C1h2e1 Follow

Dec 21, 2019 · 11 min read · Listen

Save

# BUG BOUNTY CHECK LIST BY C1

**I just want to write a check list for myself. This article includes various vulnerability discovery method bypass methods. I hope you can read it carefully .**

Twitter @C1h2e11

Wechat : C1h2e1

## RECON

Most of my recon ideas come from nahamsec, he is really good

When I get a target, I first do a lot of information collection, such as Subdomain, IP, Port, File I get a target, I first do a lot of information collection, such as Subdomain, IP, Port, Endpoint

For subdomains, I will use crt.sh to find them. In the face of big goals, I will choose some interesting words, such as api, prod, dev, stage,backend, admin. Etc.

### Subdomian

Let’s take yahoo as an example

**crt.sh | %.yahoo.com**

Free CT Log Certificate Search Tool from Sectigo (formerly Comodo CA)

crt.sh

Use % to find the domain name you want . Here is a shell script to quickly collect some subdomains

```
curl https://www.threatcrowd.org/searchApi/v2/domain/report/\?
domain=$1 |jq .subdomains |grep -o ‘\w.*$1’

curl https://api.hackertarget.com/hostsearch/\?q\=$1 | grep -o
'\w.*$1'
curl https://crt.sh/?q=%.$1 | grep "$1" | cut -d '>' -f2 | cut -d '<'
-f1 | grep -v " " | sort -u

curl https://certspotter.com/api/v0/certs?domain=$1 | grep  -o '\
[\".*\"\]'
```

Many times we will encounter domain can not be accessed at this time we can use httprobe to detect

**tomnomnom/httprobe**

Take a list of domains and probe for working http and https servers. ▶ go get -u github.com/tomnomnom/httprobe httprobe…

github.com

But certificate-based subdomains are incomplete and require some bruteforce I recommend using Sublist3r

**aboul3la/Sublist3r**

Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and…

github.com

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or...

github.com

Documents here

**GitHub tools collection**

This is the current thread in the bug hunter community: how to find sensitive informations on GitHub. Understand how to...

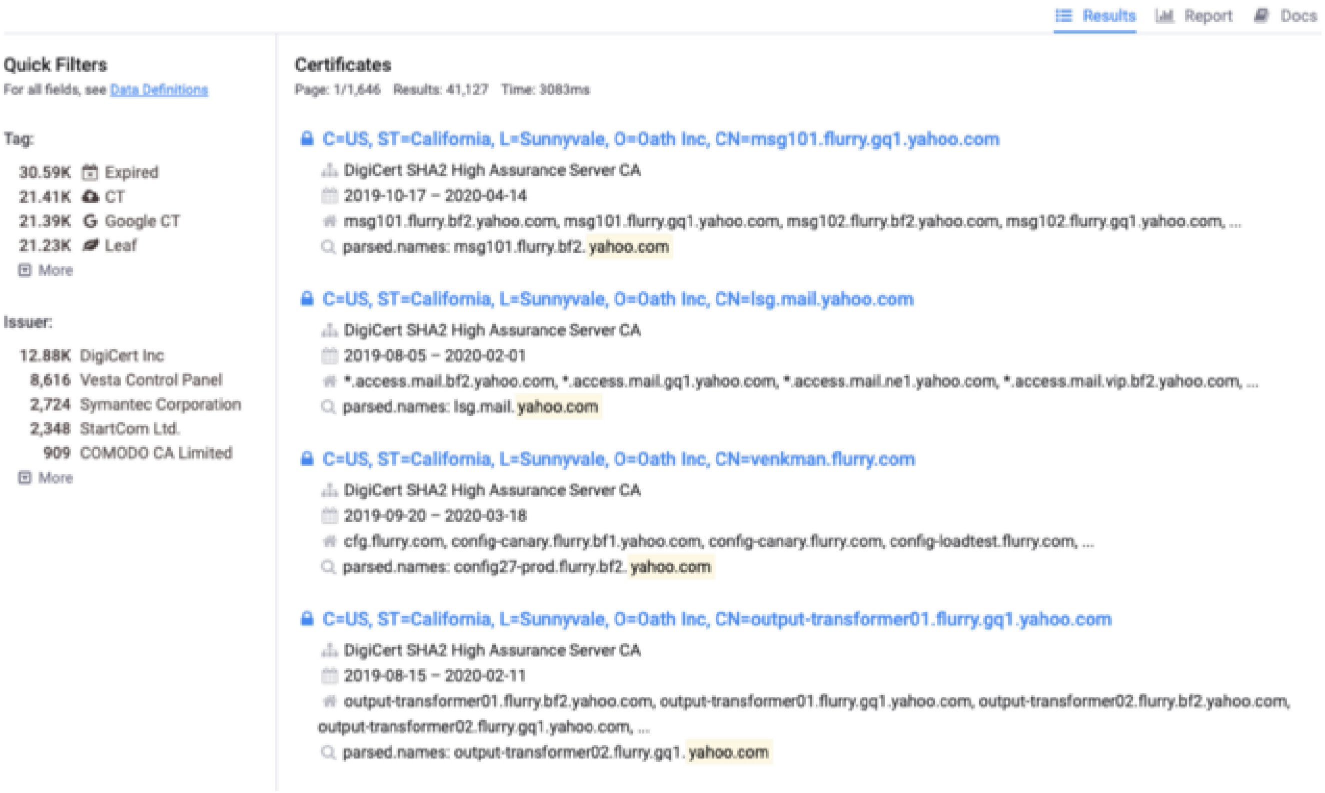
10degres.net

Here is the subdomain collection method I often use You can use platforms like shodan and zoomeye. I won't go into details here.

### IP

Censys.io ipinfo.io shodan.io

censys is a certificate-based query that can find many IP addresses I have found many bugs with it .We just need to query your target domain .You can click on the certificate on the right



Quick Filters
For all fields, see Data Definitions

Tag:

| | |
|---|---|
| 30.59K | Expired |
| 21.41K | CT |
| 21.39K | Google CT |
| 21.23K | Leaf |

More

Issuer:

| | |
|---|---|
| 12.88K | DigiCert Inc |
| 8,616 | Vesta Control Panel |
| 2,724 | Symantec Corporation |
| 2,348 | StartCom Ltd. |
| 909 | COMODO CA Limited |

More

Certificates
Page: 1/1,646 Results: 41,127 Time: 3083ms

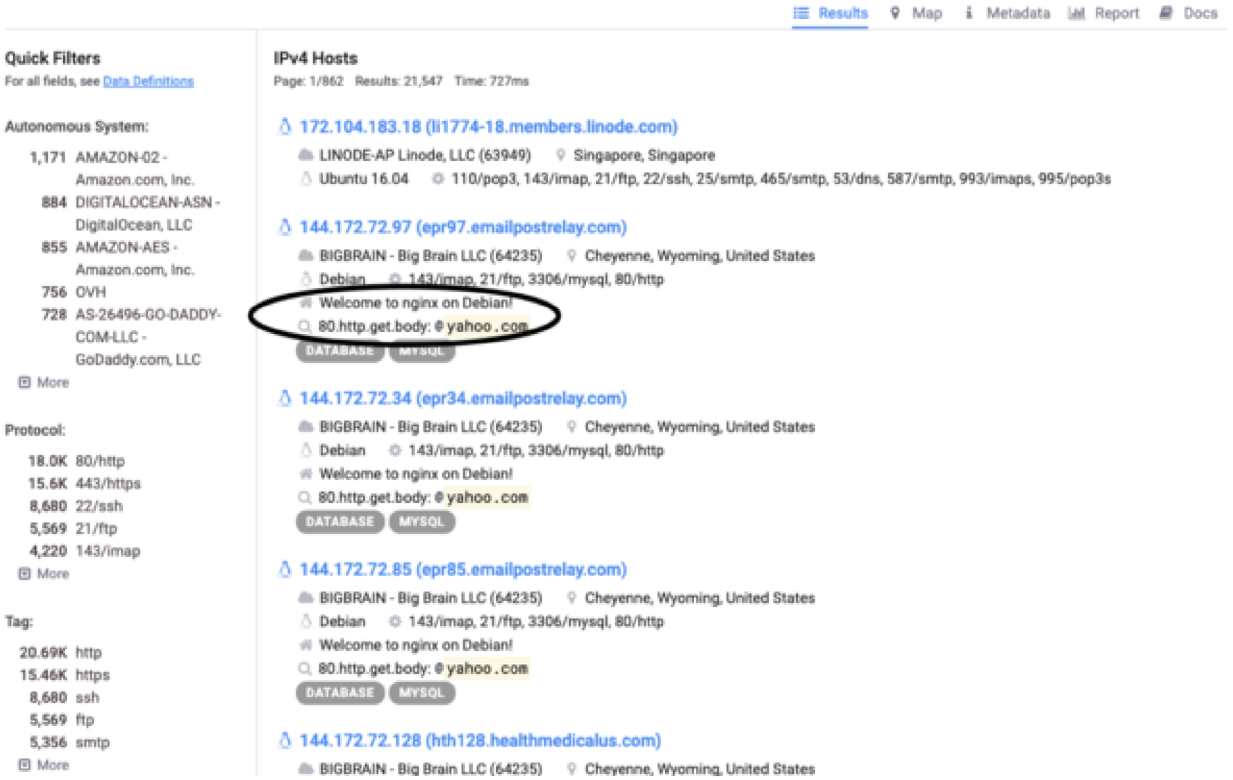
C=US, ST=California, L=Sunnyvale, O=Oath Inc, CN=msg101.flurry.gq1.yahoo.com
DigiCert SHA2 High Assurance Server CA
2019-10-17 – 2020-04-14
msg101.flurry.bf2.yahoo.com, msg101.flurry.gq1.yahoo.com, msg102.flurry.bf2.yahoo.com, msg102.flurry.gq1.yahoo.com, ...
parsed.names: msg101.flurry.bf2. yahoo.com

C=US, ST=California, L=Sunnyvale, O=Oath Inc, CN=lsg.mail.yahoo.com
DigiCert SHA2 High Assurance Server CA
2019-08-05 – 2020-02-01
*.access.mail.bf2.yahoo.com, *.access.mail.gq1.yahoo.com, *.access.mail.ne1.yahoo.com, *.access.mail.vip.bf2.yahoo.com, ...
parsed.names: lsg.mail. yahoo.com

C=US, ST=California, L=Sunnyvale, O=Oath Inc, CN=venkman.flurry.com
DigiCert SHA2 High Assurance Server CA
2019-09-20 – 2020-03-18
cfg.flurry.com, config-canary.flurry.bf1.yahoo.com, config-canary.flurry.com, config-loadtest.flurry.com, ...
parsed.names: config27-prod.flurry.bf2. yahoo.com

C=US, ST=California, L=Sunnyvale, O=Oath Inc, CN=output-transformer01.flurry.gq1.yahoo.com
DigiCert SHA2 High Assurance Server CA
2019-08-15 – 2020-02-11
output-transformer01.flurry.bf2.yahoo.com, output-transformer01.flurry.gq1.yahoo.com, output-transformer02.flurry.bf2.yahoo.com, output-transformer02.flurry.gq1.yahoo.com, ...
parsed.names: output-transformer02.flurry.gq1. yahoo.com

Here you can see the subdomain name and we can use IPV4 to query. There will be an IPV4 address. If it is in Scope, we can test it. Note the get body of this mark. He takes the content in the response, so most of it is not yours Target asset



Quick Filters
For all fields, see Data Definitions

Autonomous System:

| | |
|---|---|
| 1,171 | AMAZON-02 - Amazon.com, Inc. |
| 884 | DIGITALOCEAN-ASN - DigitalOcean, LLC |
| 855 | AMAZON-AES - Amazon.com, Inc. |
| 756 | OVH |
| 728 | AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC |

More

Protocol:

| | |
|---|---|
| 18.0K | 80/http |
| 15.6K | 443/https |
| 8,680 | 22/ssh |
| 5,569 | 21/ftp |
| 4,220 | 143/imap |

More

Tag:

| | |
|---|---|
| 20.69K | http |
| 15.46K | https |
| 8,680 | ssh |
| 5,569 | ftp |
| 5,356 | smtp |

More

IPv4 Hosts
Page: 1/862 Results: 21,547 Time: 727ms

172.104.183.18 (li1774-18.members.linode.com)
LINODE-AP Linode, LLC (63949) Singapore, Singapore
Ubuntu 16.04 110/pop3, 143/imap, 21/ftp, 22/ssh, 25/smtp, 465/smtp, 53/dns, 587/smtp, 993/imaps, 995/pop3s

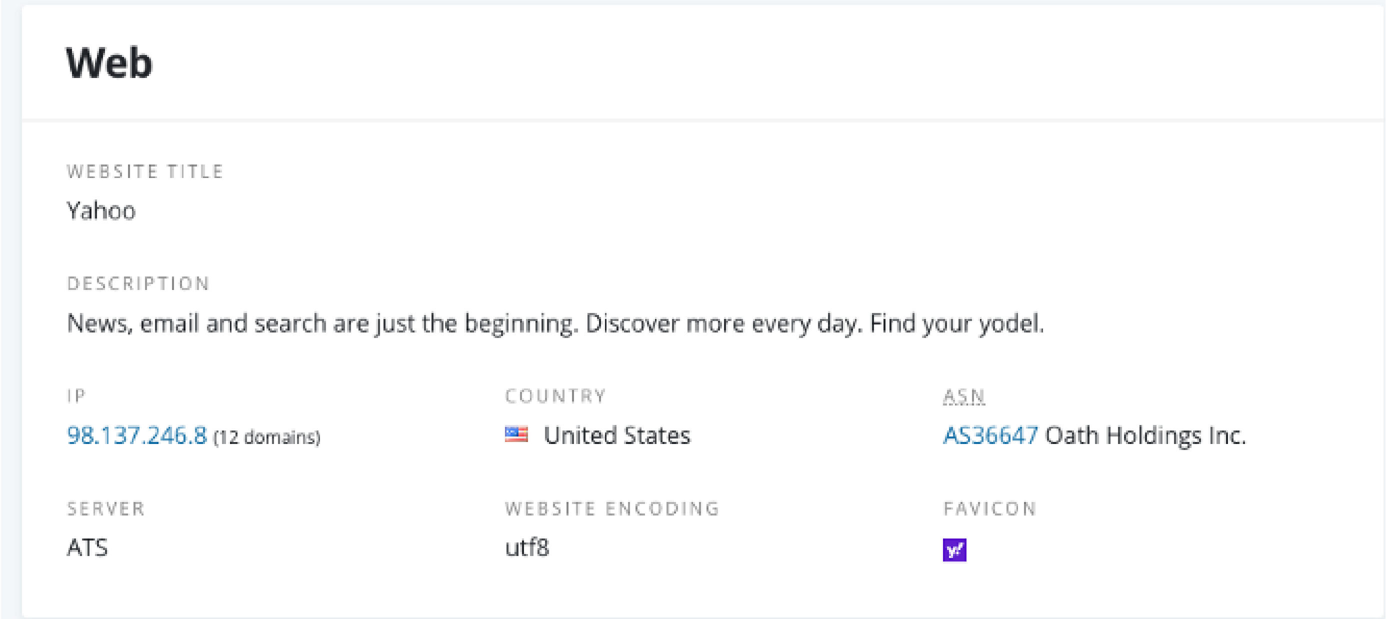
144.172.72.97 (epr97.emailpostrelay.com)
BIGBRAIN - Big Brain LLC (64235) Cheyenne, Wyoming, United States
Debian 143/imap, 21/ftp, 3306/mysql, 80/http
Welcome to nginx on Debian!
80.http.get.body: @yahoo.com
DATABASE MYSQL

144.172.72.34 (epr34.emailpostrelay.com)
BIGBRAIN - Big Brain LLC (64235) Cheyenne, Wyoming, United States
Debian 143/imap, 21/ftp, 3306/mysql, 80/http
Welcome to nginx on Debian!
80.http.get.body: @yahoo.com
DATABASE MYSQL

144.172.72.85 (epr85.emailpostrelay.com)
BIGBRAIN - Big Brain LLC (64235) Cheyenne, Wyoming, United States
Debian 143/imap, 21/ftp, 3306/mysql, 80/http
Welcome to nginx on Debian!
80.http.get.body: @yahoo.com
DATABASE MYSQL

144.172.72.128 (hth128.healthmedicalus.com)
BIGBRAIN - Big Brain LLC (64235) Cheyenne, Wyoming, United States

ipinfo and hostinfo.io can be used to query ASN codes and network segments .We can use shodan to combine with him



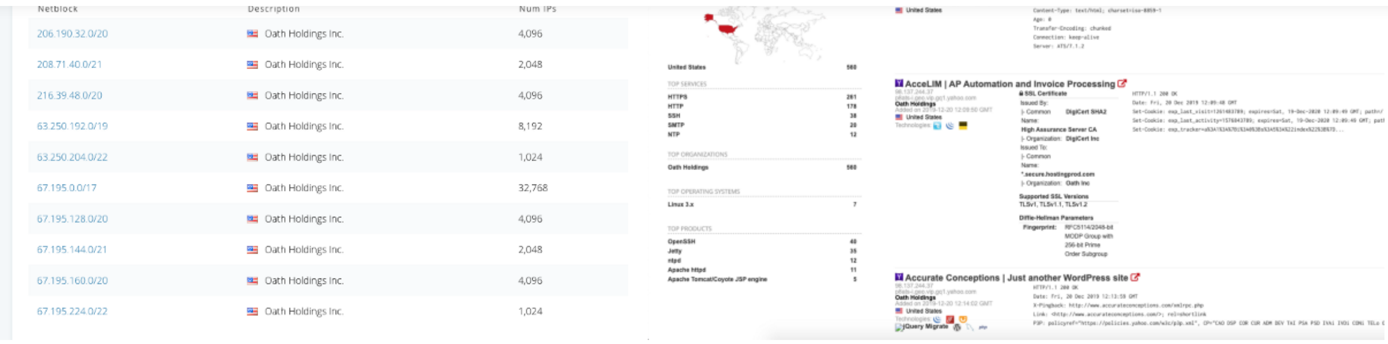
Web

WEBSITE TITLE
Yahoo

DESCRIPTION
News, email and search are just the beginning. Discover more every day. Find your yodel.

| IP | COUNTRY | ASN |
|---|---|---|
| 98.137.246.8 (12 domains) | United States | AS36647 Oath Holdings Inc. |

| SERVER | WEBSITE ENCODING | FAVICON |
|---|---|---|
| ATS | utf8 | y! |



| Netblock | Description | Num IPs |
|---|---|---|
| 206.190.32.0/20 | Oath Holdings Inc. | 4,096 |
| 208.71.40.0/21 | Oath Holdings Inc. | 2,048 |
| 216.39.48.0/20 | Oath Holdings Inc. | 4,096 |
| 63.250.192.0/19 | Oath Holdings Inc. | 8,192 |
| 63.250.204.0/22 | Oath Holdings Inc. | 1,024 |
| 67.195.0.0/17 | Oath Holdings Inc. | 32,768 |
| 67.195.128.0/20 | Oath Holdings Inc. | 4,096 |
| 67.195.144.0/21 | Oath Holdings Inc. | 2,048 |
| 67.195.160.0/20 | Oath Holdings Inc. | 4,096 |
| 67.195.224.0/22 | Oath Holdings Inc. | 1,024 |

United States 560

TOP SERVICES
HTTPS 281
HTTP 178
SSH 38
SMTP 20
NTP 12

TOP ORGANIZATIONS
Oath Holdings 560

TOP OPERATING SYSTEMS
Linux 3.x 7

TOP PRODUCTS
OpenSSH 40
Jetty 35
httpd 12
Apache httpd 11
Apache Tomcat/Coyote JSP engine 5

United States

```
Content-Type: text/html; charset=iso-8859-1
Age: 0
Transfer-Encoding: chunked
Connection: keep-alive
Server: ATS/7.1.2
```

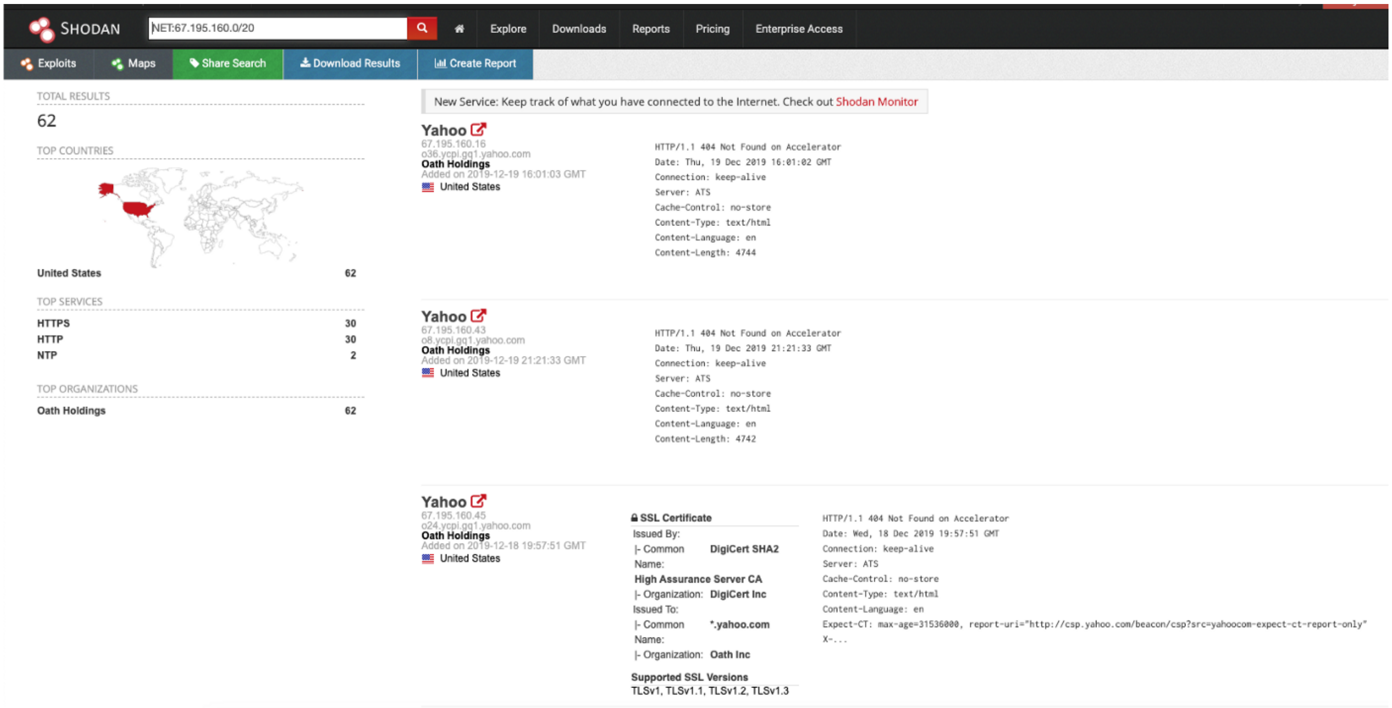
AcceLIM | AP Automation and Invoice Processing
98.137.244.37
Oath Holdings
Added on 2019-12-20 12:09:50 GMT
United States
Technologies:

SSL Certificate
Issued By:
|- Common Name: DigiCert SHA2 High Assurance Server CA
|- Organization: DigiCert Inc
Issued To:
|- Common Name: *.secure.hostingprod.com
|- Organization: Oath Inc
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Parameters
Fingerprint: RFC5114/2048-bit MODP Group with 256-bit Prime Order Subgroup

```
HTTP/1.1 200 OK
Date: Fri, 20 Dec 2019 12:09:48 GMT
Set-Cookie: exp_last_visit=1261483789; expires=Sat, 19-Dec-2020 12:09:49 GMT; path=/
Set-Cookie: exp_last_activity=1576843789; expires=Sat, 19-Dec-2020 12:09:49 GMT; path
Set-Cookie: exp_tracker=a%3A1%3A%7Bi%3A0%3Bs%3A5%3A%22index%22%3B%7D...
```

Accurate Conceptions | Just another WordPress site
98.137.244.37
Oath Holdings
Added on 2019-12-20 12:14:02 GMT
United States
Technologies:
jQuery Migrate

```
HTTP/1.1 200 OK
Date: Fri, 20 Dec 2019 12:13:58 GMT
X-Pingback: http://www.accurateconceptions.com/xmlrpc.php
Link: <http://www.accurateconceptions.com/>; rel=shortlink
P3P: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo C
```



NET:67.195.160.0/20

TOTAL RESULTS
62

TOP COUNTRIES
United States 62

TOP SERVICES
HTTPS 30
HTTP 30
NTP 2

TOP ORGANIZATIONS
Oath Holdings 62

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Yahoo
67.195.160.16
o36.ycpi.gq1.yahoo.com
Oath Holdings
Added on 2019-12-19 16:01:03 GMT
United States

```
HTTP/1.1 404 Not Found on Accelerator
Date: Thu, 19 Dec 2019 16:01:02 GMT
Connection: keep-alive
Server: ATS
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Content-Length: 4744
```

Yahoo
67.195.160.43
o8.ycpi.gq1.yahoo.com
Oath Holdings
Added on 2019-12-19 21:21:33 GMT
United States

```
HTTP/1.1 404 Not Found on Accelerator
Date: Thu, 19 Dec 2019 21:21:33 GMT
Connection: keep-alive
Server: ATS
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Content-Length: 4742
```

Yahoo
67.195.160.45
o24.ycpi.gq1.yahoo.com
Oath Holdings
Added on 2019-12-18 19:57:51 GMT
United States

SSL Certificate
Issued By:
|- Common Name: DigiCert SHA2 High Assurance Server CA
|- Organization: DigiCert Inc
Issued To:
|- Common Name: *.yahoo.com
|- Organization: Oath Inc
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 404 Not Found on Accelerator
Date: Wed, 18 Dec 2019 19:57:51 GMT
Connection: keep-alive
Server: ATS
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"
X-...
```

shodan also has many good features such as ssl-based search and favicon search can find a lot of target information . I won’t write much here

Dnsdumper Virustotal Can also find a lot of information

### Port

Port scanning can use nmap and massscan

**robertdavidgraham/masscan**

This is an Internet-scale port scanner. It can scan the entire Internet in

**Nmap: the Network Mapper - Free Security Scanner**

Nmap 7.80 was released for DEFCON 27! [release notes | download] Nmap 7.70 is now available! [release notes | download]…

nmap.org

```
nmap -sV -T3 -Pn -
p2075,2076,6443,3868,3366,8443,8080,9443,9091,3000,8000,5900,8081,6000
,10000,8181,3306,5000,4000,8888,5432,15672,9999,161,4044,7077,4040,900
0,8089,443,7447,7080,8880,8983,5673,7443,19000,19080 ${target}
```

### Endpoint

There are many ways about Endpoint

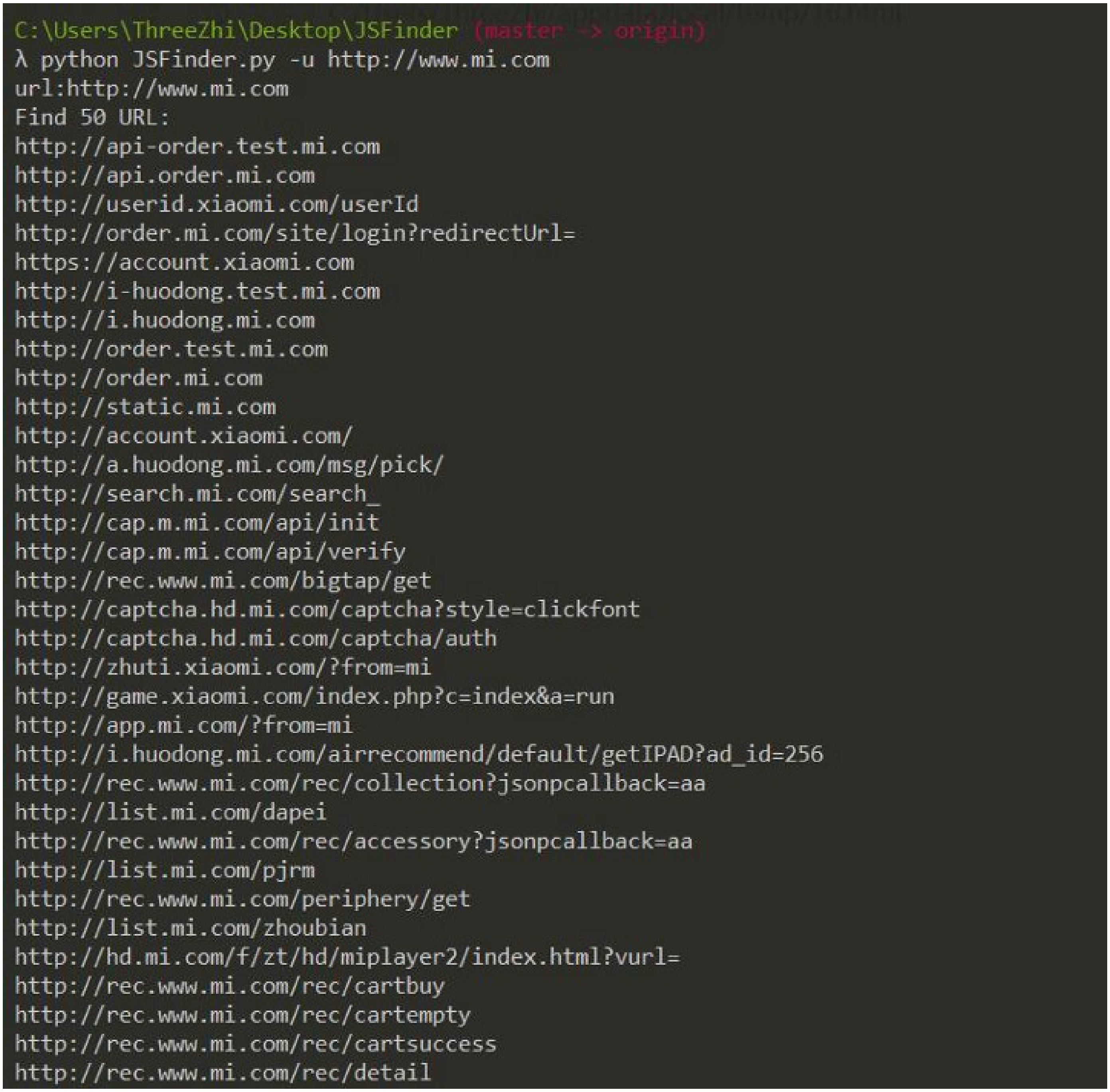
```
curl http://web.archive.org/cdx/search/cdx/search/cds?
url=*.$1/*&output=text&fl=original&collapse=urlkey
curl http://index.commoncrawl.org/CC-MAIN-2018-22-index\?
url\=\*.$1\&output\=json |jq .url
```

Commoncrawl and web archive can find many endpoints for us to test. At the same time, we can also use crawlers to get what we want. The main focus should be on JS files and API endpoints.

**Threezh1/JSFinder**

JSFinder is a tool for quickly extracting URLs and subdomains from JS files on a website.

github.com



```
C:\Users\ThreeZhi\Desktop\JSFinder (master -> origin)
λ python JSFinder.py -u http://www.mi.com
url:http://www.mi.com
Find 50 URL:
http://api-order.test.mi.com
http://api.order.mi.com
http://userid.xiaomi.com/userId
http://order.mi.com/site/login?redirectUrl=
https://account.xiaomi.com
http://i-huodong.test.mi.com
http://i.huodong.mi.com
http://order.test.mi.com
http://order.mi.com
http://static.mi.com
http://account.xiaomi.com/
http://a.huodong.mi.com/msg/pick/
http://search.mi.com/search_
http://cap.m.mi.com/api/init
http://cap.m.mi.com/api/verify
http://rec.www.mi.com/bigtap/get
http://captcha.hd.mi.com/captcha?style=clickfont
http://captcha.hd.mi.com/captcha/auth
http://zhuti.xiaomi.com/?from=mi
http://game.xiaomi.com/index.php?c=index&a=run
http://app.mi.com/?from=mi
http://i.huodong.mi.com/airrecommend/default/getIPAD?ad_id=256
http://rec.www.mi.com/rec/collection?jsonpcallback=aa
http://list.mi.com/dapei
http://rec.www.mi.com/rec/accessory?jsonpcallback=aa
http://list.mi.com/pjrm
http://rec.www.mi.com/periphery/get
http://list.mi.com/zhoubian
http://hd.mi.com/f/zt/hd/miplayer2/index.html?vurl=
http://rec.www.mi.com/rec/cartbuy
http://rec.www.mi.com/rec/cartempty
http://rec.www.mi.com/rec/cartsuccess
http://rec.www.mi.com/rec/detail
```

At the same time I will use dirsearch to brute force

**maurosoria/dirsearch**

Current Release: v0.3.9 (2019.11.26) dirsearch is a simple command line

**C1h2e1/MyFuzzingDict**

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or...

github.com

My dictionary is here

## HUNTING

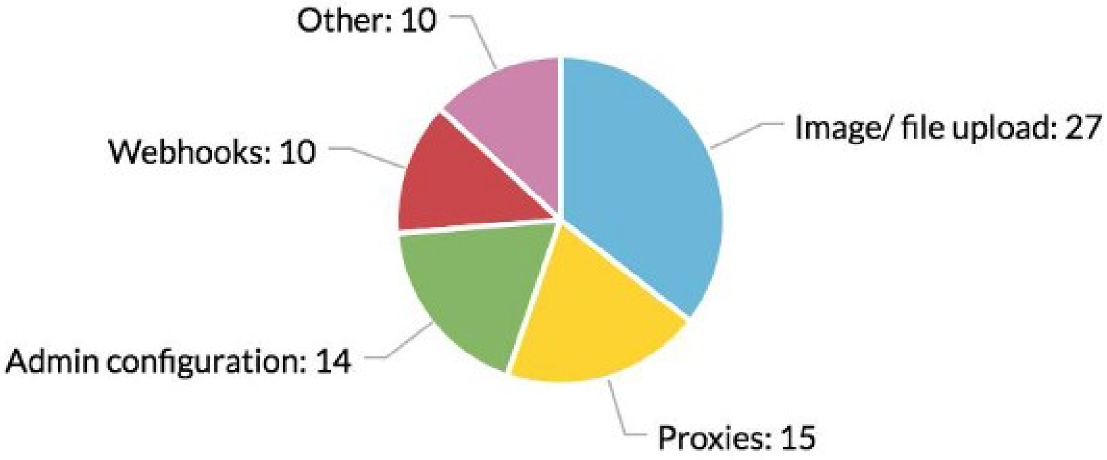
I mainly hunt some BUG below

- SSRF
- CSRF(CORS,JSONP hijacking)
- SQLi
- XSS(DOM,Stored,Reflectd)
- Weak Password
- Unauthorized access
- IDOR
- Open redirect
- Information Disclosure
- XXE
- File Upload
- Subdomain Takeover
- BLH

- Auth Bypass
- DOS
- LFI
- Command injection
- Race Condition
- S3 Bucket
- Logic Flaw
- SSTI

Let me introduce one by one and share Bypass tips

### SSRF



https://medium.com/swlh/ssrf-in-the-wild-e2c598900434

This picture is a good summary of the common locations of SSRF .We can find related

## BYPASS

tools

**Open redirect/SSRF payload generator**

Edit description

tools.intigriti.io

```
white@black.com ==> black[.]com
black[.]com?white[.]com ==> black[.]com
black[.]com#white.com ==> black[.]com Tips By @____cypher____
http://127.0.0.1
http://localhost
https://127.0.0.1/
http://127.127.127.127
http://127.0.1.3
http://127.0.0.0https://localhost/
http://[::]:80/
http://127.0.0.1.nip.io
http://[0:0:0:0:0:ffff:127.0.0.1]
http://spoofed.burpcollaborator.net
http://0177.0.0.1/
http://2130706433/
http://0/
https://10.0.0.1.xip.io
http://1.1.1.1 &@2.2.2.2# @3.3.3.3/
urllib2 : 1.1.1.1
requests + browsers : 2.2.2.2
urllib : 3.3.3.3

<?php
header("Location: http://127.0.0.1");
?>

http://       .    = example.com
List:
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳ ⑴ ⑵

  Ⓜ            Ⓢ
             ⓪ ⓫ ⓬ ⓭ ⓮ ⓯ ⓰ ⓱ ⓲ ⓳ ⓴                    ⓿
```

```
http://169.254.169.254/latest/meta-data/iam/security-credentials/aws-elasticbeanorastalk-ec2-role
http://169.254.169.254/computeMetadata/v1/
http://metadata.google.internal/computeMetadata/v1/
http://metadata/computeMetadata/v1/
http://metadata.google.internal/computeMetadata/v1/instance/hostname
http://metadata.google.internal/computeMetadata/v1/instance/id
http://metadata.google.internal/computeMetadata/v1/project/project-id
File protocol to read local file
file:///etc/passwd
http://100.100.100.200/latest/meta-data/
```

**swisskyrepo/PayloadsAllTheThings**

Server Side Request Forgery or SSRF is a vulnerability in which an attacker forces a server to perform requests on…

github.com

DNS Rebinding attack

**My First SSRF Using DNS Rebinding**

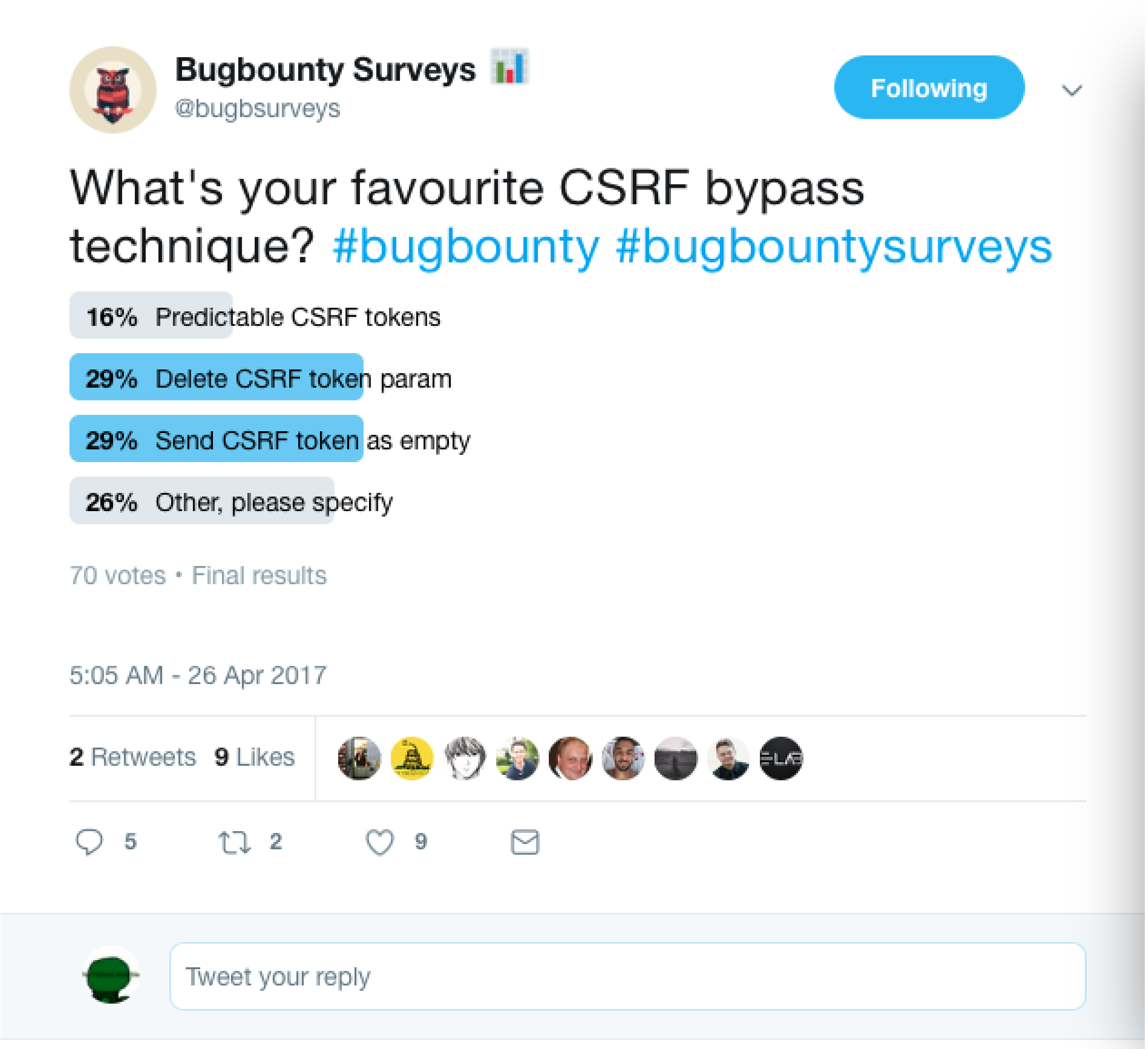
Imagine you are a computer :D People give you URLs and you load them Of course you won't load url that points to your…

geleta.eu

**cujanovic/SSRF-Testing**

http://google.com:80+&@127.88.23.245:22/#+@google.com:80/ http://127.88.23.245:22/+&@google.com:80#+@google.com:80/…

github.com



Bugbounty Surveys
@bugbsurveys

What's your favourite CSRF bypass technique? #bugbounty #bugbountysurveys

16% Predictable CSRF tokens
29% Delete CSRF token param
29% Send CSRF token as empty
26% Other, please specify

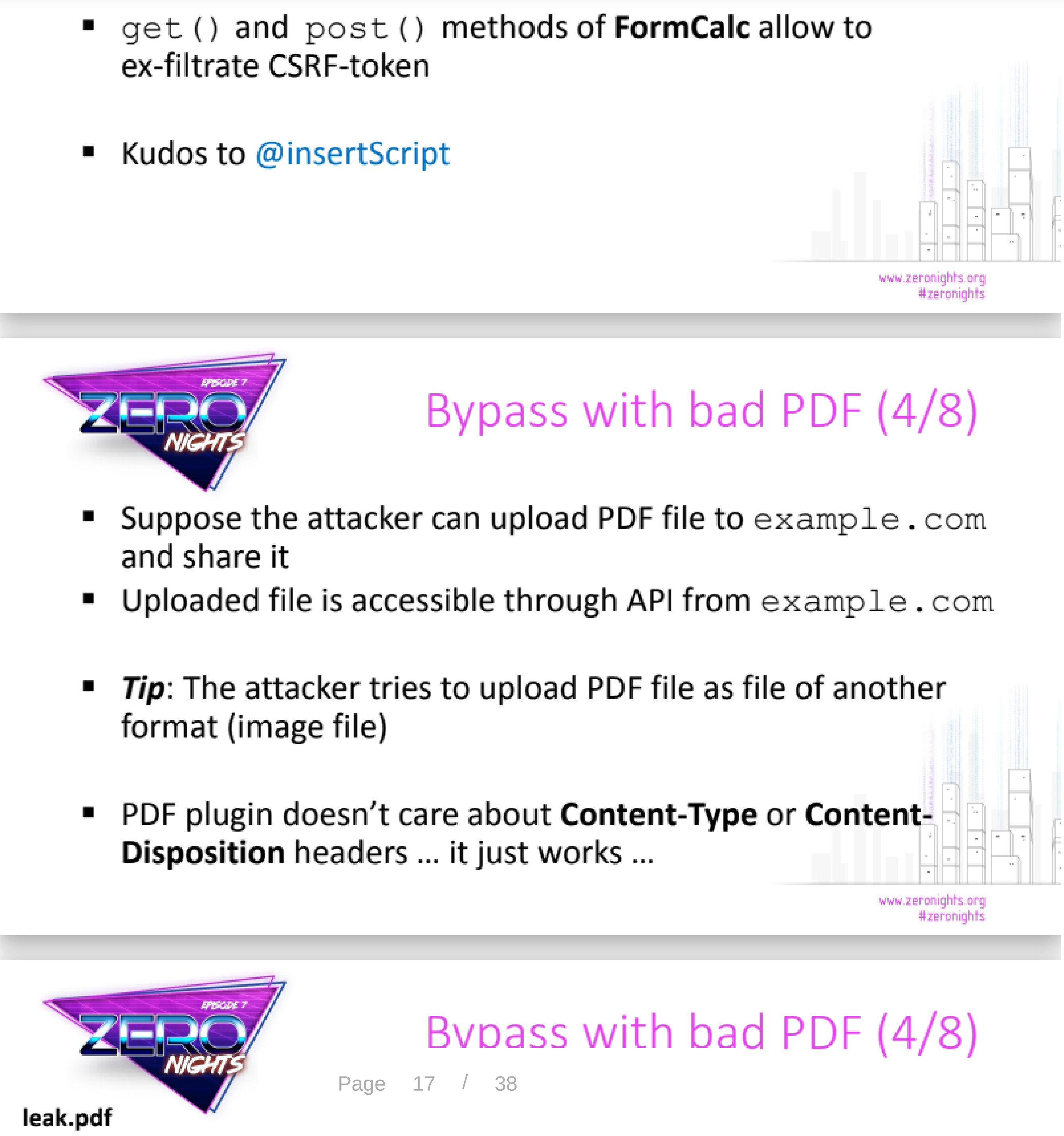
70 votes • Final results

5:05 AM - 26 Apr 2017

2 Retweets 9 Likes

```
Delete CSRF token
Null token parameter
Modify request method Form GET to POST or PUT etc.
Replace token with any string of the same length as token
Fixed token Every user's token can be shared
```

Bypass with bad PDF (4/8)



- `get()` and `post()` methods of **FormCalc** allow to ex-filtrate CSRF-token
- Kudos to @insertScript

www.zeronights.org
#zeronights

## Bypass with bad PDF (4/8)

- Suppose the attacker can upload PDF file to `example.com` and share it
- Uploaded file is accessible through API from `example.com`
- ***Tip***: The attacker tries to upload PDF file as file of another format (image file)
- PDF plugin doesn't care about **Content-Type** or **Content-Disposition** headers … it just works …

www.zeronights.org
#zeronights

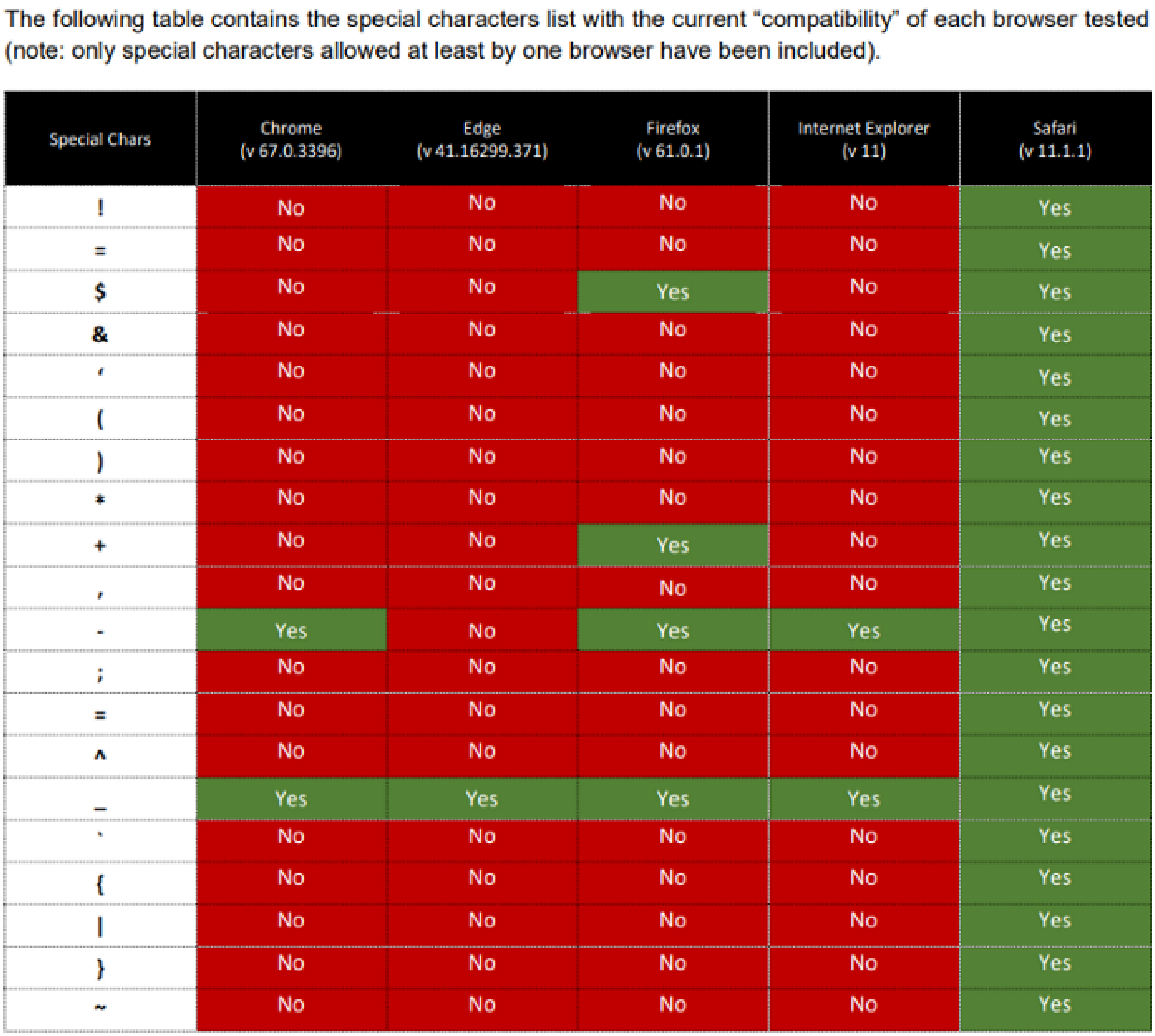
## Bypass with bad PDF (4/8)

leak.pdf

0ang3el

CORS Bypass

## OUT OF SCOPE XSS and CORS



The following table contains the special characters list with the current "compatibility" of each browser tested (note: only special characters allowed at least by one browser have been included).

| Special Chars | Chrome (v 67.0.3396) | Edge (v 41.16299.371) | Firefox (v 61.0.1) | Internet Explorer (v 11) | Safari (v 11.1.1) |
|---|---|---|---|---|---|
| ! | No | No | No | No | Yes |
| = | No | No | No | No | Yes |
| $ | No | No | Yes | No | Yes |
| & | No | No | No | No | Yes |
| ' | No | No | No | No | Yes |
| ( | No | No | No | No | Yes |
| ) | No | No | No | No | Yes |
| * | No | No | No | No | Yes |
| + | No | No | Yes | No | Yes |
| , | No | No | No | No | Yes |
| - | Yes | No | Yes | Yes | Yes |
| ; | No | No | No | No | Yes |
| = | No | No | No | No | Yes |
| ^ | No | No | No | No | Yes |
| _ | Yes | Yes | Yes | Yes | Yes |
| ` | No | No | No | No | Yes |
| { | No | No | No | No | Yes |
| \| | No | No | No | No | Yes |
| } | No | No | No | No | Yes |
| ~ | No | No | No | No | Yes |

## Use Safari's URL feature to bypass

## JSONP hijacking

Burp suite Extension to discover JSONP func

**FUZZ Callback Parameter**

In another test, I found a JSONP hijacking at a.redacted.com. When I looked for a vulnerability in b.redacted.com, I found a JSON response, but there was no parameter in the requested URL. I tried the FUZZ parameter. But in the dictionary, Without _cb_ this parameter eventually I added _cb_ of a.redacted.com to b.redacted.com and successfully found JSONP hijacking

```
callback=gh0stkey
cb=gh0stkey
jsonp=gh0stkey
jsonpcallback=gh0stkey
jsonpcb=gh0stkey
jsonp_cb=gh0stkey
json=gh0stkey
jsoncallback=gh0stkey
jcb=gh0stkey
call=gh0stkey
cb_=gh0stkey
_cb_=gh0stkey
```

## SQLi

SQL injection is always there. Actually all the key is to be careful.I found SQLi in my two most recent tests.Just need you to search all the parameters of each page carefully and add single quotes or %df or look for Time-Based SQLi

**tennc/fuzzdb**

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or…

Tips : SQL INJECTION VIA HTTP HEADER!

I can’t think of anything to write here so SQL i is over.

XSS

We can use the endpoints obtained in the information collection to find reflected XSS,There are many positions for XSS. We should pay attention to Bypass’s payload.

**XSS in hidden input fields**

Gareth Heyes | 16 November 2015 at 11:25 UTC Updated: 14 June 2019 at 12:03 UTC At PortSwigger, we regularly run…

portswigger.net

**XSS in Oculus Rifts CDN**

After looking through Oculus Rifts site I came across the developer section for making apps. I quickly made a test app…

medium.com

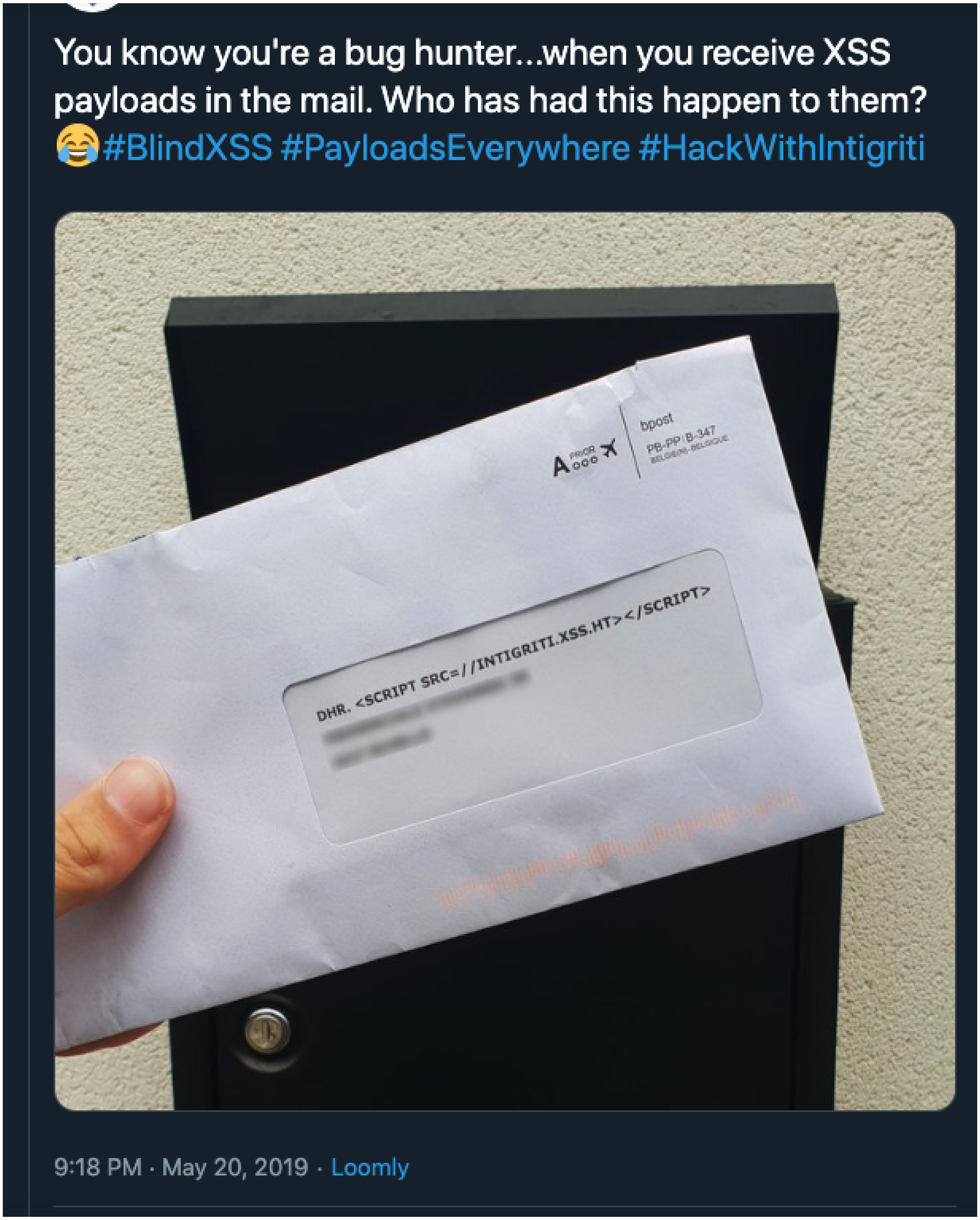
I found a lot of Blind XSS in recent tests. I think that the location of the HTTP HEADER and some XSS and SQLi Payloads will have unexpected results.

I use XSS HUNTER for BlindXSS

**XSS Hunter**

Edit description

xsshunter.com



You know you're a bug hunter...when you receive XSS payloads in the mail. Who has had this happen to them? 😂#BlindXSS #PayloadsEverywhere #HackWithIntigriti

9:18 PM · May 20, 2019 · Loomly

!!BlindXSSEveryWhere!!

My Blog about XSS!

### Weak Password

Try more

### Unauthorized access

Most of the unauthorized access I usually find comes from brute force cracking of directories.Find more ports, more IPs, more services

### IDOR

**Quitten/Autorize**

Autorize is an automatic authorization enforcement detection extension for Burp Suite. It was written in Python by…

github.com

Burp suite Extension to find IDOR

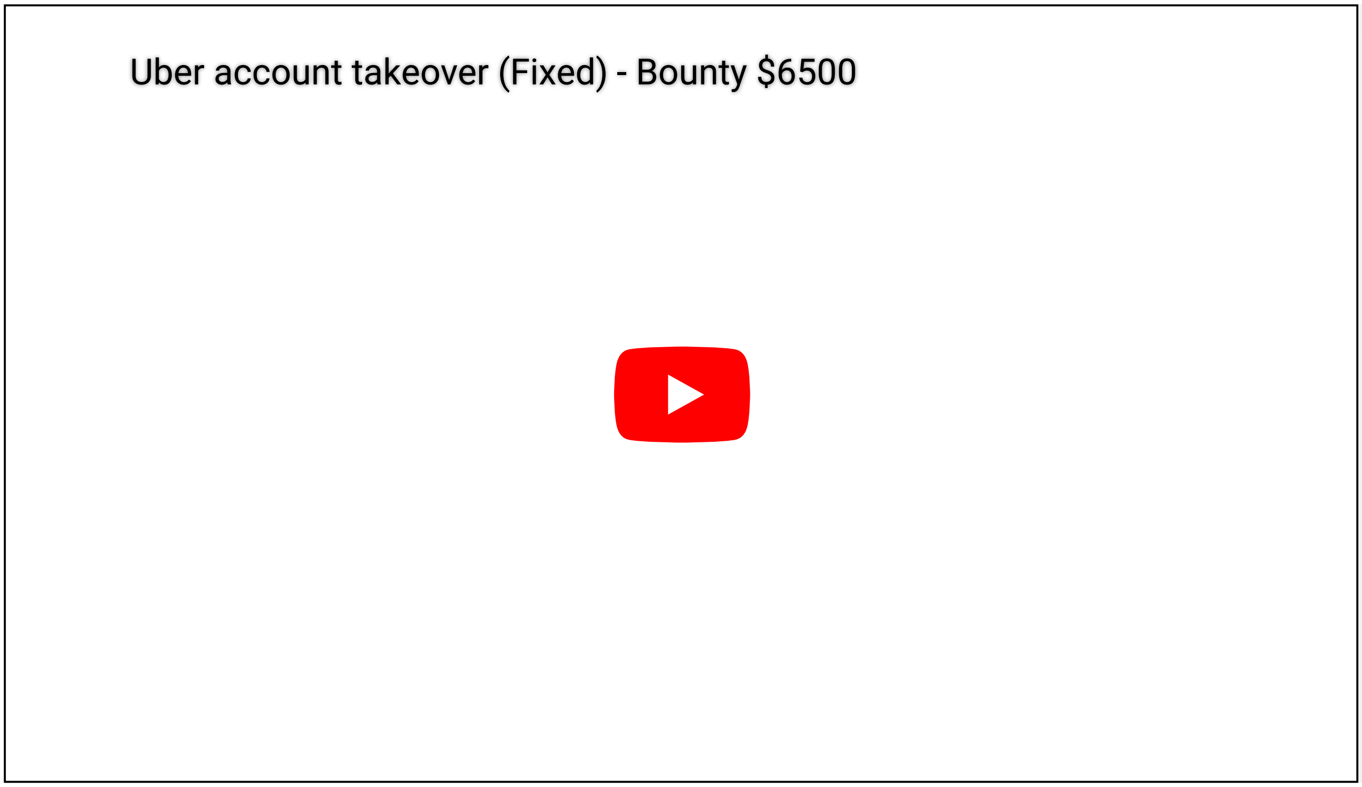
**One Way to Find Hidden IDOR Vulnerability**

I received an invitation for an internal project, i found an interesting vulnerability in this project. After…

gh0st.cn

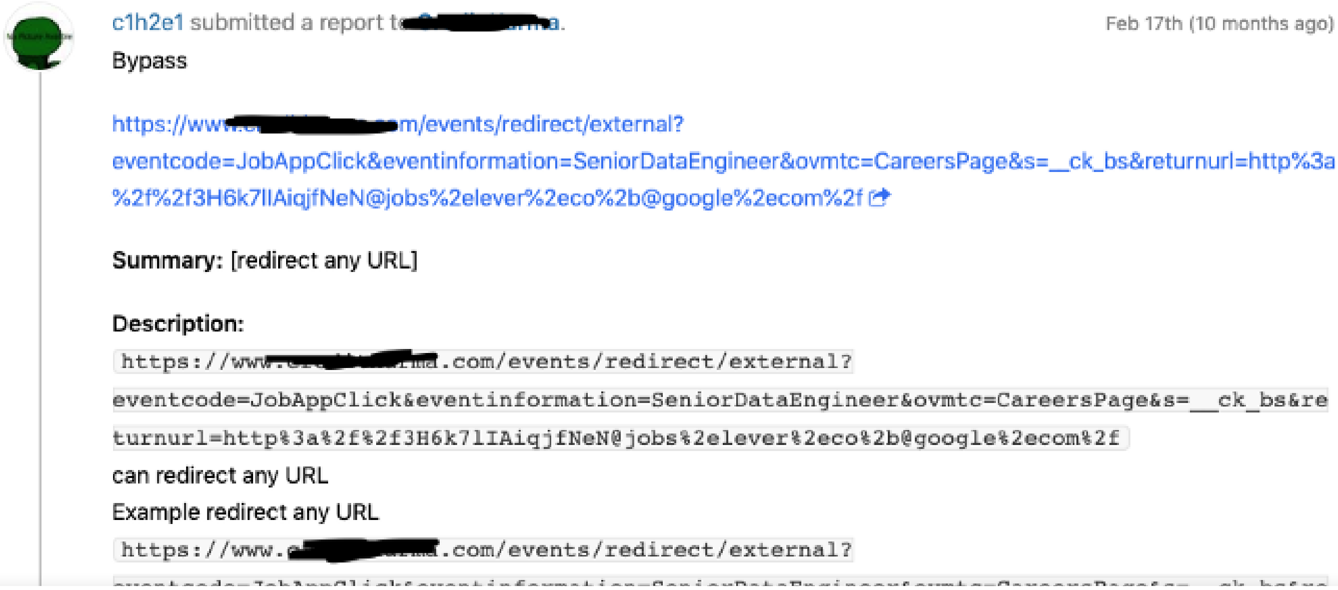
The case of IDOR

There are many different test methods in the IDOR search process.We should pay attention to unique parameters and pages, and pay attention to the function of each



**Open redirect**

When testing Open redirect, we can try to combine XSS to try to redirect javascript:alert (1)



c1h2e1 submitted a report to [redacted]. Feb 17th (10 months ago)

Bypass

https://www[redacted]m/events/redirect/external?eventcode=JobAppClick&eventinformation=SeniorDataEngineer&ovmtc=CareersPage&s=__ck_bs&returnurl=http%3a%2f%2f3H6k7lIAiqjfNeN@jobs%2elever%2eco%2b@google%2ecom%2f

**Summary:** [redirect any URL]

**Description:**

```
https://www[redacted].com/events/redirect/external?eventcode=JobAppClick&eventinformation=SeniorDataEngineer&ovmtc=CareersPage&s=__ck_bs&returnurl=http%3a%2f%2f3H6k7lIAiqjfNeN@jobs%2elever%2eco%2b@google%2ecom%2f
```

can redirect any URL

Example redirect any URL

```
https://www.[redacted].com/events/redirect/external?
```

Payload list

**C1h2e1/c1h2e1.github.io**

Contribute to C1h2e1/c1h2e1.github.io development by creating an account on GitHub.

github.com

**Open Redirect Cheat Sheet**

Hi, this is a cheat sheet for Open redirect vulnerabilities. It's a first draft. I will update it every time I find a…

pentester.land

```
Replace whitelisted.com with your target
```

### Information Disclosure

Github Pastebin Google etc.

Most of my information collection is found directly from recon

SO JUST RECON CAREFUL

Use github and pastebin to search for some sensitive information such as API key, token.

### XXE

1. Upload File

**Exploiting XXE with Excel**

XML External Entity attacks are very common, particularly through HTTP-based APIs, and we regularly encounter and…

www.4armed.com

2.OOB ATTACK

3.Modify Content-Type

**U.S. Dept Of Defense disclosed on HackerOne: XXE in DoD website…**

Summary:** XXE in https://[redacted] **Description:** A malicious user can modify an XML-based request to include XML…

hackerone.com

**Starbucks disclosed on HackerOne: XXE at…**

johnstone discovered that both ecjobs.starbucks.com.cn/retail/hxpublic_v6/hxdynamicpage6.aspx &…

hackerone.com

### File Upload

**Exploiting File Uploads Pt. 1 - MIME Sniffing to Stored XSS #bugbounty**

While bug hunting on a private program I was able to find a Stored XSS vulnerability through a file upload…

anotherhackerblog.com

vulnerability on a private program through…

anotherhackerblog.com

We can test XSS and SSRF when uploading and ImageTragick RCE ,This idea is really hard for me to write.I will write the tips of Bypass

- Add dot after the file name
- File name with special symbol before or after
- Delete meta-data
- Race condition

**modzero/mod0BurpUploadScanner**

A Burp Suite Pro extension to do security tests for HTTP file uploads. Table of Contents Testing web applications is a…

github.com

I was writing this article after a day of school today. My mind is a bit messy XD

### Subdomain Takeover

**Echocipher/Subdomain-Takeover**

一个子域名接管检测工具 author：Echocipher mail：echocipher@163.com blog： https://echocipher.github.io 本项目是我…

github.com

**haccer/subjack**

Subjack is a Subdomain Takeover tool written in Go designed to scan a

Still no good tips, more subdomains have a higher chance of taking over

### BLH

**Command Injection Through BLH**

Hi I am Shankar R ( @trapp3r_hat) from Tirunelveli (India). I hope you all doing good. I am a security researcher from…

medium.com

**Broken Link Hijacking - How expired links can be exploited.**

Broken Link Hijacking (BLH) exists whenever a target links to an expired domain or page. Broken Link Hijacking comes in…

edoverflow.com

tools

**stevenvachon/broken-link-checker**

Find broken links, missing images, etc within your HTML. ✅ Complete: Unicode, redirects, compression, basic auth…

github.com

### HTTP Requests Smuggling

**Write up of two HTTP Requests Smuggling**

This article about how I found two sites for HTTP Request Smuugling

### CRLF

**#BugBounty — Exploiting CRLF Injection can lands into a nice bounty**

Hi Guys,

medium.com

### Auth Bypass

**Phabricator disclosed on HackerOne: Bypass auth.email-domains**

Email addresses are stored as `VARCHAR(128)`. However, Phabricator does not verify the length of an email address upon…

hackerone.com

Oauth2 CSRF Modify the redirect_url to get the victim token .Can be bypassed using bypass open redirect

### DOS

**QIWI disclosed on HackerOne: apache access.log leakage via long…**

Issue access.log is leaked by attacker who trying send many requests. #Explain: Honestly i don't know how the bug is…

hackerone.com

imagesize size DOS

```
https://target.com/Verification/?high=100&weigh=100
```

```
width=250&height=250
height=250
width=250
w=250&h=250
h=250
w=250
size=250&width=250&height=250
size=250&w=250&h=250
size=250
margin=250
margin=250&width=250&height=250
margin=250&w=250&h=250
size=250&margin=250
size=250&margin=250&width=250&height=250
```

Bypass some restrictions that affect the normal use of the user .Is what I think is the most meaningful DOS

**[Writeup — FB] Crash web — app through application form of job application pages**

It's me again, after my first write-up bounty.

medium.com

I think using a lot of characters or very special characters may cause DOS

### LFI

**LFI Cheat Sheet**

LFI stands for Local File Includes - it's a file local inclusion vulnerability that allows an attacker to include files...

highon.coffee

**Submission**

Summary:** This report describes a Race Condition Vulnerability which allow an authenticated user to submit the same…

hackerone.com

**HackerOne disclosed on HackerOne: Race condition in performing…**

Summary There exists a race condition in performing retests. By executing multiple requests to confirm a retest at the…

hackerone.com

### HPP

**Testing for HTTP Parameter pollution (OTG-INPVAL-004)**

This article is part of the new OWASP Testing Guide v4. Back to the OWASP Testing Guide v4…

www.owasp.org