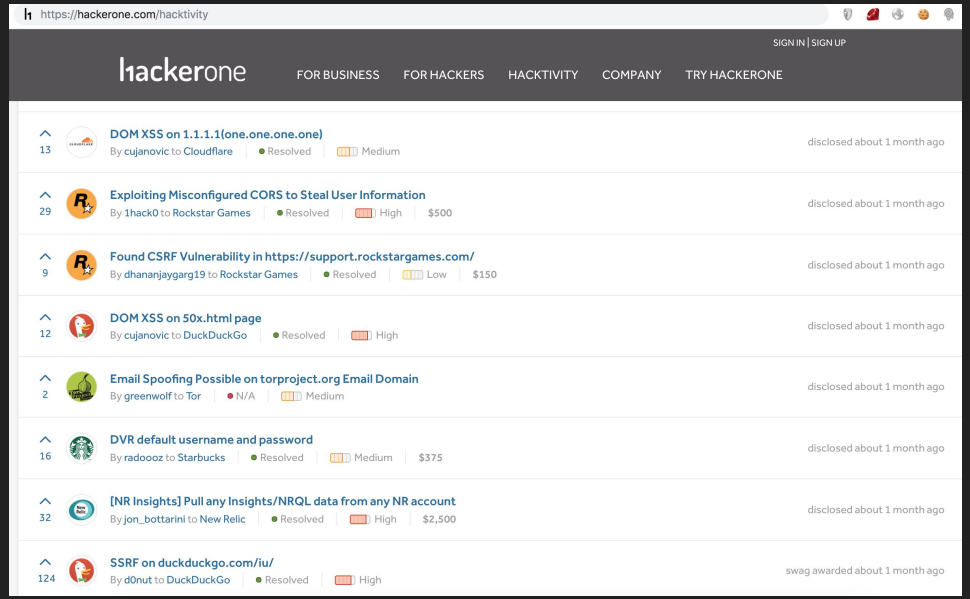


IT'S ALL ABOUT SOURCES

The Hacker News

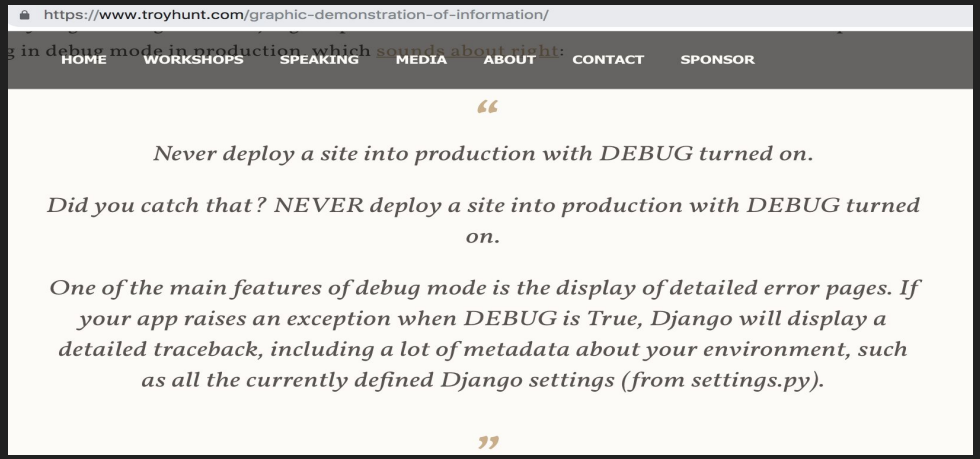
Keeping up with new trends

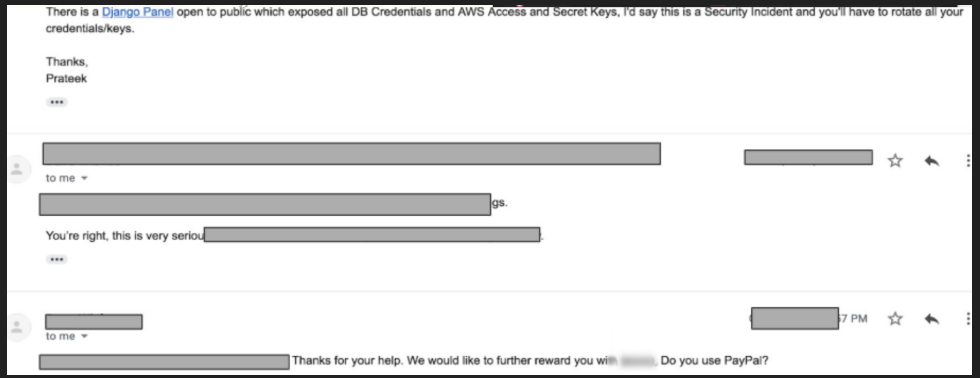
Hacktivity! https://hackerone.com/hacktivity

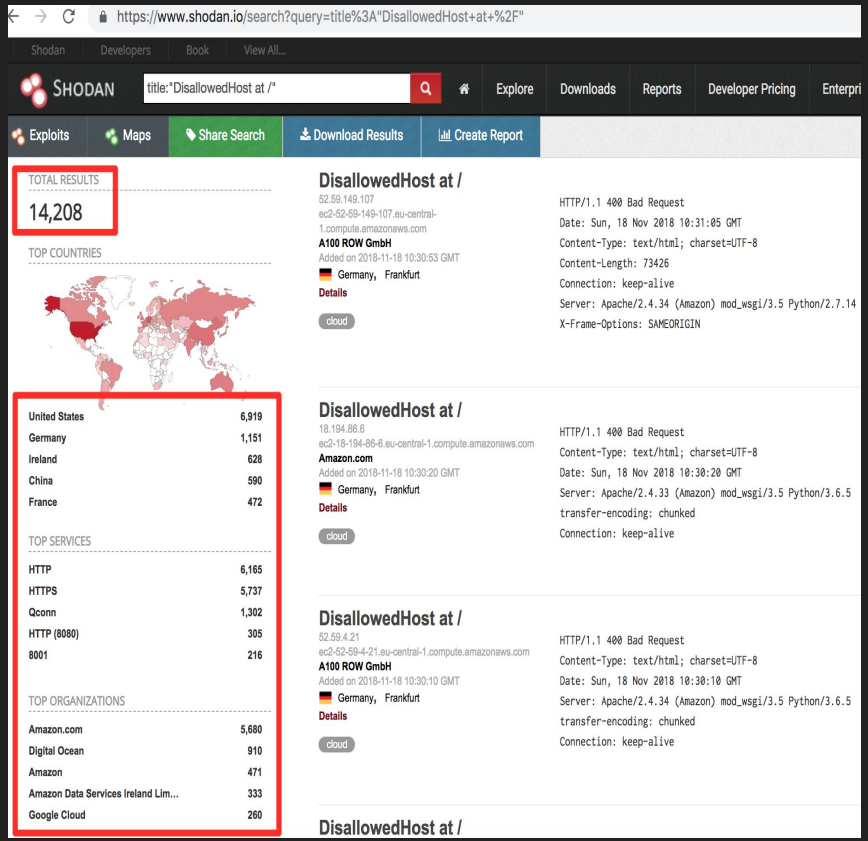


ZERO DAILY!
https://hackerone.com/zerodaily

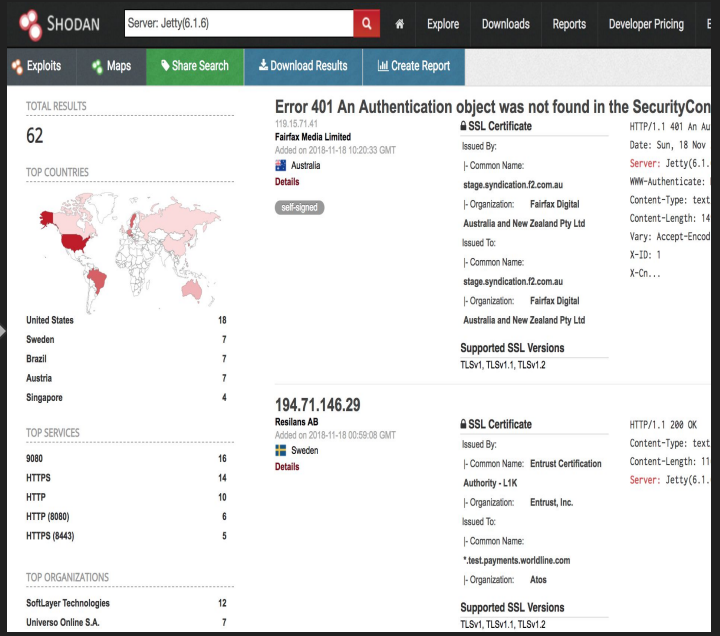
Profit!! Time to earn bounties...



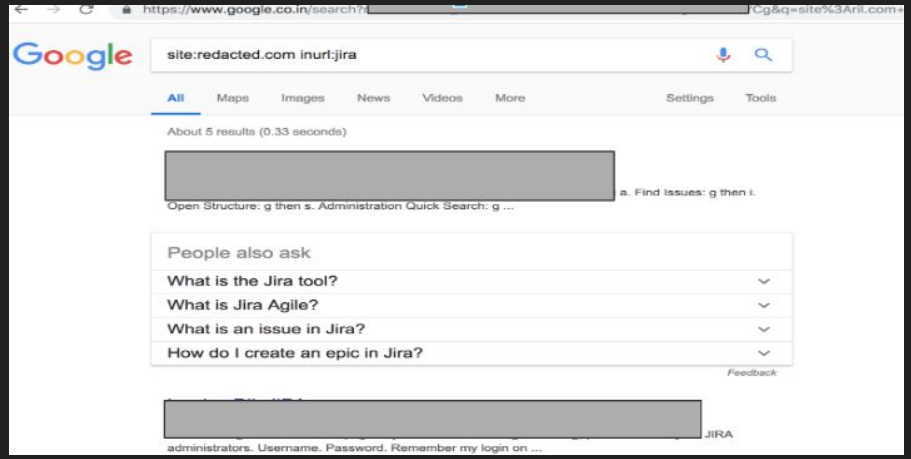




Profit!! Time to earn bounties...

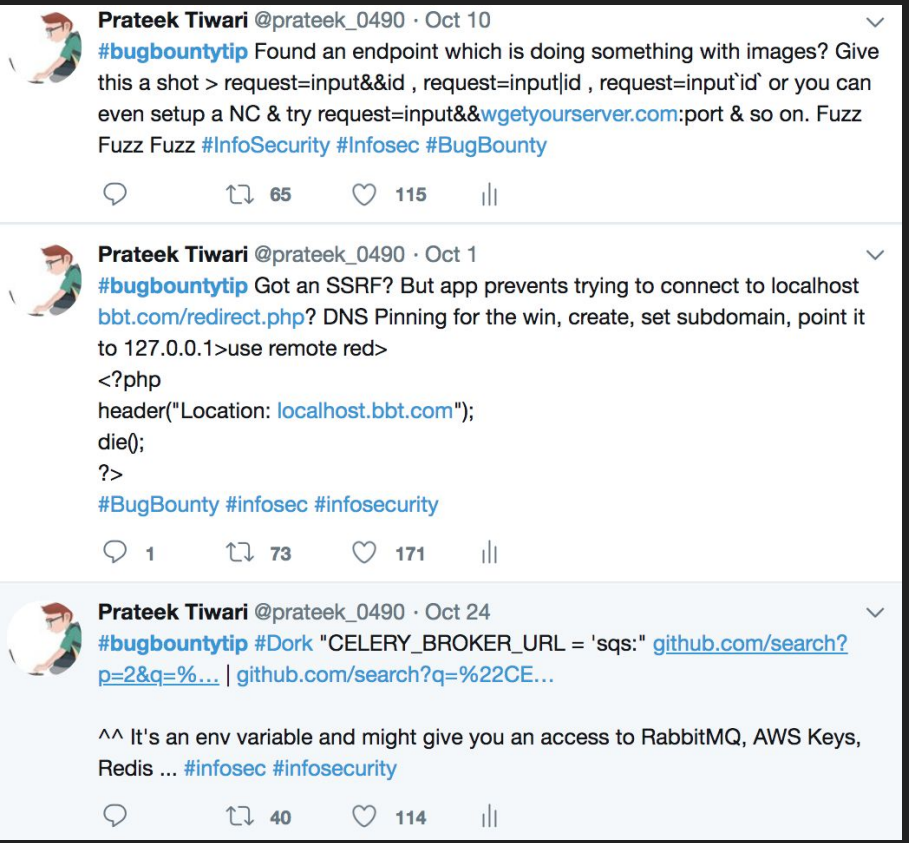


Profit!! Time to earn bounties...



LIVE BURP SUITE SESSION

#bugbountytip



Prateek Tiwari @prateek_0490 · Oct 10

#bugbountytip Found an endpoint which is doing something with images? Give this a shot > request=input&&id , request=input|id , request=input`id` or you can even setup a NC & try request=input&&wgetyourserver.com:port & so on. Fuzz Fuzz Fuzz #InfoSecurity #Infosec #BugBounty

65 115

Prateek Tiwari @prateek_0490 · Oct 1

#bugbountytip Got an SSRF? But app prevents trying to connect to localhost bbt.com/redirect.php? DNS Pinning for the win, create, set subdomain, point it to 127.0.0.1>use remote red>

```
<?php
header("Location: localhost.bbt.com");
die();
?>
```

#BugBounty #infosec #infosecurity

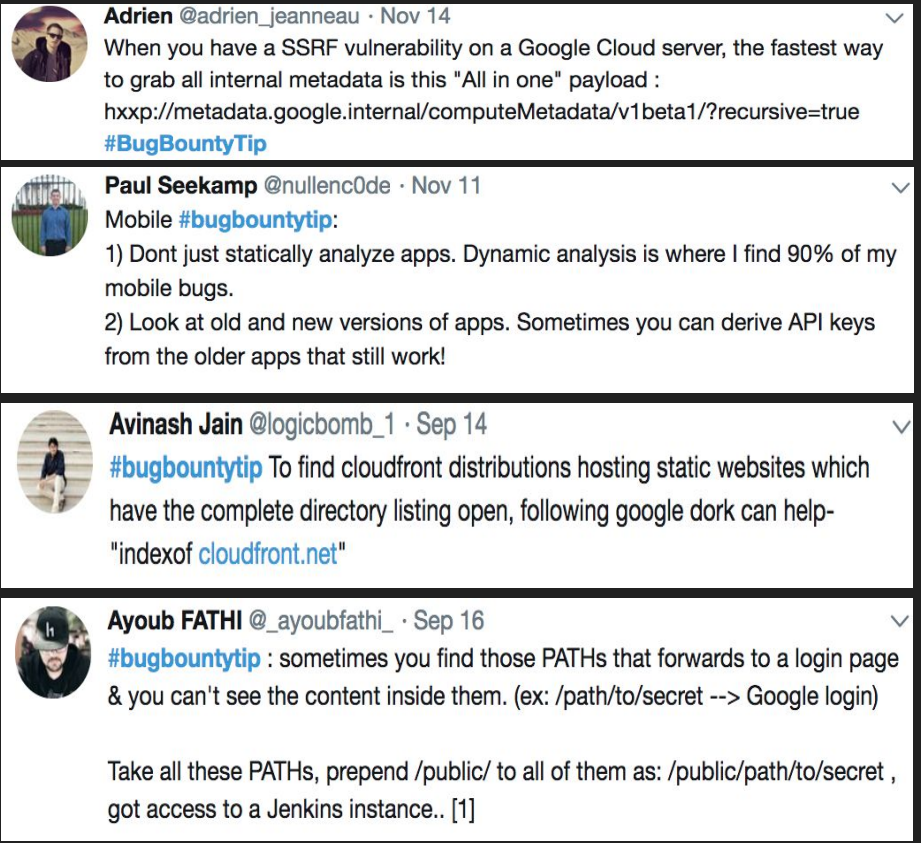
1 73 171

Prateek Tiwari @prateek_0490 · Oct 24

#bugbountytip #Dork "CELERY_BROKER_URL = 'sqs:" github.com/search?p=2&q=%… | github.com/search?q=%22CE…

^^ It's an env variable and might give you an access to RabbitMQ, AWS Keys, Redis ... #infosec #infosecurity

40 114



Adrien @adrien_jeanneau · Nov 14

When you have a SSRF vulnerability on a Google Cloud server, the fastest way to grab all internal metadata is this "All in one" payload : hxxp://metadata.google.internal/computeMetadata/v1beta1/?recursive=true #BugBountyTip

Paul Seekamp @nullenc0de · Nov 11

Mobile #bugbountytip:

1) Dont just statically analyze apps. Dynamic analysis is where I find 90% of my mobile bugs.

2) Look at old and new versions of apps. Sometimes you can derive API keys from the older apps that still work!

Avinash Jain @logicbomb_1 · Sep 14

#bugbountytip To find cloudfront distributions hosting static websites which have the complete directory listing open, following google dork can help- "indexof cloudfront.net"

Ayoub FATHI @_ayoubfathi_ · Sep 16

#bugbountytip : sometimes you find those PATHs that forwards to a login page & you can't see the content inside them. (ex: /path/to/secret --> Google login)

Take all these PATHs, prepend /public/ to all of them as: /public/path/to/secret , got access to a Jenkins instance.. [1]

#bugbountytip

Streaak2 @streaak · Jul 6

bug bounty tip: Use commoncrawl for finding subdomains and endpoints. Sometimes you find endpoints that can't directly be visited from the UI but has been indexed from other sites-
curl -sX GET "index.commoncrawl.org/CC-MAIN-2018-2..." | jq -r .url | sort -u
#bugbounty **#bugbountytip**

BugBountyTips @TipsBug · Jul 18

Use whoxy.com and community.riskiq.com to find more about your target, it can return much more results than active scanning tools! **#bugbountytip** #OSINT

Paresh @Paresh_parmar1 · Jul 30

#bugbountytip
purchase paid version of product, list out all the endpoints which is only available for paid user.
and try to play those endpoints in free version of product. see if you can use paid version's features in free version.

Prateek Tiwari @prateek_0490 · May 22

#bugbountytip If you come across a request which has diff action(s), ex - example[dot]com/someendpoint?type=search&query=test, always try different action like `type=users`, `type= accounts`, `type= details`, you might get some good surprises ;) #BugBounty #TogetherWeHitHarder

Procrastinator @tweetrpersonal9 · Apr 21

#bugbountytip Try to recon storage.googleapis.com/Org-name-here you may find internal documentation which aren't supposed to be public.

Kushagra Pathak @xKushagra · Apr 25

#bugbountytip #osint: Search for public Trello boards of companies, to find login credentials, API keys, etc. or if you aren't lucky enough, then you may find companies' Team Boards sometimes with tasks to fix security vulnerabilities

ak1t4 @akita_zen · Apr 21

Bug bounty tip: If you got 'Subdomain Takeover' don't report it yet, look at the main site/app for gain privileges: like a potential CSP policy bypass (or session hijacking via Set-cookie: *.domain.com. When you got ST you have P0wer!
#bugbounty **#bugbountytip**

Sami @SamiDrif · Apr 28

#bugbountytip: remember that Github is your friend
- Check dotfiles of company's employees
- Search for DevOps projects shared (fork) between employees (ansible, Cassandra, Azure,..) => you get Login credential, API key, Private keys
- Always follow the manual approach 😀

#bugbountytip

#bugbountytip

Waybackurls

Scrape URLs using - https://github.com/tomnomnom/waybackurls/

root@pt:**~/tools/recon/waybackurl**$ cat domains.txt | waybackurls > urls

root@pt:**~/tools/recon/waybackurl**$ cat urls | grep ".js"

```
http://www.zomato.com:80/auckland/restaurants/tag-ajs-work
http://www.zomato.com:80/auckland/restaurants/tag-auntie-js-rolled-pavlova
http://www.zomato.com:80/auckland/restaurants?q=ljs
https://www.zomato.com/austin/gtm.js
https://www.zomato.com/australian-capital-territory/gtm.js
https://www.zomato.com/baltimore/gtm.js
https://www.zomato.com/bowral-nsw/gtm.js
https://www.zomato.com/braidwood-nsw/gtm.js
https://www.zomato.com/byron-bay-nsw/gtm.js
https://www.zomato.com/gtm.js
https://www.zomato.com/melbourne/gtm.js
https://www.zomato.com/new-york-city/gtm.js
https://www.zomato.com/perth/gtm.js
https://www.zomato.com/pl/mumbai/restauracje/nowoczesne-indyjskie
```

waybackurls

Accept line-delimited domains on stdin, fetch known URLs from the Wayback Machine for `*.domain` and output them on stdout.

Usage example:

```
▶ cat domains.txt | waybackurls > urls
```

Install:

```
▶ go get github.com/tomnomnom/waybackurls
```

#bugbountytip

Bringing few more #tips:

- Search for developers, QA on Stackoverflow
- Always run wfuzz / dirsearch on all subdomain(s) found to discover more content, more bounties?
- Earlier this year, I got a bounty for redacted.corp.com/documentation and found an excel spreadsheet of the database, eehhh, easy money 🤑
- Can’t CSRF delete method? Few frameworks / API(s) allows to “fake” methods by additional parameters, ex:
    - Adding a parameter such as: method=delete | _method=delete -> API will parse it as a Delete request.

#bugbountytip

Sir, please one more! Okay, take this ezzy money!

- Always check if Strict transport security is enforced? Many a times, hxxp://redacted.com is not redirected to https, many companies are interested to hear about “Weak Login function over HTTP”.

[redacted]login] - Misconfigured SSL leading to cleartext submission of password at [redacted]/login

State	● Resolved (Closed)	Severity	No Rating (---)
Reported To	[redacted]	Participants	
Weakness	Cleartext Transmission of Sensitive Information	Visibility	Private
Bounty	$[redacted]		

Recap | Let’s Roll It Back

- Dive deep into the target using Passive techniques:
  - Virustotal
  - crt.sh
  - censys.io
  - https://transparencyreport.google.com/https/certificates?hl=en
  - https://developers.facebook.com/tools/ct
  - CSP Headers
  - Don't forget the third party services, those are so helpful and always helps you to learn more about the target
- Shodan.io and fofa.so will give you a lot of juicy stuffs.
- Always give a shot at Mobile Apps - use apkscan.nviso.be | virustotal …
- Submit better reports, think from the other side about the impact before submitting.
- Keeping up with what’s happening around will help you earn more bounties.

Thank You

Prateek Tiwari

 prateek0490@gmail.com

 @prateek_0490

 linkedin.com/in/prateek-tiwari-867b905a/

 facebook.com/prateek0490