The writeup for 1600 LiveCD Intro Challenge: ZAP Proxy

Introduction

This is a writeup for learning how to use ZAP Proxy.

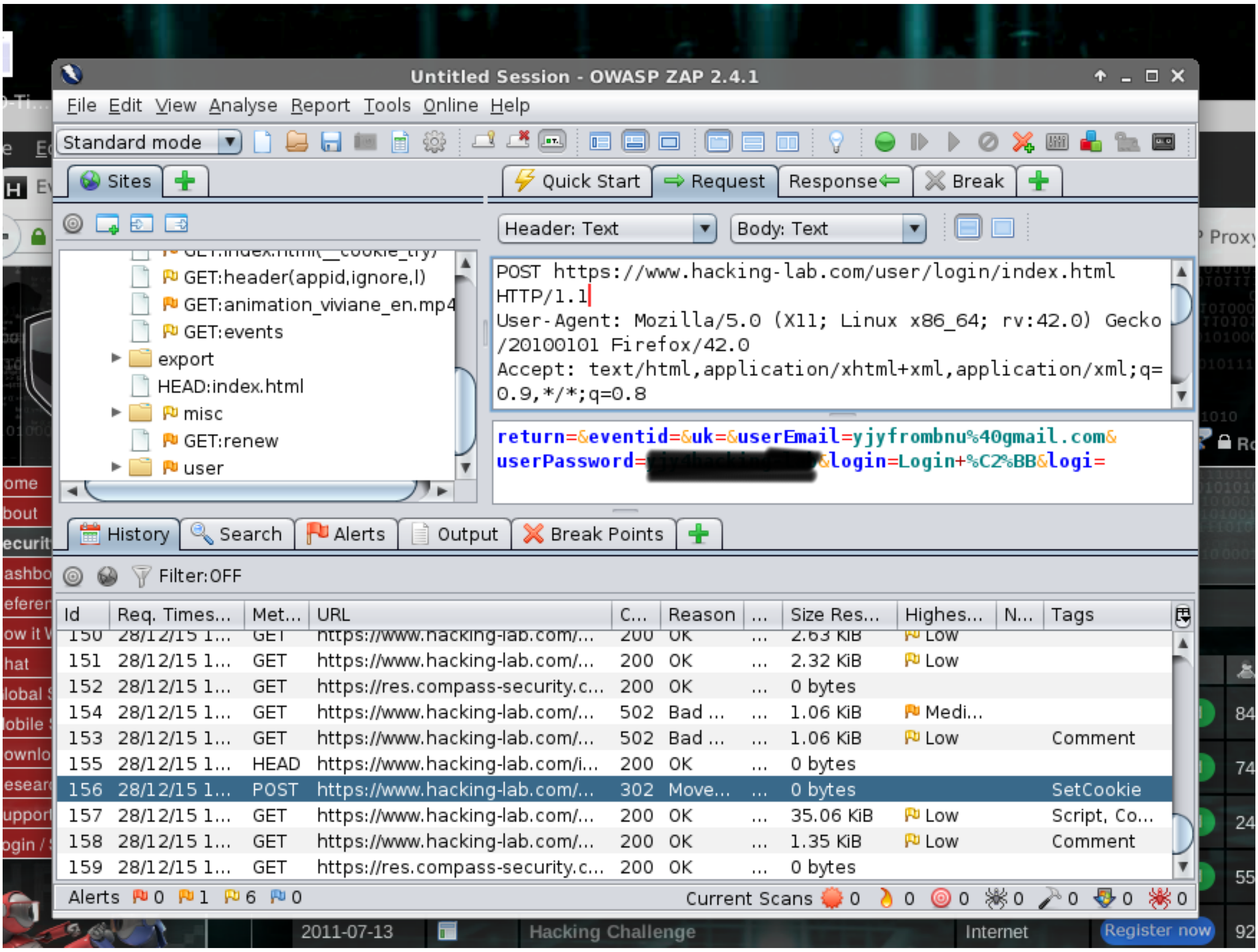
Steps

The mission is to analyse the web requests between your browser and www.hacking-lab.com.

Login request

The request is a POST request with URL https://www.hacking-lab.com/user/login/index.html. The login parameters are userEmail and userPassword. However, the password is transported in plaintext.

The snapshot is followed.



```
POST https://www.hacking-lab.com/user/login/index.html
HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:42.0) Gecko
/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=
0.9,*/*;q=0.8
```

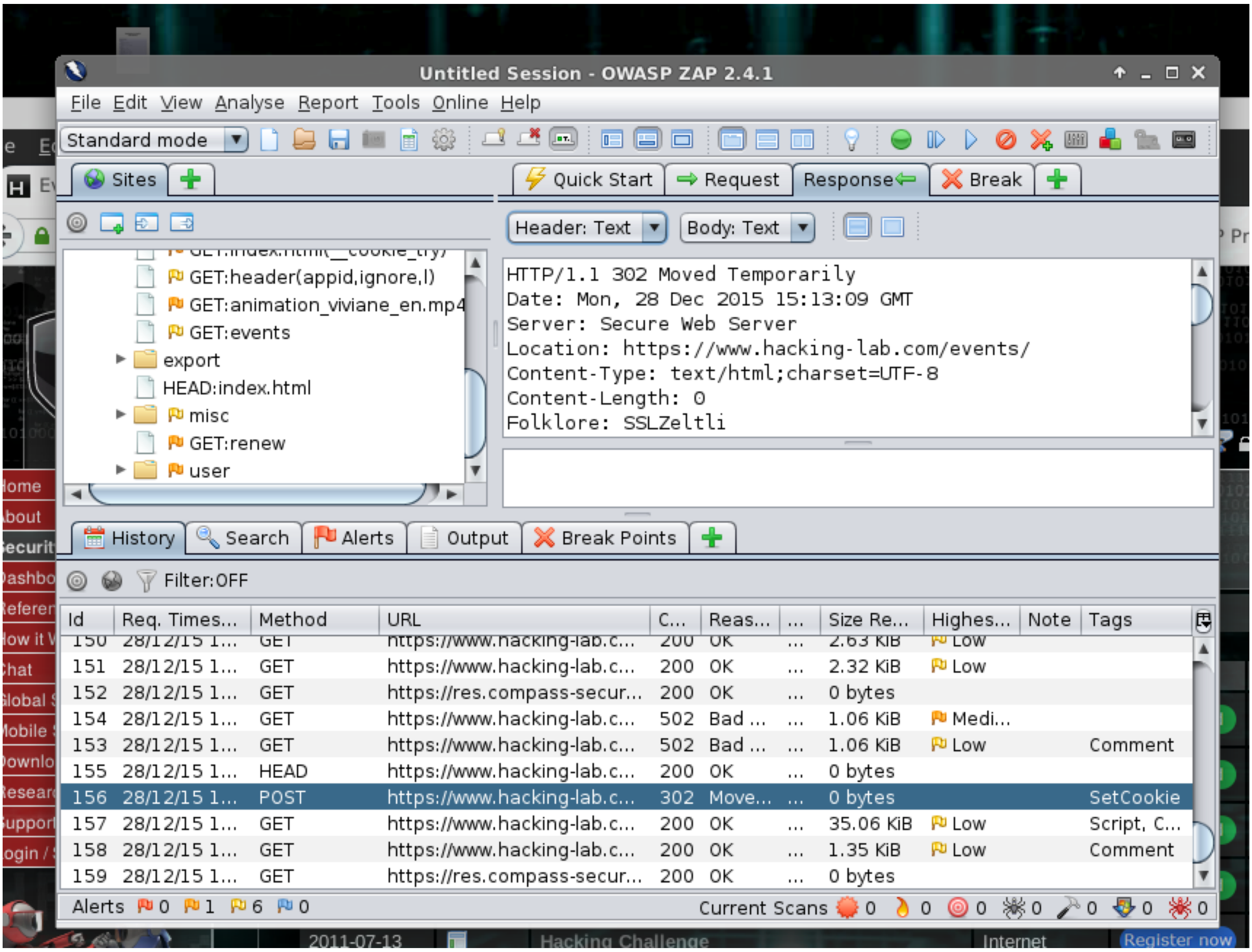
```
return=&eventid=&uk=&userEmail=yjyfrombnu%40gmail.com&
userPassword=[redacted]&login=Login+%C2%BB&logi=
```

Id	Req. Times...	Met...	URL	C...	Reason	...	Size Res...	Highes...	N...	Tags
150	28/12/15 1...	GET	https://www.hacking-lab.com/...	200	OK	...	2.63 KiB	Low		
151	28/12/15 1...	GET	https://www.hacking-lab.com/...	200	OK	...	2.32 KiB	Low		
152	28/12/15 1...	GET	https://res.compass-security.c...	200	OK	...	0 bytes			
154	28/12/15 1...	GET	https://www.hacking-lab.com/...	502	Bad ...	...	1.06 KiB	Medi...		
153	28/12/15 1...	GET	https://www.hacking-lab.com/...	502	Bad ...	...	1.06 KiB	Low		Comment
155	28/12/15 1...	HEAD	https://www.hacking-lab.com/i...	200	OK	...	0 bytes			
156	28/12/15 1...	POST	https://www.hacking-lab.com/...	302	Move...	...	0 bytes			SetCookie
157	28/12/15 1...	GET	https://www.hacking-lab.com/...	200	OK	...	35.06 KiB	Low		Script, Co...
158	28/12/15 1...	GET	https://www.hacking-lab.com/...	200	OK	...	1.35 KiB	Low		Comment
159	28/12/15 1...	GET	https://res.compass-security.c...	200	OK	...	0 bytes			

Server response (succeeded)

After successful authentication, the server sent a 302 Moved Temporarily response with URL https://www.hacking-lab.com/events/

The snapshot is followed.


Untitled Session - OWASP ZAP 2.4.1
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Quick Start
Request
Response
Break
Header: Text
Body: Text
GET:index.html(__cookie_try)
GET:header(appid,ignore,l)
GET:animation_viviane_en.mp4
GET:events
export
HEAD:index.html
misc
GET:renew
user
History
Search
Alerts
Output
Break Points
Filter:OFF
Alerts 0 1 6 0
Current Scans 0 0 0 0 0 0 0

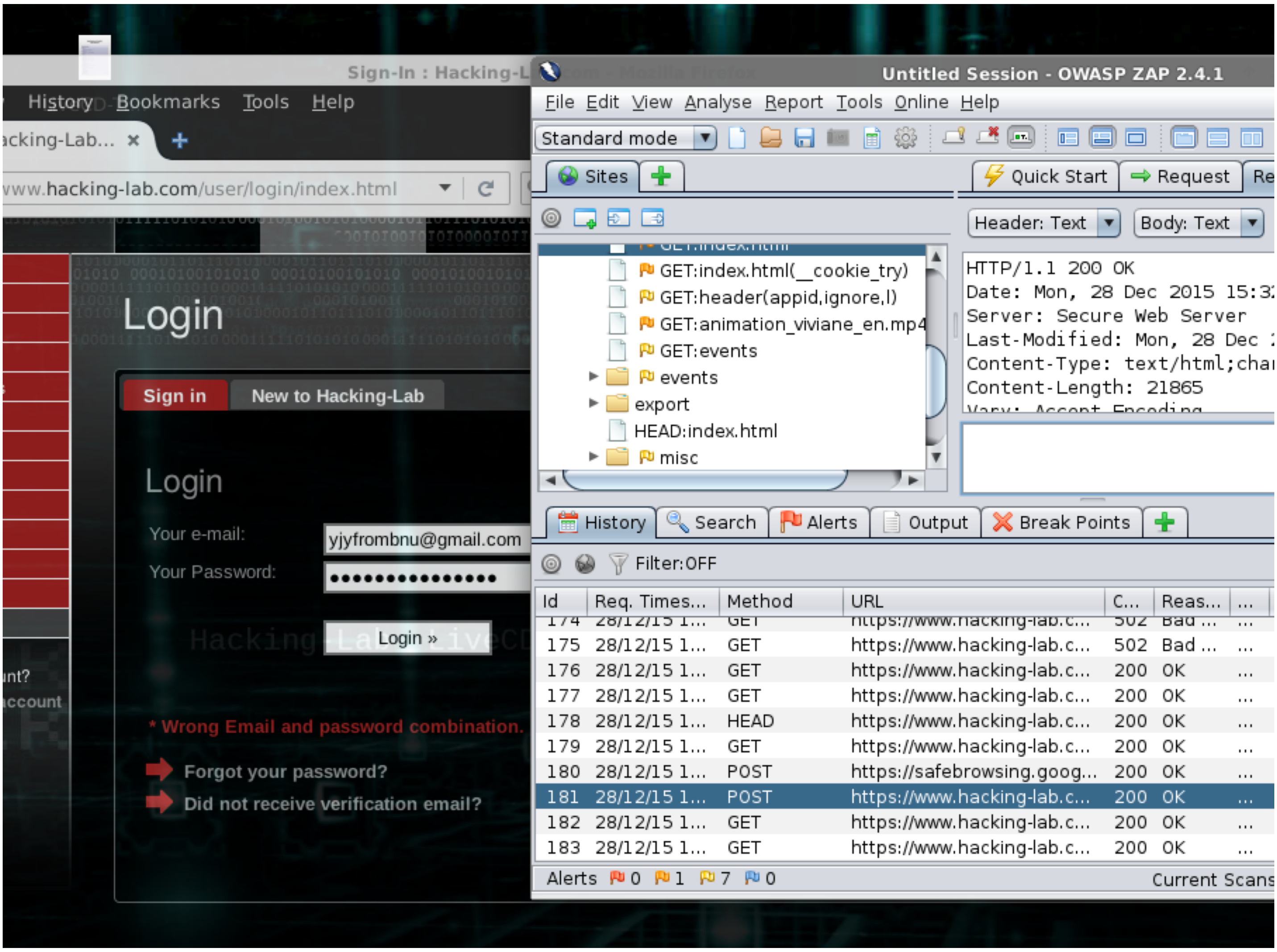
```
HTTP/1.1 302 Moved Temporarily
Date: Mon, 28 Dec 2015 15:13:09 GMT
Server: Secure Web Server
Location: https://www.hacking-lab.com/events/
Content-Type: text/html;charset=UTF-8
Content-Length: 0
Folklore: SSLZeltli
```

Id	Req. Times...	Method	URL	C...	Reas...	...	Size Re...	Highes...	Note	Tags
150	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...	2.63 KiB	Low		
151	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...	2.32 KiB	Low		
152	28/12/15 1...	GET	https://res.compass-secur...	200	OK	...	0 bytes			
154	28/12/15 1...	GET	https://www.hacking-lab.c...	502	Bad ...	...	1.06 KiB	Medi...		
153	28/12/15 1...	GET	https://www.hacking-lab.c...	502	Bad ...	...	1.06 KiB	Low		Comment
155	28/12/15 1...	HEAD	https://www.hacking-lab.c...	200	OK	...	0 bytes			
156	28/12/15 1...	POST	https://www.hacking-lab.c...	302	Move...	...	0 bytes			SetCookie
157	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...	35.06 KiB	Low		Script, C...
158	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...	1.35 KiB	Low		Comment
159	28/12/15 1...	GET	https://res.compass-secur...	200	OK	...	0 bytes			

Server Response (failed)

If I input a wrong password, the server will send a 200 OK response. The content of website will show a error message 'Wrong Email and password combination'.

The snapshot is followed.



Your e-mail: yjyfrombnu@gmail.com

Your Password: ••••••••••••••••

* Wrong Email and password combination.

```
HTTP/1.1 200 OK
Date: Mon, 28 Dec 2015 15:3
Server: Secure Web Server
Last-Modified: Mon, 28 Dec 
Content-Type: text/html;char
Content-Length: 21865
Vary: Accept-Encoding
```

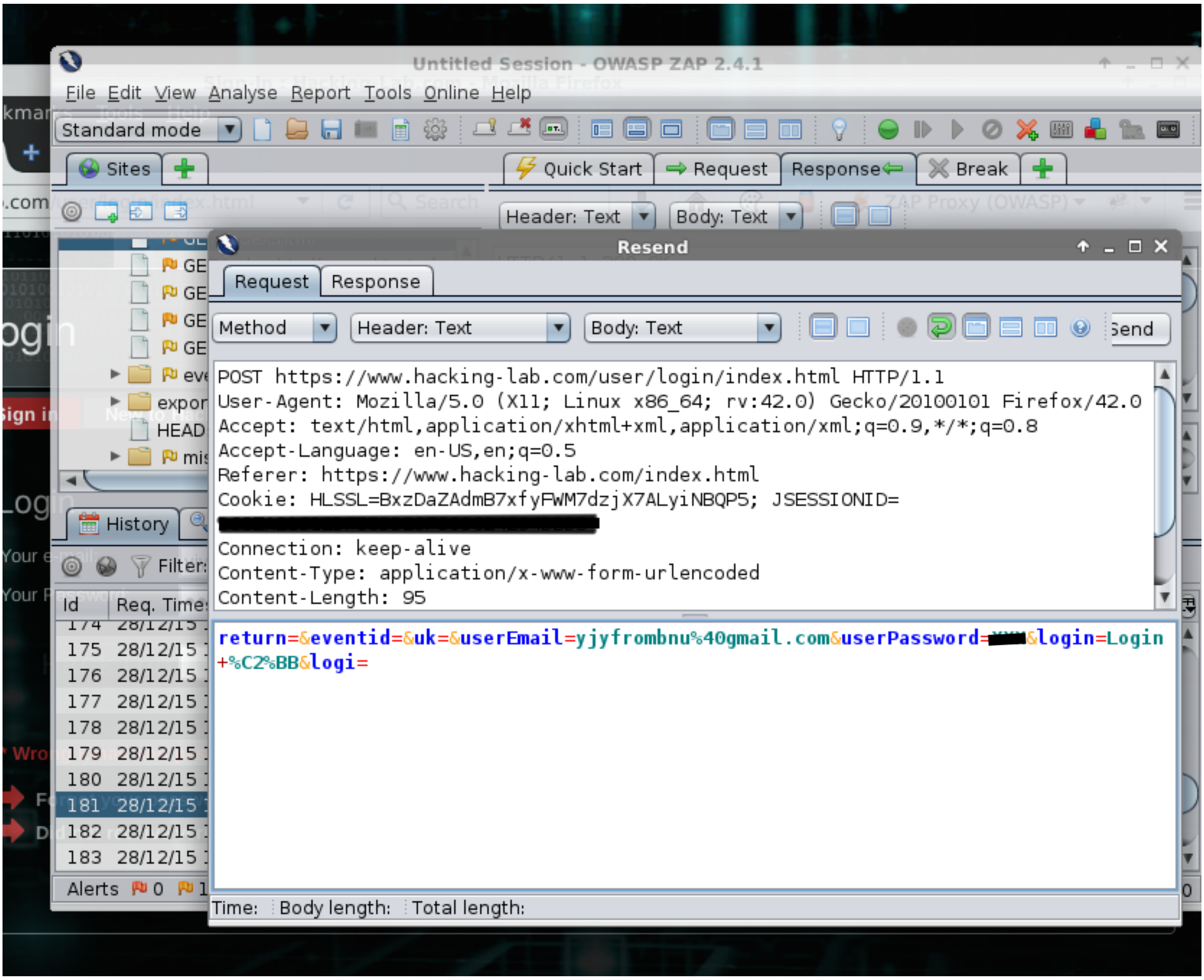
Id	Req. Times...	Method	URL	C...	Reas...	...
174	28/12/15 1...	GET	https://www.hacking-lab.c...	502	Bad ...	...
175	28/12/15 1...	GET	https://www.hacking-lab.c...	502	Bad ...	...
176	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...
177	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...
178	28/12/15 1...	HEAD	https://www.hacking-lab.c...	200	OK	...
179	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...
180	28/12/15 1...	POST	https://safebrowsing.goog...	200	OK	...
181	28/12/15 1...	POST	https://www.hacking-lab.c...	200	OK	...
182	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...
183	28/12/15 1...	GET	https://www.hacking-lab.c...	200	OK	...

Alerts 0 1 7 0

Resend Feature

The resend feature can be used by right clicking the login request item, and choosing resend item. And then the http parameters can be modified manually.

The snapshot is followed.



```
POST https://www.hacking-lab.com/user/login/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://www.hacking-lab.com/index.html
Cookie: HLSSL=BxzDaZAdmB7xfyFWM7dzjX7ALyiNBQP5; JSESSIONID=
[redacted]
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 95

return=&eventid=&uk=&userEmail=yjyfrombnu%40gmail.com&userPassword=[redacted]&login=Login
+%C2%BB&logi=
```

Conclusion

This is a beginner practice for ZAP Proxy. The trap and resend feature is cool.