

<b><u>1.2 Web Programming</u></b>	<b>4</b>
<b>5. Run sequential program</b>	4
<b>7. Run multiprocessing program</b>	5
<b>9. Run matplotlib program on repl.it</b>	6
<b>12. Run asyncio program on repl.it</b>	7
<b>1.3 Broken Authentication</b>	9
<b>2. Login form</b>	9
<b>3. authentication/password-based (1)</b>	10
<b>4. authentication/password-based (2)</b>	10
<b>5. authentication/password-based (3)</b>	10
<b>6. oauth</b>	11
<b>7. -</b>	12
<b>8. -</b>	12
<b>10. -</b>	13

<b><u>1.5 Broken Access Control</u></b>	<b>13</b>
<b>1. file-path-traversal (1)</b>	13
<b>simple</b>	13
<b>absolute-path-bypass</b>	14
<b>sequences-stripped-non-recursively</b>	14
<b>2. file-path-traversal (2)</b>	15
<b>superfluous-url-decode</b>	15
<b>validate-start-of-path</b>	15
<b>validate-file-extension-null-byte-bypass</b>	15
<b>3. access-control (1)</b>	16
<b>unprotected-admin-functionality</b>	16
<b>unprotected-admin-functionality-with-unpredictable-url</b>	16

<b>4. access-control (2)</b>	17
<b>User-role-controlled-by-request-parameter</b>	17
<b>5. access-control (3)</b>	17
<b>user-role-can-be-modified-in-user-profile</b>	17
<b>6. access-control (4)</b>	18
<b>url-based-access-control-can-be-circumvented</b>	18
<b>method-based-access-control-can-be-circumvented</b>	18
<b>7. access-control (5)</b>	19
<b>user-id-controlled-by-request-parameter</b>	19
<b>user-id-controlled-by-request-parameter-with-unpredictable-user-ids</b>	19
<b>8. access-control (6)</b>	19
<b>user-id-controlled-by-request-parameter-with-data-leakage-in-redirect</b>	19
<b>user-id-controlled-by-request-parameter-with-password-disclosure</b>	20
<b>insecure-direct-object-references</b>	20
<b>9. access-control (7)</b>	21
<b>multi-step-process-with-no-access-control-on-one-step</b>	21
<b>Referer-based-access-control</b>	21
<b>10. Information-disclosure</b>	21
<b>lab-infoleak-in-error-messages</b>	21
<b>lab-infoleak-on-debug-page</b>	22
<b>lab-infoleak-via-backup-files</b>	22
<b>11. WFP1: File upload</b>	23
<b>Example #1</b>	23
<b>Example #2</b>	23
<b>12. file-upload (1)</b>	23
<b>13. file-upload (2)</b>	24
 <b><u>1.6: SSRF</u></b>	
	25

2. ssrf (2)	25
3. ssrf (3)	25
4. ssrf (4)	26
5. ssrf/blind	26

<b><u>1.7: XXE</u></b>	27
1. xxe (1)	27
2. xxe (2)	27
3. xxe (3)	27
4. xxe (4)	27
5. -	28

## 1.2 Web Programming

### 5. Run sequential program

- Take a screenshot of the output of your program's execution that includes your OdinId for your lab notebook.

The screenshot shows the Visual Studio Code interface. The top bar displays 'hw1.py — madler (Workspace)'. Below the bar, there are tabs for 'pyvenv.cfg' and 'hw1.py'. The main editor area contains the following Python code:

```
42     titles = []
43     for titles: list
44     || titles.append(getUrlTitle(u))
45     return(titles)
46
47 urls = ['https://pdx.edu', 'https://oregonctf.org']
48
49 print(getSequential(urls))
50 elapsedSequential = getSequential(urls)
51 print(f'{elapsedSequential:.2f} secs')
```

Below the editor, the terminal tab is selected, showing the following output:

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
(base) Matthews-MacBook-Air:w21websec-matt-adler matthewadler$ source /Users/matthewadler/Desktop/w21websec-matt-adler/.venv/bin/activate
(.venv) (base) Matthews-MacBook-Air:w21websec-matt-adler matthewadler$ /Users/matthewadler/Desktop/w21websec-matt-adler/.venv/bin/python3 /Users/matthewadler/Desktop/w21websec-matt-adler/hw1.py
Function returned: ['<title>Portland State University – PSU | Portland OR</title>', '<title>Oregon CTF</title>']
1.4596384329999998
Function returned: ['<title>Portland State University – PSU | Portland OR</title>', '<title>Oregon CTF</title>']
1.42 secs
```

## 7. Run multiprocessing program

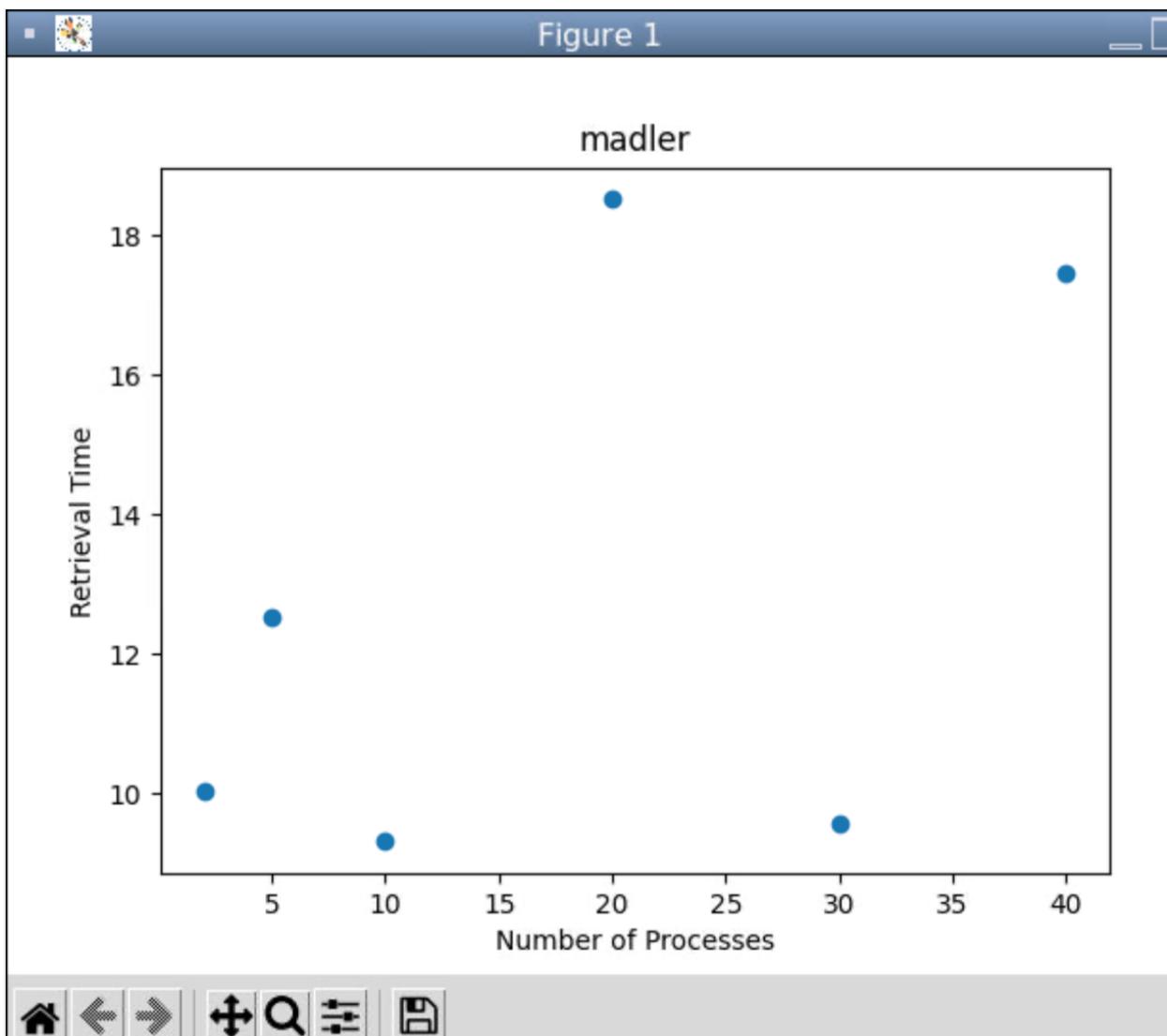
- Take a screenshot of the output of your program's execution that includes your OdinId for your lab notebook.

The screenshot shows a code editor interface with a dark theme. On the left, there's a sidebar with icons for pyenv.cfg and hw1.py. The main area displays the content of hw1.py. The code defines a function getSequential(urls) that prints the titles of URLs. It includes a docstring and type annotations. The code editor has tabs for PROBLEMS, OUTPUT, DEBUG CONSOLE, and TERMINAL. The TERMINAL tab is active, showing the output of running the script. The output shows three runs of the function, each taking approximately 2 seconds and returning a list of titles. The last run shows the command being run from a .venv environment.

```
w21websec-matt-adler > hw1.py > ...
30     print(f'Function returned: {return_vals}')
31     return(elapsed)
32     return(inner)
33
34
35 @time_decorator
36 def getSequential(urls):
37     """
38         Given a list of URLs, retrieve the title for each one using a single synchronous pro
39         :param urls: List of URLs to retrieve
40         :type urls: list of str
41         :return: list of titles for each URL
42         :rtype: list of str
43     """
44     titles = []
45     for u in urls:
46         titles.append(u.title())
47
48     return(titles)
49
50
51 if __name__ == '__main__':
52     urls = [
53         "https://www.google.com",
54         "https://www.facebook.com",
55         "https://www.portlandstate.edu"
56     ]
57
58     elapsed = timeit.timeit(lambda: getSequential(urls), number=1)
59
60     print(f'{elapsed} secs')
61
62     print(f'Function returned: {getSequential(urls)}')
63
64     print(f'{len(urls)} 1.00')
65
66     print(f'{len(urls)} 1.11')
67
68     print(f'{len(urls)} 1.40')
69
70     print(f'{len(urls)} 2.48')
71
72     print(f'{len(urls)} 5.11')
73
74     print(f'{len(urls)} 5.11')
75
76     print(f'{len(urls)} 10 1.10')
77
78     print(f'(.venv) (base) Matthews-MacBook-Air:w21websec-matt-adler matthewadler$
```

## 9. Run matplotlib program on repl.it

Figure 1



12. Run asyncio program on repl.it

madler (Workspace)

⟳ ⌂ + ☰

⟳ AnxiousForsakenFolder - Replit

👤+ Invite 🔎

Console Shell

```
tle>', '<title>Sign in - Google Accounts</title>', '<title>Google &gt; X /title>', '<title>Google</title>', '<title>Privacy & Terms - Google</title>', '<title>Google News</title>', '<title>Gmail</title>', '<title>Google</title>', '<title>Google</title>', '<title>Google</title>', '<title>Google</title>', '<title>Google Developers</title>', '<title>Google M arketing Platform - Unified Advertising and Analytics</title>', '<title>Google</title>', '<title>Google</title>', '<title>Google Books</title>', '<title>Google</title>', '<title>Google</title>', '<title>Google Translate</title>', '<title>Google</title>', '<title>\n      Google Account\n    </title>', '<title>Google Chrome - Download the Fast, Secure Browser from Google</title>', '<title>Sign in - Google Accounts</title>', '<title>Google</title>', '<title>Google Photos</title>', '<title>Google</title>', '<title>Google</title>', '<title>Google</title>', '<title>Moving on from Picasa</title>', '<title>Google</title>']  
Async version: 11.73  
▶
```

## 1.3 Broken Authentication

### 2. Login form

The screenshot shows a network request and response for a login form. The request headers include Accept-Language, Host, User-Agent, Referer, Accept-Encoding, and Connection. The response is an HTTP 200 OK with Content-Encoding, Content-Type, Connection, and Content-Length. The request data shows MIME Type, username, and password.

Request Headers:

- Accept-Language: en-US,en;q=0.9
- Host: ac9b1f6b1e273f31c0d819eb008b0084.web-security-academy.net
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/605.1.15 (KHTML Gecko) Version/15.1 Safari/605.1.15
- Referer: https://ac9b1f6b1e273f31c0d819eb008b0084.web-security-academy.net/login
- Accept-Encoding: gzip, deflate, br
- Connection: keep-alive

Response Headers:

- HTTP/1.1 200 OK
- Content-Encoding: gzip
- Content-Type: text/html; charset=utf-8
- Connection: close
- Content-Length: 946

Request Data:

- MIME Type: application/x-www-form-urlencoded
- username: madler@pdx.edu
- password: CeFAC\$}7~afT3d\*bcKPgEc/7f69Jq4)2

### 3. authentication/password-based (1)

The screenshot shows a web browser window with the following details:

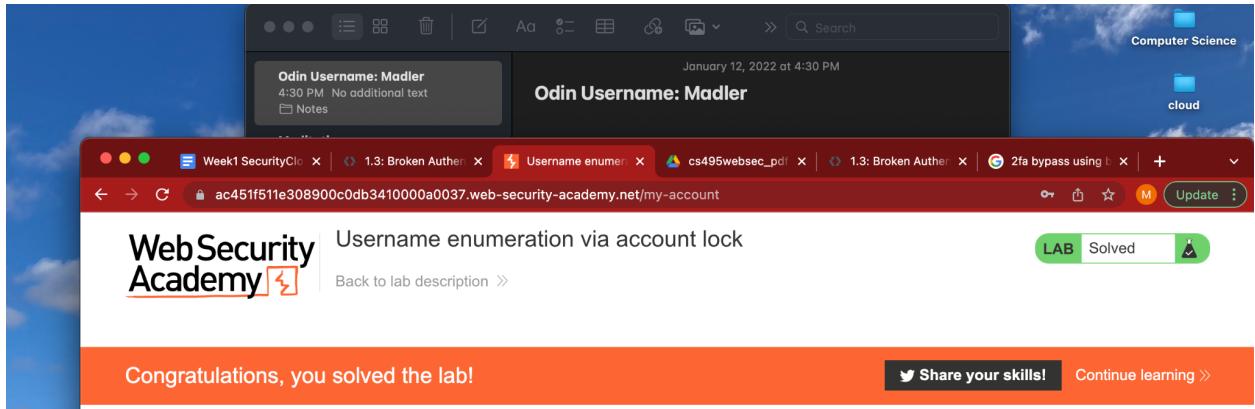
- Title Bar:** Shows the URL `ac8f1f0c1fc1cf1c003433200930047.web-security-academy.net`.
- Content Area:** Displays the title "Username enumeration via different responses".
- Right Side:** A green button labeled "LAB Solved" with a checkmark icon.
- Bottom Buttons:** Two identical orange buttons with the text "Congratulations, you solved the lab!" and "Share your skills! Continue learning >".

### 4. authentication/password-based (2)

The screenshot shows a web browser window with the following details:

- Title Bar:** Shows the URL `ac151fb31e9d3a63c04419f1007b0008.web-security-academy.net`.
- Content Area:** Displays the title "Broken brute-force protection, IP block".
- Right Side:** A green button labeled "LAB Solved" with a checkmark icon.
- Bottom Buttons:** Two identical orange buttons with the text "Congratulations, you solved the lab!" and "Share your skills! Continue learning >".
- Bottom Navigation:** Links to "Home" and "My account".

### 5. authentication/password-based (3)



## 6. oauth

- What is the DNS name of the identity provider? **oauthWebSecurity.net**

**client\_id: a72barbz7xqq8oo3e8n8k**

- 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 authorization is performed?

**redirect\_uri: https://ac801f4c1e42579ac0ea036b00db0099.web-security-academy.net/oauth-callback**

- What scopes are being requested by the client application for the user to authorize?

**scope: openid profile email**

- What kind of response\_type is being requested from the identity provider?

**response\_type: token**

View the response headers of the request.

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

**Location: /interaction/uVMtXRk1h\_U595IgcxPZi**

7. -

- What is URL is the form data sent to when the user logs in as specified in the `action` attribute of the form?  
`<form autocomplete="off" action="/interaction/ExDgvG3Q-H_MbvV6y3ycV/login">`
- What is the URL the form is sent to?

`<form autocomplete="off" action="/interaction/td0rC8iAwFbmSqYB4XMPw/confirm" method="post">`

- What is the access token the user will relay to the client application via its OAuth callback URL? **Begins with 'access\_token='**

**Location: https://ac691ff91fa86f68c0cc6e36007e0037.web-security-academy.net/oauth-callback#access\_token=kqr0sBw-BwMjMk04qiBrLMwx4kpvsGT7lsuM-G1hMp5&expires\_in=3600&token\_type=Bearer&scope=openid%20profile%20email**

8. -

- What is the e-mail address associated with the `wiener` account?

**email: "wiener@hotdog.com"**

## 10. -

- What is the function of the first two `const` lines? To get an access token

```
const urlSearchParams = new URLSearchParams(window.location.hash.substr(1));
const token = urlSearchParams.get('access_token');
```

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

```
fetch('https://oauth-acd41faf1e45d32bc0f63dbe02fb0021.web-security-academy.net/me', {
    method: 'GET',
    headers: {
        'Authorization': 'Bearer ' + token,
        'Content-Type': 'application/json'
    }
}
```

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

```
, {
    email: j.email,
    username: j.sub,
    token: token
})
```

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

```
.then(r => document.location = '/')
```

## 1.5 Broken Access Control

### 1. file-path-traversal (1)

[simple](#)

A screenshot of a Mac OS X desktop environment. The Dock at the bottom shows several open applications, including '1.5: Broken Access Control', 'Week1 SecurityCloud', 'File path traversal', 'pernod - Google', 'The Handmaid', 'Web Security /', 'My Drive - Goog', and others. The main window is a web browser displaying a page from 'Web Security Academy'. The title bar says 'MADLER' and the date is 'January 16, 2022 at 7:49 PM'. The page content includes the heading 'File path traversal, simple case', a 'Back to lab description' link, and a message 'Congratulations, you solved the lab!'. A green button in the top right corner says 'LAB Solved' with a trophy icon. Below the message are two buttons: 'Share your skills!' with a Twitter icon and 'Continue learning >'.

## absolute-path-bypass

A screenshot of a Mac OS X desktop environment. The Dock at the bottom shows several open applications, including 'cs495websec\_pdf - Google', '1.5: Broken Access Control', 'Lab: File path traversal, traversal', 'File path traversal, traversal', 'Week1 SecurityCloud - Google', and others. The main window is a web browser displaying a page from 'Web Security Academy'. The title bar says 'MADLER' and the date is 'January 17, 2022 at 4:03 PM'. The page content includes the heading 'File path traversal, traversal sequences blocked with absolute path bypass', a 'Back to lab description' link, and two messages: 'Congratulations, you solved the lab!' and 'Congratulations, you solved the lab!'. A green button in the top right corner says 'LAB Solved' with a trophy icon. Below the messages are two buttons: 'Share your skills!' with a Twitter icon and 'Continue learning >'.

## sequences-stripped-non-recursively

A screenshot of a Mac OS X desktop environment. The Dock at the bottom shows several open applications, including 'cs495websec\_pdf - Google', '1.5: Broken Access Control', 'Lab: File path traversal, traversal', 'File path traversal, traversal', 'Week1 SecurityCloud - Google', and others. The main window is a web browser displaying a page from 'Web Security Academy'. The title bar says 'MADLER' and the date is 'January 17, 2022 at 4:03 PM'. The page content includes the heading 'File path traversal, traversal sequences stripped non-recursively', a 'Back to lab description' link, and a message 'Congratulations, you solved the lab!'. A green button in the top right corner says 'LAB Solved' with a trophy icon. Below the message are two buttons: 'Share your skills!' with a Twitter icon and 'Continue learning >'.

## 2. file-path-traversal (2)

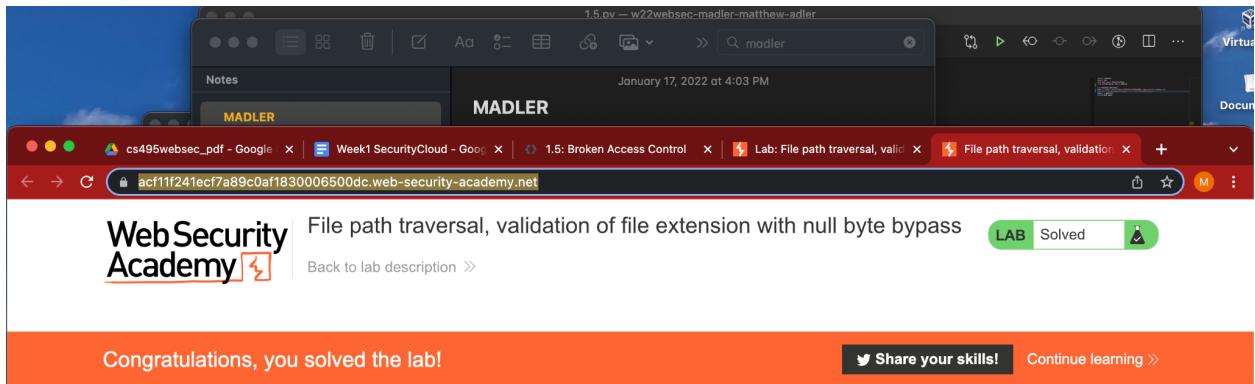
### superfluous-url-decode

The screenshot shows a browser window with a tab for 'Lab: File path traversal, traversal sequences stripped with superfluous URL-decode'. The status bar indicates 'LAB Solved'. The page content includes two 'Congratulations, you solved the lab!' messages and social sharing buttons for Twitter and LinkedIn.

### validate-start-of-path

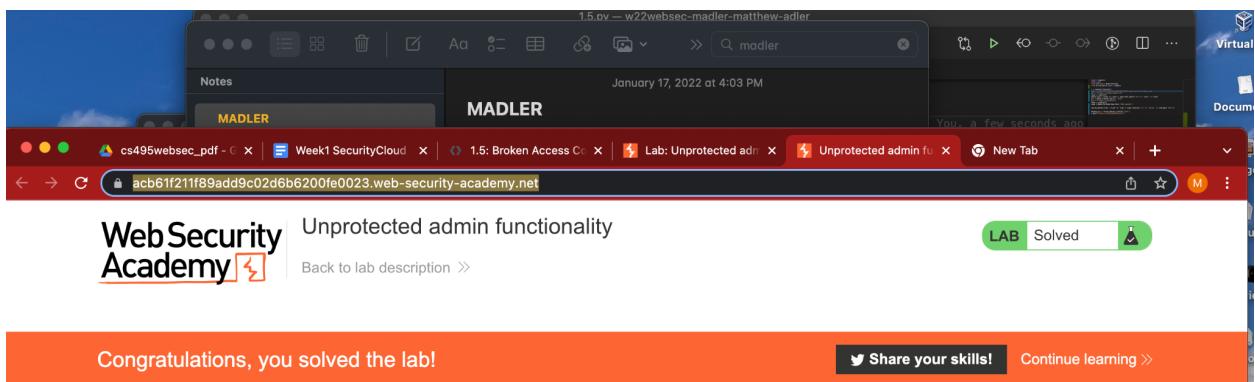
The screenshot shows a browser window with a tab for 'Lab: File path traversal, validation of start of path'. The status bar indicates 'PRACTITIONER LAB Solved'. The page content includes a 'Track your progress' sidebar showing learning materials at 0% and vulnerability labs at 4%. The main content area describes a file path traversal vulnerability in product image display and provides instructions to solve the lab by retrieving the contents of the /etc/passwd file.

### validate-file-extension-null-byte-bypass



### 3. access-control (1)

#### unprotected-admin-functionality



#### unprotected-admin-functionality-with-unpredictable-url

Top Hits

MADLER

Unprotected admin functionality

https://ace31f6a1f9681c0c091093e003300d9.web-security-academy.net/admin-5s8oxo

Web Security Academy

Unprotected admin functionality with unpredictable URL

Back to lab description >

Congratulations, you solved the lab!

User deleted successfully!

Share your skills! Continue learning >

Home | My account

1.3: Do unprotected-admin-functionality-with-unpredictable-url

```
match_line = [line for line in script.split('\n') if 'admin-' in line]
uri = match_line[0].split("'''")[3]

carlos_delete_link = [link for link in soup.find_all('a') if 'carlos' in link.get('href')]
delete_uri = carlos_delete_link[0]['href']
```

#### 4. access-control (2)

##### [User-role-controlled-by-request-parameter](#)

MADLER

1.3: Do unprotected-admin-functionality-with-unpredictable-url

User role controlled by request parameter

Back to lab description >

Congratulations, you solved the lab!

Share your skills! Continue learning >

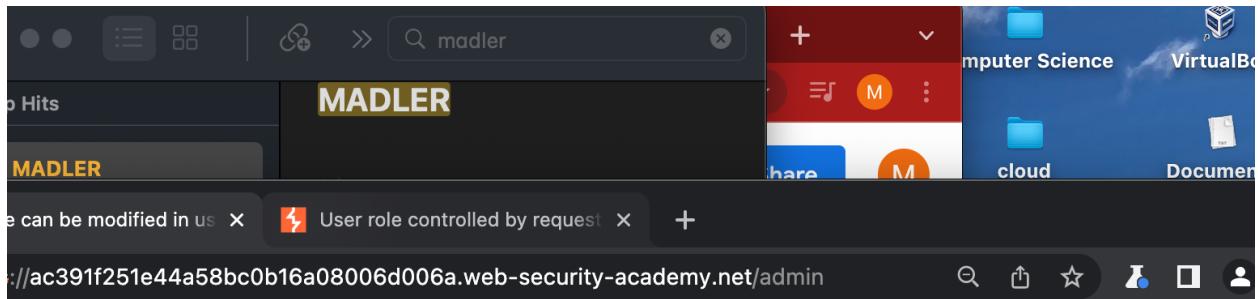
Share your skills! Continue learning >

```
match_line = [line for line in script.split('\n') if 'admin-' in line]
uri = match_line[0].split("'''")[3]

carlos_delete_link = [link for link in soup.find_all('a') if 'carlos' in link.get('href')]
delete_uri = carlos_delete_link[0]['href']
```

#### 5. access-control (3)

##### [user-role-can-be-modified-in-user-profile](#)



Congratulations, you solved the lab!

Share your skills! Continue learning >

User deleted successfully!

Home | Admin panel | My account

## 6. access-control (4)

### [url-based-access-control-can-be-circumvented](#)

2022 Winter Web | cs495websec\_pd | Week1 SecurityChallenger | 1.5: Broken Access Control | URL-based access control | URL based access | +

ac951fde1eeeb0a4c03f603c0014004f.web-security-academy.net

Web Security Academy

URL-based access control can be circumvented

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | Admin panel | My account

Top Hits

MADLER

Wednesday 13: Do u... [Notes](#)

1.3: Do [unprotected-admin-functionality-with-unpredictable-url](#)

### [method-based-access-control-can-be-circumvented](#)

## 7. access-control (5)

### user-id-controlled-by-request-parameter

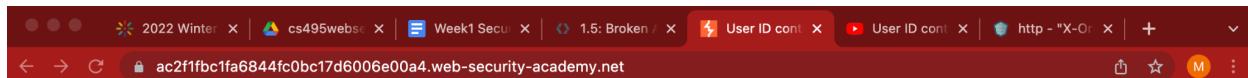
The screenshot shows a browser window for the 'User ID controlled by request parameter' lab on the Web Security Academy. The URL in the address bar is `accf1f1c1eb66c1c075f36600dc0068.web-security-academy.net/my-account?id=carlos`. The page title is 'User ID controlled by request parameter'. A green 'LAB Solved' button is visible. The main content area displays a message: 'Congratulations, you solved the lab!' with options to 'Share your skills!' and 'Continue learning >'. Below this, a screenshot of a terminal window shows the command `madler` being run, resulting in the output 'MADLER'. The terminal also shows a note: '1.3: Do unprotected-admin-functionality-with-unpredictable-url'. At the bottom of the page, there are links for 'Home', 'My account', and 'Log out'.

### user-id-controlled-by-request-parameter-with-unpredictable-user-ids

The screenshot shows a browser window for the 'User ID controlled by request parameter, with unpredictable user IDs' lab on the Web Security Academy. The URL in the address bar is `ace51fd61f37c1f8c0885e16000e0046.web-security-academy.net`. The page title is 'User ID controlled by request parameter, with unpredictable user IDs'. A green 'LAB Solved' button is visible. The main content area displays a message: 'Congratulations, you solved the lab!' with options to 'Share your skills!' and 'Continue learning >'. Below this, a screenshot of a terminal window shows the command `madler` being run, resulting in the output 'MADLER'. The terminal also shows a note: '4:46 PM 1.3: Do unpr...'. At the bottom of the page, there are links for 'Home', 'My account', and a developer tools panel showing CSS styles for the body element.

## 8. access-control (6)

### user-id-controlled-by-request-parameter-with-data-leakage-in-redirect



User ID controlled by request parameter with data leakage in redirect

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account

Top Hits

January 21, 2022 at 4:46 PM

MADLER

Yesterday 1.3: Do un... Notes

## [user-id-controlled-by-request-parameter-with-password-disclosure](#)

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete

## [insecure-direct-object-references](#)

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Live chat

Top Hits

January 21, 2022 at 4:46 PM

MADLER

Yesterday 1.3: Do un... Notes

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Live chat

Top Hits

January 21, 2022 at 4:46 PM

MADLER

Yesterday 1.3: Do un... Notes

## 9. access-control (7)

### [multi-step-process-with-no-access-control-on-one-step](#)

The screenshot shows a browser window for a lab titled "Multi-step process with no access control on one step". The URL in the address bar is `ac8a1f6a1f715a84c0224ac700aa00d4.web-security-academy.net`. The page content includes the title, a "Back to lab description" link, and a "Solved" badge. A prominent orange banner at the top says "Congratulations, you solved the lab!". Below the banner is a screenshot of a Mac OS X desktop showing a search result for "madler" in Spotlight. The result shows a file named "MADLER" from January 22, 2022, at 1:01 PM. The page also features social sharing buttons for Twitter and LinkedIn, and links for "Home" and "My account".

### [Referer-based-access-control](#)

The screenshot shows a browser window for a lab titled "Referer-based access control". The URL in the address bar is `acb81fc31fabfa8cc0186ad500e80010.web-security-academy.net/my-account`. The page content includes the title, a "Back to lab description" link, and a "Solved" badge. A prominent orange banner at the top says "Congratulations, you solved the lab!". Below the banner is a screenshot of a Mac OS X desktop showing a search result for "madler" in Spotlight. The result shows a file named "MADLER" from January 22, 2022, at 1:01 PM. The page also features links for "Home", "My account", and "Log out".

## 10. Information-disclosure

### [lab-infoleak-in-error-messages](#)

← → C ac3e1fe41ff287fac0e2baab00d300c6.web-security-academy.net

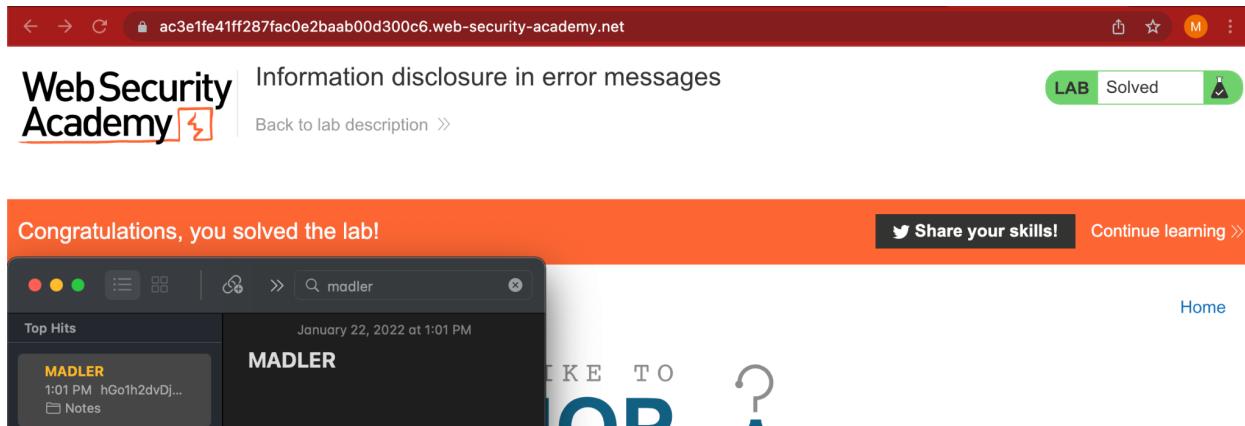
Web Security Academy Information disclosure in error messages LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning »

Top Hits January 22, 2022 at 1:01 PM MADLER

MADLER 1:01 PM hGo1h2dvDj... Notes

Home



## lab-infoleak-on-debug-page

← → C acb61f1f1e0a6185c0ed52ac002f002a.web-security-academy.net

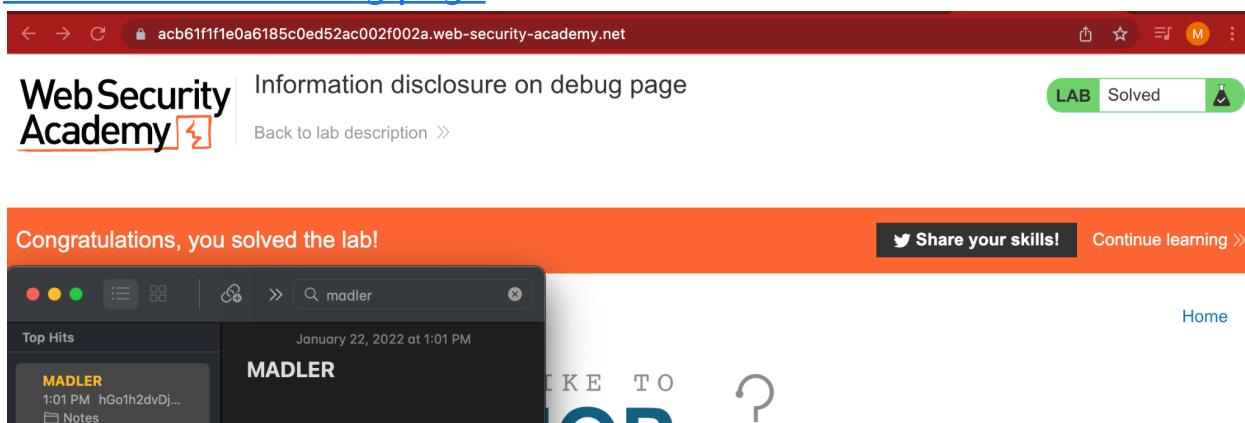
Web Security Academy Information disclosure on debug page LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning »

Top Hits January 22, 2022 at 1:01 PM MADLER

MADLER 1:01 PM hGo1h2dvDj... Notes

Home



## lab-infoleak-via-backup-files

← → C acf81f5c1f4c2ebcc0414d600048009e.web-security-academy.net

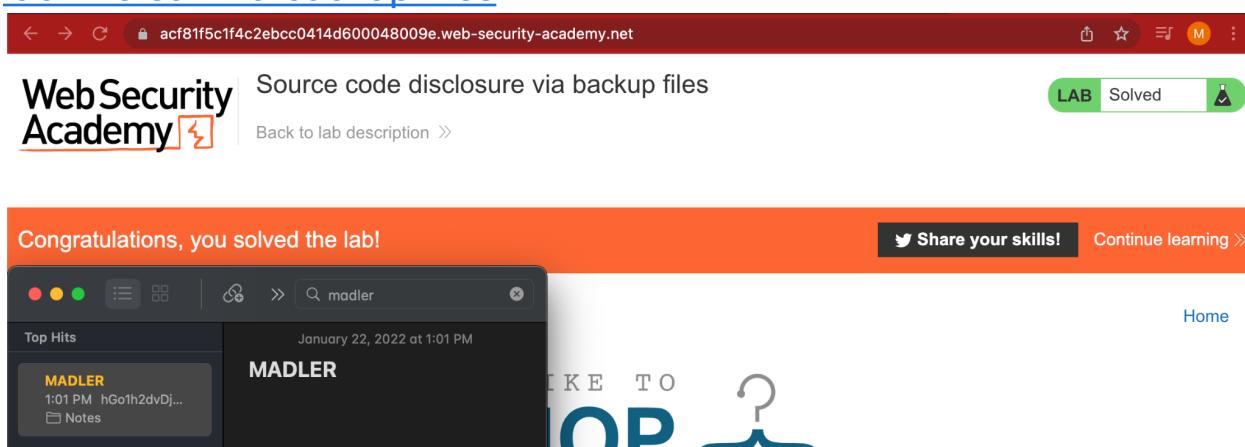
Web Security Academy Source code disclosure via backup files LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning »

Top Hits January 22, 2022 at 1:01 PM MADLER

MADLER 1:01 PM hGo1h2dvDj... Notes

Home



## 11. WFP1: File upload

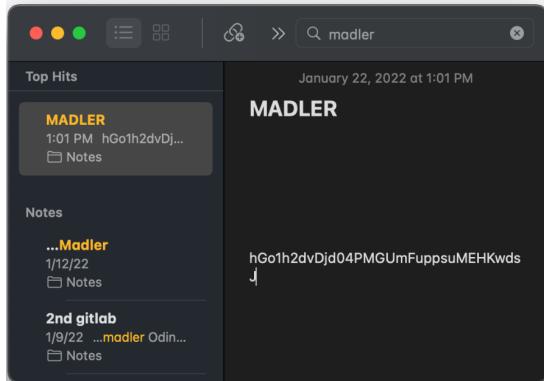
### Example #1

```
1.php  
1.txt  
hacker.jpg
```

---

Last line of the output: hacker.jpg

Return value: 0



### Example #2

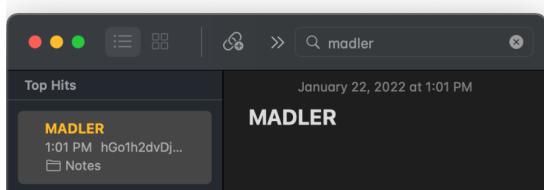
---

/var/www/upload/images

---

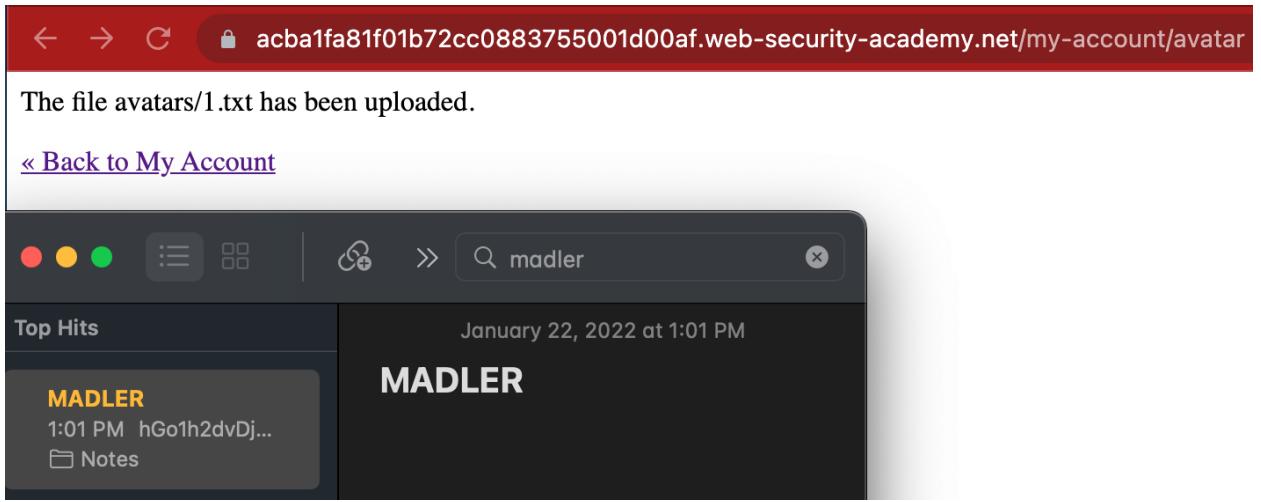
Last line of the output: /var/www/upload/images

Return value: 0



## 12. file-upload (1)

- What are the names of the form fields that are of type hidden? CSRF, user.
- Take a screenshot of the message and the URL the avatar is stored at on the server
-



## 13. file-upload (2)

- Take a screenshot of the message that is returned when you attempt to visit the `/admin` path of your site.

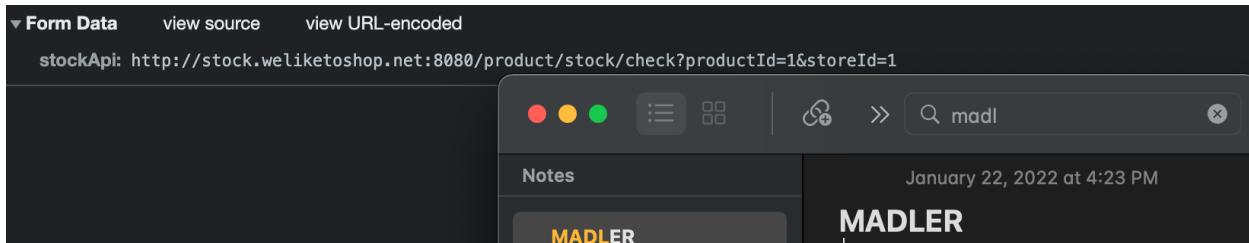
The screenshot shows a web browser window with the URL `ac261f3f1f6447fbc0db8f06008a0051.web-security-academy.net/admin`. The page title is "Basic SSRF against the local server". It includes a "Back to lab description" link and a "Home | My account" navigation bar at the bottom. A note states: "Admin interface only available if logged in as an administrator, or if requested from loopback". The browser's address bar shows the same URL.

- Take a screenshot that shows the Content-Type: request header that specifies the format of the form submission

The screenshot shows a web browser window with the URL `ac261f3f1f6447fbc0db8f06008a0051.web-security-academy.net/admin`. The page displays a list of request headers:  
Content-Type: application/x-www-form-urlencoded  
Cookie: session=amcS0gavKw0hKc7VGpNNcumva8FnI63  
Host: ac261f3f1f6447fbc0db8f06008a0051.web-security-academy.net  
Origin: https://ac261f3f1f6447fbc0db8f06008a0051.web-security-academy.net  
Pragma: no-cache

On the right, there is a file viewer interface similar to the one in the previous screenshot, showing a file named "MADLER" with the timestamp "4:23 PM".

- Then, take a screenshot of the form submission payload.



- Take a screenshot showing completion of the level that includes your OdinId

Week1 SecurityCloud | 1.6: SSRF | Lab: Basic SSRF against the local server | Basic SSRF against another back-end system | Quickstart — Requests | GitHub - jdonsec/All | +

**Web Security Academy** Basic SSRF against the local server LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Notes January 22, 2022 at 4:23 PM  
**MADLER**

## 1.6: SSRF

### 2. ssrf (2)

ace61fa51e6816d4c08c521500ad00fe.web-security-academy.net/product?productId=1

**Web Security Academy** Basic SSRF against another back-end system LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Notes January 22, 2022 at 4:23 PM  
**MADLER**

### 3. ssrf (3)



SSRF with blacklist-based input filter

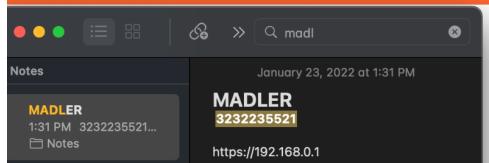
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

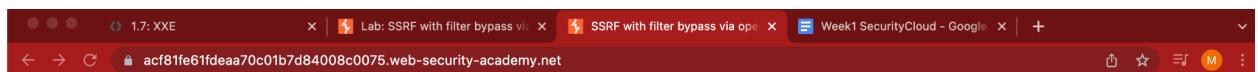
[Share your skills!](#)

[Continue learning >>](#)



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

## 4. ssrf (4)



SSRF with filter bypass via open redirection vulnerability

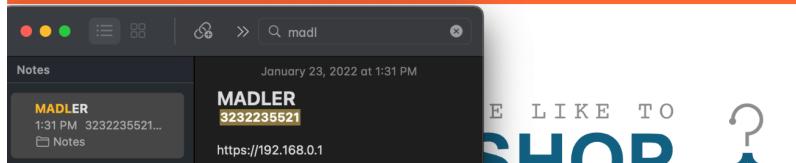
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)



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

## 5. ssrf/blind



Blind SSRF with out-of-band detection

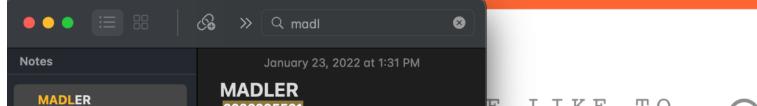
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)



[Home](#)

## 1.7: XXE

### 1. xxe (1)

1.7: XXE

Lab: Exploiting XXE using external entities

Exploiting XXE using external entities to retrieve files

Congratulations, you solved the lab!

January 23, 2022 at 5:36 PM

MADLER

E LIKE TO

?

Share your skills! Continue learning >

Home

### 2. xxe (2)

WebSecurity Academy

Exploiting XXE to perform SSRF attacks

Congratulations, you solved the lab!

January 23, 2022 at 5:36 PM

MADLER

E LIKE TO

?

Share your skills! Continue learning >

Home

### 3. xxe (3)

aca71fd71fc67599c067585c003f0007.web-security-academy.net

WebSecurity Academy

Exploiting XInclude to retrieve files

Congratulations, you solved the lab!

January 23, 2022 at 5:36 PM

MADLER

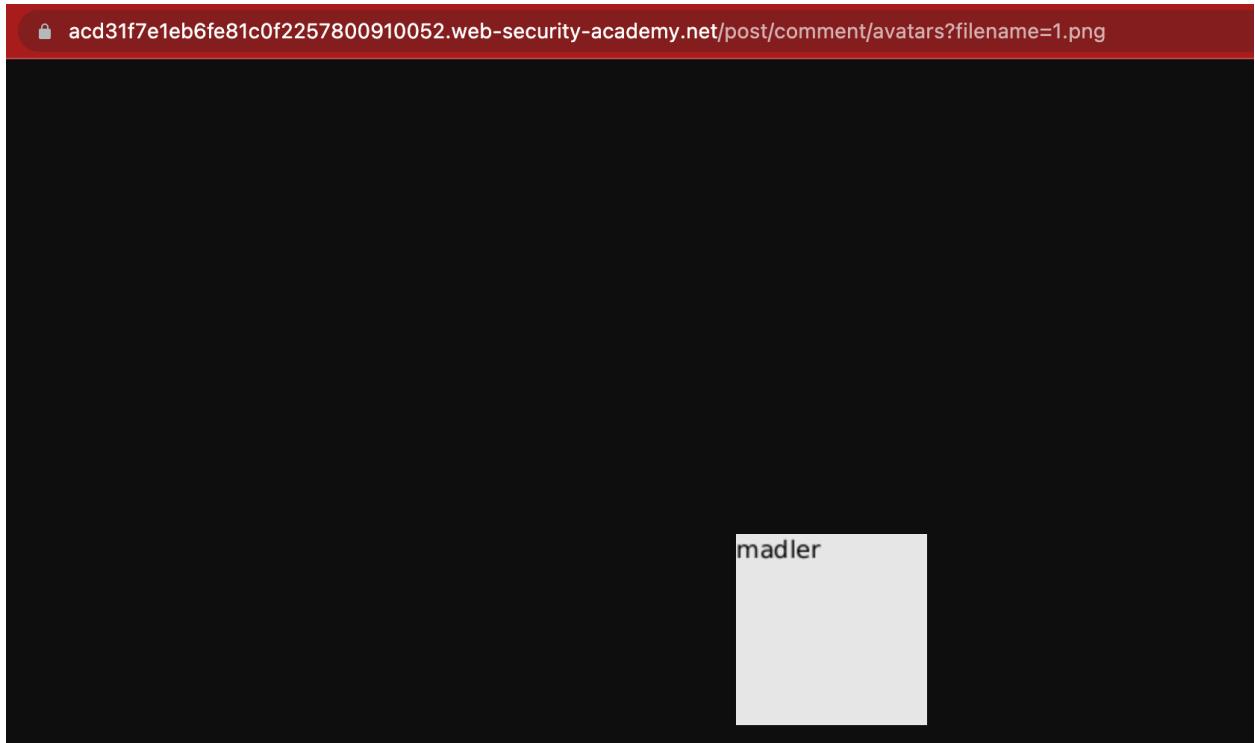
E LIKE TO

?

Share your skills! Continue learning >

Home

### 4. xxe (4)



5. -

A screenshot of the Web Security Academy website. The URL in the address bar is "acad1fc41ed483bcc0e1a4d4001f000b.web-security-academy.net/post?postId=1". The page title is "Exploiting XXE via image file upload". On the right, there is a green button labeled "LAB Solved" with a checkmark icon. Below the title, there is a link "Back to lab description >".

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

1.7 step4  
4:28 PM post\_url = f...  
Notes

January 23, 2022 at 6:54 PM  
MADLER

A large image of a glowing, blue and purple eye is displayed on the right side of the interface.