Tips and tricks for Burp Suite Pro

Ten years later...

Nicolas Grégoire aka @Agarri_FR

Northsec 2023

Intro

Who am I?

Nicolas Grégoire

Twitter → `@Agarri_FR`
Email → `nicolas.gregoire@agarri.fr`

Founder & owner of Agarri

Pentest, training and research

Official Burp Suite training partner

Mostly for Europe (I cover North America too)
100+ trainees per year (either on-site and online)

What is the plan?

Core tools

Proxy History / Repeater
Intruder/ Collaborator

Extensions

Hackvertor / Piper / Burp Bounty

Other subjects

Hotkeys / Poor-man automation
Performances / How to stay up to date

Enjoy Montreal

Core tools

Proxy History

Avoid scrolling

Problem

Need to scroll to see fresh entries

Cause → Burp Suite shows the oldest entry on top

Solution

Reverse the sorting order

Click on the header of the # column

Watch out for the small arrow pointing down!

That also works in Logger (core tool) and Logger++ (extension)

Identify sequences

Problem

Mapping actions to traffic is hard

Solution #1

Highlight the top row before triggering an action

- I would use the grey color

Solution #2

When intercepting, highlight and comment the first request

- I would use the yellow color

Core tools

Repeater

Avoid scrolling

Problem

You want to see a specific piece of the response

Like the element `<div class="status">`

Solution

Enter a search criteria

Check "Auto-scroll to match when text changes"

Search among tabs

Problem

Tabs are propely labeled, and groups too

How to search among them?

Solution

Use `Control + Shift + S` (action "Search tabs")

That also works in Intruder and Collaborator

Core tools

Intruder

Built-in wordlists

Burp Suite Pro ships with ~ 50 wordlists

They can be accessed in two clicks

Relevant payload types

- Simple list
- Character substitution
- Case modification
- Illegal Unicode

Built-in wordlists

Built-in wordlists can be exported

Adding lists (possibly from 3rd-parties) is also doable

From the menu bar

Use "Intruder > Configure predefined payload lists"

Built-in wordlists

A dozen of wordlists contain placeholders

Naming isn't standardized

`{FILE}` versus `{KNOWNFILE}`

`{domain}` versus `<yourservername>`

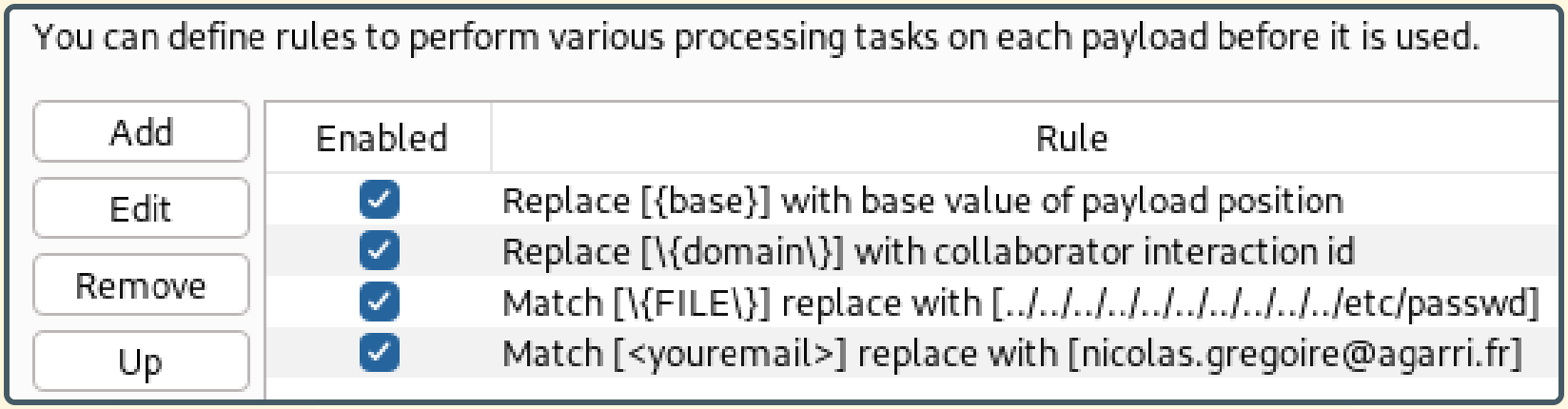
Replacements must be manually configured

Check next page for details

Built-in wordlists

Relevant payload processing rules

"Replace `{base}` with base value of payload position"
"Replace `{domain}` with collaborator interaction id"
"Match/replace" (for `{FILE}`, `<youremail>`, ...)



Core tools

Collaborator

Sneaky interactions

Common assumption

Pingbacks must use the Collaborator domain name

Is that really true? 🤔

Sneaky interactions

Yes, it's true

For DNS interactions

No, it isn't true

For HTTP interactions

Sneaky interactions

Let's look at IP addresses...

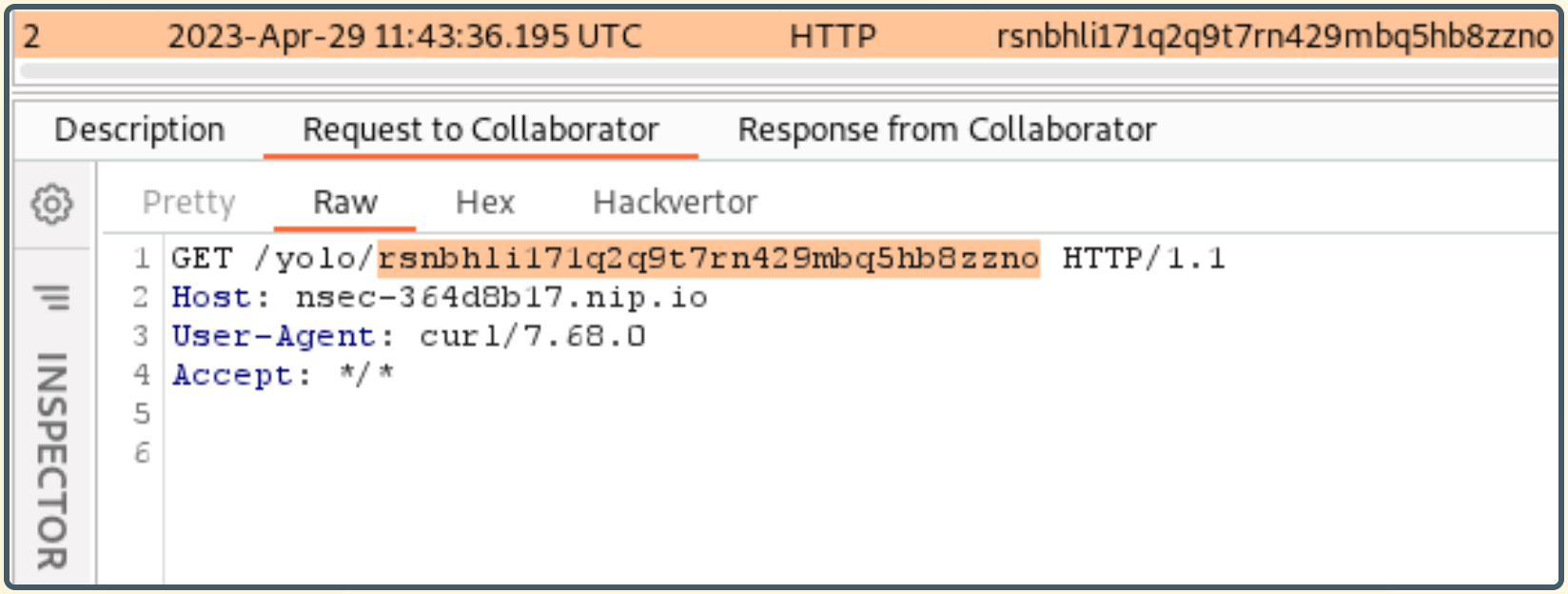
rsnbh[...]8zzno.oastify.com
→ 54.77.139.23 (and 3.248.33.252 too)

nsec-364d8b17.nip.io
→ 54.77.139.23

My correlation ID is `rsnbh[...]8zzno`

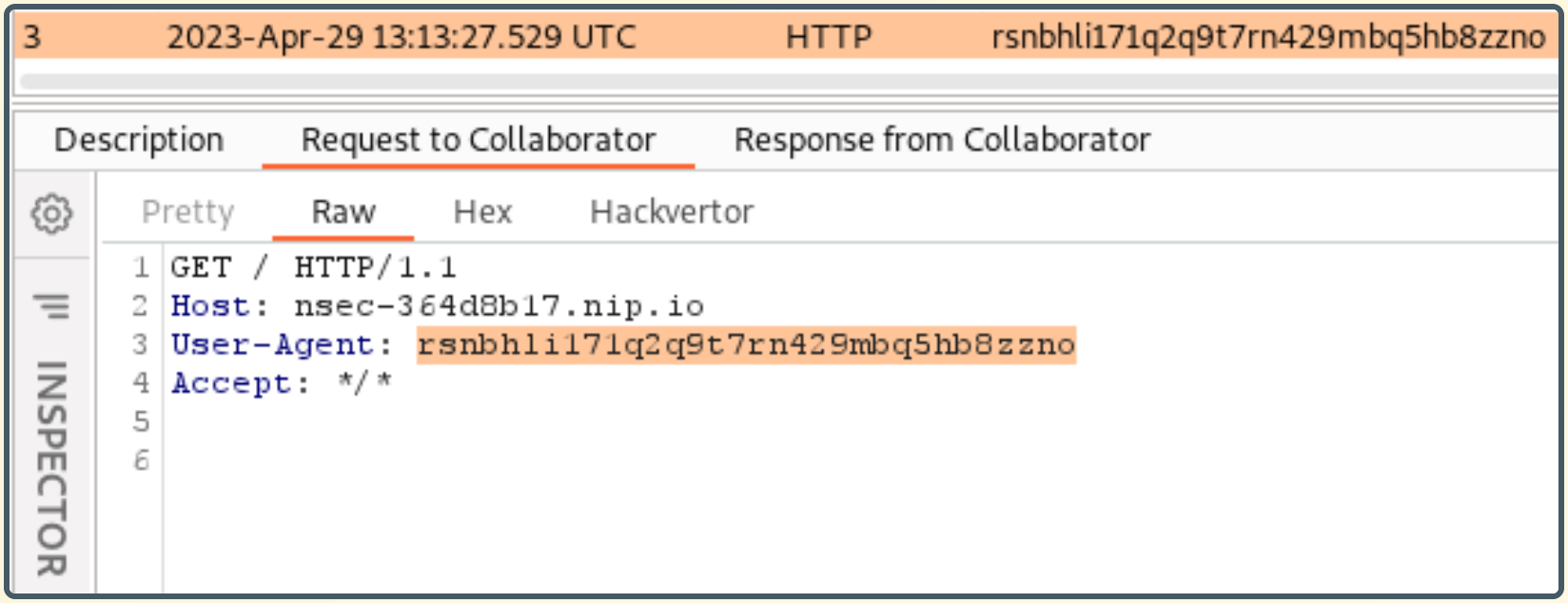
Sneaky interactions

```
$ curl http://nsec-364d8b17.nip.io/yolo/rsnbh[...]8zzno
```



Sneaky interactions

```
$ curl -A rsnbh[...]8zzno http://nsec-364d8b17.nip.io/
```



Extensions

Hackvertor

Hackvertor

Provides more than 200 transformers

And hundreds of charsets

Transformers can be chained

Simply stack them up!

Transformation happens on-the-fly

Hackvertor

Basic example

```
<@base64><@gzip_compress>Hello Northsec!<@/gzip_compress><@/base64>
```

↓

```
H4sIAAAAAAAAA//NIzcnJV/DLLyrJKE5NVgQAA4ANhw8AAAA=
```

Hackvertor

Generate fake data

```
<@fake_hacker("Does the $adjective $noun $verb?","en-GB")/>
```

↓

```
Does the optical hard drive back up?
Does the digital transmitter parse?
Does the multi-byte alarm copy?
```

This feature is provided by `com.github.javafaker`

Hackvertor

Set a global variable

```
<@set_email(true)><@base64>nicolas.gregoire@agarri.fr<@/base64><@/set_email>
```

Generate a signed JWT

```
<@jwt('HS256','secretkey')>{"email":"<@get_email/>","uid":12345}<@/jwt>
```

The `true` flag defines the `email` variable as global

Hackvertor

Exploit a TE.CL vulnerability

```
POST / HTTP/1.1
Host: vulnerable-website.com
Content-Length: <@arithmetic(2,'+')><@length>[...]<@/length><@/arithmetic>
Transfer-Encoding: chunked

<@chunked_dec2hex><@length><@get_chunk/><@/length><@/chunked_dec2hex>
<@set_chunk(false)>SMUGGLED SMUGGLED<@/set_chunk>
0
```

Hackvertor

Sign the body of a request

```
[...]
X-Token: <@set_token(false)>foobar123456<@/set_token>
X-Sig: <@hmac_sha1('<@get_token/>')><@get_body/><@/hmac_sha1>
[...]

<@set_body(false)>name=joe&surname=john&role=admin<@/set_body>
```

Hackvertor

Well-known transformations

`<@base64>`, `<@sha256>`, `<@length>`, `<@lowercase>`,...

Access to the base request

`<@context_url>`, `<@context_param>`, `<@context_header>`, ...

Script execution

`<@python>` (Jython v2.7.0), `<@groovy>` (v3.0.7), `<@java>`, ...

Command execution

`<@system>`

Hackvertor

⚠️ Warning ⚠️

Hackvertor will break Burp syntax parsing

That will impact

Syntax highlighting
Automatic detection of injection points
Automatic URL-encoding

Extensions

Piper

Piper

Executes anything within Burp Suite

Interpeters, CLI and GUI tools, ...

Numerous use-cases

Display JSON data using `gron`
Open a PDF file using `Okular`
Compare messages using `delta` or `Meld`
Uniquely identify bodies using `md5sum`
Detect JWT-authenticated requests using `grep`
Bypass WAF by modifying Scanner payloads using `sed`

Piper + Gron

Demo!

Display JSON data using `gron`

Piper + Okular

Demo!

Open a PDF file using `Okular`

Piper + Meld

Demo!

Compare three requests using `Meld`

Extensions

Burp Bounty

Burp Bounty

Extension that allows to add scan checks

No need to write your own extension

Useful when farming 1-day vulnerabilities 😉

Should be superseded by `BChecks`

Something like "Nuclei for Burp Suite"

It will be released as a core feature in the next weeks

BChecks

```
metadata:
  language: v1-beta
  name: "Collaborator based check"
  description: "Blind SSRF with out-of-band detection"
  author: "Peter Wiener"

given request then
  send request:
    headers:
      "Referer": `{generate_collaborator_address()}`

    if any interactions then
      report issue:
        severity: high
        confidence: firm
        detail: "This site fetches arbitrary URLs specified in the
                 Referer header."
        remediation: "Ensure that the site does not directly request
                      URLS from the Referer header."
    end if
```

Burp Scanner for pentesters
https://www.youtube.com/watch?v=mDYsmfeSxd8&t=2241s

Other subjects

Keyboard shortcuts

Use combos

Problem

Multi-step interactions are executed dozens of times a day
Like sending a request from Proxy History to Repeater

Solution

Use a combination of keyboard shortcuts

`Control + R` → Send to Repeater
`Control + Shift + R` → Switch to Repeater
`Control + Space` → Issue Repeater request

Other subjects

Poor-man automation

Poor-man automation

We need two ingredients

A live task in Burp Suite

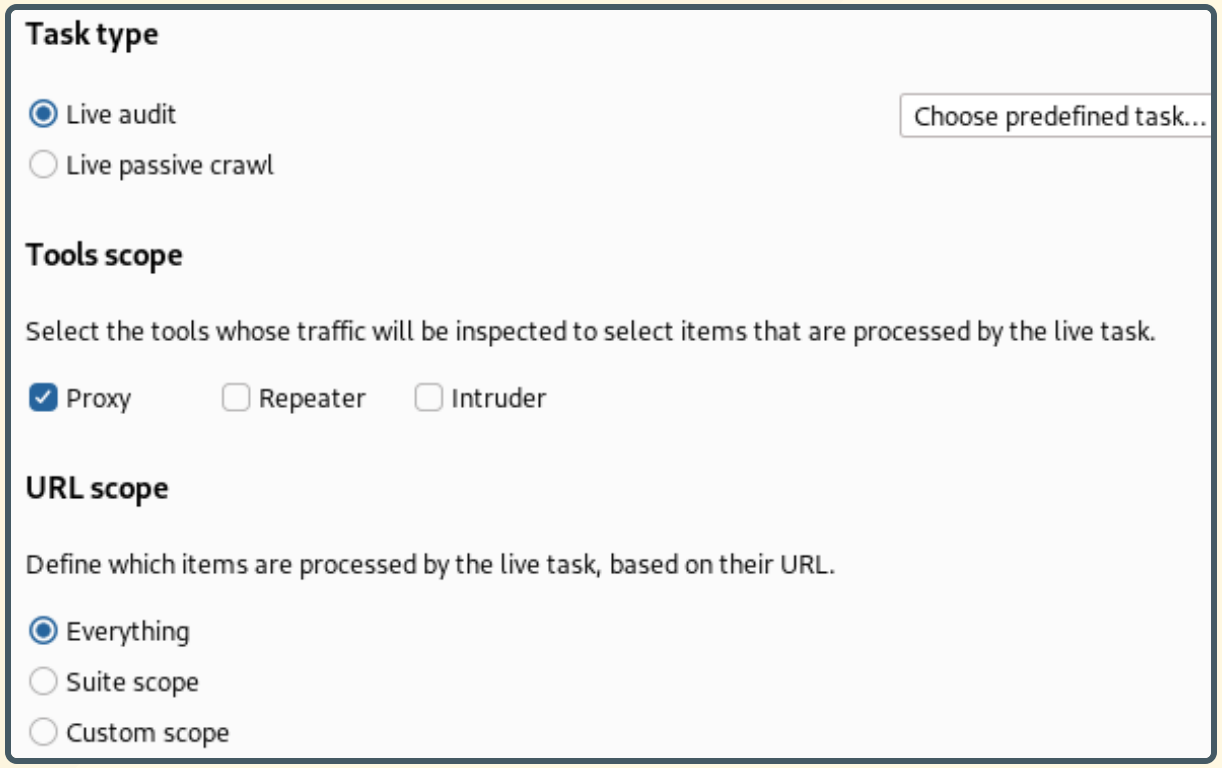
- Configured to scan everything passing through the proxy

The command-line tool `ffuf`

- Configured to replay findings through a proxy

Poor-man automation

Configure the live task



Poor-man automation

Run `ffuf`

```
$ ffuf  -u https://www.agarri.fr/FUZZ
        -w wordlist.txt
        -mc 200
        -replay-proxy http://127.0.0.1:8080
```

Other subjects

Performances

Performances

Problem

Burp Suite consumnes a lot of resources

Opinion

Computers are way cheaper than brains

Solution

Use an oversized computer (CPU, RAM and screen estate)

Other subjects

How to stay up to date

How to stay up to date

PortSwigger on Youtube

https://www.youtube.com/@PortSwiggerTV

PortSwigger on Twitter

https://twitter.com/PortSwigger

https://twitter.com/Burp_Suite

https://twitter.com/BApp_Store

My own dedicated account

https://twitter.com/MasteringBurp

Outro

Want the slides?

https://www.agarri.fr/docs/nsec23-burp_tips_n_tricks.pdf

Want more content?

I'll soon release an online workshop

Details

Cost → Free
Subject → Session management for Apps and APIs
Date → During NahamCon (June 16th, 2023)

Thanks for listening!

Any questions?