PROJECT : 1

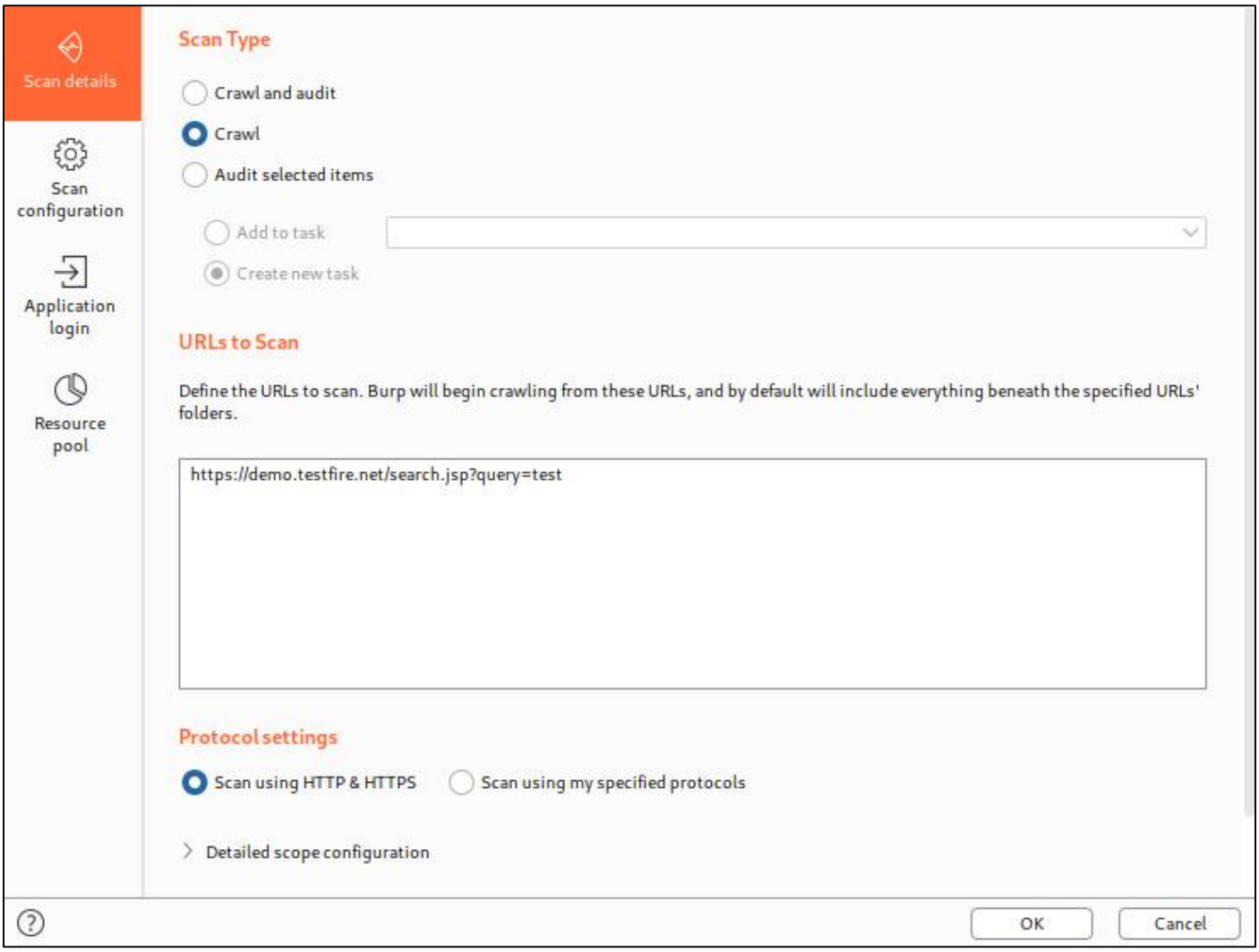
DATE:-03-12-2021

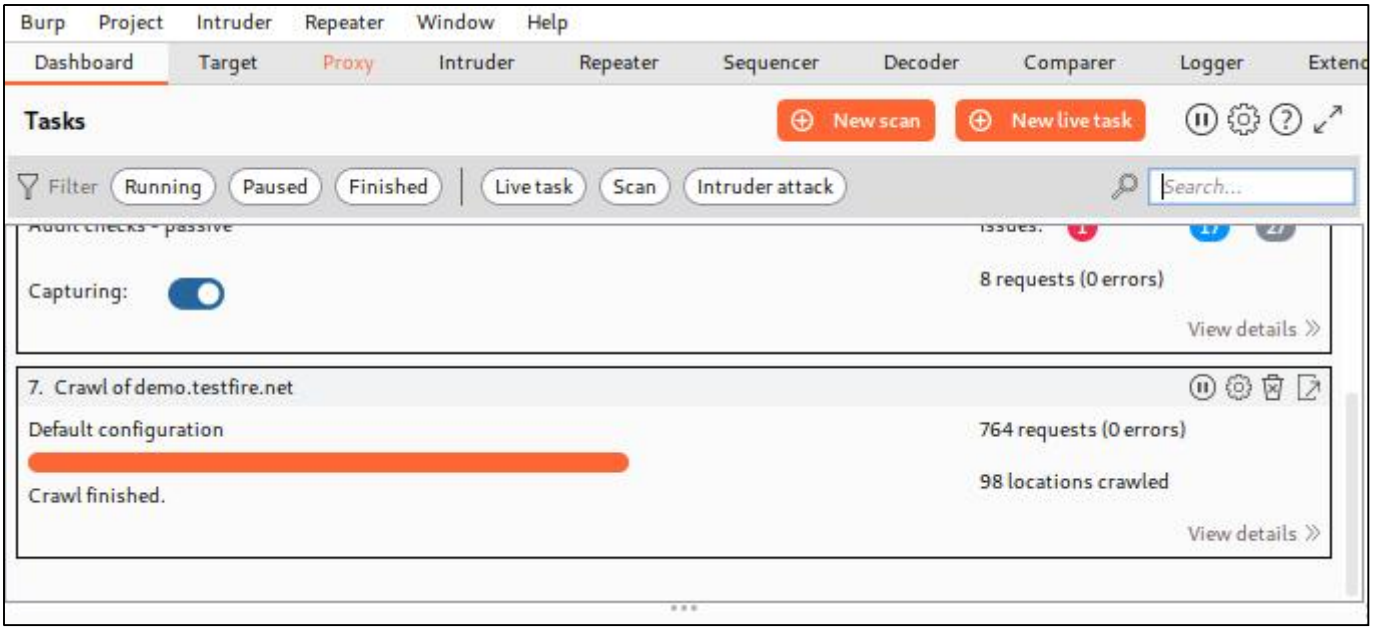
TOPIC:-Perform the following attacks:-

a. Crawling on testfire.net
b. Directory bruteforcing on testfire.net
c. XSS bruteforcing on testfire.net
d. SQL fuzzing testphp.vulnweb.com

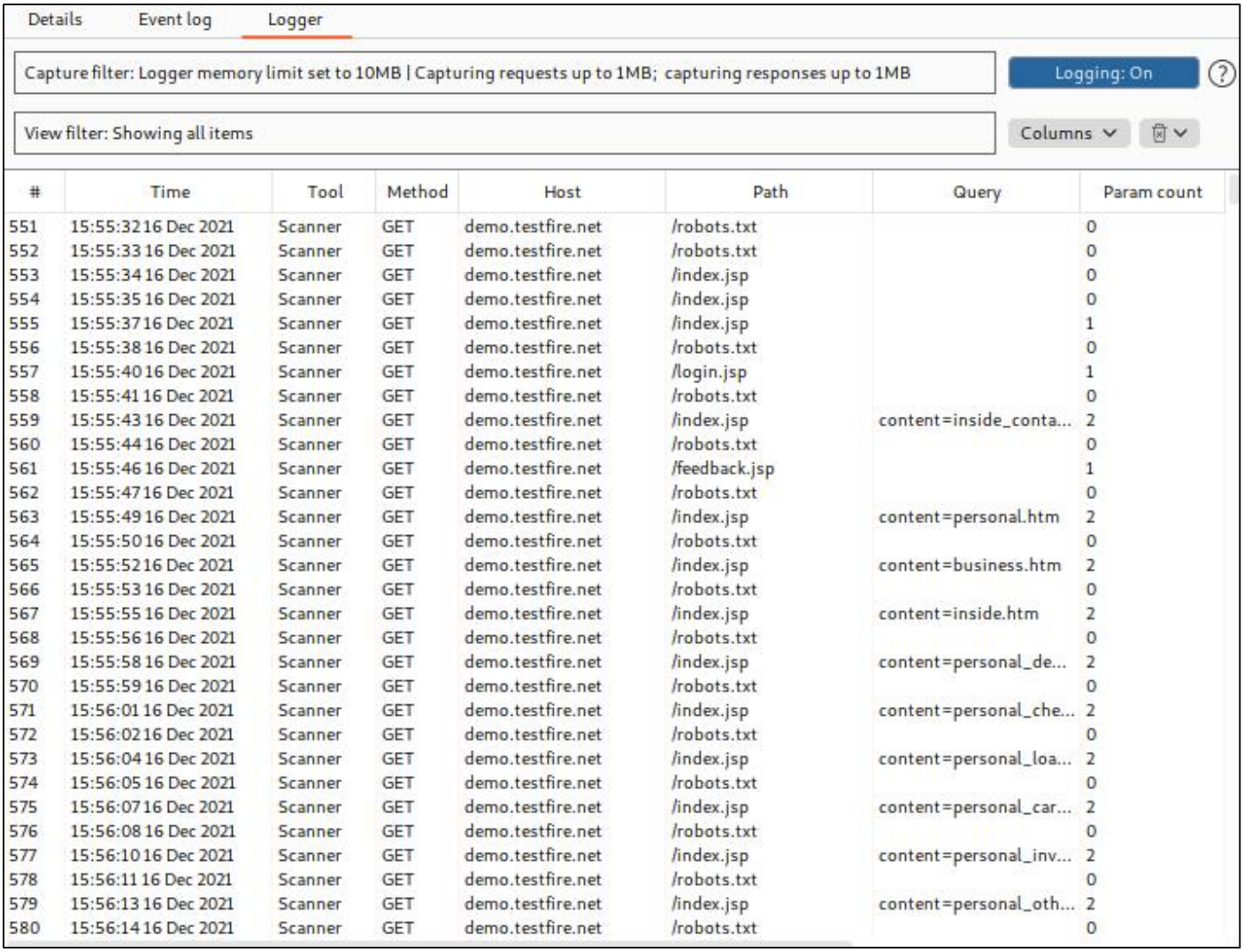
Crawling on testfire.net

1. Intercept the request in burpsuite, and right-click, select scan.





2. Let's see event logs



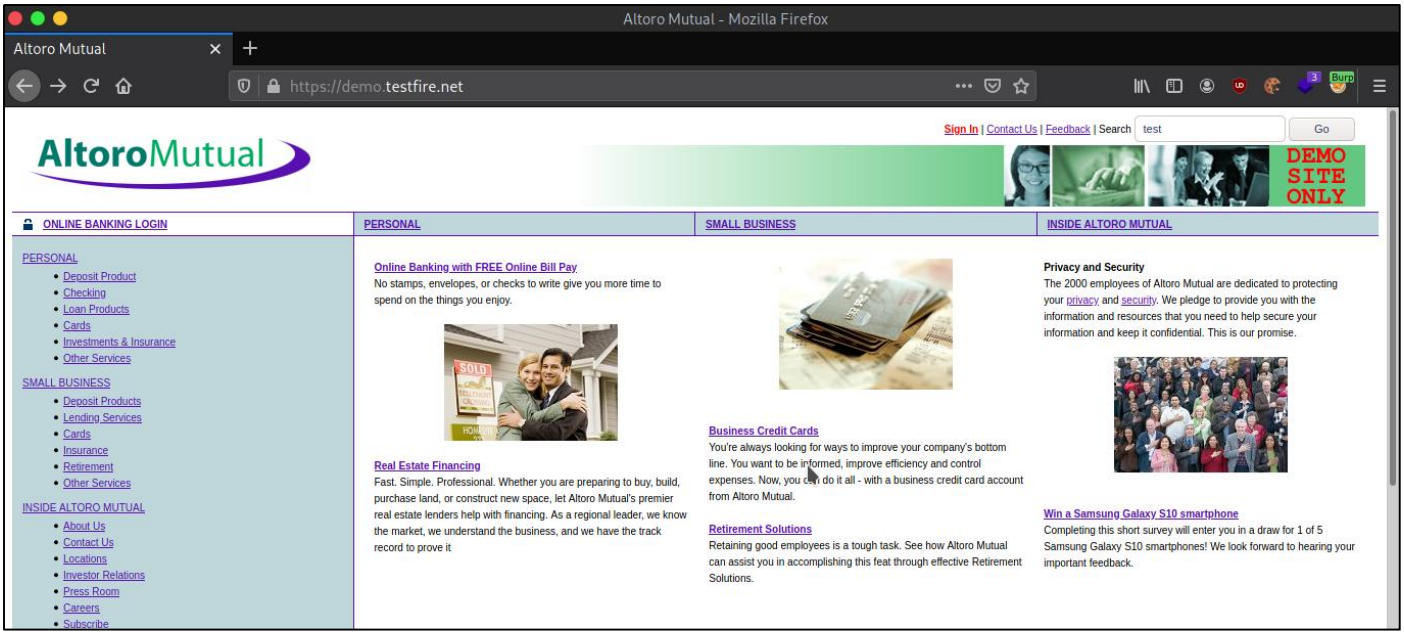
#	Time	Tool	Method	Host	Path	Query	Param count
551	15:55:32 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
552	15:55:33 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
553	15:55:34 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp		0
554	15:55:35 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp		0
555	15:55:37 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp		1
556	15:55:38 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
557	15:55:40 16 Dec 2021	Scanner	GET	demo.testfire.net	/login.jsp		1
558	15:55:41 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
559	15:55:43 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=inside_conta...	2
560	15:55:44 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
561	15:55:46 16 Dec 2021	Scanner	GET	demo.testfire.net	/feedback.jsp		1
562	15:55:47 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
563	15:55:49 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal.htm	2
564	15:55:50 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
565	15:55:52 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=business.htm	2
566	15:55:53 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
567	15:55:55 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=inside.htm	2
568	15:55:56 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
569	15:55:58 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_de...	2
570	15:55:59 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
571	15:56:01 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_che...	2
572	15:56:02 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
573	15:56:04 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_loa...	2
574	15:56:05 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
575	15:56:07 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_car...	2
576	15:56:08 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
577	15:56:10 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_inv...	2
578	15:56:11 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
579	15:56:13 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_oth...	2
580	15:56:14 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0

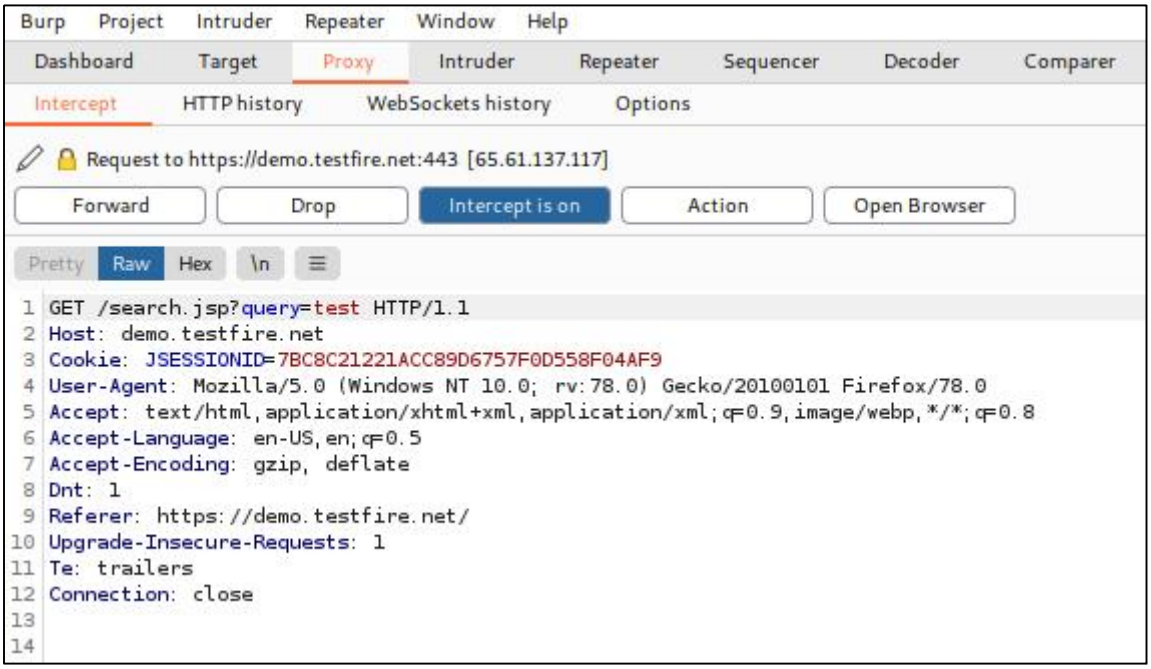
Directory bruteforcing on testfire.net

```
┌──[x]─[parrot@parrot-virtualbox]─[~]
└─── $dirb https://demo.testfire.net/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Dec 16 13:53:36 2021
URL_BASE: https://demo.testfire.net/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://demo.testfire.net/ ----
+ https://demo.testfire.net/admin (CODE:302|SIZE:0)
+ https://demo.testfire.net/aux (CODE:200|SIZE:0)
+ https://demo.testfire.net/bank (CODE:302|SIZE:0)
+ https://demo.testfire.net/com1 (CODE:200|SIZE:0)
+ https://demo.testfire.net/com2 (CODE:200|SIZE:0)
+ https://demo.testfire.net/com3 (CODE:200|SIZE:0)
+ https://demo.testfire.net/con (CODE:200|SIZE:0)
+ https://demo.testfire.net/images (CODE:302|SIZE:0)
+ https://demo.testfire.net/lpt1 (CODE:200|SIZE:0)
+ https://demo.testfire.net/lpt2 (CODE:200|SIZE:0)
+ https://demo.testfire.net/nul (CODE:200|SIZE:0)
+ https://demo.testfire.net/pr (CODE:302|SIZE:0)
+ https://demo.testfire.net/prn (CODE:200|SIZE:0)
+ https://demo.testfire.net/static (CODE:302|SIZE:0)
+ https://demo.testfire.net/util (CODE:302|SIZE:0)

-----------------
END_TIME: Thu Dec 16 14:17:24 2021
DOWNLOADED: 4612 - FOUND: 15
```

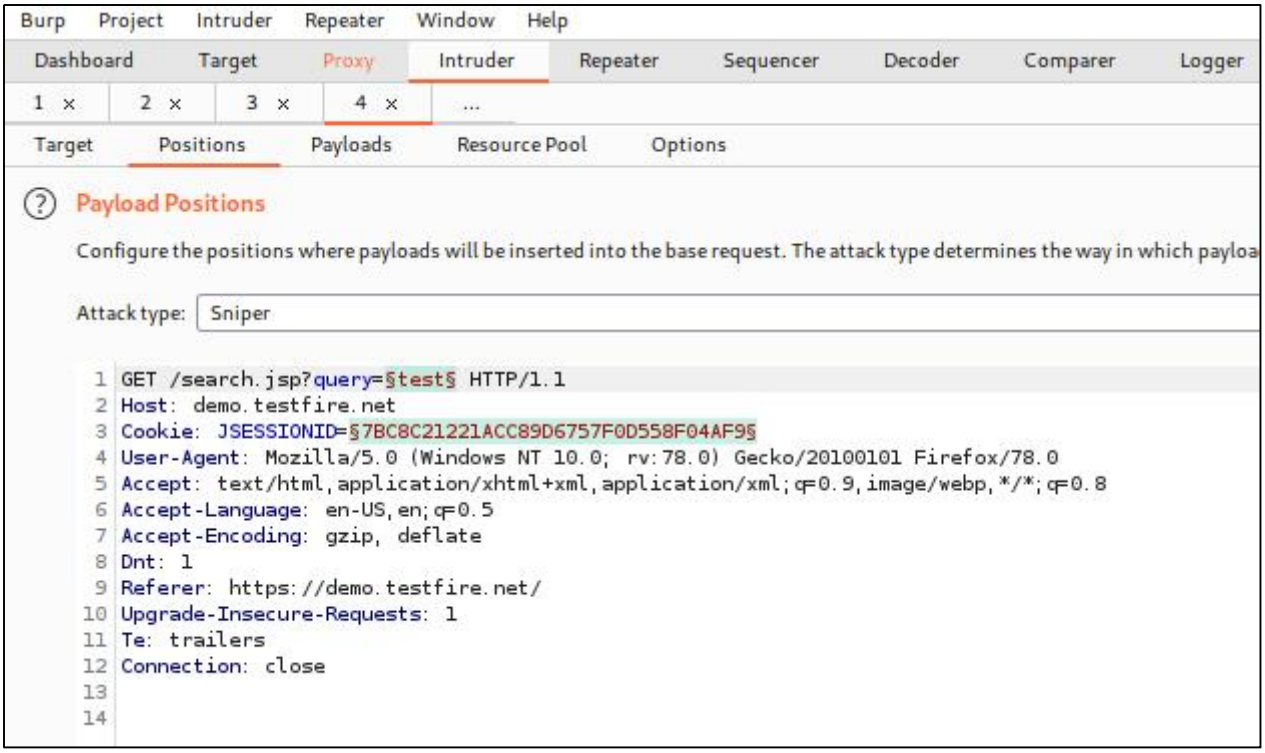
XSS bruteforcing on testfire.net

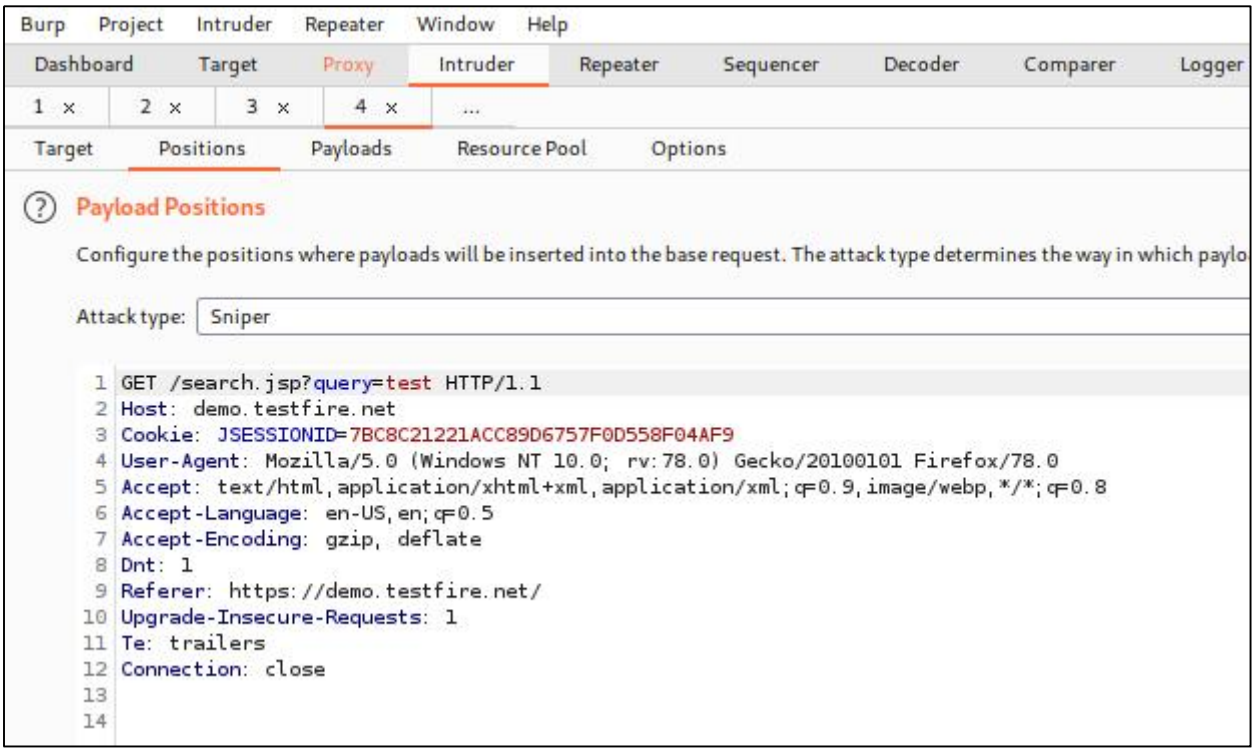
3. In testfire.net, enter dummy values in search bar and intercept request

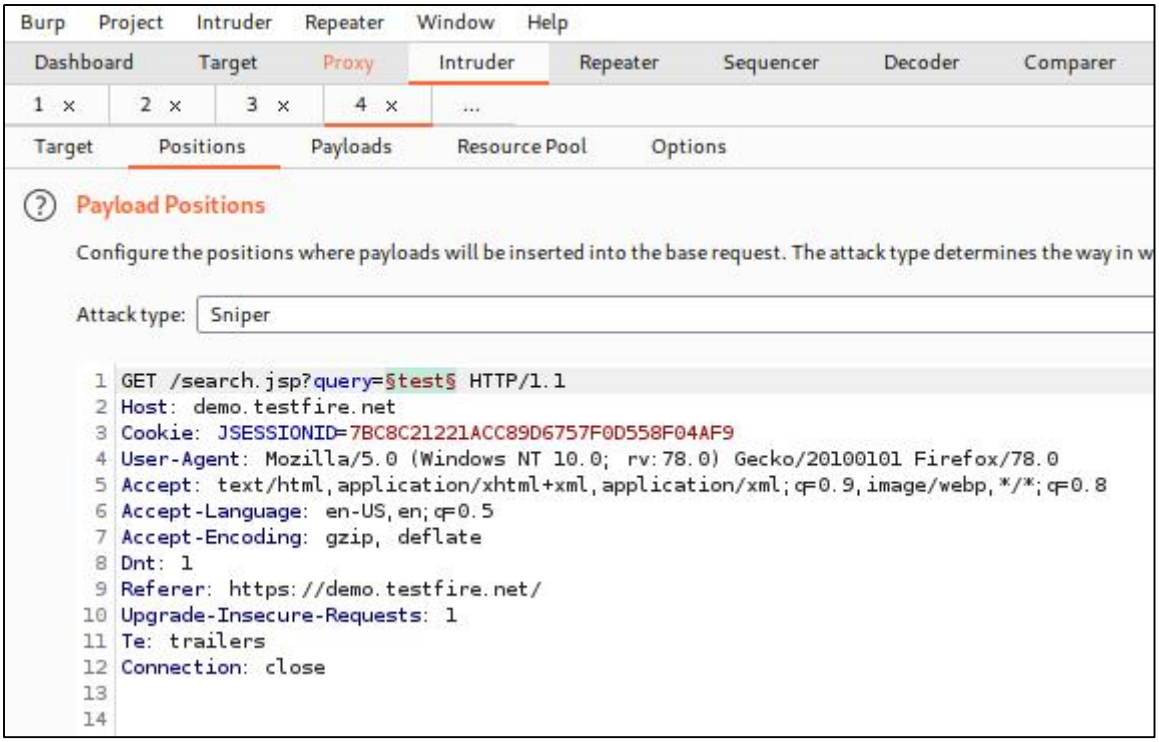




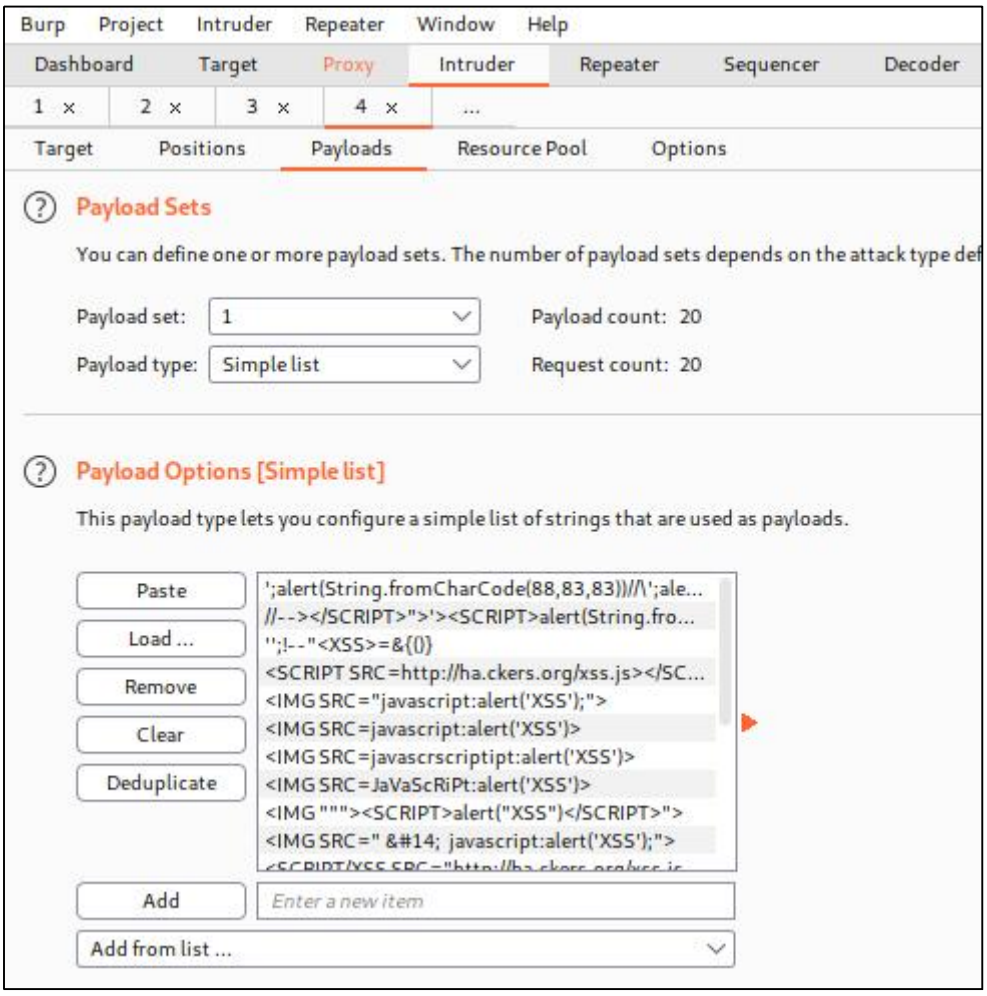
4. Send to intruder and set insertion point


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger
1 × 2 × 3 × 4 × ...
Target Positions Payloads Resource Pool Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloa
Attack type: Sniper
1 GET /search.jsp?query=§test§ HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=§7BC8C21221ACC89D6757F0D558F04AF9§
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Dnt: 1
9 Referer: https://demo.testfire.net/
10 Upgrade-Insecure-Requests: 1
11 Te: trailers
12 Connection: close
13
14

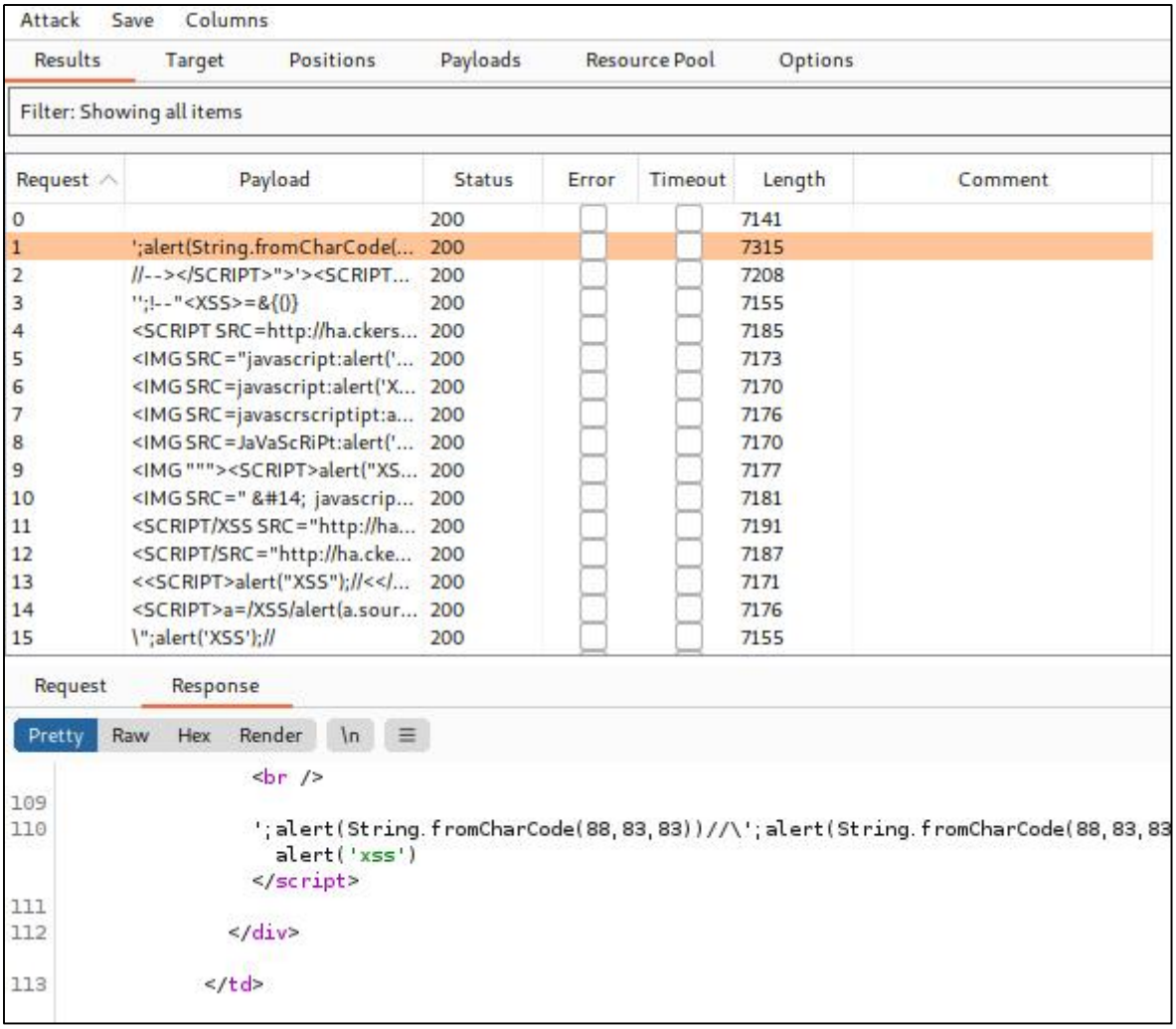

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger
1 × 2 × 3 × 4 × ...
Target Positions Payloads Resource Pool Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which paylo
Attack type: Sniper
1 GET /search.jsp?query=test HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=7BC8C21221ACC89D6757F0D558F04AF9
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Dnt: 1
9 Referer: https://demo.testfire.net/
10 Upgrade-Insecure-Requests: 1
11 Te: trailers
12 Connection: close
13
14



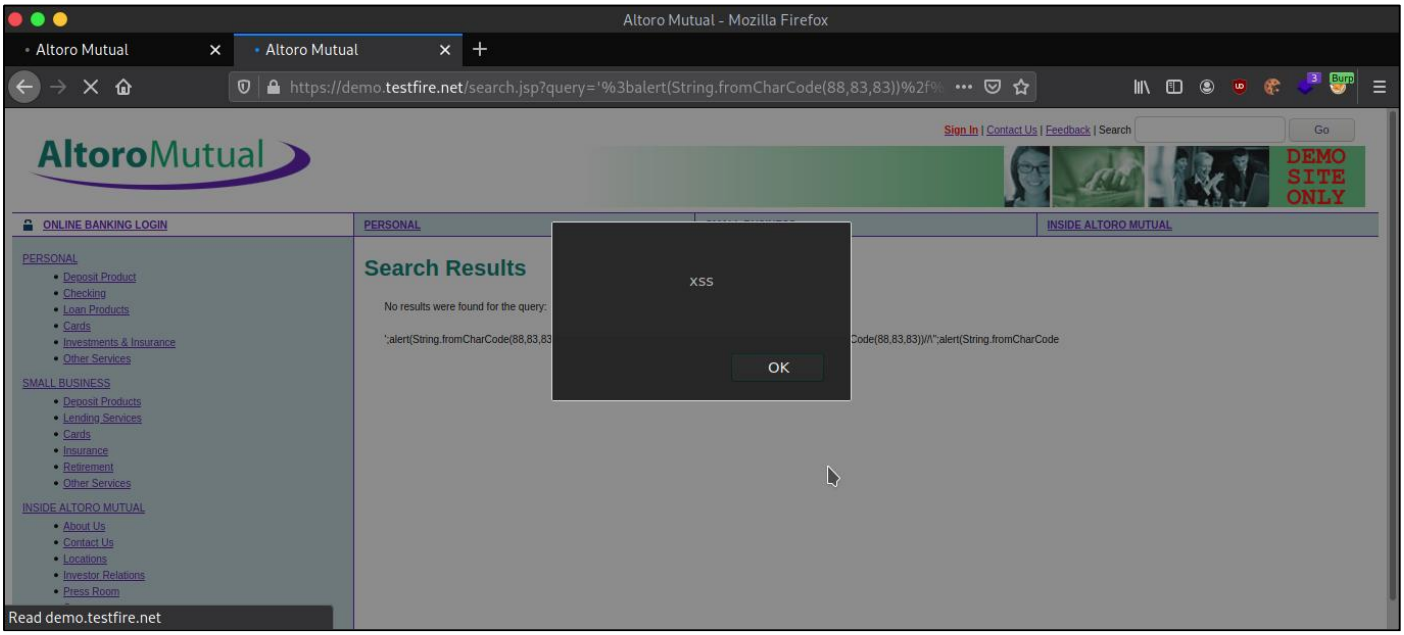
We have inbuilt payloads in Burpsuite



5. Start attack

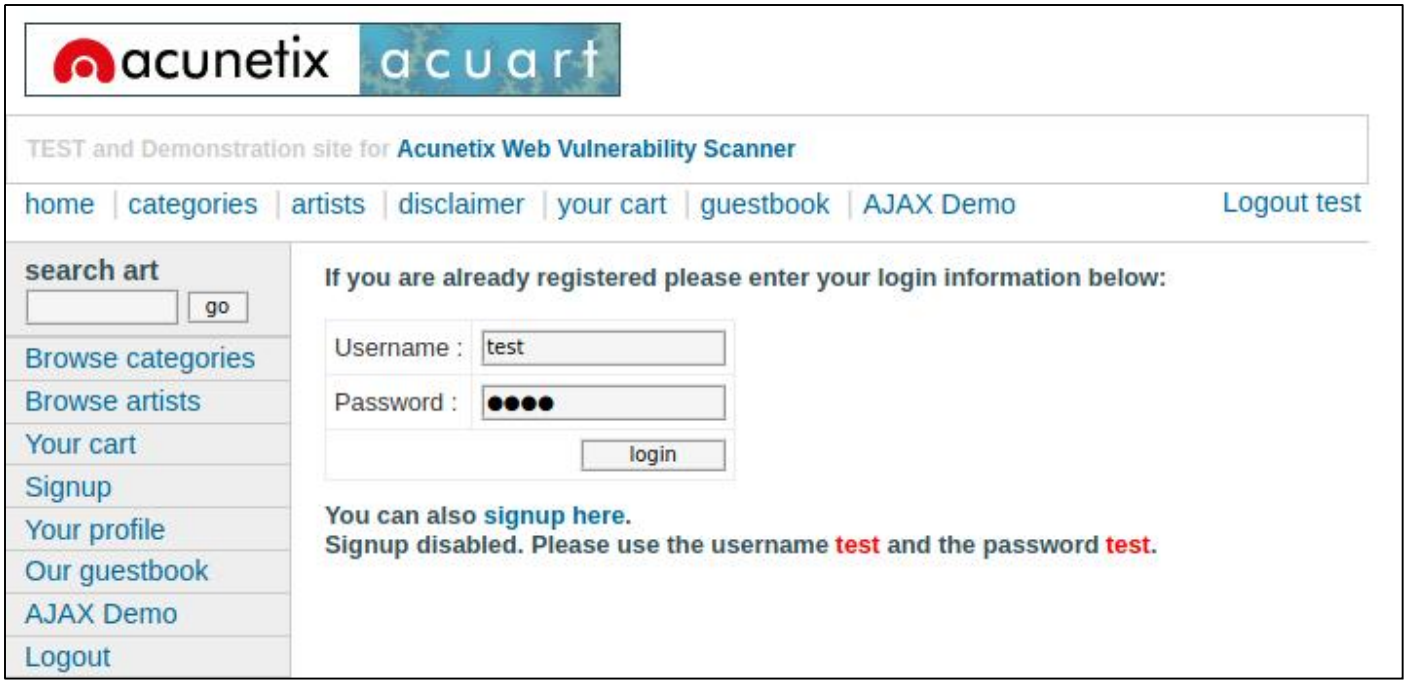


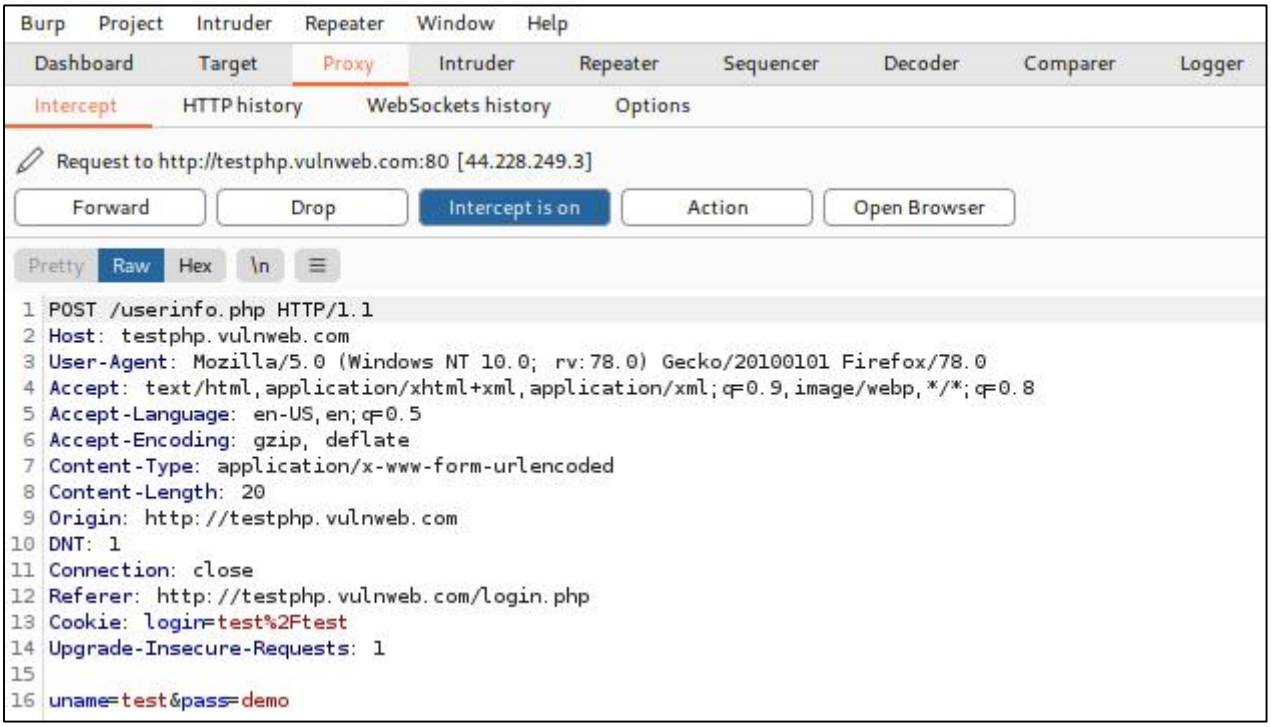
6. Let's see response in browser



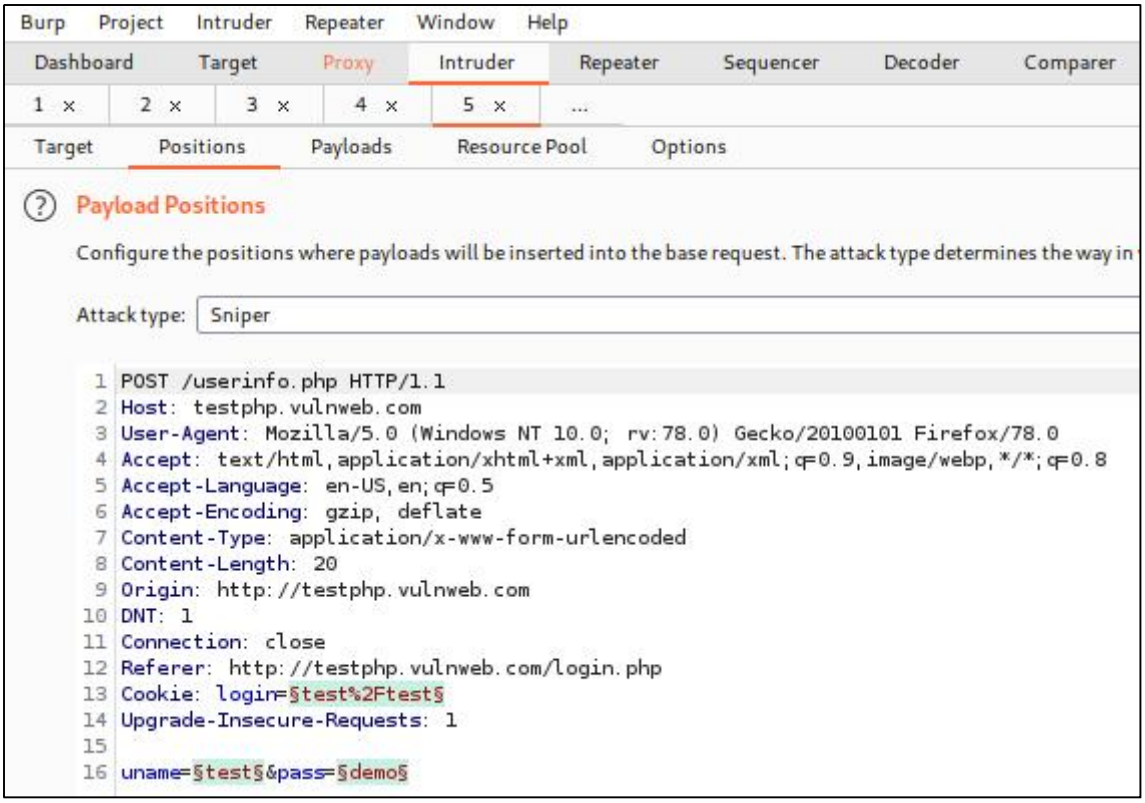
SQL fuzzing on testphp.vulnweb.com

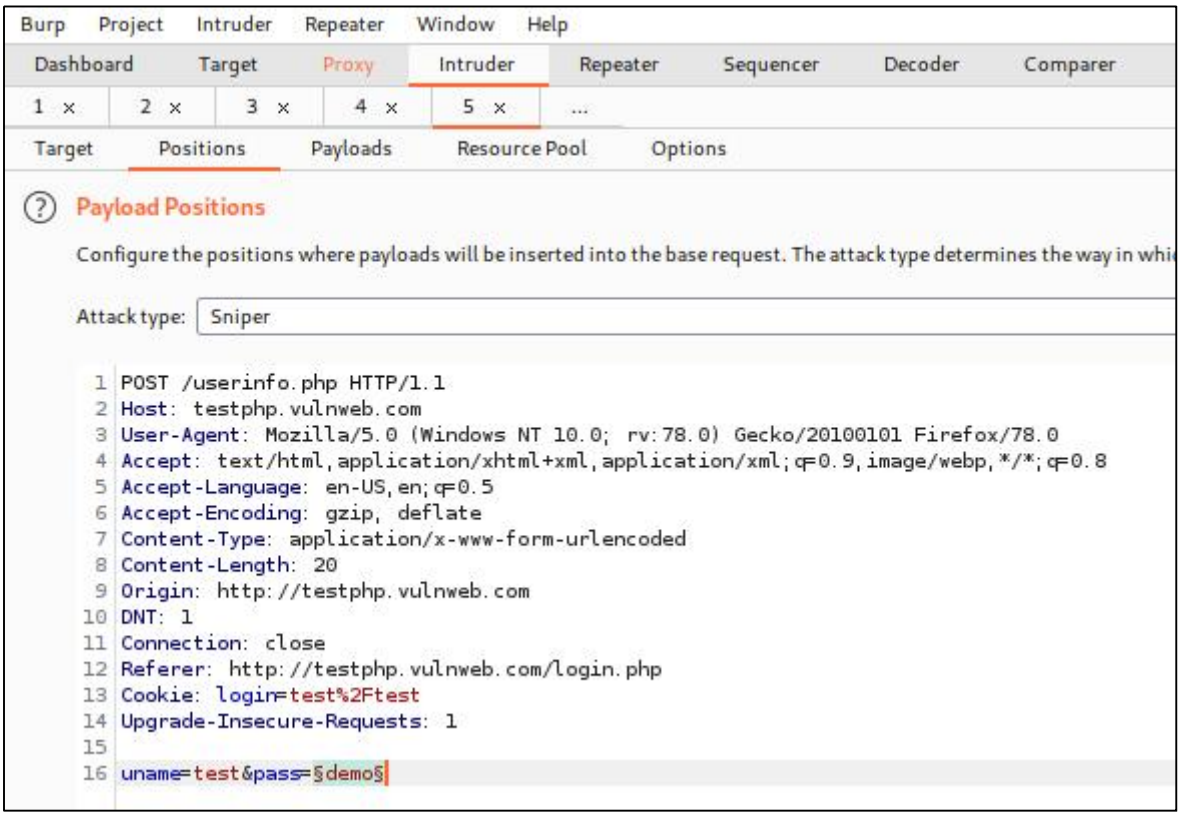
7. Sign-up on this website and intercept the request



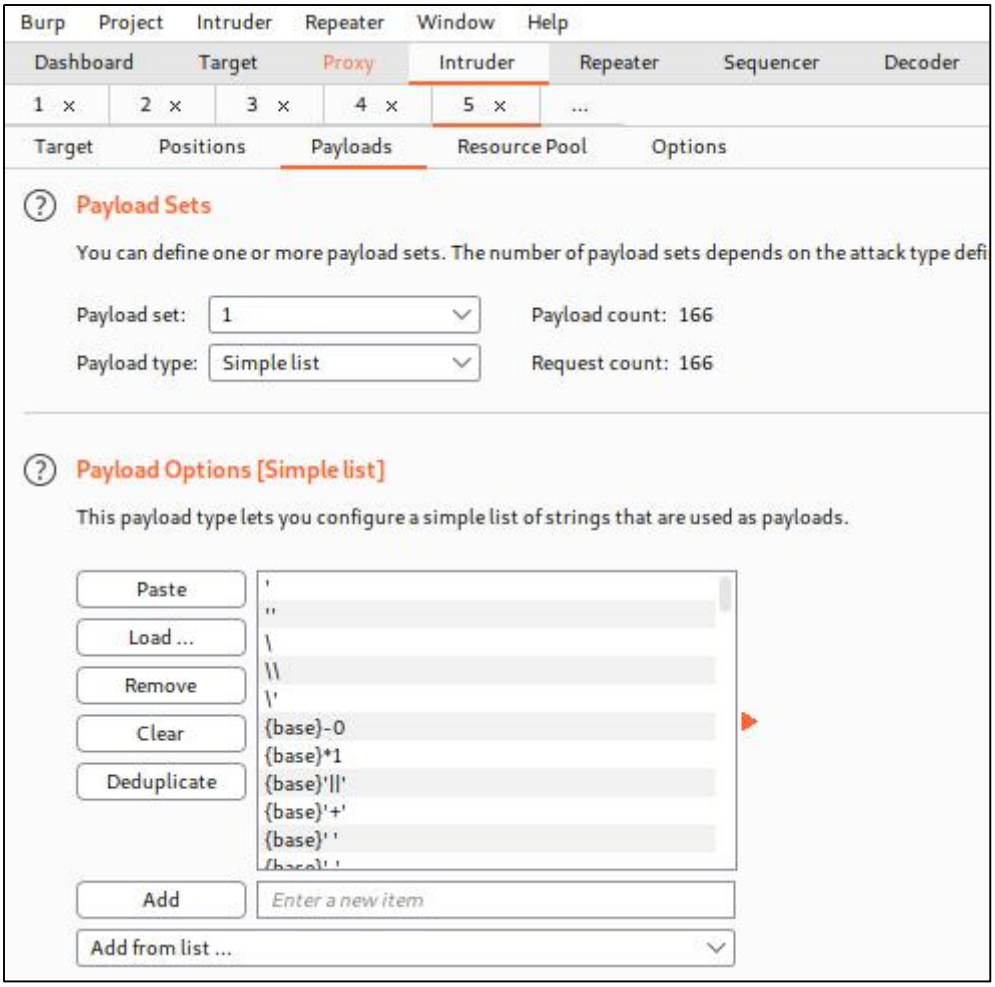


8. Send to intruder, select insertion point

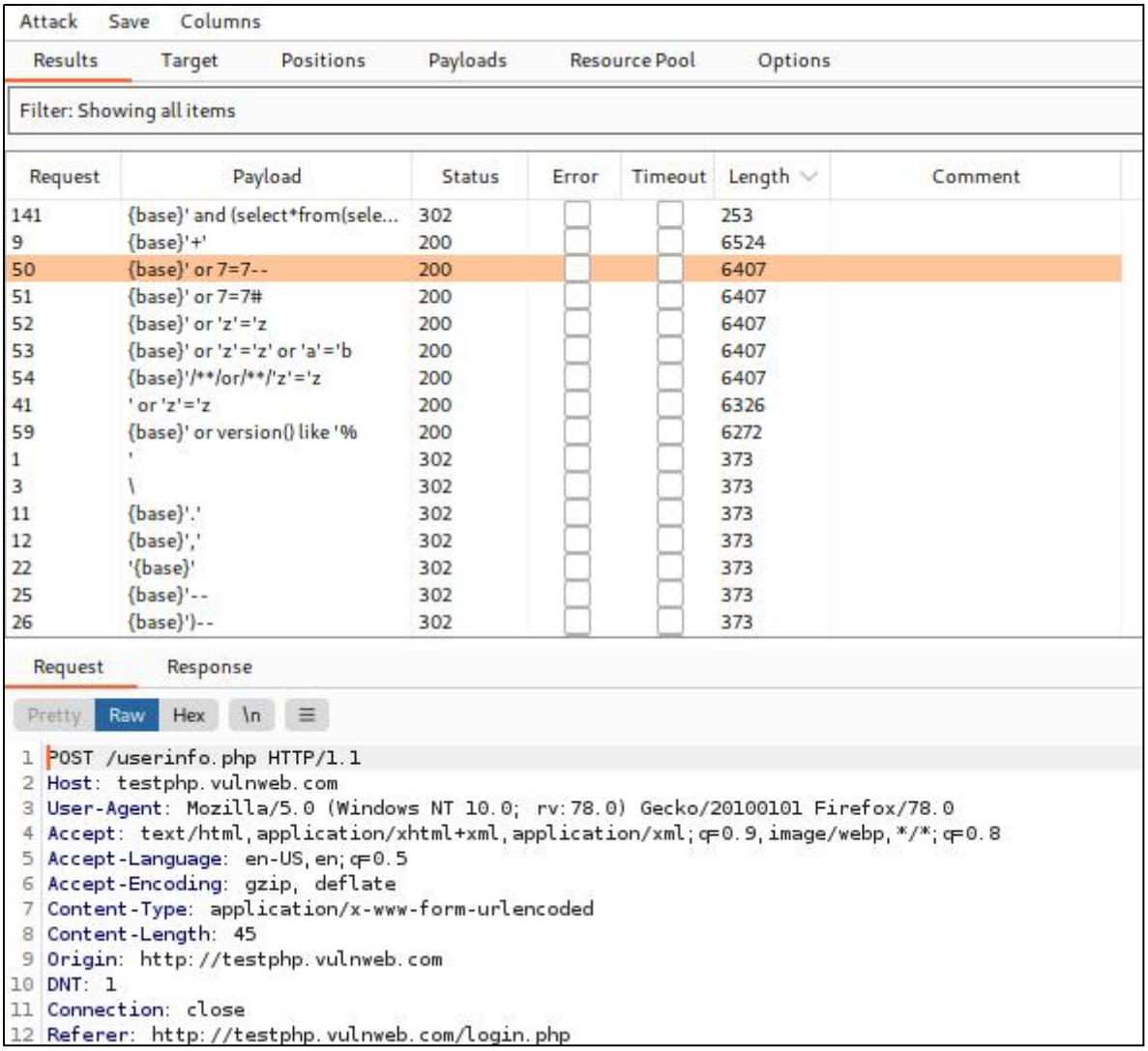




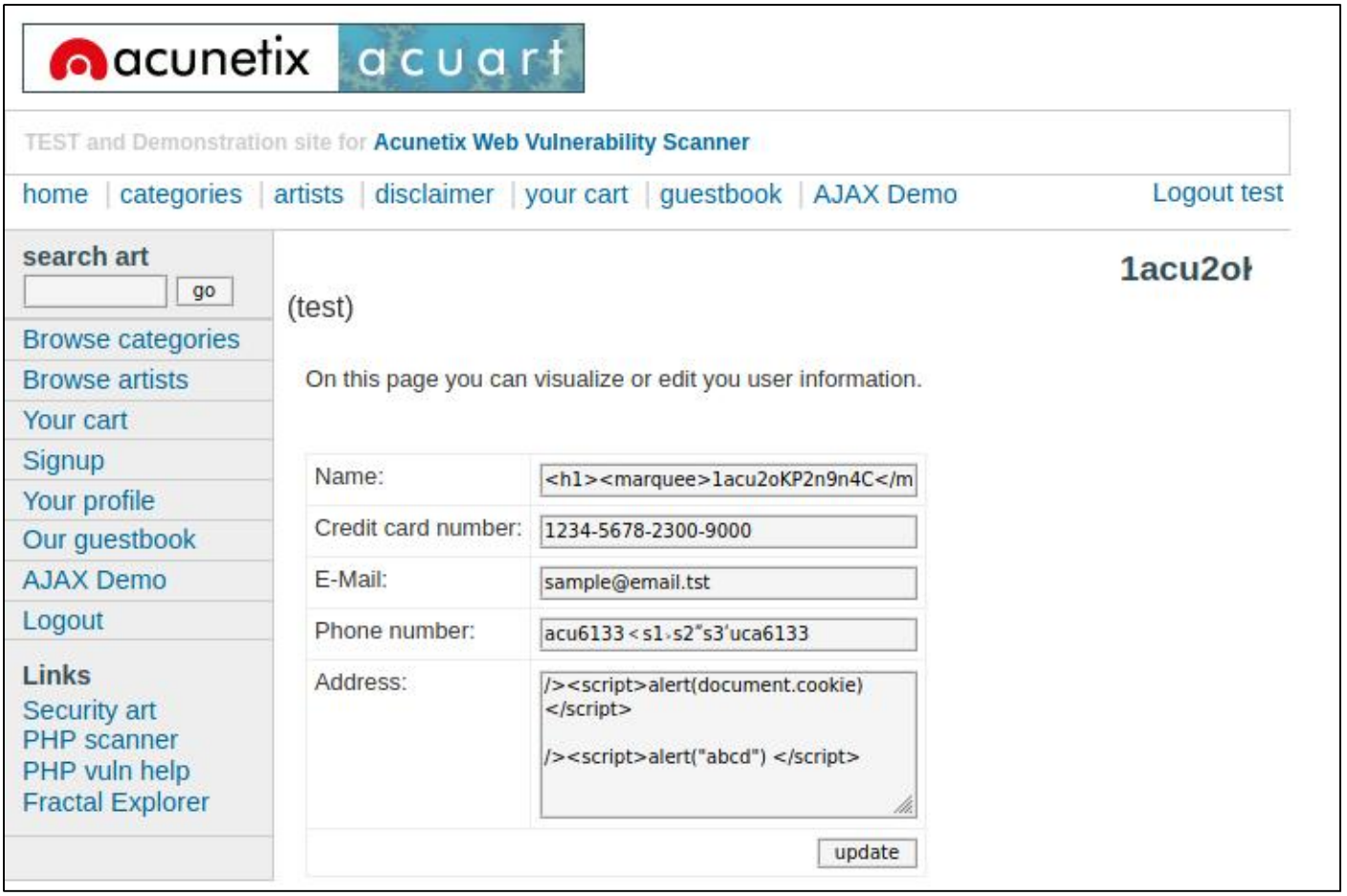
9. We use inbuilt SQL injection payload



10. Start attack



11. We can see sensitive data even if we haven't logged in.


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
1acu2oł
(test)
On this page you can visualize or edit you user information.
Name:
<h1><marquee>1acu2oKP2n9n4C</m
Credit card number:
1234-5678-2300-9000
E-Mail:
sample@email.tst
Phone number:
acu6133<s1›s2"s3'uca6133
Address:
/><script>alert(document.cookie)
</script>
/><script>alert("abcd") </script>
update