

Python3-based read/write editors in Burp Suite

Nicolas Grégoire
TumpiCon 2025

Intro

Whoami? 🧐

Nicolas Grégoire 🇫🇷

Portswigger's official trainer 🇪🇺

Soon giving a 4-day training in Roma 🇮🇹

Menu

Intro to the *toi/33t* challenge

Using the *Piper* extension

<https://github.com/silentsignal/burp-piper>

Using the *Scalpel* extension

<https://github.com/ambionics/scalpel>

toil33t

Overview

CTF challenge from *"La nuit du hack 2016"*

Cookie **session**

JSON encrypted with AES-**ECB**

Two JSON values under our control

Unkown structure

Goals

Manipulate JSON by shuffling blocks

Pretend to be an admin

The targeted cookie

Request

Pretty

Raw

Body params

Name	Value
name	AA...
password	zzz
email	BB...

Response

Pretty

Raw

Hex

Render

Headers

toil33t

```
1 HTTP/2 302 Found
2 Content-Type: text/html; charset=utf-8
3 Location: https://www.toil33t.pwn/?success=1
4 Set-Cookie: session=
939c4dcbc5c09d3aaa00469fc65bbd6b1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e
9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a
3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b391
cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9
dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b394c7f066a912d8a35534fc4d
a87c8f76e3758e2604a11b75246b4f7fd9d14df598ac9ee8270fdde8d052e27be7d93dd3a84
ba33f9f4ec42a91b026353fd6badbad0fac2ea8776f4050e931562a15794ecd0fac2ea8776f
4050e931562a15794ecd0fac2ea8776f4050e931562a15794ecd0fac2ea8776f4050e931562
a15794ecd0fac2ea8776f4050e931562a15794ec294801fec399c051d1f58e5f464d7053765
e6f7fb0e286a68db97afe700645f2; HttpOnly; Path=/
5 Content-Length: 229
```

With some alignment

Request

Pretty Raw Body params

Name	Value
name	AA...
password	zzz
email	BBB...

Response

Pretty Raw Hex Render Headers tail33t

```
1 HTTP/2 302 Found
2 Content-Type: text/html; charset=utf-8
3 Location: https://www.toil33t.pwn/?success=1
4 Set-Cookie: session=
939c4dcbc5c09d3aaa00469fc65bbd6b1cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b394c7f066a912d8a35534fc4da87c8f76e
3758e2604a11b75246b4f7fd9d14df598ac9ee8270fddde8d052e27be7d93dd3a
84ba33f9f4ec42a91b026353fd6badbad0fac2ea8776f4050e931562a15794ec
d0fac2ea8776f4050e931562a15794ecd0fac2ea8776f4050e931562a15794ec
d0fac2ea8776f4050e931562a15794ecd0fac2ea8776f4050e931562a15794ec
294801fec399c051d1f58e5f464d7053765e6f7fb0e286a68db97afe700645f2
; HttpOnly; Path=/
5 Content-Length: 229
```

Searching for 1cc38f

Request
Pretty Raw Body params

Name	Value
name	AA...
password	zzz
email	BBB...

Response
Pretty Raw Hex Render Headers tail33t
1 HTTP/2 302 Found
2 Content-Type: text/html; charset=utf-8
3 Location: https://www.toil33t.pwn/?success=1
4 Set-Cookie: session=
939c4dcbc5c09d3aaa00469fc65bbd6b1cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b39
1cc38f6fb5e9dee5ec287a3a83bc0b394c7f066a912d8a35534fc4da87c8f76e
3758e2604a11b75246b4f7fd9d14df598ac9ee8270fdde8d052e27be7d93dd3a
84ba33f9f4ec42a91b026353fd6badbad0fac2ea8776f4050e931562a15794ec
d0fac2ea8776f4050e931562a15794ecd0fac2ea8776f4050e931562a15794ec
d0fac2ea8776f4050e931562a15794ecd0fac2ea8776f4050e931562a15794ec
294801fec399c051d1f58e5f464d7053765e6f7fb0e286a68db97afe700645f2
; HttpOnly; Path=/
5 Content-Length: 229

Piper

Overview

Allows to execute binaries from Burp

WP *"Unix-style approach to web application testing"*

<https://www.agarri.fr/docs/GWAPT-Piper.pdf>

Use-cases

Execute `gron` or `jq` on JSON responses

Execute `pdftotext` on PDF responses

Execute `meld` or `git diff` if 2 or 3 entries are selected

Viewer (read only)

Basic shell script working on `stdin`

```
grep ^Set- | cut -d= -f2 | cut -d\; -f1 | fold -w32 -
```

Configured in section "Message viewers"

Make sure to enable "Pass HTTP headers to command"

Viewer (read only)

Request

PrettyRawBody params

NameValue

nameAA...>

passwordzzz>

emailBB...>

Response

PrettyRawHexRenderHeaderstail33t

1939c4dcbc5c09d3aaa00469fc65bbd6b

21cc38f6fb5e9dee5ec287a3a83bc0b39

31cc38f6fb5e9dee5ec287a3a83bc0b39

41cc38f6fb5e9dee5ec287a3a83bc0b39

51cc38f6fb5e9dee5ec287a3a83bc0b39

61cc38f6fb5e9dee5ec287a3a83bc0b39

71cc38f6fb5e9dee5ec287a3a83bc0b39

81cc38f6fb5e9dee5ec287a3a83bc0b39

91cc38f6fb5e9dee5ec287a3a83bc0b39

101cc38f6fb5e9dee5ec287a3a83bc0b39

111cc38f6fb5e9dee5ec287a3a83bc0b39

124c7f066a912d8a35534fc4da87c8f76e

133758e2604a11b75246b4f7fd9d14df59

148ac9ee8270fdde8d052e27be7d93dd3a

1584ba33f9f4ec42a91b026353fd6badba

16d0fac2ea8776f4050e931562a15794ec

17d0fac2ea8776f4050e931562a15794ec

18d0fac2ea8776f4050e931562a15794ec

19d0fac2ea8776f4050e931562a15794ec

20d0fac2ea8776f4050e931562a15794ec

21294801fec399c051d1f58e5f464d7053

22765e6f7fb0e286a68db97afe700645f2

13

Scalpel

Overview

Modifies the traffic using CPython3

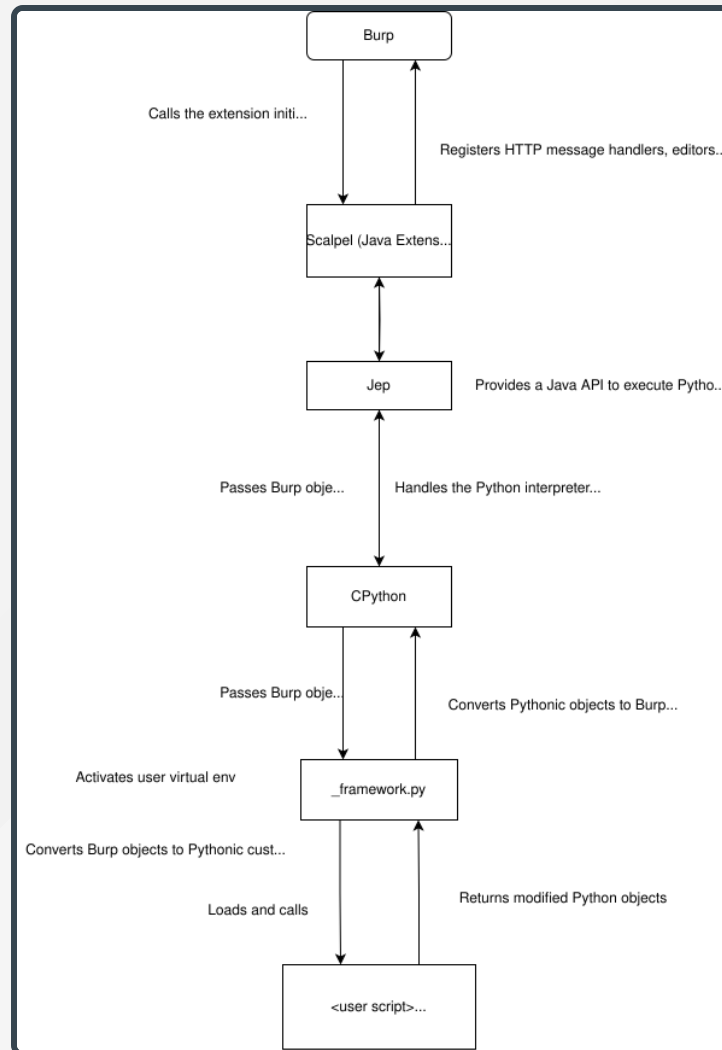
Provides **r/w** editors

Functions `req_edit_*` and `res_edit_*`

Includes a notion of scope

Function `match`

CPython3 in Burp Suite? 🤔



Viewer (read only)

Implement `match` and `req_edit_in`

And a helper splitting the cookie

Viewer (read only)

```
def match(flow: Flow) -> bool:
    ...snip...

def req_edit_in(req: Request) -> bytes | None:
    return blocks_to_lines(req.cookies['session']).encode()

def blocks_to_lines(blob: str) -> str:
    block_size = 32
    ...snip...
    return '\n'.join(blocks)
```

Viewer (read only)

[illegible]

Editor (read/write)

Add `req_edit_out`

And a second helper converting back

Editor (read/write)

```
def match(flow: Flow) -> bool:
    ...snip...

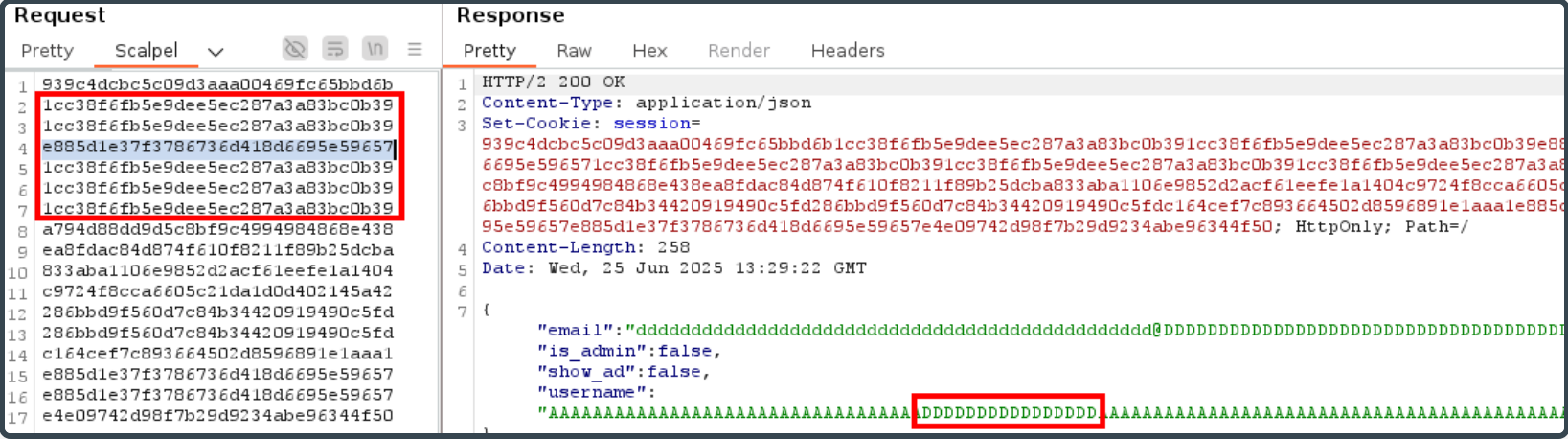
def req_edit_in(req: Request) -> bytes | None:
    ...snip...

def req_edit_out(req: Request, edited_text: bytes) -> Request:
    req.cookies['session'] = lines_to_blocks(edited_text.decode())
    return req

def blocks_to_lines(blob: str) -> str:
    ...snip...

def lines_to_blocks(lines: str) -> str:
    ...snip...
```

Editor (read/write)



Editor (r/w) with context

Add a `dict` storing known blocks

Adapt the two helpers

Editor (r/w) with context

```
known_blocks = {  
    'SPACE x16': 'a9b216c560f781f1c5b7e7abfeb7239e',  
    'A x16'      : '1cc38f6fb5e9dee5ec287a3a83bc0b39',  
    'C x16'      : 'eb68a901042101f80e57b747c5febb82',  
    ...snip...  
    'true'       : 'fcfcfeedc17bd4ffa2bd43c62bc303ff',  
    'false'      : 'a9a52891f5860c2393de568725fb86fd',  
}
```

```
...snip...
```

```
def lines_to_blocks(lines: str) -> str:
```

```
...snip...
```

```
for line in lines:  
    for k, v in known_blocks.items():  
        if line == k:  
            line = v  
        blocks.append(line)
```

```
...snip...
```

Editor (r/w) with context

Request	Response
<pre>1 939c4dcbc5c09d3aaa00469fc65bbd6b 2 A x16 3 A x16 4 true 5 A x16 6 A x16 7 A x16 8 a7940b8dd9d5c8bf9c4994984868e438 9 ea8fdac84d874f610f8211f89b25dcba 10 833aba1106e9852d2acf61eefelal404 11 c9724f8cca6605c21da1d0d402145a42 12 286bbd9f560d7c84b34420919490c5fd 13 286bbd9f560d7c84b34420919490c5fd 14 c164cef7c893664502d8596891e1aaa1 15 SPACE x16 16 D x16 17 e4e09742d98f7b29d9234abe96344f50</pre>	<pre>1 HTTP/2 200 OK 2 Content-Type: application/json 3 Set-Cookie: session= 939c4dcbc5c09d3aaa00469fc65bbd6b1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0 c62bc303ff1cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec287a3a83bc0b391cc38f6fb5e9dee5ec1 c8bf9c4994984868e438ea8fdac84d874f610f8211f89b25dcba833aba1106e9852d2acf61eefelal404c9724f8cc 6bbd9f560d7c84b34420919490c5fd286bbd9f560d7c84b34420919490c5fd164cef7c893664502d8596891e1aaa feb7239ee885d1e37f3786736d418d6695e59657e4e09742d98f7b29d9234abe96344f50; HttpOnly; Path=/ 4 Content-Length: 258 5 Date: Wed, 25 Jun 2025 13:35:14 GMT 6 7 { "email": "dddddddddddddddddddddddddddddddddddd@DDDDDDDDDD" "is_admin": false, "show_ad": false, "username": "AA true AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"</pre>

Conclusion

Wanna play with `toil33t`?

I can share the Docker container
Or let you play on my own setup

Contacts

Email: `nicolas.gregoire@agarri.fr`

LinkedIn:  Nicolas Gregoire

Discord: `agarri_fr`

Bluesky: `agarri.fr`

Bluesky: `mastering-burp.agarri.fr`