Session Management and Session Macros in Burp Suite

Andrej Šimko @ Accenture

AI-AI-AI

- „An Incredibly Annoying, Insufferable Authentication Implementation“

- Made entirely in ChatGPT4

- I have no idea how it works, or what could go wrong :-D
  - Resulting in a real-life real-time demo with debugging

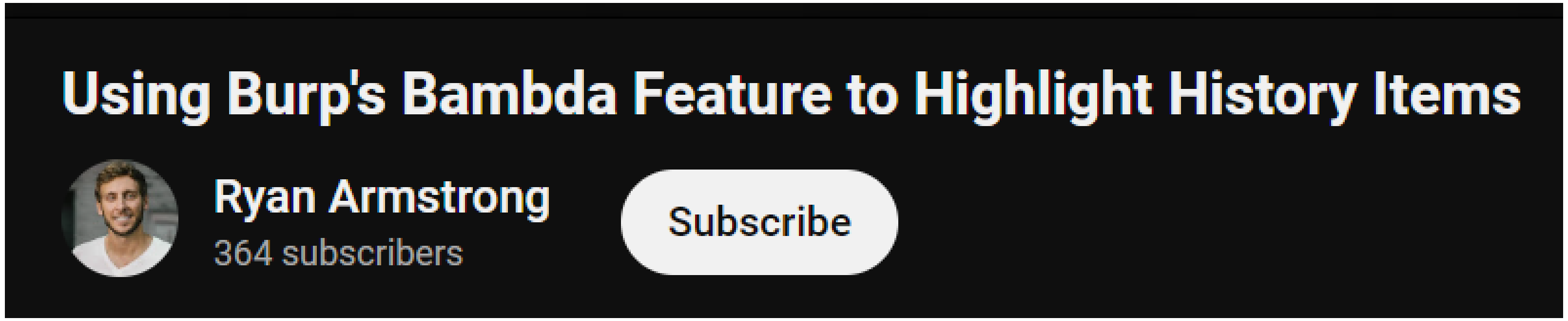
- /hi => no XSS, only input reflected in response
- /hi2 => stored XSS injection
- /names => get all stored values

Iterative approach

- Try to induce as many failures as possible
  - Out of session requests
  - Wrong CSRF tokens
  - Unrecoverable server/environment errors
- Create color highlights and watch out!!!
- Create a session handling rule
  - Does it work on edge cases?
- Set up CSRF token parsing mechanism
  - Does it work on edge cases?

Color highlights

- Bambdas
  - https://www.youtube.com/watch?v=8wqV4zFLviQ

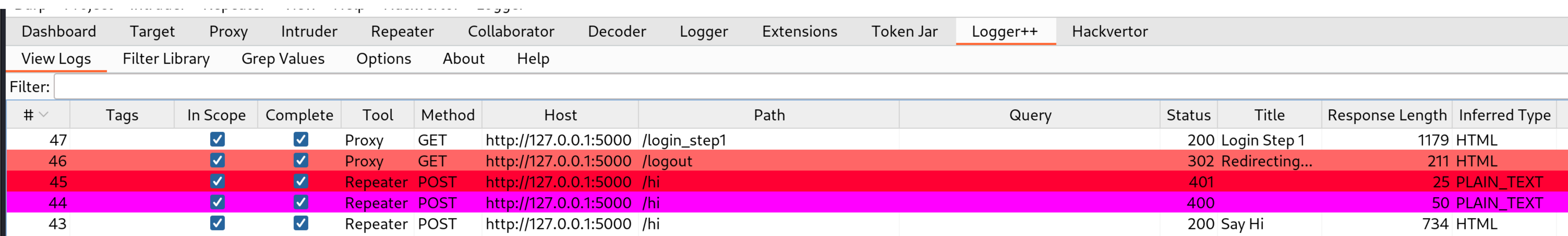


Using Burp's Bambda Feature to Highlight History Items

Ryan Armstrong

364 subscribers

- Logger++ extension



Filter:

#	Tags	In Scope	Complete	Tool	Method	Host	Path	Query	Status	Title	Response Length	Inferred Type
47		☑	☑	Proxy	GET	http://127.0.0.1:5000	/login_step1		200	Login Step 1	1179	HTML
46		☑	☑	Proxy	GET	http://127.0.0.1:5000	/logout		302	Redirecting...	211	HTML
45		☑	☑	Repeater	POST	http://127.0.0.1:5000	/hi		401		25	PLAIN_TEXT
44		☑	☑	Repeater	POST	http://127.0.0.1:5000	/hi		400		50	PLAIN_TEXT
43		☑	☑	Repeater	POST	http://127.0.0.1:5000	/hi		200	Say Hi	734	HTML

CSRF token update

- For our purpose, CSRF token is “any” parameter which needs to be refreshed in order for the request to work.

- Which one is your use-case?
  - Static value
    - Tied to the whole session. If you are logged in, the value does not change
  - One-time value
    - After the backend consumes token, it can no longer be used again

- When to use what?
  - TokenJar
  - Burp Macros
  - Burp Check Session is Valid
  - CPH (Custom Parameter Handler)

TokenJar

- Ideal for on-the-fly updates without the need for pre-request macros

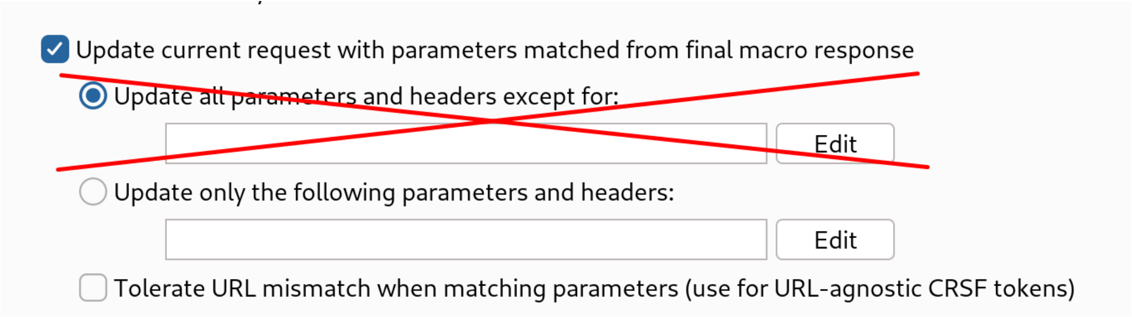
- For 1-time tokens, for successful scenario, usually works

- But what if during Scanner, response is 4xx or 5xx?
    - A single failure can result in a complete failure of Scanner

- Cannot update URL paths, e.g. /api1/{ID}/read

Session Handling Rules

- You can sacrifice speed for reliability
- Native Burp feature
- But beware of settings!!!



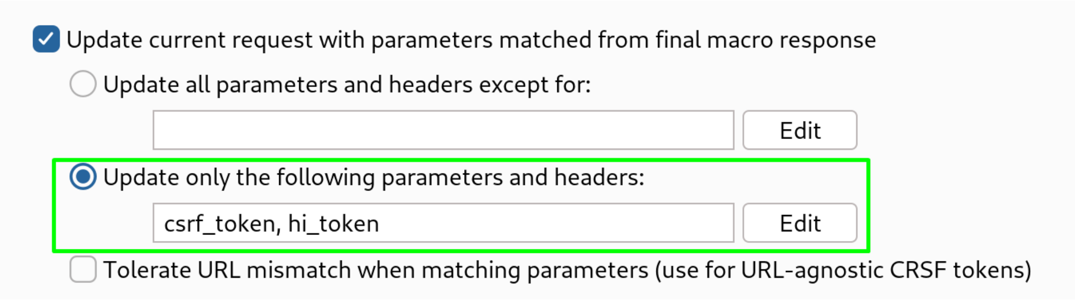
☑ Update current request with parameters matched from final macro response

~~● Update all parameters and headers except for:~~

○ Update only the following parameters and headers:

☐ Tolerate URL mismatch when matching parameters (use for URL-agnostic CRSF tokens)

- Always only update relevant parameters



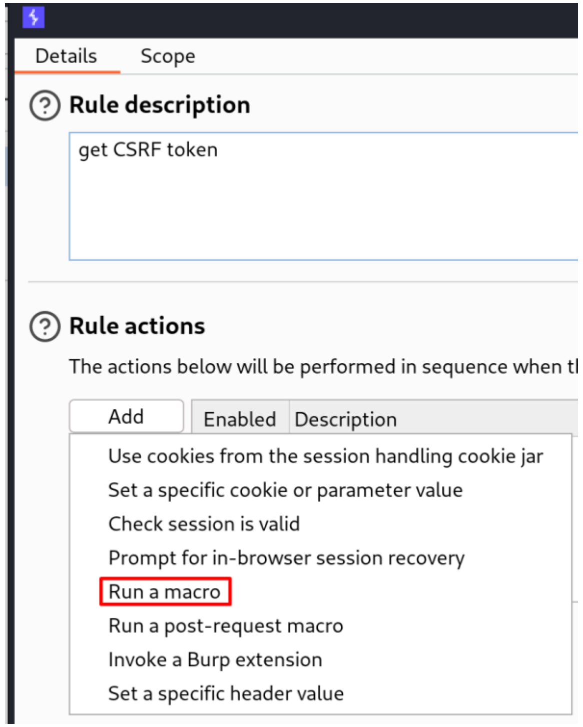
☑ Update current request with parameters matched from final macro response

○ Update all parameters and headers except for:

● Update only the following parameters and headers:

csrf_token, hi_token

☐ Tolerate URL mismatch when matching parameters (use for URL-agnostic CRSF tokens)



Rule description

get CSRF token

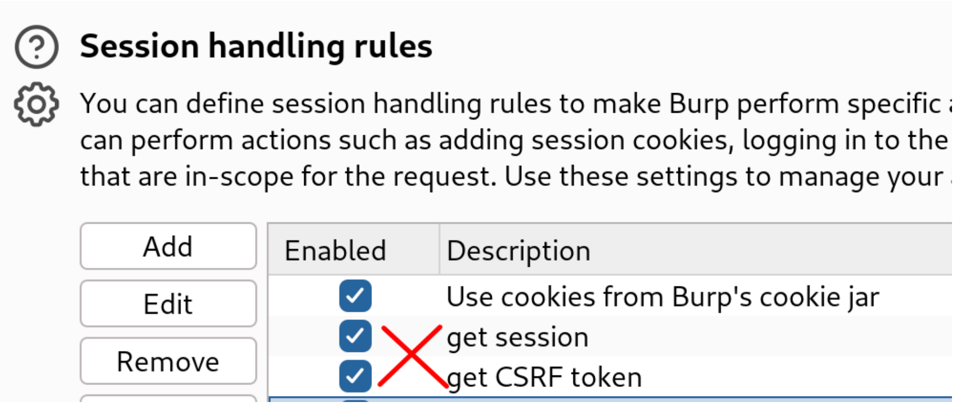
Rule actions

The actions below will be performed in sequence when tl

Details
Scope
Add
Enabled
Description
Use cookies from the session handling cookie jar
Set a specific cookie or parameter value
Check session is valid
Prompt for in-browser session recovery
Run a macro
Run a post-request macro
Invoke a Burp extension
Set a specific header value

The priority of items – Session handling rules

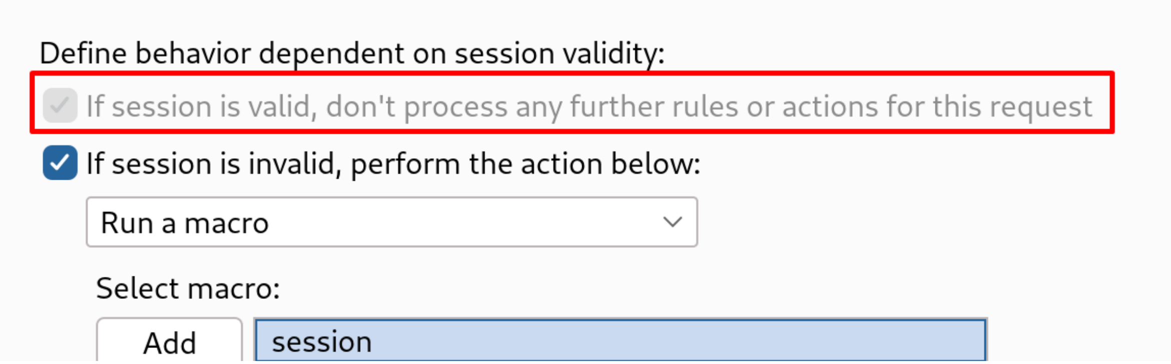
- Establish session -> get CSRF will fail if the session is valid



Session handling rules

You can define session handling rules to make Burp perform specific
can perform actions such as adding session cookies, logging in to the
that are in-scope for the request. Use these settings to manage your

Enabled	Description
☑	Use cookies from Burp's cookie jar
☑	get session
☑	get CSRF token



Define behavior dependent on session validity:

☑ If session is valid, don't process any further rules or actions for this request

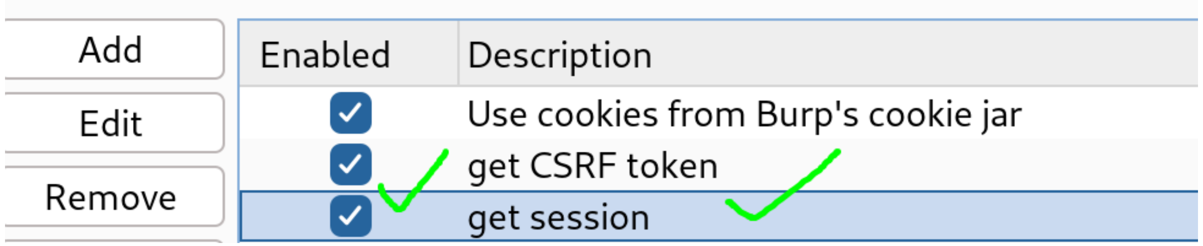
☑ If session is invalid, perform the action below:

Run a macro

Select macro:

session

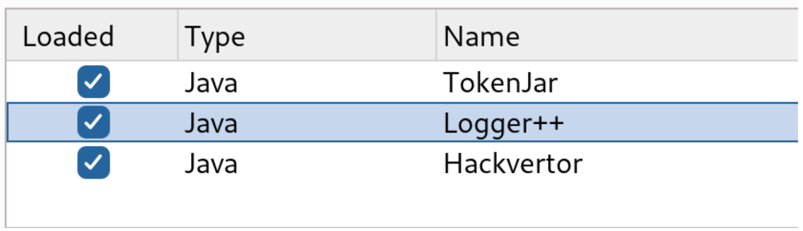
- get CSRF -> Establish session will succeed (will fail for 1 request per out of session)



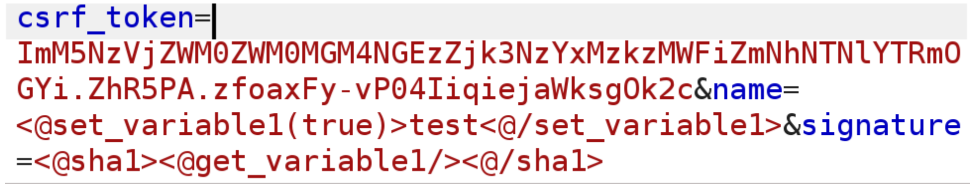
Enabled	Description
☑	Use cookies from Burp's cookie jar
☑	get CSRF token
☑	get session

The priority of items matter - Extenders

Good for debugging to see Logger traffic before rules are applied

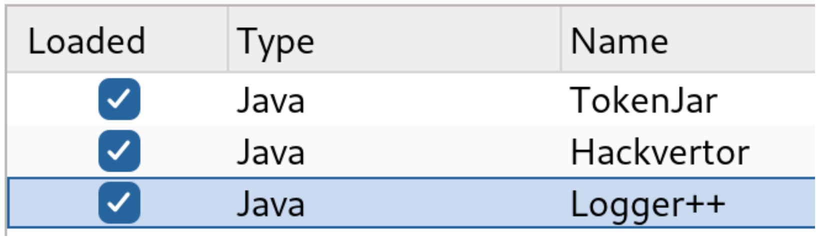


Loaded	Type	Name
☑	Java	TokenJar
☑	Java	Logger++
☑	Java	Hackvertor

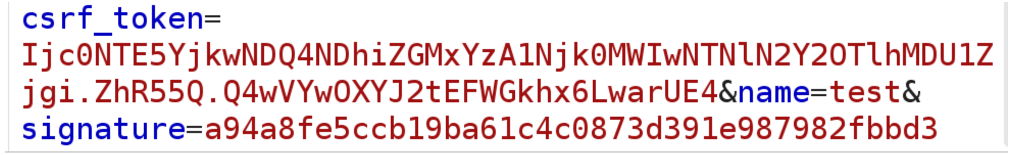


```
csrf_token=
ImM5NzVjZWM0ZWM0MGM4NGEzZjk3NzYxMzkzMWFiZmNhNTNlYTRmO
GYi.ZhR5PA.zfoaxFy-vP04IiqiejaWksgOk2c&name=
<@set_variable1(true)>test<@/set_variable1>&signature
=<@sha1><@get_variable1/><@/sha1>
```

Burp’s Logger does this out of the box



Loaded	Type	Name
☑	Java	TokenJar
☑	Java	Hackvertor
☑	Java	Logger++



```
csrf_token=
Ijc0NTE5YjkwNDQ4NDhiZGMxYzA1Njk0MWIwNTNlN2Y2OTlhMDU1Z
jgi.ZhR55Q.Q4wVYwOXYJ2tEFWGkhx6LwarUE4&name=test&
signature=a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
```