Cybersecurity Pre-work: Brute force attacks

1. The Mission

The owner of a blog has contracted your security firm to test their website for vulnerabilities.

Your mission is to hack into their blog. You suspect that you can find a user whose password is too simple. First, you need to find a registered user, and then you're going to attempt dozens of different common passwords.

This would be a tedious process, but luckily, you have Burp, and its trusty Intruder tool that's built for this very purpose.

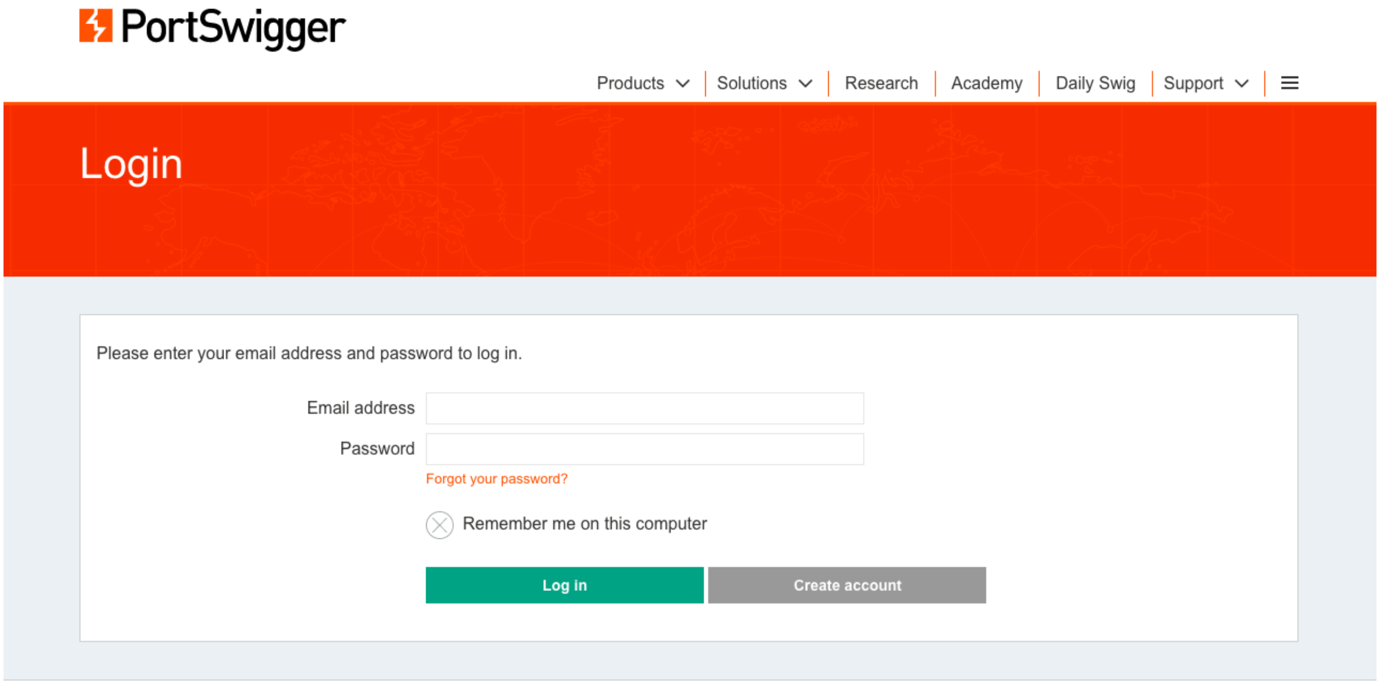
2. Setup

1. Install Burp - Burp is used by cybersecurity professionals everywhere to view network traffic and test for security vulnerabilities.
2. Create a Portswigger account - Portswigger is the maker of Burp and has an Academy to hone your cybersecurity skills.

> <img alt="link" title="link" src="/images/emoji/unicode/1f517.png"}" style="vertical-align:middle" width="20" height="20" /> Important Links:
>
> - Username Enumeration via Different responses
> - Candidate usernames
> - Candidate passwords

Step 1: Find the login url

1. Login to your Portswigger account



Login

Please enter your email address and password to log in.

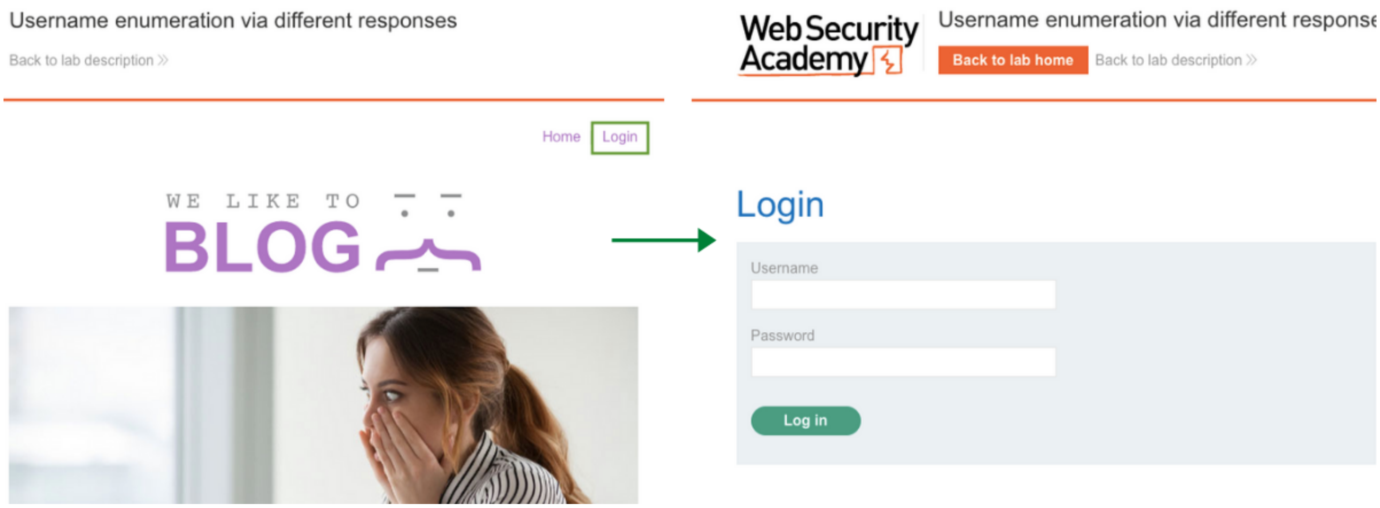
Email address

Password

Forgot your password?

○ Remember me on this computer

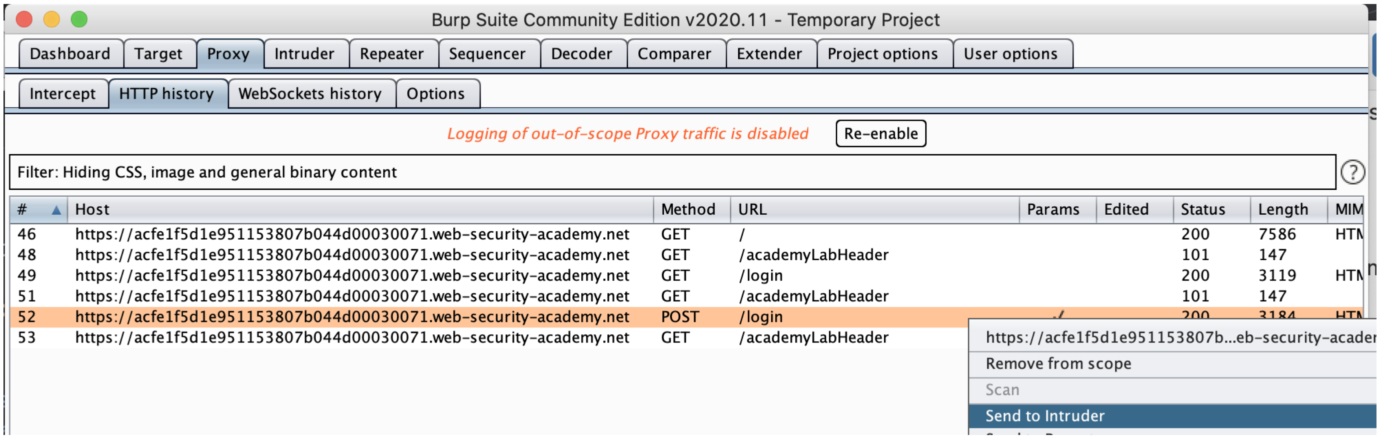
2. Fire up Burp, and attempt to login to the blog with a **RANDOM** username and password. The blog login looks like the image below. If you see the Portswigger login, you should login with your Portswigger account credentials first, then it will redirect you to the blog page.



Username enumeration via different responses
Back to lab description »
Home
Login
WE LIKE TO
BLOG
Web Security Academy
Username enumeration via different response
Back to lab home
Back to lab description »
Login
Username
Password
Log in

3. In Burp, go to **"Proxy"** -> **"HTTP history"**, and find the network request of the attempted login. You'll recognize it because it's a POST request to the login url of the blog.

4. Right-click the request and click "Send to Intruder"



Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding CSS, image and general binary content

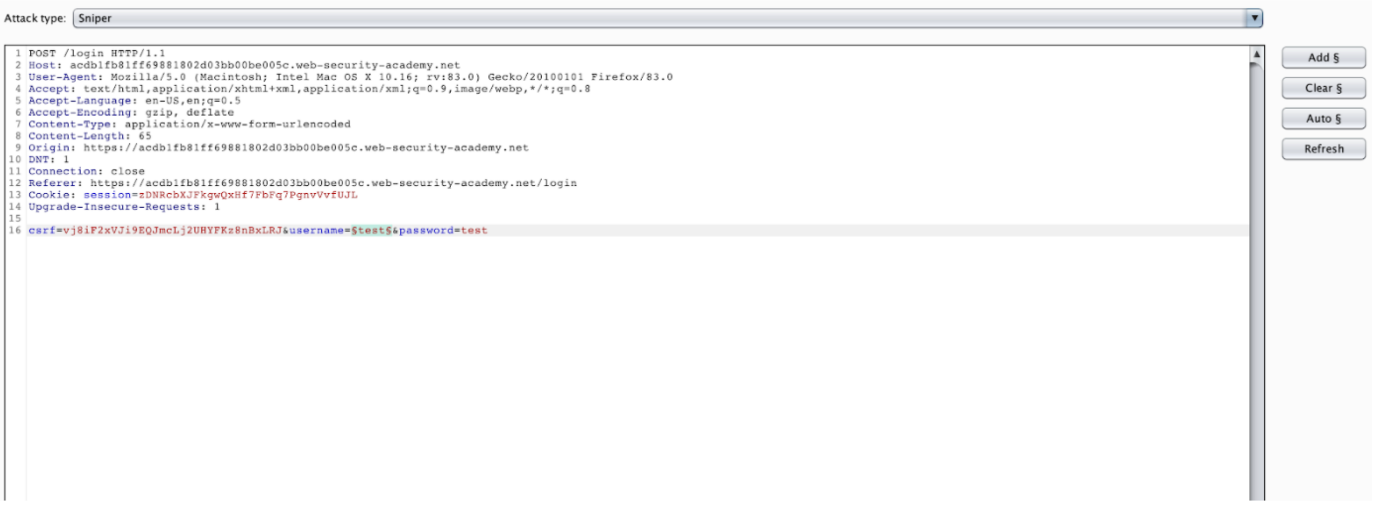
# ▲	Host	Method	URL	Params	Edited	Status	Length	MIM
46	https://acfe1f5d1e951153807b044d00030071.web-security-academy.net	GET	/			200	7586	HTN
48	https://acfe1f5d1e951153807b044d00030071.web-security-academy.net	GET	/academyLabHeader			101	147	
49	https://acfe1f5d1e951153807b044d00030071.web-security-academy.net	GET	/login			200	3119	HTN
51	https://acfe1f5d1e951153807b044d00030071.web-security-academy.net	GET	/academyLabHeader			101	147	
52	https://acfe1f5d1e951153807b044d00030071.web-security-academy.net	POST	/login	✓		200	3184	HTN
53	https://acfe1f5d1e951153807b044d00030071.web-security-academy.net	GET	/academyLabHeader					

Not seeing any requests? Check the intercept. **"Proxy"** -> **"Intercept"** and click the intercept button to say **"Intercept is off"**

Step 2: Find a registered user

Burp Intruder allows you to make the same request over and over again, except you can specify a part of the request to change. This makes it perfect for attempting to login as many different users with thousands of passwords, known as a brute force attack.

1. In Burp Intruder, go to the **"Positions"** tab. Make sure that the attack type **"Sniper"** is selected.
2. Click **"Clear"** to remove any automatically assigned payload positions. In the username parameter, highlight the value and click **"Add"** to add a payload position to this parameter. This position will be indicated by two § symbols, for example: **username=§random_username§**

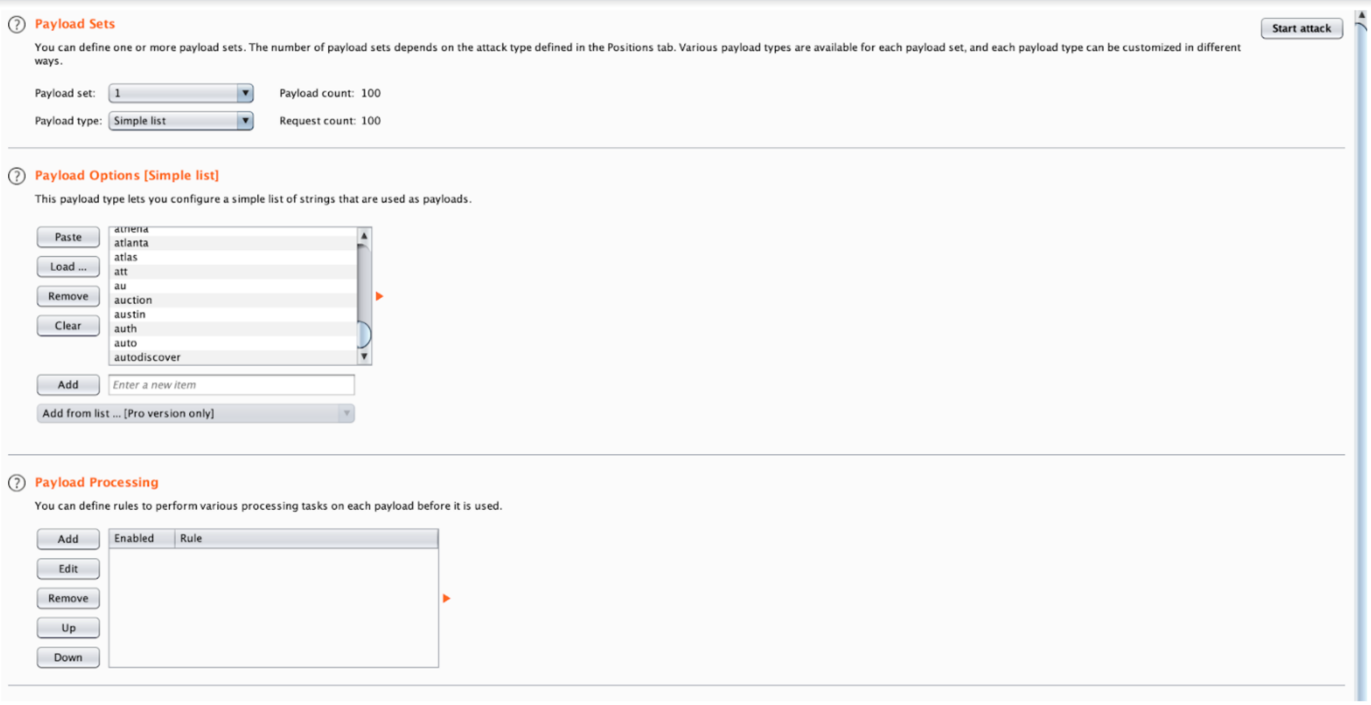


Attack type: Sniper

```
POST /login HTTP/1.1
Host: acdb1fb81ff69881802d03bb00be005c.web-security-academy.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:83.0) Gecko/20100101 Firefox/83.0
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: 65
Origin: https://acdb1fb81ff69881802d03bb00be005c.web-security-academy.net
DNT: 1
Connection: close
Referer: https://acdb1fb81ff69881802d03bb00be005c.web-security-academy.net/login
Cookie: session=zDNRcbXJFkgwQxHf7FbFq7PgnvVvfUJL
Upgrade-Insecure-Requests: 1

csrf=vj8iF2xVJi9EQJmcLj2UHYFKz8nBxLRJ&username=§test§&password=test
```

3. Do not change anything related to the password for now.
4. On the **"Payloads"** tab, select palyload set -> **"1"** and payload type -> **"Simple list".**
5. Under "Payload options", paste the list of candidate usernames and click "Start attack". The attack will start in a new window.



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 types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 100

Payload type: Simple list Request count: 100

Payload Options [Simple list]

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

athena
atlanta
atlas
att
au
auction
austin
auth
auto
autodiscover

Enter a new item

Add from list ... [Pro version only]

Payload Processing

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

Enabled	Rule

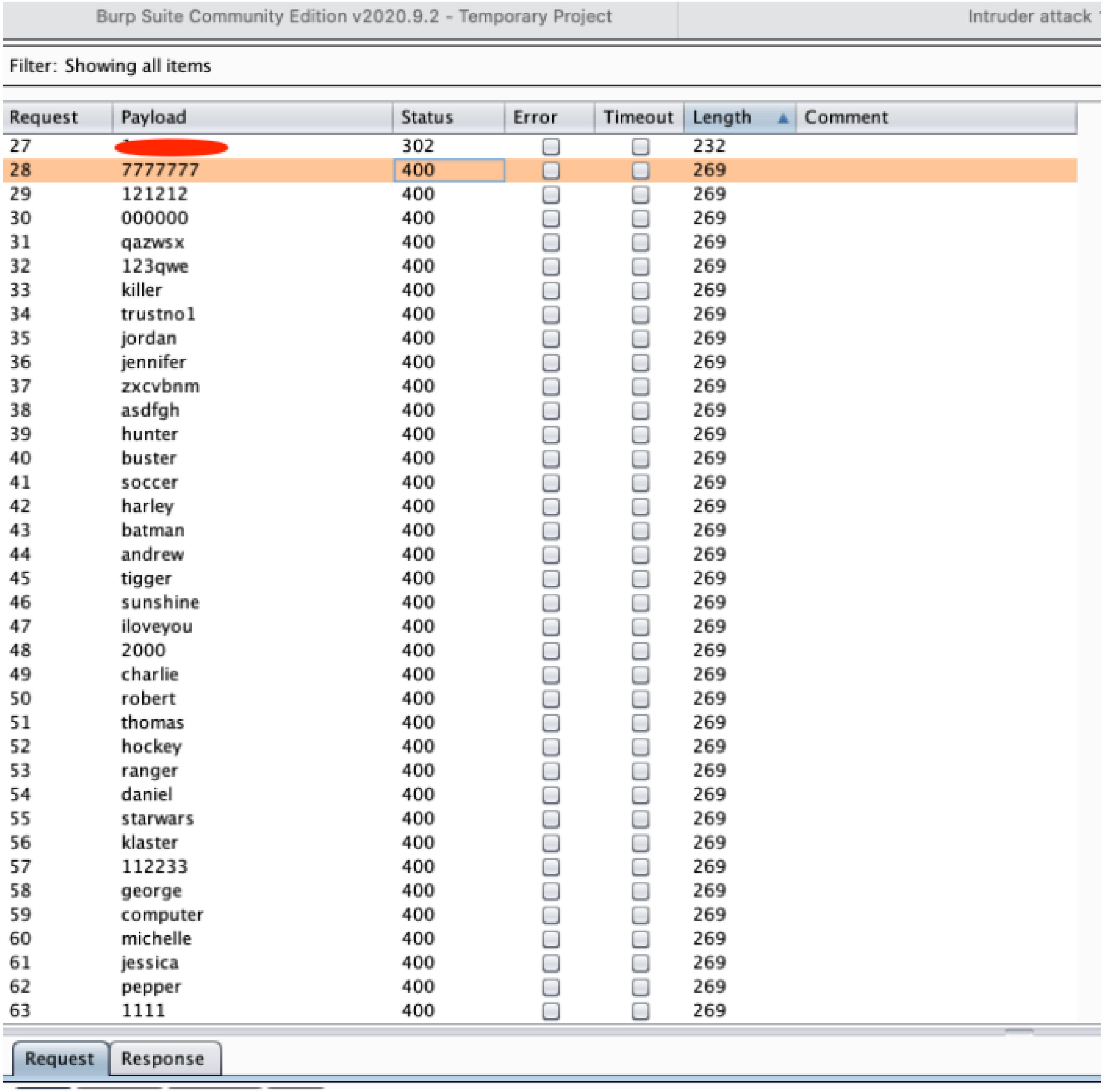
6. When the attack is finished, on the **"Results"** tab, examine the **"Length"** column. Click on the column header to sort the results. Notice that one of the entries is different to the other ones -- usually, 3186 is the one with a successful username.
7. Examine this response. Notice that other responses contain the message Invalid username, but this response says Incorrect password. Take note of this username. **The successful username will vary for each login and will only works until the session is valid.**

If you've completed the steps above, you've identified the username of a registered user of the blog, although you don't know their password...yet.

Step 3: Find the password

Now that you have a registered user, you want to attempt to login as that user with dozens of simple passwords.

1. Close the attack and go back to the **"Positions"** tab. Click **"Clear"** again and change the username parameter to the username you just identified. Add a payload position to the password parameter.Now you should see something like this **username=identifiedUser&password=§invalid-password§**
2. On the "Payloads" tab, clear the list of usernames and replace it with the list of candidate passwords. Then click "Start attack".
3. When the attack is finished, look at the "Status" column. Notice that each request returned a 400 status code, until eventually one returns 302. This suggests that the login attempt was successful. Take note of the password.


Burp Suite Community Edition v2020.9.2 - Temporary Project
Intruder attack
Filter: Showing all items
Request
Response

Request	Payload	Status	Error	Timeout	Length ▲	Comment
27	[redacted]	302	□	□	232	
28	7777777	400	□	□	269	
29	121212	400	□	□	269	
30	000000	400	□	□	269	
31	qazwsx	400	□	□	269	
32	123qwe	400	□	□	269	
33	killer	400	□	□	269	
34	trustno1	400	□	□	269	
35	jordan	400	□	□	269	
36	jennifer	400	□	□	269	
37	zxcvbnm	400	□	□	269	
38	asdfgh	400	□	□	269	
39	hunter	400	□	□	269	
40	buster	400	□	□	269	
41	soccer	400	□	□	269	
42	harley	400	□	□	269	
43	batman	400	□	□	269	
44	andrew	400	□	□	269	
45	tigger	400	□	□	269	
46	sunshine	400	□	□	269	
47	iloveyou	400	□	□	269	
48	2000	400	□	□	269	
49	charlie	400	□	□	269	
50	robert	400	□	□	269	
51	thomas	400	□	□	269	
52	hockey	400	□	□	269	
53	ranger	400	□	□	269	
54	daniel	400	□	□	269	
55	starwars	400	□	□	269	
56	klaster	400	□	□	269	
57	112233	400	□	□	269	
58	george	400	□	□	269	
59	computer	400	□	□	269	
60	michelle	400	□	□	269	
61	jessica	400	□	□	269	
62	pepper	400	□	□	269	
63	1111	400	□	□	269	

4. Back in your browser, click the "Login" link in the upper-right corner to open a fresh login page and using the username and password that you identified. You must click "My account" to solve the lab.

Congratulations, young apprentice, you've hacked your first site! The blog owner is grateful to you for reporting a vulnerable user.

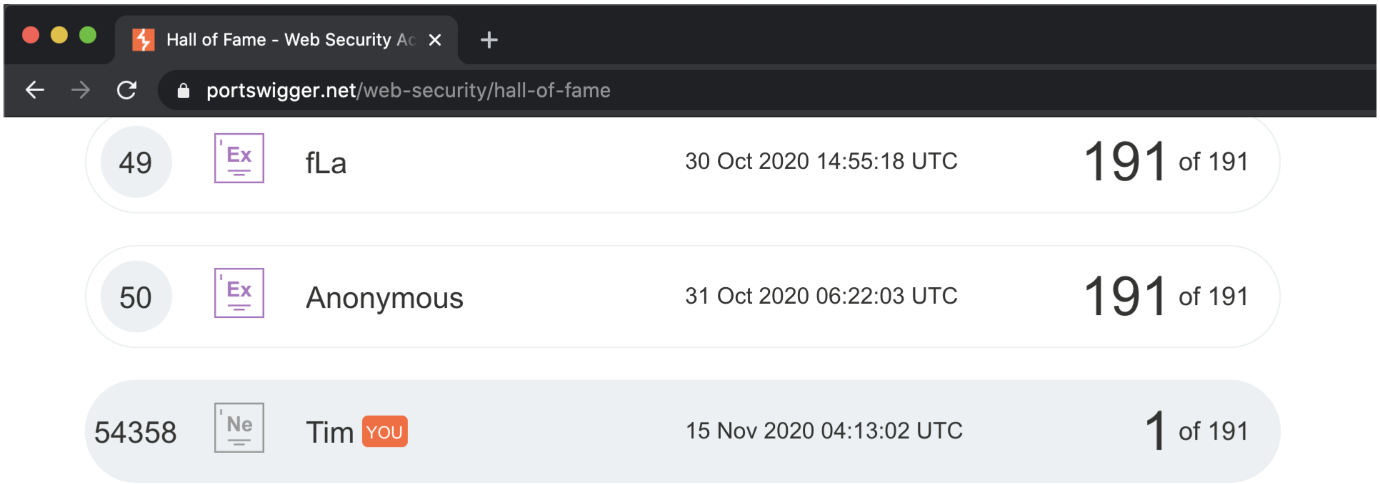
Getting an error?

- Make sure you are only sending one request to the site. Sending multiple request will result in different sessions casuing a timeout error.
- In general the sesssion will expire ever 15 minutes. You may need to redo the challenge if you exceed the time.

- CSRF error? The CSRF token in the request is no longer valid as it was already used to succesfully login. Use a fresh login page to avoid an error.

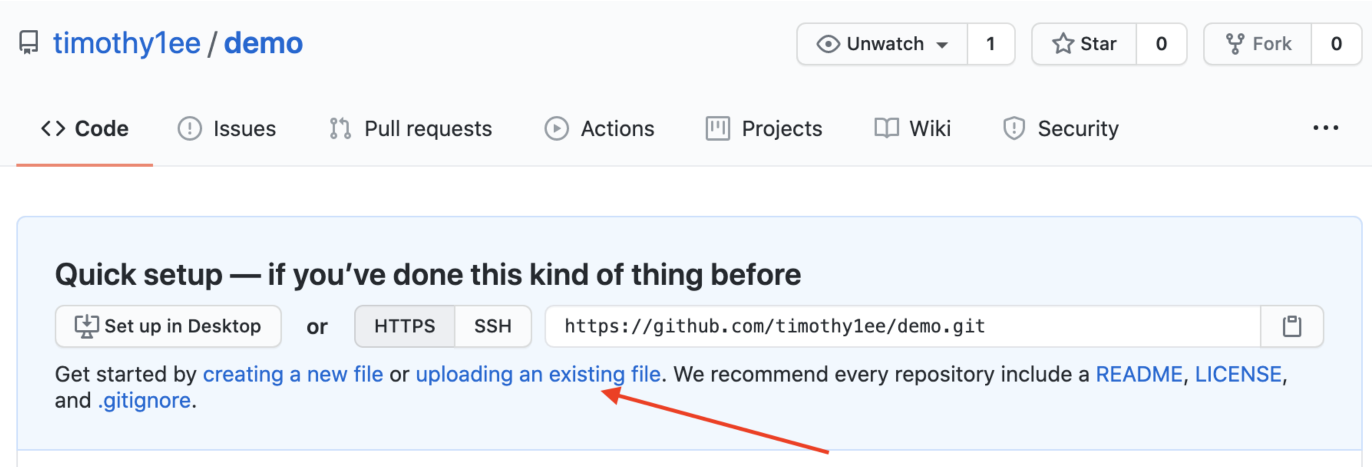
3. Submission

1. Go to the Hall of Fame, scroll to the bottom, and take a screenshot of your entry. The bottom of the screenshot must include your username and indicate the completion of the lab with **"1 of ###".**


Hall of Fame - Web Security Ac
portswigger.net/web-security/hall-of-fame

49	Ex	fLa	30 Oct 2020 14:55:18 UTC	191 of 191
50	Ex	Anonymous	31 Oct 2020 06:22:03 UTC	191 of 191
54358	Ne	Tim YOU	15 Nov 2020 04:13:02 UTC	1 of 191

2. Go to GitHub and create a new repository to store your work for the class.
3. Add your screenshot to your repository by clicking **"upload an existing file".**

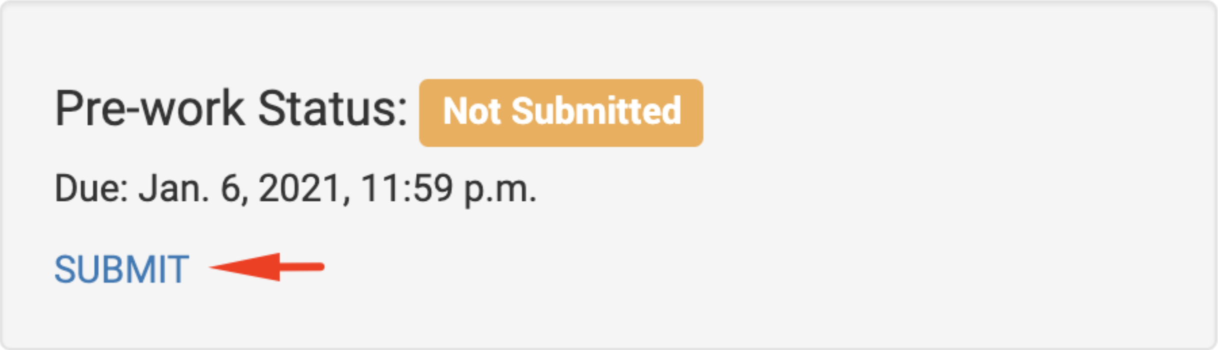


Quick setup — if you've done this kind of thing before

```
https://github.com/timothy1ee/demo.git
```

Get started by creating a new file or uploading an existing file. We recommend every repository include a README, LICENSE, and .gitignore.

4. Go to the CodePath application status dashboard and then press the "SUBMIT" button in the pre-work section:



Pre-work Status: Not Submitted

Due: Jan. 6, 2021, 11:59 p.m.

SUBMIT

5. In the pre-work submission form, link to your GitHub repo.

Still have questions about pre-work?

- If you encounter technical difficulties while submitting your work, please join our Pre-work Support Workspace **here**.
  - This workspace is intended to support applicants with pre-work completion difficulties.
  - Make sure to join and create an account with us to get assistance from our awesome team of tech experts and other students who may have encountered the same technical issues as yours!

Quick Jump