A Burp Extender for HMAC Authentication

Wanchun (Paul) Li

The Roadmap

- Introduction of Burp Extender API
- Use Case of the Extender
- Implementation of the Extender
- Comments of the Burp Extender API

Introduction of Burp Extender API

- Burp GUI is Implemented as Listener Pattern
  - GUI has a set of Events
    - HTTP Event
    - Proxy Event
    - Repeater Event
    - Intruder Event
  - Each Event has its listener interface to implement the actions when the event occurs

- Burp Extender API is a set of APIs for creating customized Burp event actions

Use-Case of this Extender

Testing Scenario

- An HTTP request to www.service.com/handle?name=abc
  - Having an header whose value is a HMAC digest of “handle?name=abc” and a timestamp

Host: www.service.com
Accept: application/json
Authentication: 1377961385093;UO9u4pyMbNsb0Hz6LPlQmXW8hurbkxnFh1Wqh/sOVP8=

- www.service.com authenticates the request
  - If HMAC header does not match the URL, returns error
  - If HMAC header matches the URL, handles the request

Use-Case of this Extender (cont.)

Testing Plan

Use Burp to fuzz the URL “handle?name=abc”

- Replace “abc” in the URL by testing payloads (e.g., </foo>)

The Issue

A testing request of “b/handle?name=</foo>” will get only an error message from the server, because the HMAC header is generated using “b/handle?name=abc”

The Solution

Use Burp Extender to automatically update the HMAC header according the testing payload

Implementation of the Burp Extender

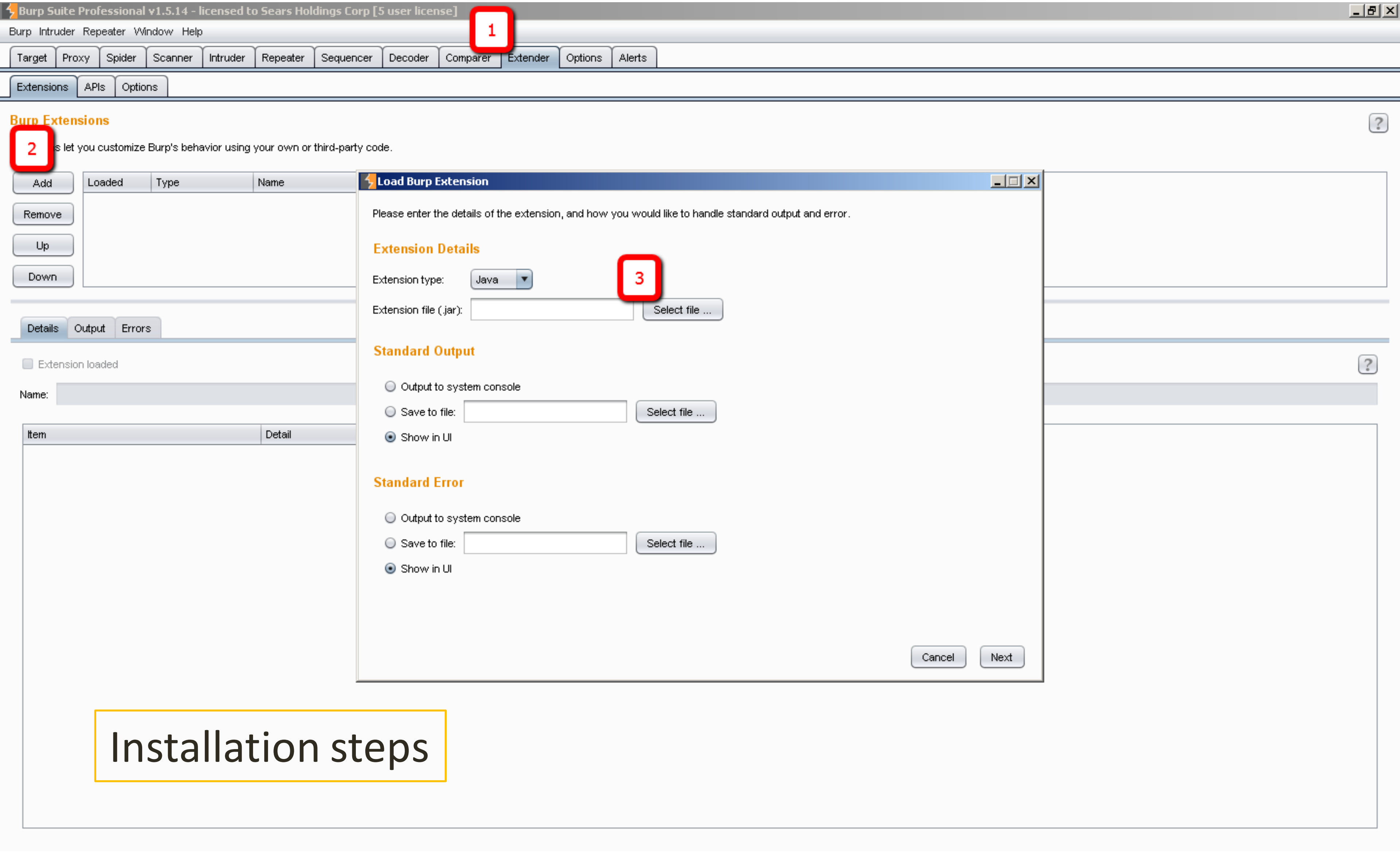
Implement an HTTP event listener to modify the request and Burp GUI behavior

1. Modify the Request

- Capture the testing request URL (e.g., handle?name=</foo>”)
- Computes HMAC of the new URL with a new timestamp
- Add HMAC and timestamp header

2. Modify Burp GUI

- Capture the response of the server handling the testing request
- Add an log panel to GUI to display the server response



Burp Suite Professional v1.5.14 - licensed to Sears Holdings Corp [5 user license]

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Extensions APIs Options
1
2
3

Burp Extensions

...s let you customize Burp's behavior using your own or third-party code.

Add
Remove
Up
Down
Loaded Type Name
Details Output Errors

□ Extension loaded

Name:

Load Burp Extension

Please enter the details of the extension, and how you would like to handle standard output and error.

Extension Details

Extension type: Java

Extension file (.jar): Select file ...

Standard Output

○ Output to system console

○ Save to file: Select file ...

● Show in UI

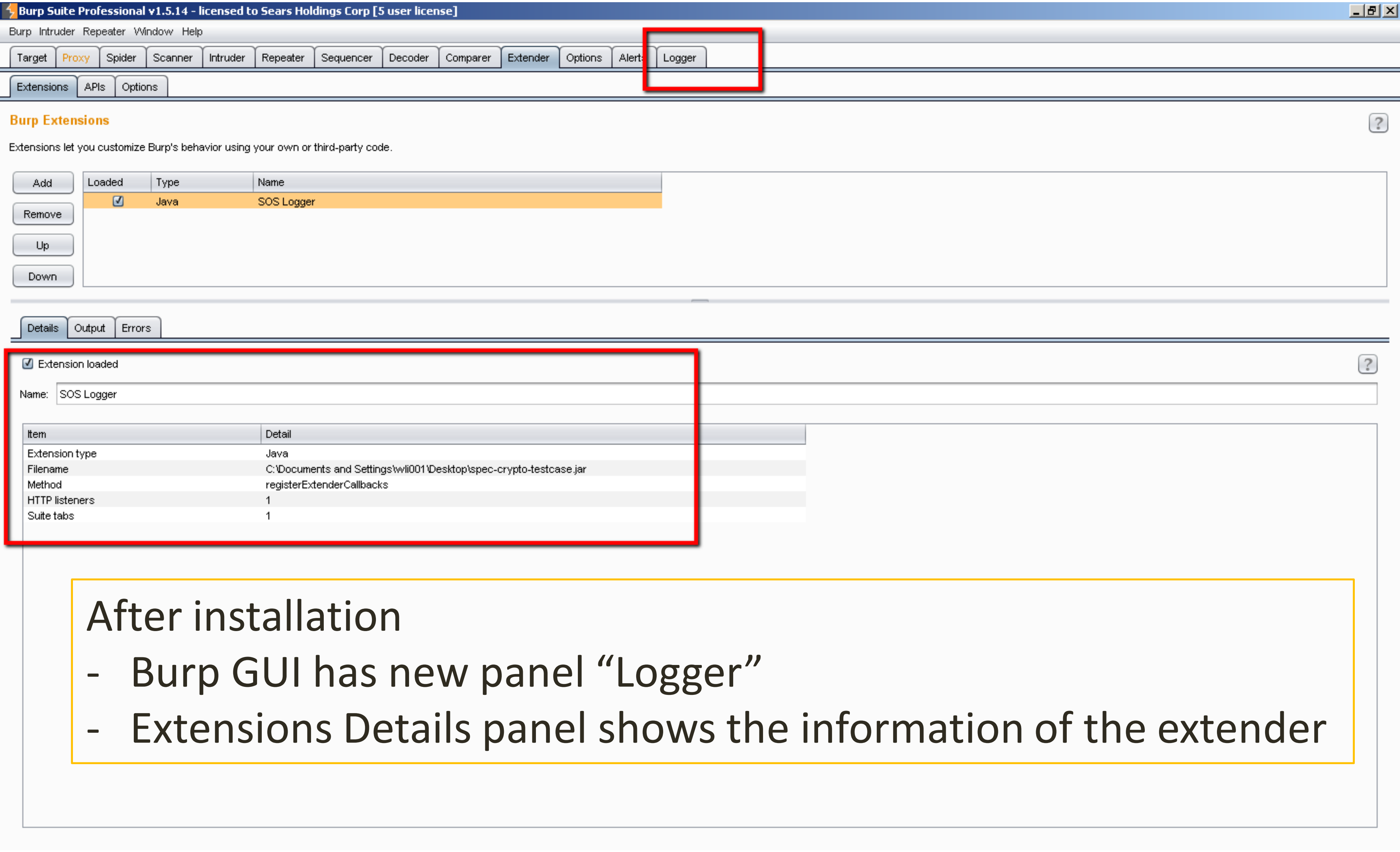
Standard Error

○ Output to system console

○ Save to file: Select file ...

● Show in UI

Installation steps


Burp Suite Professional v1.5.14 - licensed to Sears Holdings Corp [5 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Logger
Extensions APIs Options
Add
Remove
Up
Down
Details Output Errors

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

Loaded	Type	Name
☑	Java	SOS Logger

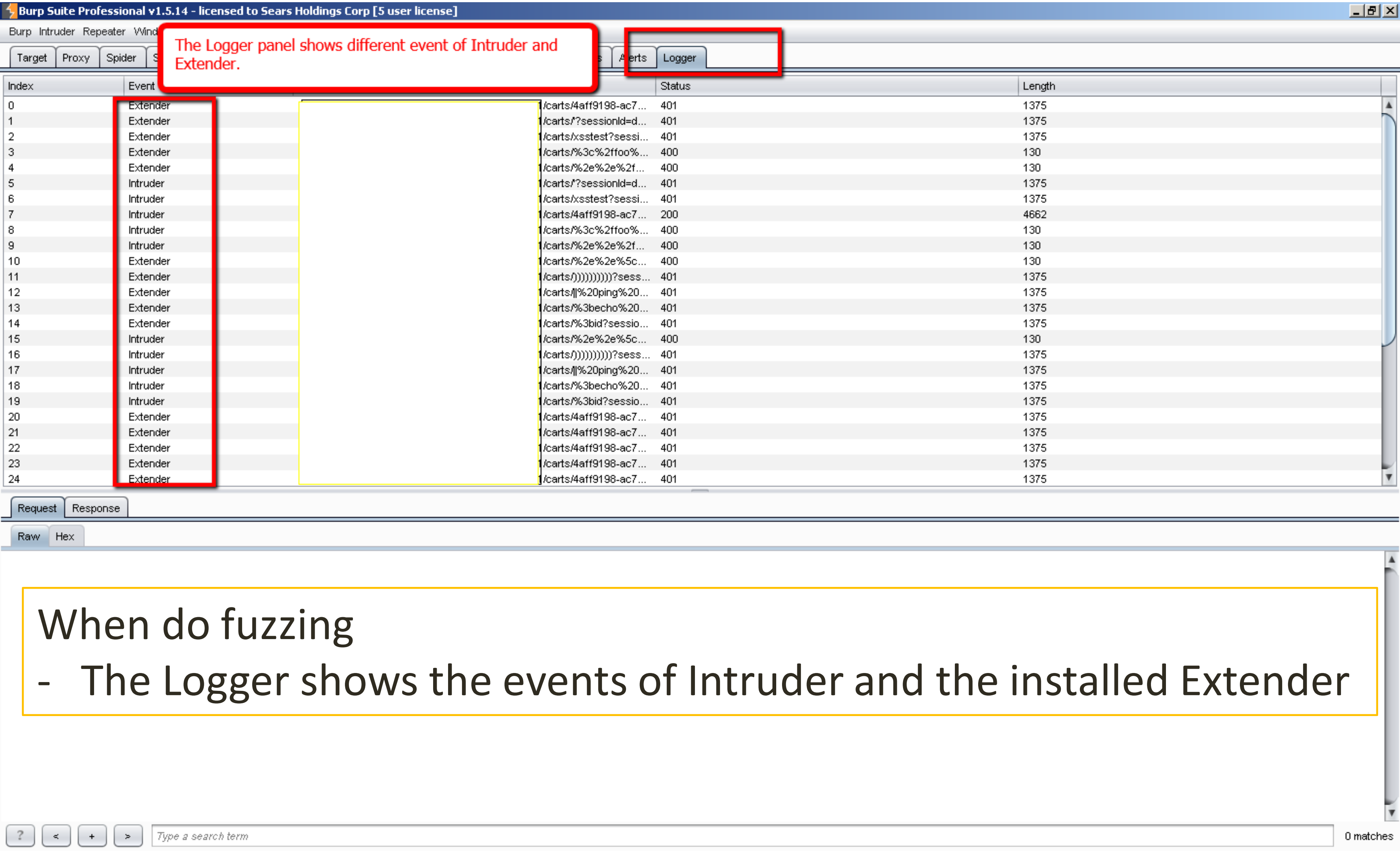
☑ Extension loaded

Name: SOS Logger

Item	Detail
Extension type	Java
Filename	C:\Documents and Settings\wli001\Desktop\spec-crypto-testcase.jar
Method	registerExtenderCallbacks
HTTP listeners	1
Suite tabs	1

After installation

- Burp GUI has new panel “Logger”
- Extensions Details panel shows the information of the extender



Burp Suite Professional v1.5.14 - licensed to Sears Holdings Corp [5 user license]

The Logger panel shows different event of Intruder and Extender.

Index	Event			Status	Length
0	Extender	[redacted]	/carts/4aff9198-ac7...	401	1375
1	Extender	[redacted]	/carts/'?sessionId=d...	401	1375
2	Extender	[redacted]	/carts/xsstest?sessi...	401	1375
3	Extender	[redacted]	/carts/%3c%2ffoo%...	400	130
4	Extender	[redacted]	/carts/%2e%2e%2f...	400	130
5	Intruder	[redacted]	/carts/'?sessionId=d...	401	1375
6	Intruder	[redacted]	/carts/xsstest?sessi...	401	1375
7	Intruder	[redacted]	/carts/4aff9198-ac7...	200	4662
8	Intruder	[redacted]	/carts/%3c%2ffoo%...	400	130
9	Intruder	[redacted]	/carts/%2e%2e%2f...	400	130
10	Extender	[redacted]	/carts/%2e%2e%5c...	400	130
11	Extender	[redacted]	/carts/))))))))))?sess...	401	1375
12	Extender	[redacted]	/carts/||%20ping%20...	401	1375
13	Extender	[redacted]	/carts/%3becho%20...	401	1375
14	Extender	[redacted]	/carts/%3bid?sessio...	401	1375
15	Intruder	[redacted]	/carts/%2e%2e%5c...	400	130
16	Intruder	[redacted]	/carts/))))))))))?sess...	401	1375
17	Intruder	[redacted]	/carts/||%20ping%20...	401	1375
18	Intruder	[redacted]	/carts/%3becho%20...	401	1375
19	Intruder	[redacted]	/carts/%3bid?sessio...	401	1375
20	Extender	[redacted]	/carts/4aff9198-ac7...	401	1375
21	Extender	[redacted]	/carts/4aff9198-ac7...	401	1375
22	Extender	[redacted]	/carts/4aff9198-ac7...	401	1375
23	Extender	[redacted]	/carts/4aff9198-ac7...	401	1375
24	Extender	[redacted]	/carts/4aff9198-ac7...	401	1375

When do fuzzing

- The Logger shows the events of Intruder and the installed Extender

Comments on Extension API

Positive

- Easy to load/unload
- Relatively clear document of APIs
- Good example code

To Improve

- Not enough APIs; make some implementation impossible
    - UI Sort, get attack payload
- “Hardcoded” Extender class
- Cannot export external library
- Buggy; Or I used it in a wrong way