

Lab 2 - Vulnerability Scanning

Secure System Development - Spring 2025

In this lab, you'll:

- Test out popular Static Application Security Testing (SAST) tools with different programming languages.
- Learn how to exploit basic web app vulnerabilities.
- Create a report with screenshots and explanations of your findings.

Task 1 - SAST Tools

1.1 Bandit (Python)

```
python3 -m venv venv
source venv/bin/activate
pip install bandit
git clone git@github.com:fportantier/vulpy.git
bandit -r vulpy/ > bandit_scan.log
```

```
(venv) mohamad@mohamad-HP-ProBook-430-G7:~/Desktop/thirdYear/second-semester/secure-system-development/lab2$ bandit -r vulpy/ > bandit_scan.log
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
[main] INFO running on Python 3.10.12
(venv) mohamad@mohamad-HP-ProBook-430-G7:~/Desktop/thirdYear/second-semester/secure-system-development/lab2$
```

Low Severity Issue:

```
-- 
>> Issue: [B404:blacklist] Consider possible security implications
associated with the subprocess module.
Severity: Low Confidence: High
CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
More Info:
https://bandit.readthedocs.io/en/1.8.3/blacklists/blacklist\_imports.html#b404-import-subprocess
Location: vulpy/bad/brute.py:3:0
2
3 import subprocess
4 import sys
```

Explanation:

The `subprocess` module in Python is used to execute system commands. If we don't handle inputs properly, attackers could inject malicious commands. This can result in a security hole where someone could execute arbitrary commands on the system.

CWE-78 deals with improper handling of input, which can lead to command injection.

Solution: Be careful when using **subprocess**. Always sanitize input properly or use safer alternatives.

Medium Severity Issue:

```
-----  
>> Issue: [B113:request_without_timeout] Call to requests without timeout  
Severity: Medium Confidence: Low  
CWE: CWE-400 (https://cwe.mitre.org/data/definitions/400.html)  
More Info:  
https://bandit.readthedocs.io/en/1.8.3/plugins/b113\_request\_without\_timeout.html  
Location: vulpy/bad/api_post.py:30:8  
29     api_key = api_key_file.open().read()  
30     r = requests.post('http://127.0.1.1:5000/api/post', json=  
{'text':message}, headers={'X-APIKEY': api_key})  
31     print(r.text)
```

Explanation:

When you make HTTP requests without setting a timeout, your program might freeze if the server doesn't respond quickly enough. This could lead to performance issues or cause the system to become unresponsive.

CWE-400 covers how missing timeouts in requests can lead to denial of service attacks.

Solution: Always add a timeout when making HTTP requests. This ensures the program doesn't hang indefinitely if something goes wrong with the request.

High Severity Issue:

```
-----  
>> Issue: [B201:flask_debug_true] A Flask app appears to be run with  
debug=True, which exposes the Werkzeug debugger and allows the execution of  
arbitrary code.  
Severity: High Confidence: Medium  
CWE: CWE-94 (https://cwe.mitre.org/data/definitions/94.html)  
More Info:  
https://bandit.readthedocs.io/en/1.8.3/plugins/b201\_flask\_debug\_true.html  
Location: vulpy/bad/vulpy-ssl.py:29:0  
28  
29 app.run(debug=True, host='127.0.1.1', ssl_context=('/tmp/acme.cert',  
'/tmp/acme.key'))
```

Explanation:

Running a Flask app with **debug=True** exposes detailed error messages and the Werkzeug debugger, which could allow attackers to execute arbitrary code on your system. This is a significant risk in production environments.

CWE-94 is about code injection, where attackers can execute their code remotely due to poor security

configurations.

Solution: Always disable debugging (`debug=False`) in production to avoid exposing sensitive information and prevent remote code execution.

1.2 Flawfinder (C)

```
pip install flawfinder
git clone git@github.com:hardik05/Damn_Vulnerable_C_Program.git
flawfinder Damn_Vulnerable_C_Program/ > flawfinder_scan.log
```

Level 1 (Low Severity):

```
Damn_Vulnerable_C_Program/linux/imgRead_socket.c:74: [1] (buffer) read:
Check buffer boundaries if used in a loop including recursive loops
(CWE-120, CWE-20).
```

Explanation:

The `read` function is being used to read data into a buffer, but it's not checking if the buffer is large enough. This can cause a **buffer overflow** if more data is read than the buffer can handle, leading to potential security risks.

CWE-120 refers to buffer overflows, and **CWE-20** addresses improper input validation.

Solution: Make sure to check the size of the buffer before using the `read` function. It's a good practice to use safer functions that limit the amount of data being read.

Level 2 (Medium Severity):

```
Damn_Vulnerable_C_Program/dvcp.c:58: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-
120).
Make sure destination can always hold the source data.
```

Explanation:

The `memcpy` function is used to copy data, but if it's not properly checked, it can overwrite memory areas, causing a **buffer overflow**. This can lead to crashes or, in the worst case, allow attackers to execute malicious code.

CWE-120 again refers to buffer overflows, and **CWE-120** refers to improper input validation.

Solution: Always ensure that both source and destination buffers are large enough before using `memcpy`. Using safer alternatives can also help avoid these issues.

False positive:

```
Damn_Vulnerable_C_Program/dvcp.c:33: [2] (misc) fopen:  
    Check when opening files - can an attacker redirect it (via symlinks),  
    force the opening of special file type (e.g., device files), move things  
    around to create a race condition, control its ancestors, or change its  
    contents? (CWE-362).
```

Explanation:

One false-positive finding from the logs could be the warning related to the use of `fopen`. The warning suggests checking for potential security risks, like attackers redirecting files or causing race conditions. However, this might not be an issue if the program carefully controls where files are opened, such as ensuring the file path is always secure and validated. If there's no user input involved in choosing the file, and proper checks are in place, then this warning doesn't apply and can be considered a false positive.

1.3 njsscan (NodeJS)

```
pip install njsscan  
git clone git@github.com:appsecco/dvna.git  
njsscan dvna/
```

INFO Severity:

RULE ID	cookie_session_default
CWE	CWE-522: Insufficiently Protected Credentials
OWASP-WEB	A2: Broken Authentication
DESCRIPTION	Consider changing the default session cookie name. An attacker can use it to fingerprint the server and target attacks accordingly.
SEVERITY	INFO
FILES	 File dvna/server.js

```
| |  
| | Match Position | 9 - 3  
| |  
| | Line Number(s) | 23: 28  
| |  
| | Match String | app.use(session({  
| | | secret: 'keyboard cat',  
| | | resave: true,  
| | | saveUninitialized: true,  
| | | cookie: { secure: false }  
| | | }))  
| |
```

Explanation:

The default session cookie name could reveal information about the server, making it easier for an attacker to recognize and target specific vulnerabilities.

CWE-522 relates to insufficient protection of credentials, meaning that sensitive information, like session cookies, is not sufficiently protected from attackers.

Solution: Change the default session cookie name to make it harder for attackers to detect and exploit the server based on the cookie name.

WARNING Severity:

RULE ID	cookie_session_no_secure
---------	--------------------------

CWE	cwe-614
-----	---------

OWASP-WEB	A2: Broken Authentication
-----------	---------------------------

DESCRIPTION	Default session middleware settings: `secure` not set. It ensures the browser only sends the cookie over HTTPS.
SEVERITY	WARNING
FILES	
	File dvna/server.js
	Match Position 9 - 3
	Line Number(s) 23: 28
	Match String app.use(session({
	secret: 'keyboard cat',
	resave: true,
	saveUninitialized: true,
	cookie: { secure: false }
	}))

Explanation:

The `secure` flag on cookies ensures they are only sent over secure HTTPS connections. Without this flag, the cookie could be exposed during transmission over an insecure connection, making it vulnerable to interception by attackers.

CWE-614 refers to session fixation, where improper session management can allow attackers to hijack or manipulate sessions.

Solution: Always set the `secure` flag for session cookies so they are transmitted only over HTTPS. This minimizes the risk of data being intercepted.

ERROR Severity:

RULE ID	node_xxe
CWE Reference	CWE-611: Improper Restriction of XML External Entity
OWASP-WEB	A4: XML External Entities (XXE)
DESCRIPTION	User controlled data in XML parsers can result in XML External or Internal Entity (XXE) Processing vulnerabilities
SEVERITY	ERROR
FILES	
File	dvna/core/appHandler.js
Match Position	18 - 111
Line Number(s)	235
Match String	var products = libxmljs.parseXmlString(req.files.products.data.toString('utf8'), {noent:true,no blanks:true})

Explanation:

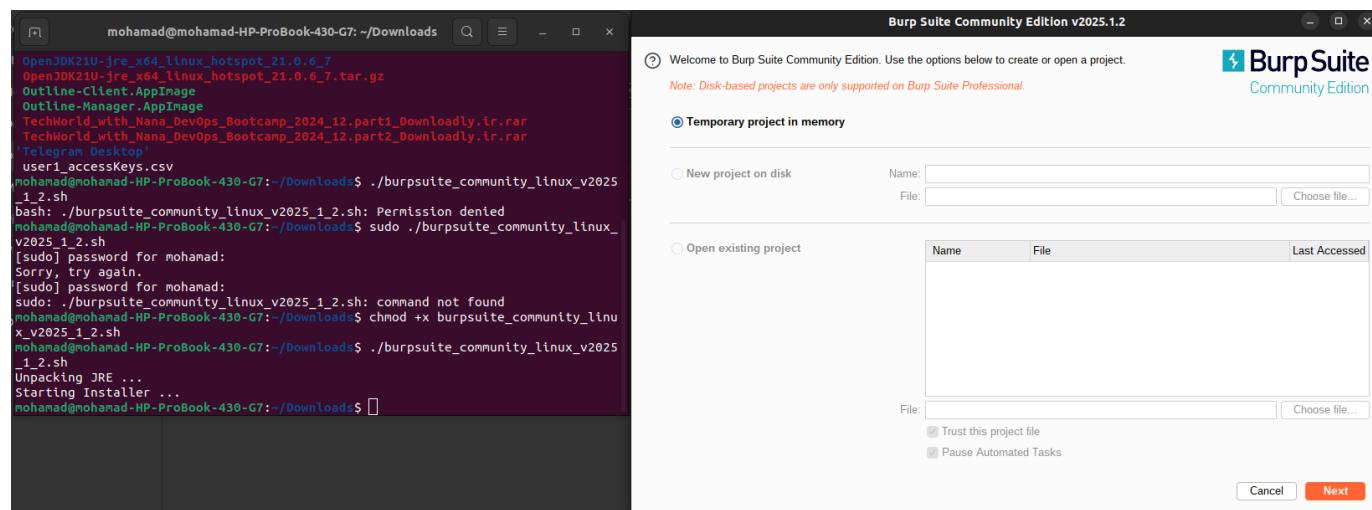
The vulnerability here is due to improper handling of XML data. An attacker can exploit a system by sending specially crafted XML that includes external entity references. These references can cause the system to process unintended data, leading to security issues like data leakage or remote code execution.

CWE-611 addresses vulnerabilities related to XML External Entity (XXE) attacks, where an attacker manipulates XML parsers to gain access to sensitive information.

Solution: Disable external entity processing in XML parsers to prevent XXE attacks. This helps secure the system from potentially dangerous XML inputs.

Task 2 - Web Security Mini Labs

1. Install BurpSuite (Community Edition)



2. Running Vulnerable Applications

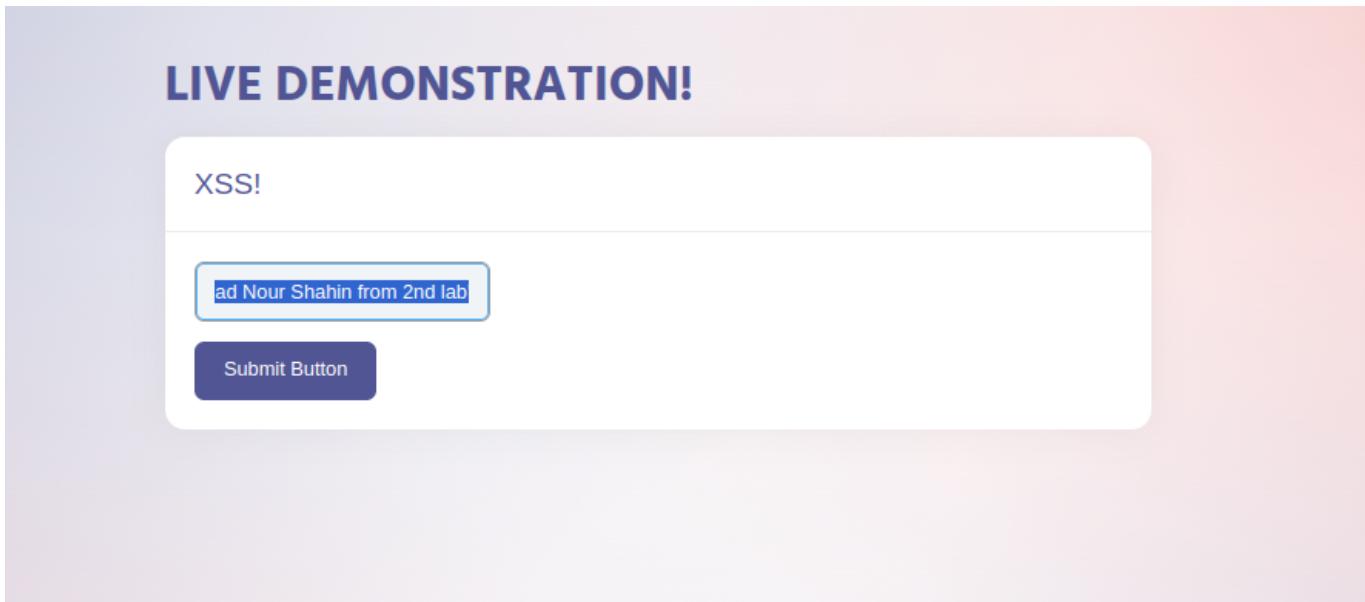
2.1 Cross-Site Scripting (XSS)

Running the XSS image

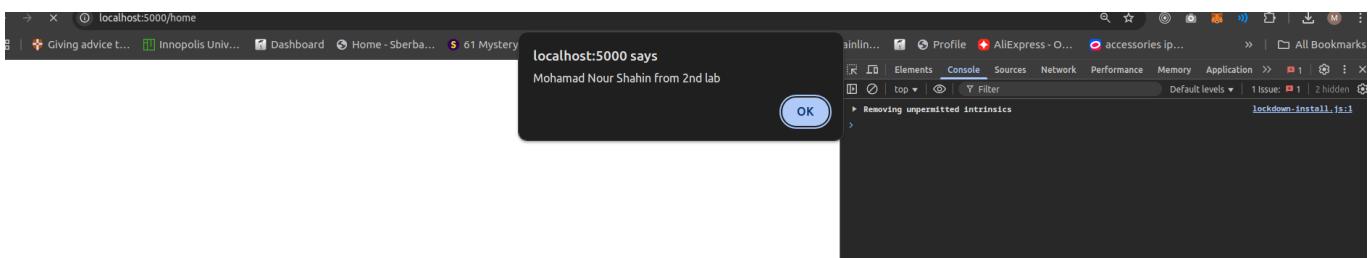
```
docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:xss
```

```
chahad@mohamed-HP-ProBook-430-G7:~/Downloads$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:xss
unable to find image 'sh3b0/vuln:xss' locally
ss: Pulling from sh3b0/vuln
d20c808ce19c: Pull complete
3879ca88737: Pull complete
5f42fd8906f: Pull complete
557e2c8196f: Pull complete
217645038d7: Pull complete
38bc1756869: Pull complete
f4fb700ef54: Pull complete
fdce7af2d85: Pull complete
27da1379ac0: Pull complete
d9dce4a769d: Pull complete
5b2c35b71b7: Pull complete
Digest: sha256:f0f97aaa3494122a41f2746851f3474c4f6899948e4509212cabf39796530a71
Status: Downloaded newer image for sh3b0/vuln:xss
* Running http://0.0.0.0:5000/ (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 254-198-468
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET / HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/css/Normalize.css HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/css/daterangepicker3.css HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/css/styles.css HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/js/lumino_glyphs.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/js/hints.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/img/badge.svg HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:14] "GET /static/js/jquery-3.6.0.min.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:15] "GET /static/js/bootstrap.min.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:16] "GET /static/fonts/fontawesome.woff2?51654781 HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:17] "GET /favicon.ico HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:50] "POST /home HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:40:51] "GET /favicon.ico HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:05] "POST /home HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:06] "GET /favicon.ico HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:26] "POST /home HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:27] "GET /favicon.ico HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:34] "GET /home HTTP/1.1" 405 -
72.17.0.1 - - [26/Feb/2025 12:41:37] "GET /favicon.ico HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET / HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/css/Normalize.css HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/css/daterangepicker3.css HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/css/styles.css HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/js/lumino_glyphs.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/js/hints.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/img/badge.svg HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:42] "GET /static/js/jquery-3.6.0.min.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:43] "GET /static/fonts/fontawesome.woff2?51654781 HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:46] "POST /home HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:47] "GET /favicon.ico HTTP/1.1" 200 -
```

Injecting a script



Results of injection



Captured in Burp Suite

The screenshot shows the Burp Suite interface with the following details:

- Network Tab:** Displays a list of captured requests and responses. The requests show various HTTP methods (POST, GET) and paths (e.g., /home, /css2) from localhost and fonts.googleapis.com.
- Request and Response panes:** Show the raw, pretty-printed, and hex representations of the selected request and response. The selected request is a POST to /favicon.ico with a string payload containing a script.
- Decoded from:** Set to URL encoding, showing the decoded payload: <script>Mohamad Nour Shahin from 2nd lab</script>.
- Selected text:** Contains the injected script: <script>Mohamad Nour Shahin from 2nd lab</script>.
- Request attributes, Request body parameters, Request headers, Response headers:** Lists the corresponding fields for the selected request.

Why XSS is Dangerous: XSS allows attackers to inject malicious scripts into web pages viewed by other users. This can lead to session hijacking, data theft, and even malware distribution. To mitigate this, websites should sanitize and validate user inputs, implement Content Security Policy (CSP), and use secure frameworks that prevent script injection.

2.2 Path Traversal

Running the path traversal image

```
docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:path-traversal
```

The terminal output shows the Docker container's logs:

```
cr.10/k8s-minikube/kubectl v0.8.46          e/2c9cb9b29 6 weeks ago  1.31GB
mohamad@mohamad-HP-ProBook-430-G7:~/Downloads$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:path-traversal
unable to find Image 'sh3b0/vuln:path-traversal' locally
path-traversal: Pulling from sh3b0/vuln
d20c808ce19: Already exists
3879cab8737: Already exists
5f42fd8960f: Already exists
557e2c8196f: Already exists
217645038d7: Already exists
a77e59174fc: Pull complete
f4fb700ef54: Pull complete
21a2ce6161f: Pull complete
f31cf9a1019: Pull complete
500c92841ea: Pull complete
bf693f5f7e35: Pull complete
Digest: sha256:4a29c3b12fa2dcf1e44b22f210e8b9785649fd00bd7cfcc8655cf7dde9021a35e
Status: Downloaded newer image for sh3b0/vuln:path-traversal
* Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 281-048-755
72.17.0.1 - - [26/Feb/2025 13:02:42] "POST /home HTTP/1.1" 400 -
72.17.0.1 - - [26/Feb/2025 13:02:44] "GET /favicon.ico HTTP/1.1" 404 -
72.17.0.1 - - [26/Feb/2025 13:02:46] "GET / HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 13:02:51] "POST /home HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 13:02:56] "POST /home HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 13:03:23] "POST /home HTTP/1.1" 200 -
```

Exploiting path traversal by modifying a request

Changing the value to `../../../../etc/passwd`

LIVE DEMONSTRATION!

Local file inclusion/path traversal

Selects Intro

Submit Button

© rip - Visit website

FileNotFoundError: [Errno 2] No such file or directory: '../etc/passwd'

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1475, in full_dispatch_request

rv = self.dispatch_request()

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1461, in dispatch_request

return self.view_functions[rule.endpoint](**req.view_args)

File "/home/app/LFI/LFI.py", line 18, in home

f = open(filename,'r')

FileNotFoundError: [Errno 2] No such file or directory: '/etc/passwd'

172.17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=debugger.js HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=style.css HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=jquery.js HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:12:04] "POST /home HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:16:11] "POST /home HTTP/1.1" 500 -

Traceback (most recent call last):

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1836, in __call__

return self.wsgi_app(environ, start_response)

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1820, in wsgi_app

response = self.make_response(self.handle_exception(e))

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1403, in handle_exception

reraise(exc_type, exc_value, tb)

File "/home/app/.local/lib/python3.6/site-packages/flask_compat.py", line 33, in reraise

raise value

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1817, in wsgi_app

response = self.full_dispatch_request()

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1477, in full_dispatch_request

rv = self.handle_user_exception(e)

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1381, in handle_user_exception

reraise(exc_type, exc_value, tb)

File "/home/app/.local/lib/python3.6/site-packages/flask_compat.py", line 33, in reraise

raise value

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1475, in full_dispatch_request

rv = self.dispatch_request()

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1461, in dispatch_request

return self.view_functions[rule.endpoint](**req.view_args)

File "/home/app/LFI/LFI.py", line 18, in home

f = open(filename,'r')

FileNotFoundError: [Errno 2] No such file or directory: '../etc/passwd'

172.17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=style.css HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=jquery.js HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=debugger.js HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

172.17.0.1 - - [26/Feb/2025 13:16:45] "POST /home HTTP/1.1" 400 -

172.17.0.1 - - [26/Feb/2025 13:17:01] "POST /home HTTP/1.1" 200 -

After submitting

```

root:x:0:root:/root/bin/ash
bin:x:1:bin:/bin/sbin/nologin
daemon:x:2:daemon:/sbin/sbin/nologin
adm:x:3:4:adm:/var/adm/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd/sbin/nologin
sync:x:5:0:sync:/sbin/bin/sync
shutdown:x:6:0:shutdown:/sbin/sbin/shutdown
halt:x:7:0:halt:/sbin/sbin/halt
mail:x:8:12:mail:/var/spool/mail/sbin/nologin
news:x:9:13:news:/usr/lib/news/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic/sbin/nologin
operator:x:11:0:operator:/root/bin/sh
man:x:13:15:man:/usr/man/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail/sbin/nologin
cron:x:16:16:cron:/var/spool/cron/sbin/nologin
ftp:x:21:21::/var/lib/ftp/sbin/nologin
sshd:x:22:22:sshd:/dev/null/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs/sbin/nologin
games:x:35:35:games:/usr/games/sbin/nologin
postgres:x:70:70:/var/lib/postgresql/bin/sh
cyrus:x:85:12:/usr/cyrus/sbin/nologin

```

Original Code ...

FileNotFoundError: [Errno 2] No such file or directory: '../etc/passwd'

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1475, in full_dispatch_request

rv = self.dispatch_request()

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1461, in dispatch_request

return self.view_functions[rule.endpoint](**req.view_args)

File "/home/app/LFI/LFI.py", line 18, in home

f = open(filename,'r')

FileNotFoundError: [Errno 2] No such file or directory: '/etc/passwd'

17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=debugger.js HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=style.css HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=jquery.js HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:11:46] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:12:04] "POST /home HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:16:11] "POST /home HTTP/1.1" 500 -

Traceback (most recent call last):

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1836, in __call__

return self.wsgi_app(environ, start_response)

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1820, in wsgi_app

response = self.make_response(self.handle_exception(e))

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1403, in handle_exception

reraise(exc_type, exc_value, tb)

File "/home/app/.local/lib/python3.6/site-packages/flask_compat.py", line 33, in reraise

raise value

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1817, in wsgi_app

response = self.full_dispatch_request()

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1477, in full_dispatch_request

rv = self.handle_user_exception(e)

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1381, in handle_user_exception

reraise(exc_type, exc_value, tb)

File "/home/app/.local/lib/python3.6/site-packages/flask_compat.py", line 33, in reraise

raise value

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1475, in full_dispatch_request

rv = self.dispatch_request()

File "/home/app/.local/lib/python3.6/site-packages/flask/app.py", line 1461, in dispatch_request

return self.view_functions[rule.endpoint](**req.view_args)

File "/home/app/LFI/LFI.py", line 18, in home

f = open(filename,'r')

FileNotFoundError: [Errno 2] No such file or directory: '../etc/passwd'

17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=style.css HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=jquery.js HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=debugger.js HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:16:11] "GET /home?__debugger__=yes&cmd=resource&f=console.png HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:16:45] "POST /home HTTP/1.1" 400 -

17.0.1 - - [26/Feb/2025 13:17:01] "POST /home HTTP/1.1" 200 -

17.0.1 - - [26/Feb/2025 13:19:08] "POST /home HTTP/1.1" 200 -

Captured in Burp Suite-1

The screenshot shows the Burp Suite interface. The top menu bar includes Project, Intruder, Repeater, View, Help, Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger (selected), Organizer, Extensions, and Learn. A settings icon is in the top right.

The main window has two panes: 'Request' and 'Response'. The Request pane shows a raw HTTP request with various headers (Cache-Control, sec-ch-ua, sec-ch-ua-mobile, sec-ch-ua-platform, Accept, User-Agent, Accept-Encoding, Connection) and a body containing a file traversal payload. The Response pane shows a raw HTML response from a Flask application, which includes a file not found error and a stack trace. The status code is 200, and the length is 1411MB.

At the bottom, there are search and highlight tools, and a memory usage indicator of 141.1MB.

Why Path Traversal is Dangerous: Path traversal attacks allow attackers to access restricted directories and files, potentially exposing sensitive data such as configuration files or credentials. To prevent this, developers should normalize input paths, use allowlists for file access, and restrict user input.

2.3 SQL Injection

Running the SQL Injection image

```
docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:sql-injection
```

```
mohamad@mohamad-HP-ProBook-430-G7:~/Downloads$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:sql-injection
Unable to find image 'sh3b0/vuln:sql-injection' locally
sql-injection: Pulling from sh3b0/vuln
5d20c808ce19: Already exists
53879ca88737: Already exists
05f42fd8906f: Already exists
0557e2c8196f: Already exists
6217645038d7: Already exists
c9f825b634f3: Pull complete
4f4fb700ef54: Pull complete
e1b23c1d8253: Pull complete
9eb3f3200d49: Pull complete
cb923e1a6dc9: Pull complete
cde4e8e06b00: Pull complete
Digest: sha256:1570e12ac6c5faf1f96f9b37cb30c52b9e8fa258f7a6e611644b7f88cda0ea69
Status: Downloaded newer image for sh3b0/vuln:sql-injection
 * Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 137-810-963
```

Attempting SQL Injection

Injecting `1 UNION SELECT * FROM users` into an input field.

LIVE DEMONSTRATION!

SQL injection!

Welcome

About us

Admin
Ocef1fb10f60529028a71f58e54ed07b

Name	Status	Type	Initiator	Size	Time
	50 ms	100 ms	150 ms	200 ms	250 ms
	300 ms	350 ms	400 ms	450 ms	500 ms

Network

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder DOM Invader

Filter

All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other

172.17.0.1 - - [27/Feb/2025 08:39:13] "GET /home/1%20union%20password%20from%20users?_debugger_=yes&cmd=resource&f=sty06-

172.17.0.1 - - [27/Feb/2025 08:39:14] "GET /home/1%20union%20password%20from%20users?_debugger_=yes&cmd=resource&f=console.png HTTP/1.1 200 -

172.17.0.1 - - [27/Feb/2025 08:39:18] "GET /home/1%20union%20password%20from%20users?_debugger_=yes&cmd=resource&f=con200-

172.17.0.1 - - [27/Feb/2025 08:39:30] "GET /home/1%20union%20password%20from%20users HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:39:31] "GET /home/1%20union%20password%20from%20users?_debugger_=yes&cmd=resource&f=con200-

172.17.0.1 - - [27/Feb/2025 08:39:36] "GET /favicon.ico HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:39:45] "GET / HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:40:01] "GET /home/1%20union%20password%20from%20users HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:40:02] "GET /favicon.ico HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:40:43] "GET /home/1%20union%20password%20from%20users?_debugger_=yes&cmd=resource&f=con200-

172.17.0.1 - - [27/Feb/2025 08:40:43] "GET /favicon.ico HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:40:52] "GET /home/1%20union%20password%20from%20users HTTP/1.1" 200 -

172.17.0.1 - - [27/Feb/2025 08:40:52] "GET /favicon.ico HTTP/1.1" 200 -

Why SQL Injection is Dangerous: SQL Injection can allow attackers to manipulate database queries, potentially exposing or modifying sensitive data. To prevent this, use prepared statements, ORM frameworks, and enforce strict input validation.

2.4 File Upload Exploit

Running the file upload image

```
docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:file-upload
```

```
Chahandighohmehad@HP-Probook-430-G7:~/Downloads$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:file-upload
Unable to find image 'sh3b0/vuln:file-upload' locally
file-upload: Pulling from sh3b0/vuln
5d20c008a119: Already exists
32970e480571: Already exists
3f44f2f996ef: Already exists
b557e2c8196f: Already exists
3217645038d7: Already exists
78730a41a6d: Pull complete
ff4fb700ee54: Pull complete
3c55754045e: Pull complete
3c0f571619bd: Pull complete
57b284dia1a91: Pull complete
11a3c53f77fs: Pull complete
Digest: sha56:5522374ed424998d42cc97d2ac544796e01835c8109d10ffd776219ffbc93e88
Status: Downloaded newer image for sh3b0/vuln:file-upload
 * Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 116-993-971
172.17.0.1 - - [26/Feb/2025 14:25:12] "GET / HTTP/1.1" 200 -
172.17.0.1 - - [26/Feb/2025 14:25:15] "GET /favicon.ico HTTP/1.1" 200 -
[
```

Bypassing file upload restrictions

Uploading an HTML file and intercepting the request in Burp Suite to modify the file path.

```
ash-4.4$ cat File-upload.py
import os
from flask import Flask, request, render_template

app = Flask(__name__, static_url_path='/static', static_folder='static')
ALLOWED_EXTENSIONS = app.config['ALLOWED_EXTENSIONS'] = set(['txt', 'pdf', 'png', 'jpg', 'jpeg', 'html'])
app.config['DEBUG'] = True

def allowed_file(filename):
    return '.' in filename and \
           filename.rsplit('.', 1)[1] in ALLOWED_EXTENSIONS

app.route("/", methods=['GET', 'POST'])
def index():
    if request.method == 'POST':
        file = request.files['file']
        print(file)
        if file and allowed_file(file.filename):
            filename = file.filename
            file.save(os.path.join('uploads/', filename))
            uploaded = "File was uploaded"
            return render_template("index.html",uploaded = uploaded)
        uploaded = "something went wrong!"
        return render_template("index.html",uploaded = uploaded)
    return render_template("index.html")

app.errorhandler(404)
def page_not_found(e):
    return render_template("404.html")

if __name__ == "__main__":
    app.run(host='0.0.0.0')
```

Turning on intercept in Burp Suite

```

ls
edge.svg
ls-4.45 cd
ls-4.45 ls
ickerfile
ls-4.45 cat
port os
ron flask imp
op = Flask(_
ALLOWED_EXTENSIONS
op.config['DE
if allowed_fi
    return "."
fil
app.route("/")
def index():
    if request
        file =
        print(
        if fil
            fil
            fil
            up
            re
            upload
            return
        return re
    pretty = True
    raw = False
    hex = False
    time = 11:28:27 ...
    type = "HTTP"
    direction = "Request"
    method = "GET"
    url = "http://localhost:5000/"
    status_code = 200
    length = 157
    response = None
    content_type = "text/html; charset=utf-8"
    encoding = "utf-8"
    charset = "utf-8"
    body = b'<h1>LIVE DEMONSTRATION!</h1><form><input type="file" name="file"><input type="submit" value="Submit Button"></form>'
```

Request

	Pretty	Raw	Hex
00000000	0x01 00 2f 1f 00 0c 30 2f 00 00 20 00 00 00 00 00	1f 01 00 00 2f 1f 00 0c 30 2f 00 00 20 00 00 00 00 00	1f 01 00 00 2f 1f 00 0c 30 2f 00 00 20 00 00 00 00 00
00000001	00000000 61 67 65 2f 61 76 69 66 20 69 6d 61 67 65 2f 77	00000000 61 67 65 2f 61 76 69 66 20 69 6d 61 67 65 2f 77	00000000 61 67 65 2f 61 76 69 66 20 69 6d 61 67 65 2f 77
00000002	00000000 65 62 70 2c 69 6d 61 67 65 2f 61 70 66 67 2c 2a	00000000 65 62 70 2c 69 6d 61 67 65 2f 61 70 66 67 2c 2a	00000000 65 62 70 2c 69 6d 61 67 65 2f 61 70 66 67 2c 2a
00000003	00000000 2f 2a 3b 71 3d 30 38 2c 61 70 70 69 63 61 2f 00 00 00	00000000 2f 2a 3b 71 3d 30 38 2c 61 70 70 69 63 61 2f 00 00 00	00000000 2f 2a 3b 71 3d 30 38 2c 61 70 70 69 63 61 2f 00 00 00
00000004	00000000 74 69 6f 6e 2f 73 69 67 66 65 64 2d 65 78 63 68 2f 00 00 00	00000000 74 69 6f 6e 2f 73 69 67 66 65 64 2d 65 78 63 68 2f 00 00 00	00000000 74 69 6f 6e 2f 73 69 67 66 65 64 2d 65 78 63 68 2f 00 00 00
00000005	00000000 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 2f 00 00 00	00000000 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 2f 00 00 00	00000000 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 2f 00 00 00
00000006	00000000 03 53 65 63 2d 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00	00000000 03 53 65 63 2d 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00	00000000 03 53 65 63 2d 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00
00000007	00000000 03 65 0d 04 53 65 0d 04 53 65 62 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00	00000000 03 65 0d 04 53 65 0d 04 53 65 62 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00	00000000 03 65 0d 04 53 65 0d 04 53 65 62 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00
00000008	00000000 20 6e 0f 65 0d 04 53 65 62 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00	00000000 20 6e 0f 65 0d 04 53 65 62 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00	00000000 20 6e 0f 65 0d 04 53 65 62 46 65 74 63 60 2d 53 60 74 65 3a 2f 00 00 00
00000009	00000000 65 62 6f 64 65 3a 2e 6e 61 76 69 67 61 74 65 0d 2f 00 00 00	00000000 65 62 6f 64 65 3a 2e 6e 61 76 69 67 61 74 65 0d 2f 00 00 00	00000000 65 62 6f 64 65 3a 2e 6e 61 76 69 67 61 74 65 0d 2f 00 00 00
00000010	00000000 2d 4d 6f 64 65 3a 2e 6e 61 76 69 67 61 74 65 0d 2f 00 00 00	00000000 2d 4d 6f 64 65 3a 2e 6e 61 76 69 67 61 74 65 0d 2f 00 00 00	00000000 2d 4d 6f 64 65 3a 2e 6e 61 76 69 67 61 74 65 0d 2f 00 00 00
00000011	00000000 03 53 65 63 2d 46 65 74 63 60 2d 55 73 65 72 3a 2f 00 00 00	00000000 03 53 65 63 2d 46 65 74 63 60 2d 55 73 65 72 3a 2f 00 00 00	00000000 03 53 65 63 2d 46 65 74 63 60 2d 55 73 65 72 3a 2f 00 00 00
00000012	00000000 20 3f 31 0d 0a 53 65 63 2d 46 65 74 63 60 2d 55 73 65 72 3a 2f 00 00 00	00000000 20 3f 31 0d 0a 53 65 63 2d 46 65 74 63 60 2d 55 73 65 72 3a 2f 00 00 00	00000000 20 3f 31 0d 0a 53 65 63 2d 46 65 74 63 60 2d 55 73 65 72 3a 2f 00 00 00
00000013	00000000 65 73 74 3a 20 64 6f 63 75 6d 65 6e 74 0d 04 41 2f 00 00 00	00000000 65 73 74 3a 20 64 6f 63 75 6d 65 6e 74 0d 04 41 2f 00 00 00	00000000 65 73 74 3a 20 64 6f 63 75 6d 65 6e 74 0d 04 41 2f 00 00 00
00000014	00000000 63 63 65 70 74 2d 45 6e 63 6f 64 69 66 67 3a 20 2f 00 00 00	00000000 63 63 65 70 74 2d 45 6e 63 6f 64 69 66 67 3a 20 2f 00 00 00	00000000 63 63 65 70 74 2d 45 6e 63 6f 64 69 66 67 3a 20 2f 00 00 00
00000015	00000000 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 2c 20 62 2f 00 00 00	00000000 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 2c 20 62 2f 00 00 00	00000000 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 2c 20 62 2f 00 00 00
00000016	00000000 72 0d 0a 43 6f 66 6e 65 63 74 69 6f 6e 3a 20 6b 2f 00 00 00	00000000 72 0d 0a 43 6f 66 6e 65 63 74 69 6f 6e 3a 20 6b 2f 00 00 00	00000000 72 0d 0a 43 6f 66 6e 65 63 74 69 6f 6e 3a 20 6b 2f 00 00 00
00000017	00000000 65 65 70 2d 61 6c 69 76 65 0d 0a 0d 0a 2f 00 00 00	00000000 65 65 70 2d 61 6c 69 76 65 0d 0a 0d 0a 2f 00 00 00	00000000 65 65 70 2d 61 6c 69 76 65 0d 0a 0d 0a 2f 00 00 00

Uploading and submitting the HTML file

LIVE DEMONSTRATION!

File upload injection!

Choose File index.html

Submit Button

Memory Full

to upload file to static/img is it possible to run it to get shell

, whether you can execute it depends on several

options must be met:

copy , or .exe files to execute, then yes, you might be able

.css , .js) are served, you cannot execute them.

be files in static/img , you might be able to run a script.

files, the server will just serve them as downloads.

Name	Status	Type	Initiator	Size	Time
styles.css	200	stylesheet	(index:11)	(disk cache)	11 ms
normalize.css	200	stylesheet	(index:10)	(disk cache)	12 ms
lumino_glyphs.js	200	script	(index:14)	(disk cache)	11 ms
localhost	200	document	Other		3.2 kB
jquery-3.6.0.min.js	200	script	(index:11)	(disk cache)	8.25 ms
hints.js	200	script	(index:15)	(disk cache)	4 ms
fontello.woff2?751654781	200	font	styles.css	(disk cache)	14 ms
Favicon.ico	200	text/html	Other		2 ms
datepicker3.css	200	stylesheet	(index:10)	(disk cache)	26 ms
css2?family=Hindwght@700&display=swap	200	stylesheet	(index:16)	(disk cache)	12 ms
bootstrap.min.js	200	script	(index:14)	(disk cache)	1 ms
badge.svg	200	svg+xml	(index:37)	(disk cache)	2 ms
SuU19_a8oxmlfNjdERySjQ.woff2	200	font	css2		456 ms

Successful exploitation

The screenshot shows the Burp Suite interface with two captured requests. The first request is a GET to http://localhost:5000. The second request is a POST to the same URL. The Request tab displays the raw POST data, which includes an `Accept-Encoding: gzip, deflate, br`, `Connection: keep-alive`, and a multipart form-data boundary. The body of the POST request contains a file named `index.html` from a template directory.

Request Headers:

```

19 Accept-Encoding: gzip, deflate, br
20 Connection: keep-alive
21
22 -----WebKitFormBoundaryv1ceTAjWi5E3zRBI
23 Content-Disposition: form-data; name="file"; filename="../templates/index.html"
24 Content-Type: text/html
25
26 <!DOCTYPE html>
27 <html lang="en">
28   <head>

```

Inspector Panel:

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

Browser View:

A browser window shows a resume page for "Mohamad Nour". It includes sections for "Hello I'm", "Mohamad Nour Shahin", and "Software Engineer". It also features a "Download CV" button and social media links for LinkedIn and GitHub.

Terminal View:

A terminal window titled "mohamad@mohamad-HP-ProBook-430-G7: ~" shows Python code for handling file uploads. The code checks if a file is uploaded and saves it to the 'uploads' directory. It then renders different templates based on the file type. If no file is uploaded, it returns a 404 error.

```

if file and allowed_file(file.filename):
    filename = file.filename
    file.save(os.path.join('uploads/', filename))
    uploaded = "File was uploaded"
    return render_template("index.html", uploaded = uploaded)
uploaded = "something went wrong!"
return render_template("index.html", uploaded = uploaded)
return render_template("index.html")

@app.errorhandler(404)
def page_not_found(e):
    return render_template("404.html")

```

Network Tab:

The Network tab in the developer tools shows a list of network requests. One request to "templates" is highlighted, showing a response time of 20,000 ms. The response content shows bash shell commands being executed, including "ls", "cd", and "cat" on files like "index.html" and "404.html".

Why Unrestricted File Upload is Dangerous: Attackers can upload malicious files (e.g., scripts, executables) to execute arbitrary commands. To prevent this, validate file types, use server-side checks, and store uploads outside the web root with randomized names.

2.5 Command Injection

Running the command injection image

```
docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:file-upload
```

```
mohamad@mohamad-HP-ProBook-430-G7: ~$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:command-injection
Unable to find image 'sh3b0/vuln:command-injection' locally
command-injection: Pulling from sh3b0/vuln
5d20c808ce19: Already exists
16a1e357d681: Pull complete
d5f0e0b6ccca0: Pull complete
9dc528f883ed: Pull complete
77cc860d68fd: Pull complete
8496d86fc735: Pull complete
4f4fb700ef54: Pull complete
f61c0fb18c6a: Pull complete
5f2812bb7c7f: Pull complete
9f3af57112c1: Pull complete
d74022104470: Pull complete
Digest: sha256:9dac3a070309af595902684f2a6f56bbd96a0ff01b8f014b899ac87d1927a659
Status: Downloaded newer image for sh3b0/vuln:command-injection
 * Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 159-780-626
```

Injecting a command into an HTML element

Modifying a field to include:

```
50%; rm -rf /static/img/bones.png
```

LIVE DEMONSTRATION!

CMD Image resize!

Select image resize 50%

Submit Button

50%; rm -rf /static/img/bones.png

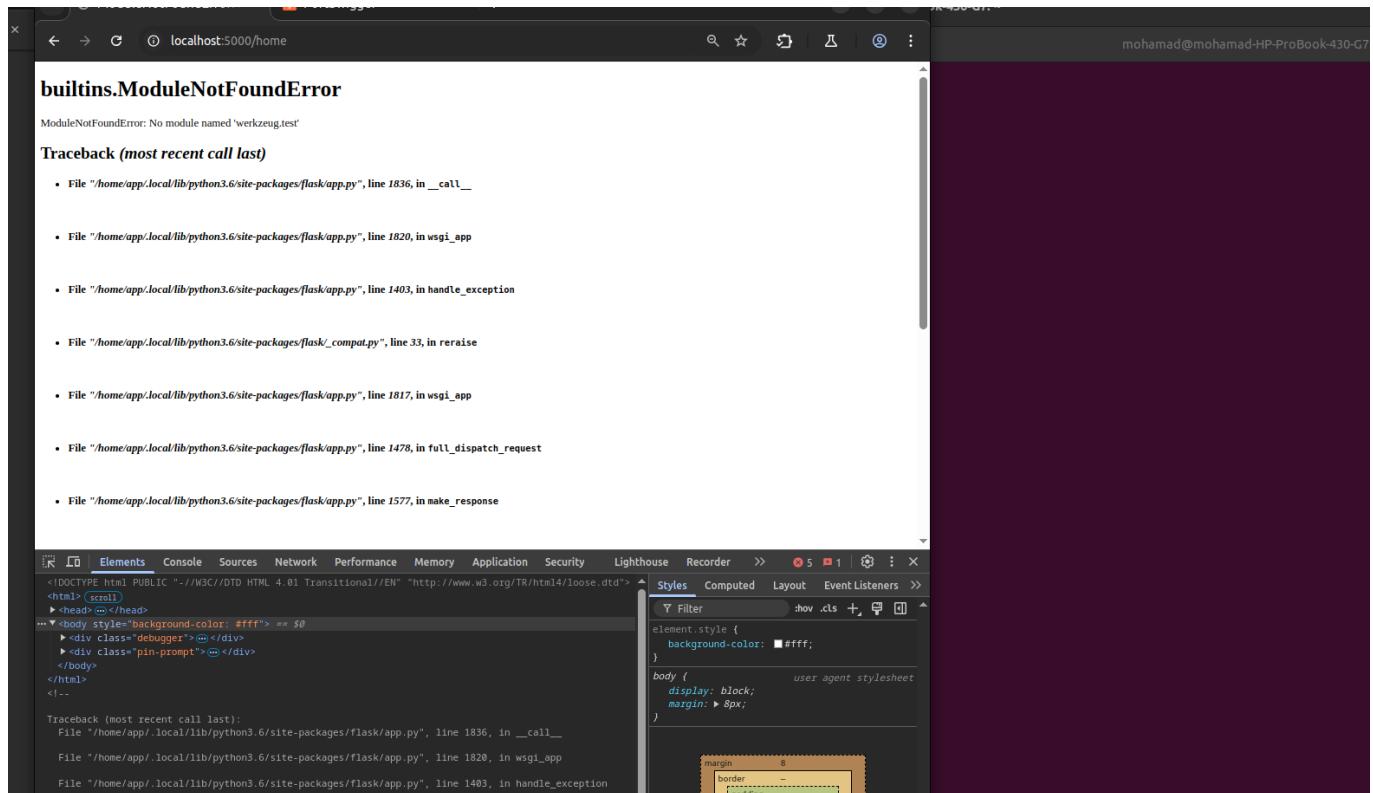
File operations in terminal:

```
-lc      Listctime
-lu      Listatime
--full-time Listfull date and time
-h      Human readable sizes (1K 243M 2G)
--group-directories-first
-S      Sort by size
-X      Sort by extension
-v      Sort by version
-t      Sort by mtime
-tc     Sort by ctime
-tu     Sort by atime
-r      Reverse sort order
-w N    Format N columns wide
--color=[always,never,auto] Control coloring
172.17.0.1 - - [27/Feb/2025 09:01:28] "POST /home HTTP/1.1" 200 -
172.17.0.1 - - [27/Feb/2025 09:01:28] "GET /favicon.ico HTTP/1.1" 200 -
convert: '50%' @ error/convert.c/ConvertImageCommand/3272.
sh: cd: line 1: can't cd to /home%
172.17.0.1 - - [27/Feb/2025 09:02:12] "POST /home HTTP/1.1" 200 -
172.17.0.1 - - [27/Feb/2025 09:02:13] "GET /favicon.ico HTTP/1.1" 200 -
```

Developer tools showing the injected CSS rule:

```
element.style {
}
* {
  box-sizing: border-box;
}
option {
  font-weight: normal;
  display: block;
  padding-block-start: 0px;
  padding-block-end: 1px;
  min-block-size: 1.2em;
  padding-inline: 2px;
}
```

After injection



Captured output in terminal

```
mohamad@mohamad-HP-ProBook-430-G7:~
```

```
rm: can't remove '/usr/share/terminfo/v/vt220-old': Permission denied
rm: can't remove '/usr/share/terminfo/v/vt100-w-am': Permission denied
rm: can't remove '/usr/share/terminfo/v': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260wy0pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100w100pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100w100w': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-7-s': Permission denied
rm: can't remove '/usr/share/terminfo/n/ndr9500-mc': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260ntpp': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp51': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp251-o': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-n-s': Permission denied
rm: can't remove '/usr/share/terminfo/n/news-42-euc': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260ntwp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100w100w': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp51': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260vt200wan': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100vt200wpp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260w50+wpp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ndr9500': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260vt100pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-16color': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-16color': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100vt300wan': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm7900iv': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100vt100pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-7-m': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-acss': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-cs7': Permission denied
rm: can't remove '/usr/share/terminfo/n/news-29-sjis': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp513-a': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260w0pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr100vt200d0': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp514': Permission denied
rm: can't remove '/usr/share/terminfo/n/nansi.sys': Permission denied
rm: can't remove '/usr/share/terminfo/n/nansi.sys': Permission denied
```

Why Command Injection is Dangerous: Command injection allows attackers to execute arbitrary commands on the server, potentially leading to data theft, system compromise, or destruction. To prevent this, avoid executing system commands with user input, use parameterized APIs, and apply strict input validation.