

Ammar Meslmani - CBS-01

a.meslmani@innopolis.university

the repo link to check the files used in this assignment: [full report](#)

Lab 2 - Vulnerability Scanning

Task1:

- in this task, **poetry** will be used as a python virtual environment, so let's check the version and initialize a project:

```
amar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry --version
Poetry (version 2.1.1)
amar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry init

This command will guide you through creating your pyproject.toml config.

Package name [lab2]:
Version [0.1.0]:
Description []:
Author [Ammar Meslmani <a.meslmani@innopolis.university>, n to skip]:
License []:
Compatible Python versions [>=3.12]:

Would you like to define your main dependencies interactively? (yes/no) [yes]
You can specify a package in the following forms:
- A single name (requests): this will search for matches on PyPI
- A name and a constraint (requests@^2.23.0)
- A git url (git+https://github.com/python-poetry/poetry.git)
- A git url with a revision (git+https://github.com/python-poetry/poetry.git#develop)
- A file path (.../my-package/my-package.whl)
- A directory (.../my-package/)
- A url (https://example.com/packages/my-package-0.1.0.tar.gz)

Package to add or search for (leave blank to skip):

Would you like to define your development dependencies interactively? (yes/no) [yes]
Package to add or search for (leave blank to skip):

Generated file

[project]
name = "lab2"
version = "0.1.0"
description = ""
authors = [
    {name = "Ammar Meslmani",email = "a.meslmani@innopolis.university"}
]
readme = "README.md"
requires-python = ">=3.12"
dependencies = [
]

[build-system]
requires = ["poetry-core>=2.0.0,<3.0.0"]
build-backend = "poetry.core.masonry.api"

Do you confirm generation? (yes/no) [yes]
amar@ubuntu:~/Desktop/SSD-Labs/lab2$
```

1.1. Bandit

- let's install **bandit**:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry add --dev bandit
Creating virtualenv lab2-Bc5w-_K2-py3.12 in /home/ammar/.cache/pypoetry/virtualenvs
Using version ^1.8.3 for bandit

Updating dependencies
Resolving dependencies... (3.0s)

Package operations: 9 installs, 0 updates, 0 removals

- Installing mdurl (0.1.2)
- Installing setuptools (75.8.2)
- Installing markdown-it-py (3.0.0)
- Installing pbr (6.1.1)
- Installing pygments (2.19.1)
- Installing pyyaml (6.0.2)
- Installing rich (13.9.4)
- Installing stevedore (5.4.1)
- Installing bandit (1.8.3)
```

- Writing lock file

- let's clone the provided **vulpy** repo:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ git clone https://github.com/fportantier/vulpy.git
Cloning into 'vulpy'...
remote: Enumerating objects: 437, done.
remote: Total 437 (delta 0), reused 0 (delta 0), pack-reused 437 (from 1)
Receiving objects: 100% (437/437), 2.90 MiB | 960.00 KiB/s, done.
Resolving deltas: 100% (223/223), done.
```

- Resolving deltas: 100% (223/223), done.
- let's run **bandit** against the cloned repo:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry run bandit -r vulpy/
[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 3.12.7
Working... ━━━━━━━━━━━━━━━━ 100% 0:00:00
Run started:2025-03-04 01:26:33.037789

Test results:
>> 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_list.py:10:8
9
10      r = requests.get('http://127.0.1.1:5000/api/post/{}'.format(username))
11      if r.status_code != 200:

-----
>> Issue: [B108:hardcoded_tmp_directory] Probable insecure usage of temp file/directory.
  Severity: Medium  Confidence: Medium
  CWE: CWE-377 (https://cwe.mitre.org/data/definitions/377.html)
  More Info: https://bandit.readthedocs.io/en/1.8.3/plugins/b108\_hardcoded\_tmp\_directory.html
  Location: vulpy/bad/api_post.py:6:20
5
6      api_key_file = Path('/tmp/supersecret.txt')
7

-----
>> 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:16:12
15
```

- findings:

- high severity finding:

```

>> 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/good/vulpy.py:53:0

52
53     app.run(debug=True, host='127.0.1.1', port=5001, extra_files='csp.txt')
54

```

- explanation:

A Flask app is being run with `debug=True`, which enables the Werkzeug debugger. This exposes the app to potential security risks, as the debugger allows arbitrary code execution if an attacker gains access to it. Moreover it provides detailed error messages and stack traces, which can reveal sensitive information about the application.

- relevant CWE:

- CWE-94: Improper Control of Generation of Code ('Code Injection')

- possible mitigation:

- disable debug mode in production

- medium severity finding:

```

>> Issue: [B108:hardcoded_tmp_directory] Probable insecure usage of temp file/directory.
Severity: Medium Confidence: Medium
CWE: CWE-377 (https://cwe.mitre.org/data/definitions/377.html)
More Info: https://bandit.readthedocs.io/en/1.8.3/plugins/b108\_hardcoded\_tmp\_directory.html
Location: vulpy/utils/ca-create.py:31:10

30
31     with open('/tmp/ca.key', 'wb') as out:
32         out.write(pem_private)

```

- explanation:

The code uses a hardcoded temporary directory (`/tmp/ca.key`), which can lead to insecure file handling.

- relevant CWE:

- CWE-377: Insecure Temporary File

- possible mitigation:

- using Python's tempfile module to create secure temporary files

- low severity finding:

```

>> Issue: [B105:hardcoded_password_string] Possible hardcoded password: '123aa8a93bdde342c871564a62282af857bda14b3359fde95d0c5e4b321610c1'
Severity: Low Confidence: Medium
CWE: CWE-259 (https://cwe.mitre.org/data/definitions/259.html)
More Info: https://bandit.readthedocs.io/en/1.8.3/plugins/b105\_hardcoded\_password\_string.html
Location: vulpy/good/vulpy.py:17:11

16     app = Flask('vulpy')
17     app.config['SECRET_KEY'] = '123aa8a93bdde342c871564a62282af857bda14b3359fde95d0c5e4b321610c1'
18

```

- explanation: The code contains a hardcoded password or secret key

(`123aa8a93bdde342c871564a62282af857bda14b3359fde95d0c5e4b321610c1`) which could be exposed to anyone with access to the codebase. Moreover, it makes it difficult to update the secret without redeploying the whole application.

- relevant CWE:

- CWE-259: Use of Hard-Coded Password

- possible mitigation:
 - Using environment variables to store secrets

1.2. Flawfinder (C)

- let's install **flawfinder**:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry add --dev flawfinder
Using version ^2.0.19 for flawfinder

Updating dependencies
Resolving dependencies... (0.7s)

Package operations: 1 install, 0 updates, 0 removals

- Installing flawfinder (2.0.19)

Writing lock file
```

- let's clone the provided repo:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ git clone https://github.com/hardik05/Damn_Vulnerable_C_Program.git
Cloning into 'Damn_Vulnerable_C_Program'...
remote: Enumerating objects: 1562, done.
remote: Counting objects: 100% (127/127), done.
remote: Compressing objects: 100% (48/48), done.
remote: Total 1562 (delta 114), reused 79 (delta 79), pack-reused 1435 (from 2)
Receiving objects: 100% (1562/1562), 67.11 MiB | 4.21 MiB/s, done.
Resolving deltas: 100% (705/705), done.
Updating files: 100% (1916/1916), done.
```

- let's run **flawfinder** against the cloned repo:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry run flawfinder Damn_Vulnerable_C_Program/
Flawfinder version 2.0.19, (C) 2001-2019 David A. Wheeler.
Number of rules (primarily dangerous function names) in C/C++ ruleset: 222
Examining Damn_Vulnerable_C_Program/dvcp.c
Warning: Skipping directory with initial dot Damn_Vulnerable_C_Program/.github
Examining Damn_Vulnerable_C_Program/imgRead.c
Examining Damn_Vulnerable_C_Program/linux/imgRead.c
Examining Damn_Vulnerable_C_Program/linux/imgRead_socket.c
Examining Damn_Vulnerable_C_Program/linux/Damn_Vulnerable_C.lib/imgReadlib.c
Examining Damn_Vulnerable_C_Program/linux/Damn_Vulnerable_C.lib/imgRead.c
Examining Damn_Vulnerable_C_Program/linux/Damn_Vulnerable_C.lib/imgReadlib.h
Examining Damn_Vulnerable_C_Program/linux/imgRead_libfuzzer.c
Warning: Skipping directory with initial dot Damn_Vulnerable_C_Program/.git
Warning: Skipping directory with initial dot Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_git/target/release/.fingerprint
Examining Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_git/imgRead.c
Examining Damn_Vulnerable_C_Program/libAFL/libafl_forkserver_fuzzer/imgRead.c
Warning: Skipping directory with initial dot Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_shmem/target/release/.fingerprint
Examining Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_shmem/imgRead.c
Examining Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_shmem/imgRead_replication.c
Examining Damn_Vulnerable_C_Program/windows/WindowsDLL/DamnVulnerableHeader.h
Examining Damn_Vulnerable_C_Program/windows/HarnessForWindowsDLL/dllTest2/dllTest2.cpp
Examining Damn_Vulnerable_C_Program/windows/HarnessForWindowsDLL/dllTest2/DamnVulnerableHeader.h
Examining Damn_Vulnerable_C_Program/dvcp_patched.c

FINAL RESULTS:

Damn_Vulnerable_C_Program/dvcp.c:16: [2] (buffer) char:
  Statically-sized arrays can be improperly restricted, leading to potential
  overflows or other issues (CWE-119!/CWE-120). Perform bounds checking, use
  functions that limit length, or ensure that the size is larger than the
  maximum possible length.
Damn_Vulnerable_C_Program/dvcp.c:19: [2] (buffer) char:
  Statically-sized arrays can be improperly restricted, leading to potential
  overflows or other issues (CWE-119!/CWE-120). Perform bounds checking, use
  functions that limit length, or ensure that the size is larger than the
  maximum possible length.
Damn_Vulnerable_C_Program/dvcp.c:23: [2] (buffer) char:
  Statically-sized arrays can be improperly restricted, leading to potential
  overflows or other issues (CWE-119!/CWE-120). Perform bounds checking, use
  functions that limit length, or ensure that the size is larger than the
  maximum possible length.
```

- findings:

- level 1:

```
Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_shmem/imgRead.c:35: [1] (buffer) strlen:
  Does not handle strings that are not \0-terminated; if given one it may
    perform an over-read (it could cause a crash if unprotected) (CWE-126).
```

- explanation: The **strlen** function is used on a string that may not be null-terminated (**\0**). If the string is not null-terminated, **strlen** will continue reading memory beyond the

intended boundary, leading to an over-read.

- relevant CWE: CWE-126: Buffer Over-read
- possible mitigation: Ensure that all strings passed to strlen are properly null-terminated.

- level 2:

```
terminal 1: ./imgRead socket.c:131: [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 from a source to a destination buffer without checking if the destination buffer is large enough to hold the data. This can lead to a buffer overflow.
- relevant CWE: CWE-120: Buffer Copy without Checking Size of Input
- possible mitigation: Always validate the size of the source and destination buffers before using `memcpy`.

- level 3:

- no such finding was found.

- **False positive:**

- considering the following finding:

- Damn_Vulnerable_C_Program/libAFL/damn_vulnerable_c_program_shmem/imgRead.c:35: [1] (buffer) strlen:
Does not handle strings that are not \0-terminated; if given one it may
perform an over-read (it could cause a crash if unprotected)
(CWE-126).

- let's check the file:

```
terminal Help
report.md u c imgRead.c
lab2 > Damn_Vulnerable_C_Program > libAFL > damn_vulnerable_c_program_shmem > C imgRead.c
19 {
20
21
22
23
24
25
26
27 int ProcessImage(char* filename){
28     FILE *fp;
29     char ch;
30     struct Image* img;
31     int bufsize;
32
33     //shared memory data will be inside buff
34     unsigned char *shmem_buf = __AFL_FUZZ_TESTCASE_BUF;
35     bufsize =strlen(shmem_buf); |
36     if(bufsize<=12){
37         return 0;
38     }
39     img = (struct Image*)shmem_buf;
40     printf("input: %s\n", shmem_buf);
41
42
43 //integer overflow 0xFFFFFFFF+1=0
44 //0xCCCCCCCC? - 1
```

- we can consider it as a false positive **only if** it's always guaranteed that the fuzzer will provide `null terminated strings` to `__AFL_FUZZ_TESTCASE_BUF`, which is a shared memory buffer used for fuzzing

1.3. njsscan

- let's install `njsscan` (after suffering with fixing versions issues and some broken packages):

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ poetry add --dev njsscan
Using version ^0.4.3 for njsscan

Updating dependencies
Resolving dependencies... (2.3s)

Package operations: 24 installs, 0 updates, 0 removals

- Installing opentelemetry-instrumentation (0.46b0)
- Installing opentelemetry-util-http (0.46b0)
- Installing billiard (4.2.1)
- Installing click-option-group (0.5.6)
- Installing colorama (0.4.6)
- Installing defusedxml (0.7.1)
- Installing exceptiongroup (1.2.2)
- Installing glom (22.1.0)
- Installing jsonpickle (4.0.2)
- Installing jsonschema (4.23.0)
- Installing opentelemetry-exporter-otlp-proto-http (1.25.0)
- Installing opentelemetry-instrumentation-requests (0.46b0)
- Installing packaging (24.2)
- Installing peewee (3.17.9)
- Installing pydantic (2.8.2)
- Installing ruamel-yaml (0.17.40)
- Installing tomli (2.0.2)
- Installing wcmatch (8.5.2)
- Installing jschema-to-python (1.2.3)
- Installing libsast (3.1.6)
- Installing sarif-om (1.0.4)
- Installing semgrep (1.86.0)
- Installing tabulate (0.9.0)
- Installing njsscan (0.4.3)
```

- Writing lock file

- let's clone the provided repo:

```
ammar@ubuntu:~/Desktop/SSD-Labs/lab2$ git clone https://github.com/appsecco/dvna.git
Cloning into 'dvna'...
remote: Enumerating objects: 645, done.
remote: Total 645 (delta 0), reused 0 (delta 0), pack-reused 645 (from 1)
Receiving objects: 100% (645/645), 3.18 MiB | 2.17 MiB/s, done.
Resolving deltas: 100% (281/281), done.
```

- let's run njsscan against the cloned repo:

ammar@ubuntu:~/Desktop/SSD-Labs/lab2\$ poetry run njsscan dvna/	148														
- Pattern Match	148														
- Semantic Grep	29														
njsscan: v0.4.3 Ajin Abraham opensecurity.in															
RULE ID	ejs_ect_template														
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')														
OWASP-WEB	A1: Injection														
DESCRIPTION	The EJS/ECT template has an unescaped variable. Untrusted user input passed to this variable results in Cross Site Scripting (XSS).														
SEVERITY	ERROR														
FILES	<table border="1"> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>1907 - 1937</td></tr> <tr> <td>Line Number(s)</td><td>51</td></tr> <tr> <td>Match String</td><td><%- output.products[i].code %></td></tr> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>2019 - 2056</td></tr> <tr> <td>Line Number(s)</td><td>53</td></tr> </table>	File	dvna/views/app/products.ejs	Match Position	1907 - 1937	Line Number(s)	51	Match String	<%- output.products[i].code %>	File	dvna/views/app/products.ejs	Match Position	2019 - 2056	Line Number(s)	53
File	dvna/views/app/products.ejs														
Match Position	1907 - 1937														
Line Number(s)	51														
Match String	<%- output.products[i].code %>														
File	dvna/views/app/products.ejs														
Match Position	2019 - 2056														
Line Number(s)	53														

- findings:

- Error:

RULE ID	ejs_ect_template																																																
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')																																																
OWASP-HEB	A1: Injection																																																
DESCRIPTION	The EJS/ECT template has an unescaped variable. Untrusted user input passed to this variable results in Cross Site Scripting (XSS).																																																
SEVERITY	ERROR																																																
FILES	<table border="1"> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>1907 - 1937</td></tr> <tr> <td>Line Number(s)</td><td>51</td></tr> <tr> <td>Match String</td><td><%- output.products[i].code %></td></tr> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>2019 - 2056</td></tr> <tr> <td>Line Number(s)</td><td>53</td></tr> <tr> <td>Match String</td><td><%- output.products[i].description %></td></tr> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>1797 - 1825</td></tr> <tr> <td>Line Number(s)</td><td>49</td></tr> <tr> <td>Match String</td><td><%- output.products[i].id %></td></tr> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>1851 - 1881</td></tr> <tr> <td>Line Number(s)</td><td>50</td></tr> <tr> <td>Match String</td><td><%- output.products[i].name %></td></tr> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>1963 - 1993</td></tr> <tr> <td>Line Number(s)</td><td>52</td></tr> <tr> <td>Match String</td><td><%- output.products[i].tags %></td></tr> <tr> <td>File</td><td>dvna/views/app/products.ejs</td></tr> <tr> <td>Match Position</td><td>721 - 745</td></tr> <tr> <td>Line Number(s)</td><td>20</td></tr> <tr> <td>Match String</td><td><%- output.searchTerm %></td></tr> </table>	File	dvna/views/app/products.ejs	Match Position	1907 - 1937	Line Number(s)	51	Match String	<%- output.products[i].code %>	File	dvna/views/app/products.ejs	Match Position	2019 - 2056	Line Number(s)	53	Match String	<%- output.products[i].description %>	File	dvna/views/app/products.ejs	Match Position	1797 - 1825	Line Number(s)	49	Match String	<%- output.products[i].id %>	File	dvna/views/app/products.ejs	Match Position	1851 - 1881	Line Number(s)	50	Match String	<%- output.products[i].name %>	File	dvna/views/app/products.ejs	Match Position	1963 - 1993	Line Number(s)	52	Match String	<%- output.products[i].tags %>	File	dvna/views/app/products.ejs	Match Position	721 - 745	Line Number(s)	20	Match String	<%- output.searchTerm %>
File	dvna/views/app/products.ejs																																																
Match Position	1907 - 1937																																																
Line Number(s)	51																																																
Match String	<%- output.products[i].code %>																																																
File	dvna/views/app/products.ejs																																																
Match Position	2019 - 2056																																																
Line Number(s)	53																																																
Match String	<%- output.products[i].description %>																																																
File	dvna/views/app/products.ejs																																																
Match Position	1797 - 1825																																																
Line Number(s)	49																																																
Match String	<%- output.products[i].id %>																																																
File	dvna/views/app/products.ejs																																																
Match Position	1851 - 1881																																																
Line Number(s)	50																																																
Match String	<%- output.products[i].name %>																																																
File	dvna/views/app/products.ejs																																																
Match Position	1963 - 1993																																																
Line Number(s)	52																																																
Match String	<%- output.products[i].tags %>																																																
File	dvna/views/app/products.ejs																																																
Match Position	721 - 745																																																
Line Number(s)	20																																																
Match String	<%- output.searchTerm %>																																																

- explanation: The <%- %> syntax in EJS directly injects data into HTML without escaping it, which makes the application vulnerable to XSS. If an attacker can manipulate `output.products[i].name` or any other variable, they could inject malicious JavaScript into the webpage.
- relevant CWE: CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting).
- possible mitigation:

Using `<%= %>` instead of `<%- %>` to automatically escape user input.

- o Warning:

RULE ID	sequelize_tls								
CWE	CWE-319: Cleartext Transmission of Sensitive Information								
OWASP-WEB	A6: Security Misconfiguration								
DESCRIPTION	The Sequelize connection string indicates that database server does not use TLS. Non TLS connections are susceptible to man in the middle (MITM) attacks.								
SEVERITY	WARNING								
FILES	<table border="1"> <tr> <td>File</td> <td>dvna/config/db.js</td> </tr> <tr> <td>Match Position</td> <td>18 - 2</td> </tr> <tr> <td>Line Number(s)</td> <td>1: 8</td> </tr> <tr> <td>Match String</td> <td> <pre>module.exports = { username: process.env.MYSQL_USER, password: process.env.MYSQL_PASSWORD, database: process.env.MYSQL_DATABASE, host: process.env.MYSQL_HOST 'mysql-db', port: process.env.MYSQL_PORT 3306, dialect: 'mysql' }</pre> </td> </tr> </table>	File	dvna/config/db.js	Match Position	18 - 2	Line Number(s)	1: 8	Match String	<pre>module.exports = { username: process.env.MYSQL_USER, password: process.env.MYSQL_PASSWORD, database: process.env.MYSQL_DATABASE, host: process.env.MYSQL_HOST 'mysql-db', port: process.env.MYSQL_PORT 3306, dialect: 'mysql' }</pre>
File	dvna/config/db.js								
Match Position	18 - 2								
Line Number(s)	1: 8								
Match String	<pre>module.exports = { username: process.env.MYSQL_USER, password: process.env.MYSQL_PASSWORD, database: process.env.MYSQL_DATABASE, host: process.env.MYSQL_HOST 'mysql-db', port: process.env.MYSQL_PORT 3306, dialect: 'mysql' }</pre>								

- explanation: The database connection is not using TLS, making it vulnerable to Man-in-the-Middle (MITM) attacks. This means an attacker could intercept credentials and queries.
- relevant CWE: CWE-319: Cleartext Transmission of Sensitive Information.
- possible mitigation: Enabling TLS in the Sequelize configuration.

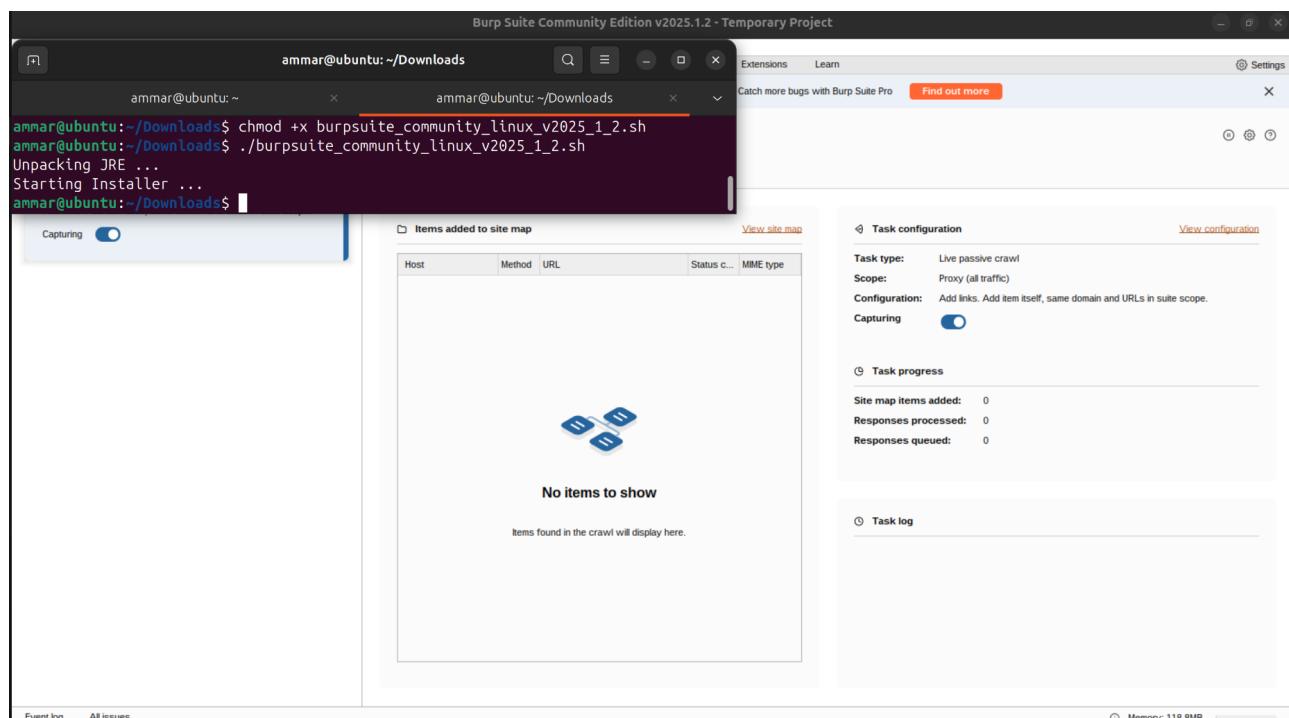
- Info:

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> <pre>app.use(session({ secret: 'keyboard cat', resave: true, saveUninitialized: true, cookie: { secure: false } }))</pre> </td> </tr> </table>	File	dvna/server.js	Match Position	9 - 3	Line Number(s)	23: 28	Match String	<pre>app.use(session({ secret: 'keyboard cat', resave: true, saveUninitialized: true, cookie: { secure: false } }))</pre>
File	dvna/server.js								
Match Position	9 - 3								
Line Number(s)	23: 28								
Match String	<pre>app.use(session({ secret: 'keyboard cat', resave: true, saveUninitialized: true, cookie: { secure: false } }))</pre>								

- explanation: The default session configuration is used, which includes secret **keyboard cat**. Attackers can fingerprint the application and potentially hijack sessions.
- relevant CWE: CWE-522: Insufficiently Protected Credentials
- possible mitigation: Changing the default session secret to a strong, random value. In addition, setting **cookie: { secure: true }** to ensure cookies are only sent over HTTPS.

Task2:

- let's install and run **burp**:



Burp Suite Community Edition v2025.1.2 - Temporary Project

ammar@ubuntu: ~/Downloads

```
ammar@ubuntu:~/Downloads$ chmod +x burpsuite_community_linux_v2025_1_2.sh
ammar@ubuntu:~/Downloads$ ./burpsuite_community_linux_v2025_1_2.sh
Unpacking JRE ...
Starting Installer ...
ammar@ubuntu:~/Downloads$
```

Capturing

Items added to site map View site map

Host	Method	URL	Status c...	MIME type
No items to show				

Items found in the crawl will display here.

Task configuration

Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same domain and URLs in suite scope.
Capturing

Task progress

Site map items added: 0
Responses processed: 0
Responses queued: 0

Task log

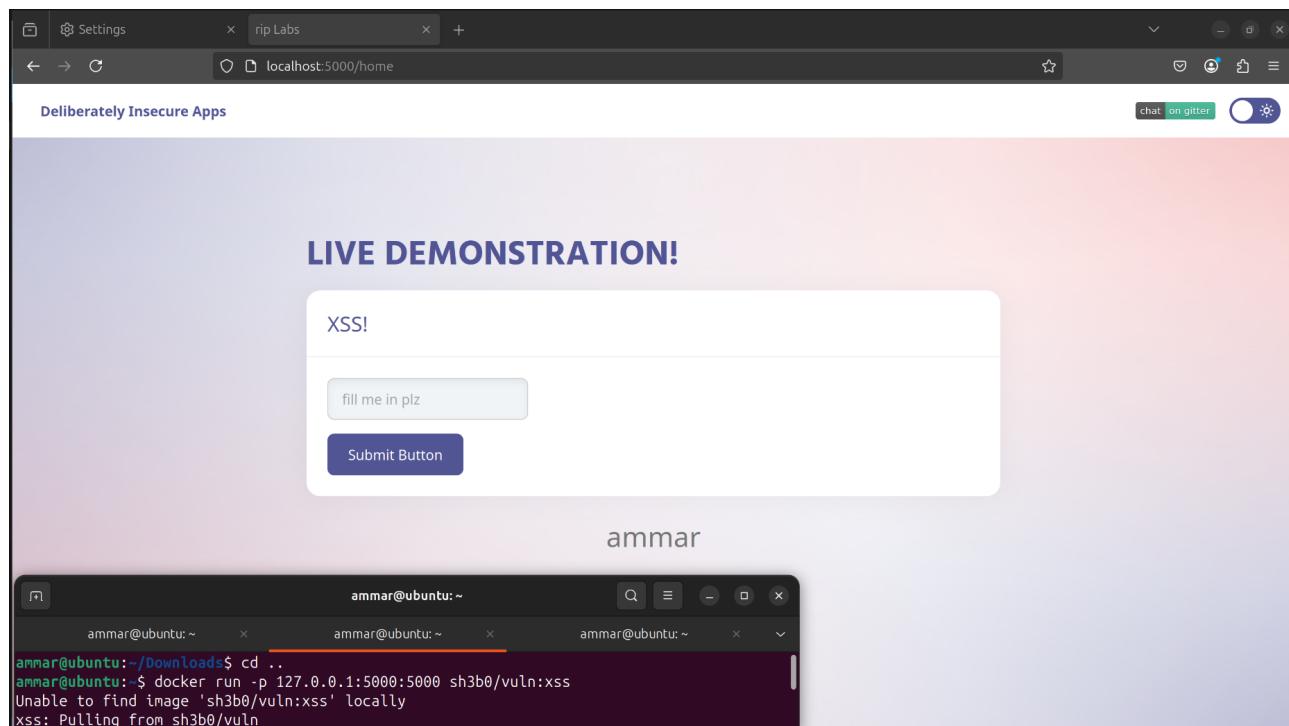
Event log All issues Memory: 118.8MB

- then let's install firefox and set the proxy to `127.0.0.1:8080` to interact with `burp` (because i use `chromium`)
- **note:** it was **painful** to find out that this little stupid flag `network.proxy.allow_hijacking_localhost` should be toggled to allow capturing the localhost

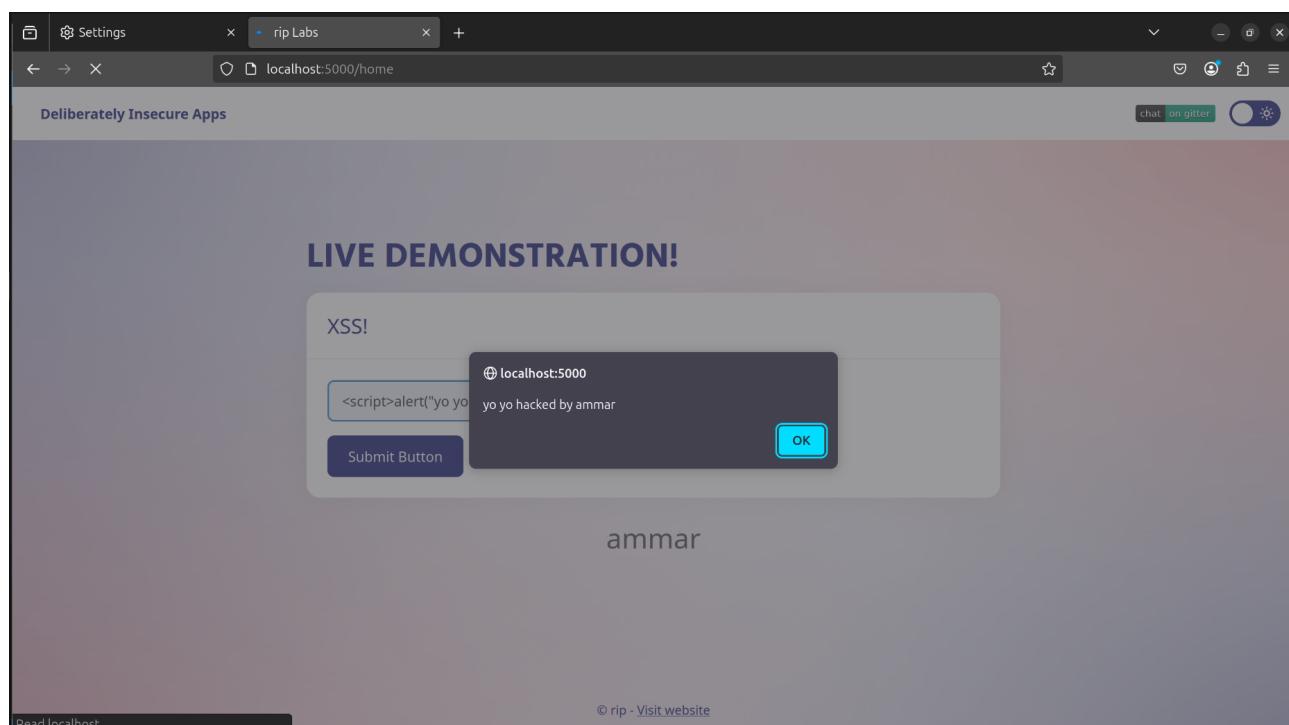


Cross Site Scripting

- let's pull and run the docker image:



- after some tries, let's try to insert :



- XSS is found!
- when i find XSS, me for no reason:

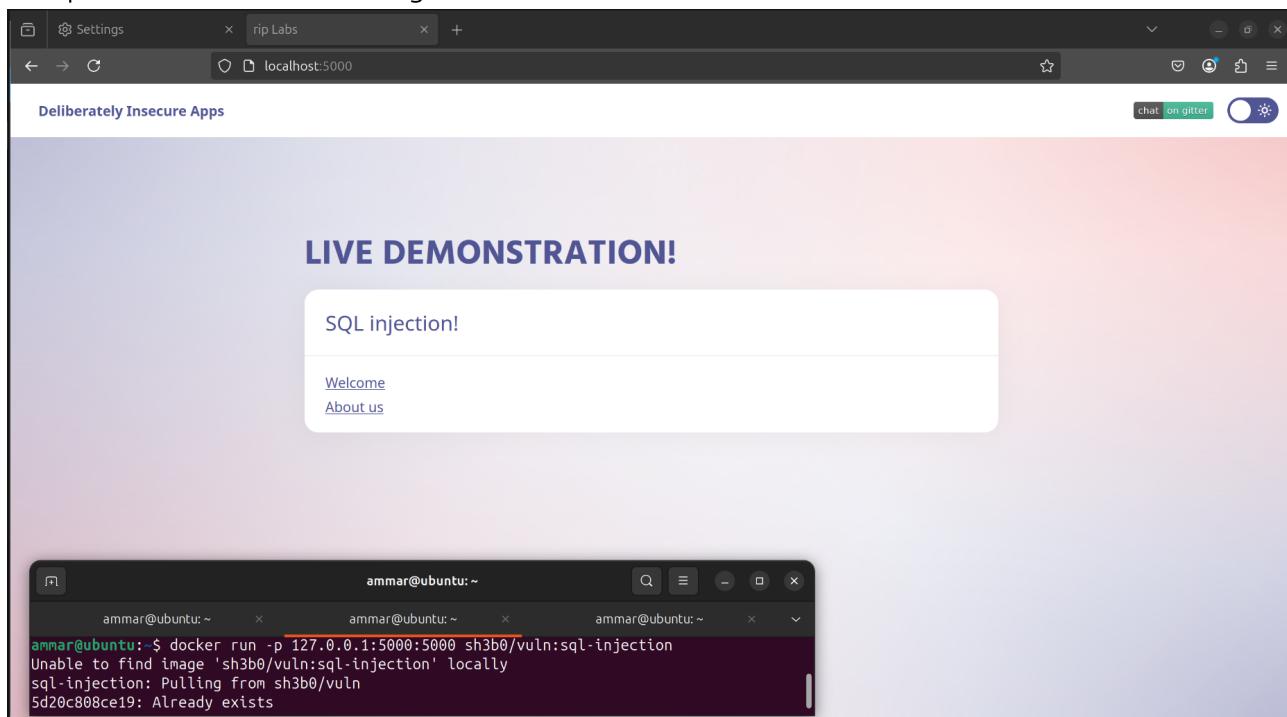


- why it's dangerous? there are a lot of reasons (like a lot!), one of them that it allows attackers to hijack cookies sessions, personal information, or login credentials
- possible mitigation:

to prevent XSS vulnerabilities, we need to ensure that user input is properly sanitized, validated, and escaped before it is rendered in the browser

SQL Injection

- let's pull and run the docker image:



- let's try to insert a ' in the url:

```

    return self.view_functions[rule.endpoint](**req.view_args)
File "/home/app/SQLI/SQLI.py", line 19, in inject
    values = sqli.getPage(pageId)
File "/home/app/SQLI/models/sqlimodel.py", line 7, in getPage
    class Pages:
        def getPage(self, pageId):
            db = database_con()
            cur = db.execute('SELECT pageId, title, content FROM pages WHERE pageId=' + pageId)
            return cur.fetchall()
sqlite3.OperationalError: unrecognized token: ""

```

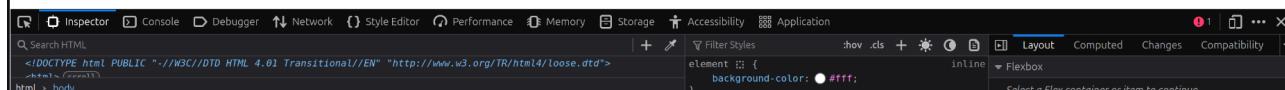
The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.

To switch between the interactive traceback and the plaintext one, you can click on the "Traceback" headline. From the text traceback you can also create a paste of it. For code execution mouse-over the frame you want to debug and click on the console icon on the right side.

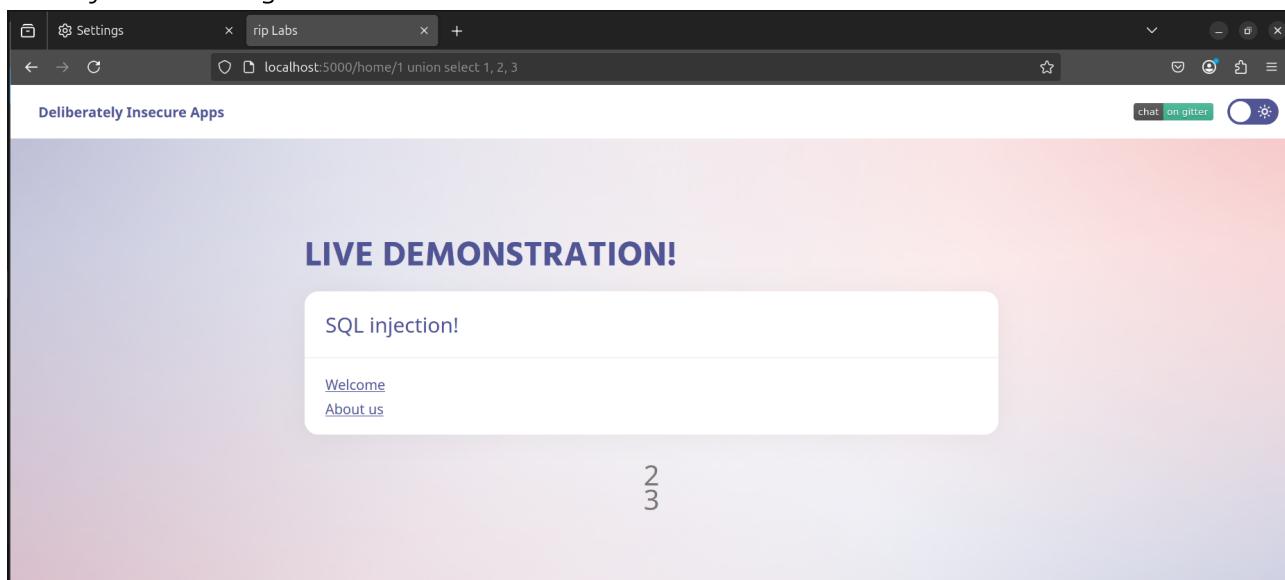
You can execute arbitrary Python code in the stack frames and there are some extra helpers available for introspection:

- `dump()` shows all variables in the frame
- `dump(obj)` dumps all that's known about the object

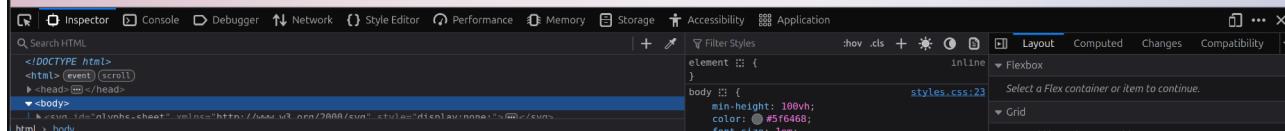
Brought to you by DON'T PANIC, your friendly Werkzeug powered traceback interpreter.



- a good start! now we know that we are dealing with 3 columns
- let's try the following:



2
3



- so `title` and `content` became placeholders for data
- let's try the following by trying some guesses for the users table (user, users, ...):
- found the correct table name, `users`, now let's append `union select * from users`

LIVE DEMONSTRATION!

SQL injection!

Welcome

About us

Admin
0cef1fb10f60529028a71f58e54ed07b

Developer Tools (CSS Inspector):

```

<!DOCTYPE html>
<html> <event scroll>
  <head></head>
  <body>
    <!-- Content -->
    <!-- Vulnerable code -->
    <!-- Exploit -->
</html>

```

Element styles:

```

element :: {
}

```

body :: {
 min-height: 100vh;
 color: #5f6468;
 font-size: 1em;
}

Computed styles:

```

Select a Flex container or item to continue.

```

Layout tab selected.

- we got the usernmae and password of the admin hehe
- why it's dangerous? for many reasons, for example attackers can extract sensitive data such as usernames, passwords, credit card numbers, and personal information from the database
- possible mitigation: using parameterized queries to separate SQL code from user input, preventing attackers from injecting malicious SQL

Path Traversal

- let's pull and run the docker image:

Not Found

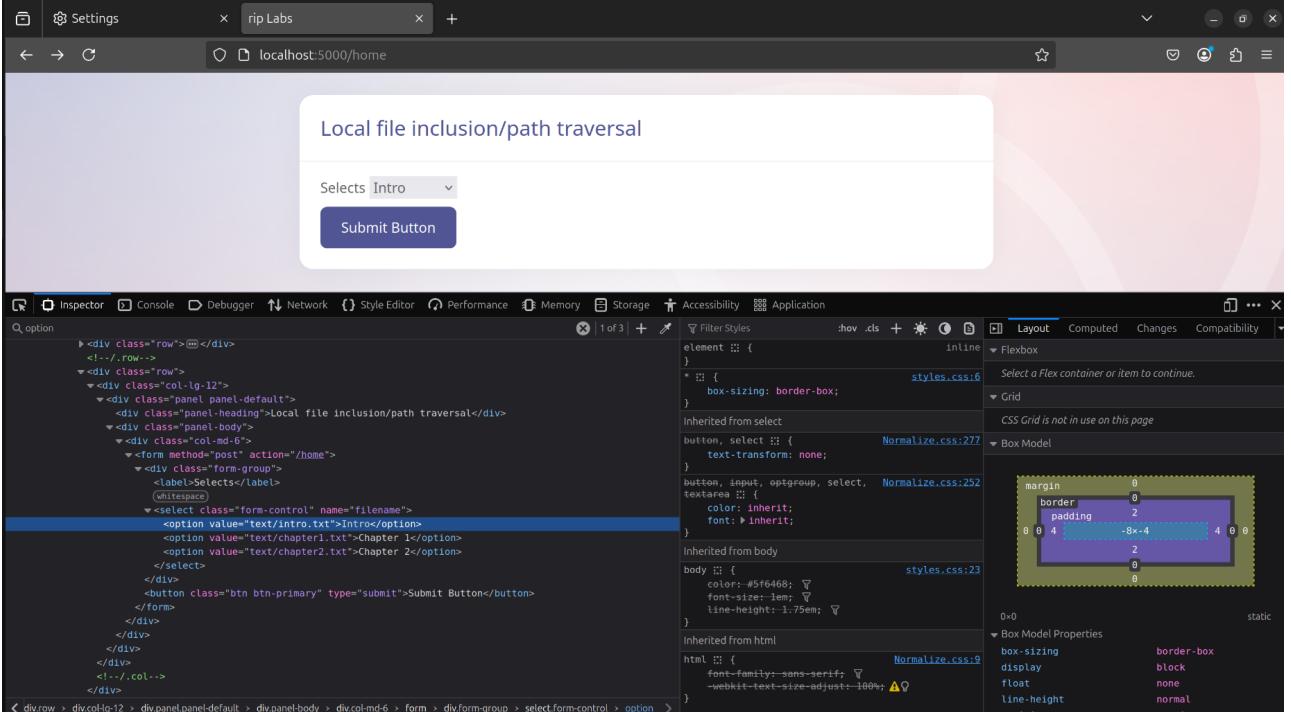
The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

```

ammar@ubuntu:~$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:path-traversal
^Camar@ubuntu:~$ docker run -p 127.0.0.1:5000:5000 sh3b0/vuln:path-traversal
Unlable to find image 'sh3b0/vuln:path-traversal' locally
path-traversal: Pulling from sh3b0/vuln
5d20c808ce19: Already exists
53879ca88737: Already exists
05f42fd8906f: Already exists

```

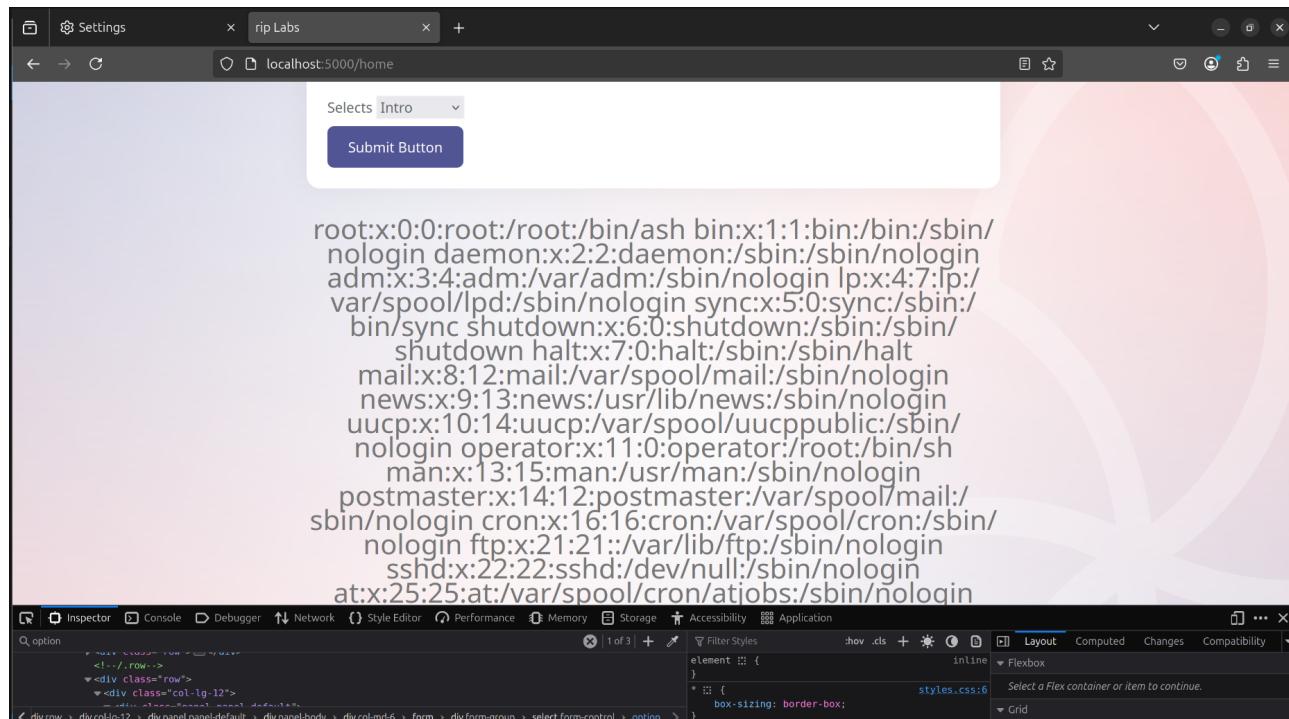
- after we inspect the page, we can see that each option is a path for a file in the system



The screenshot shows a web browser window with the URL `localhost:5000/home`. The page title is "Local file inclusion/path traversal". A dropdown menu is open, showing "Selects Intro" and a "Submit Button" button. The browser's developer tools are open, specifically the "Inspector" tab. The "Elements" panel shows the HTML structure of the page, including a `<select>` element with three options: "Intro", "Chapter 1", and "Chapter 2". The "Elements" panel has a blue selection bar over the first option. The "Styles" panel on the right shows CSS rules for various elements, including `normalize.css` and `styles.css`. The "Box Model" section of the styles panel shows the dimensions of the selected `<option>` element: margin 0, border 0, padding 2px, width 8x4, height 4, top 0, left 0.

- after modifying the first option value to `../../../../../../../../etc/passwd` we can see:

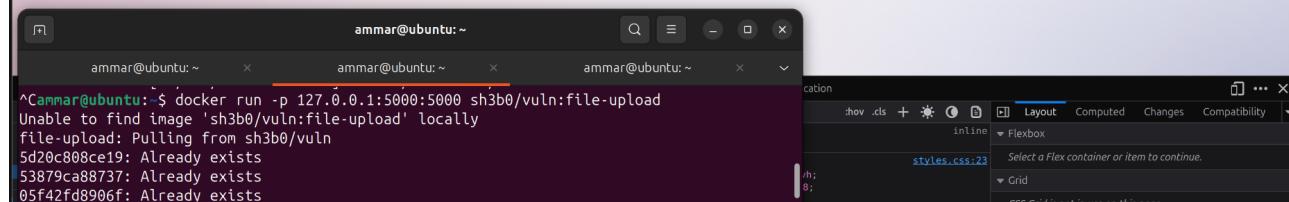
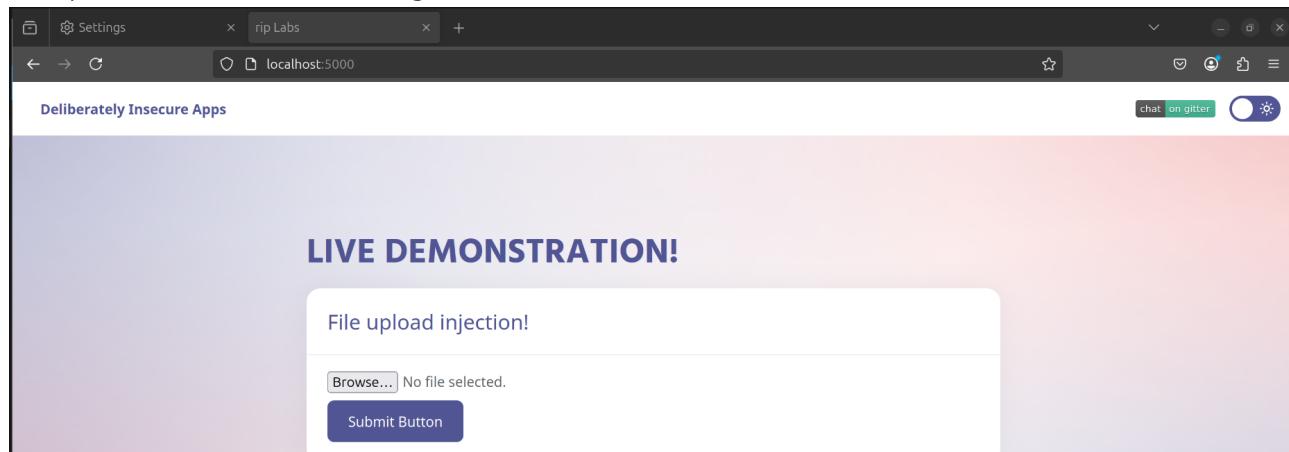




- why it's dangerous? because attackers can access sensitive files such as `/etc/passwd` (as we already did) .env, or database credentials and expose sensitive information
- possible mitigation: we need to ensure that user input is properly sanitized and validated before being used to access files

File Upload

- let's pull and run the docker image:



- let's try to upload a text file, and let's observe burp

Burp Suite Community Edition v2025.1.2 - Temporary Project

Proxy tab selected.

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
305	09:31:59 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	216	138	
306	09:31:59 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	0	200	3170	3	
307	09:31:59 4 Mar 2025	Proxy	GET	localhost	/						
308	09:31:59 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	216	133	
309	09:31:59 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	216	126	
310	09:32:02 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	298	221	
311	09:32:03 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	216	170	
312	09:32:03 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	216	170	
313	09:32:13 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	298	262	
314	09:32:13 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	216	185	
315	09:32:13 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	216	185	
316	09:32:33 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	298	156	
317	09:32:33 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	216	188	
318	09:32:33 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	216	186	
319	09:33:07 4 Mar 2025	POST	localhost	/			2	200	3187	9	
320	09:33:13 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	298	234	
321	09:33:13 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	216	189	
322	09:33:13 4 Mar 2025	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	216	186	

Request tab selected.

```

1 Content-Length: 20
2 Origin: http://localhost:5000
3 Connection: keep-alive
4 Referer: http://localhost:5000/
5 Upgrade-Insecure-Requests: 1
6 Priority: u=0, i
7 -----geckoformboundary4f6fbe57ffc434b0613818bce631607a
8 Content-Disposition: form-data; name="file"; filename="sub.txt"
9 Content-Type: text/plain
10 a.meslmani@innopolis.university
11 -----geckoformboundary4f6fbe57ffc434b0613818bce631607a-
12 Ammar Meslmani
13 CBS-01
14 a.meslmani@innopolis.university
15 -----geckoformboundary4f6fbe57ffc434b0613818bce631607a-

```

Response tab selected.

```

88 <form method="post" action="" enctype="multipart/form-data">
89   <input type="file" name="file" />
90   <br />
91   <button class="btn btn-primary" type="submit">
92     Submit Button
93   </button>
94   </div>
95   </form>
96   </div>
97   <!-- /.col-->
98   <!-- /.row -->
99   File was uploaded
100 </div>

```

Inspector tab selected.

```

Selected text
Ammar Meslmani
CBS-01
a.meslmani@innopolis.university
File was uploaded

```

- Event log (42) • All issues

- we can see that the button is performing a POST request, let's inspect this request

Burp Suite Community Edition v2025.1.2 - Temporary Project

Repeater tab selected.

Request	Response
<pre> 1 POST / HTTP/1.1 2 Host: localhost:5000 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:135.0) 4 Gecko/20100101 Firefox/135.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: multipart/form-data; 9 boundary:-----geckoformboundary4f6fbe57ffc434b0613818bce631607a 10 Content-Length: 267 11 Origin: http://localhost:5000 12 Symantec-Kernel-Page-Header 13 Referer: http://localhost:5000/ 14 Upgrade-Insecure-Requests: 1 15 Priority: u=0, i 16 -----geckoformboundary4f6fbe57ffc434b0613818bce631607a 17 Content-Disposition: form-data; name="file"; filename="sub.txt" 18 Content-Type: text/plain 19 a.meslmani@innopolis.university 20 -----geckoformboundary4f6fbe57ffc434b0613818bce631607a- </pre>	<pre> 90 <name="file" /> 91
 92 <button class="btn btn-primary" type="submit"> 93 Submit Button 94 </button> 95 </div> 96 <!-- /.col--> 97 <!-- /.row --> 98 File was uploaded 99 100 </div> 101 <!-- /.main--> 102 <!-- End Original Code --> 103 </div> 104 </section> 105 <footer class="footer"> 106 <div class="wrap wide"> 107 <div class="inner pt3 pb3 text-center"> 108 &copy; rip - <!-- rel="nofollow" href--> 109 </div> 110 </div> 111 </footer> 112 </pre>

Inspector tab selected.

```

Selected text
File was uploaded

```

- Event log (42) • All issues

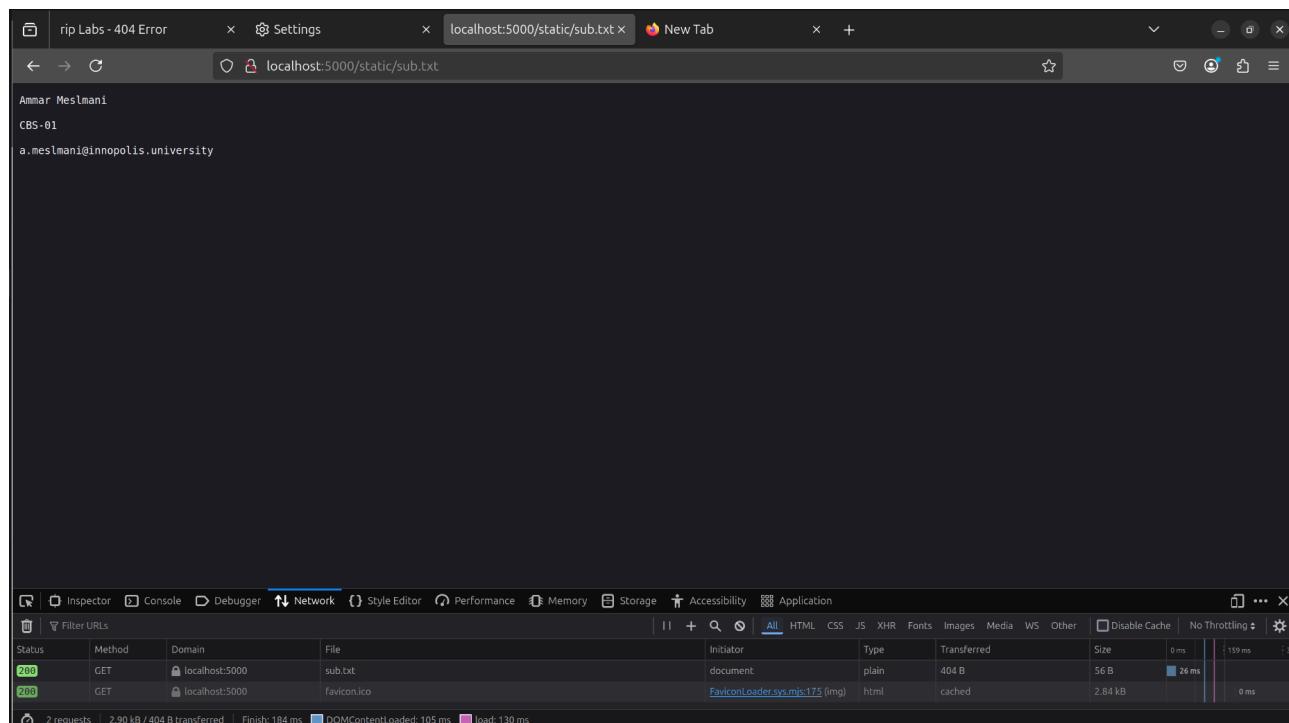
- we can see that our file got uploaded on the server, but we don't know where its location
- let's inspect the headers in the network tab

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Cache	Timings
200	GET	localhost:5000	/	document	html	3.17 kB	3.01 kB						
200	GET	localhost:5000	Normalize.css	stylesheet	css	cached	7.80 kB	GET http://localhost:5000/static/css/normalize.css					
200	GET	localhost:5000	datepicker3.css	stylesheet	css	cached	33.77 kB						
200	GET	localhost:5000	styles.css	stylesheet	css	cached	21.96 kB						
200	GET	fonts.googleapis.com	css?family=Hind:wght@700&display=swap	stylesheet	css	cached	-1 B						
200	GET	localhost:5000	lumino_glyphs.js	script	js	cached	0 B						
200	GET	localhost:5000	hints.js	script	js	cached	902 B						
200	GET	localhost:5000	jquery-3.6.0.min.js	script	js	cached	0 B						
200	GET	localhost:5000	bootstrap.min.js	script	js	cached	0 B						
200	GET	localhost:5000	Favicon.ico	FaviconLoader.sys.m...	html	cached	2.84 kB						

- we can see that there is a folder called `/static`
- let's try to repeat our request but with changing the path of the file, and let's aim to upload it to `/static` folder

Request	Response
<pre> 1 POST / HTTP/1.1 2 Host: localhost:5000 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://localhost:5000/ 8 Content-Type: multipart/form-data; boundary=----geckoformboundary4f6fbe57ffc434b0613818fce631607a 9 Content-Length: 277 10 Origin: http://localhost:5000 11 Connection: keep-alive 12 Upgrade-Insecure-Requests: 1 13 Priority: u=0, i 14 15 ----geckoformboundary4f6fbe57ffc434b0613818fce631607a 16 Content-Disposition: form-data; name="file"; filename=".../static/sub.txt" 17 Content-Type: text/plain 18 19 Amar Meslmani 20 21 CBS-01 22 23 a.meslmani@innopolis.university 24 25 ----geckoformboundary4f6fbe57ffc434b0613818fce631607a--</pre>	<pre> 72 <!-- .row--> 73 74 <div class="row"> 75 <div class="col-lg-12"> 76 <h1 class="page-header"> 77 Live demonstration! 78 </h1> 79 </div> 80 <!-- .row--> 81 82 <div class="row"> 83 <div class="col-lg-12"> 84 <div class="panel panel-default"> 85 <div class="panel-heading"> 86 File upload 87 injection! 88 </div> 89 <div class="panel-body"> 90 <form method="post" action="" enctype="multipart/form-data"> 91 <input type="file" name="file" /> 92 <button class="btn"></pre>

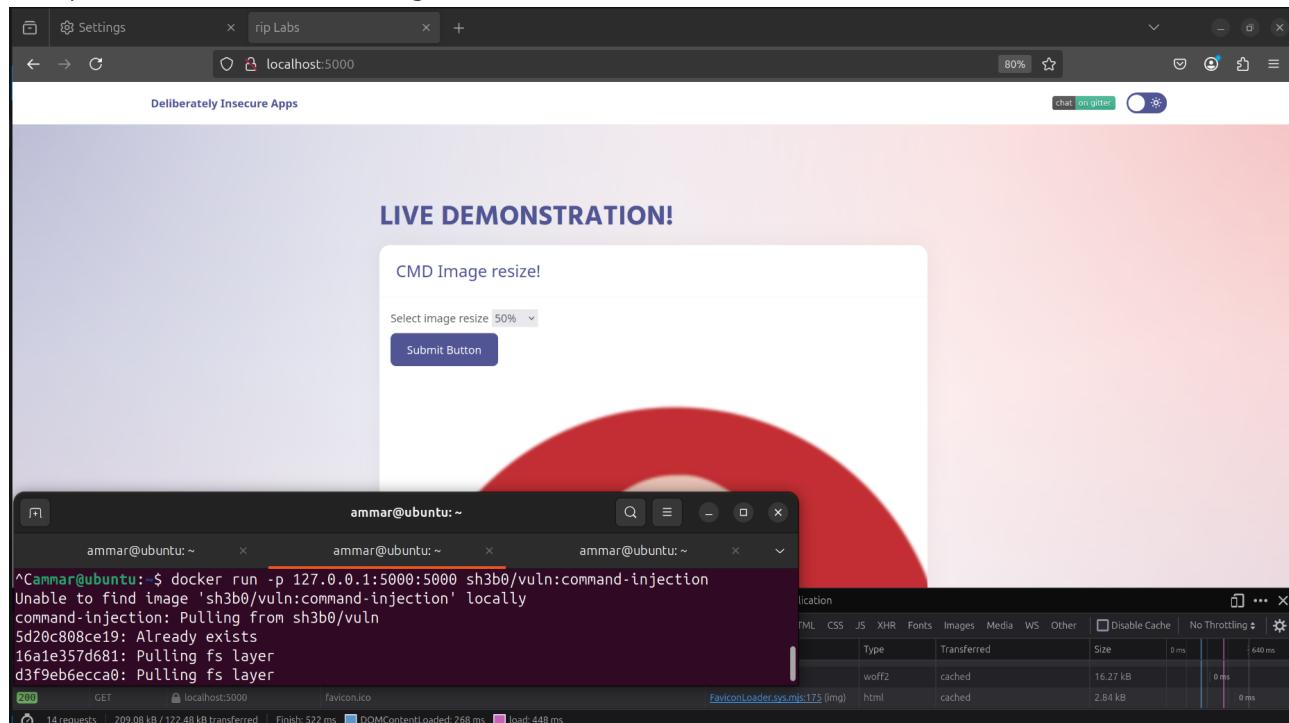
- after many trials, we succeeded!
- let's try to access the file



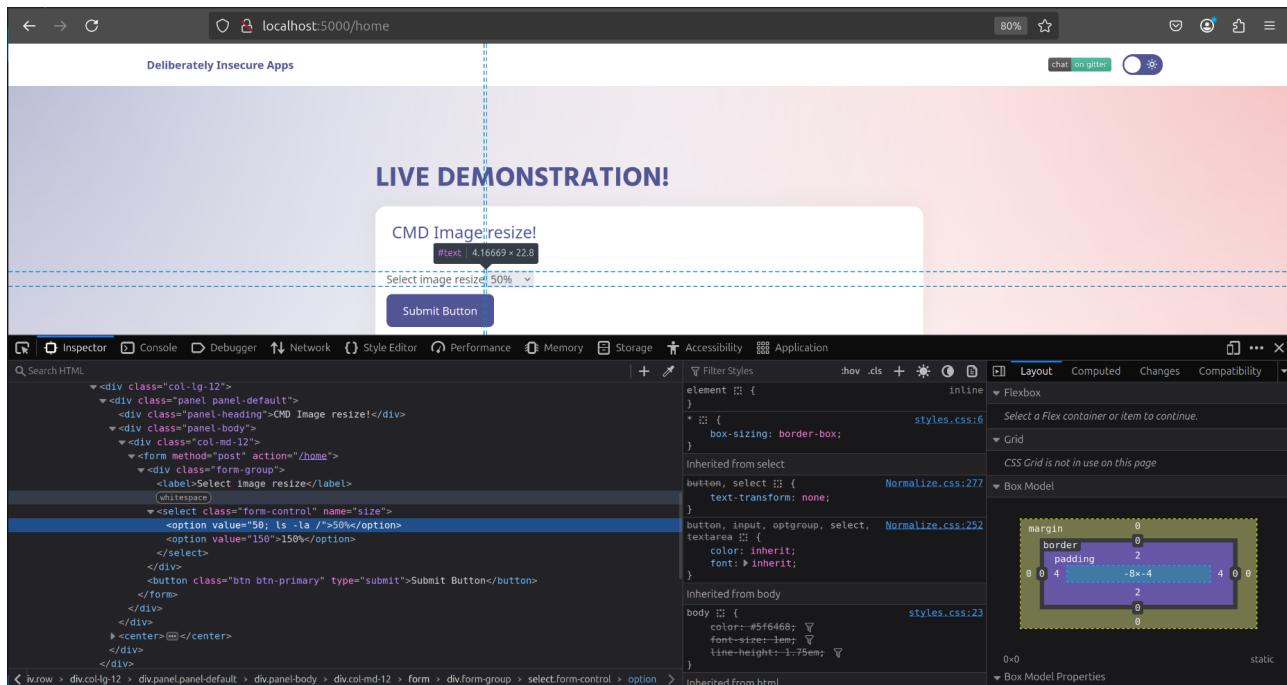
- why it's dangerous? because attackers can upload their own malicious codes and execute them on the server and cause damage or steal sensitive information, get shell access, or even perform XSS attack
- possible mitigation: the file types allowed to be uploaded should be restricted to only those that are necessary for business functionality. moreover, never accept a filename and its extension directly without having an allow list filter to avoid possible harm (for example, why a user should be able to upload a script to website of downloading and uploading images)

Command Injection

- let's pull and run the docker image:



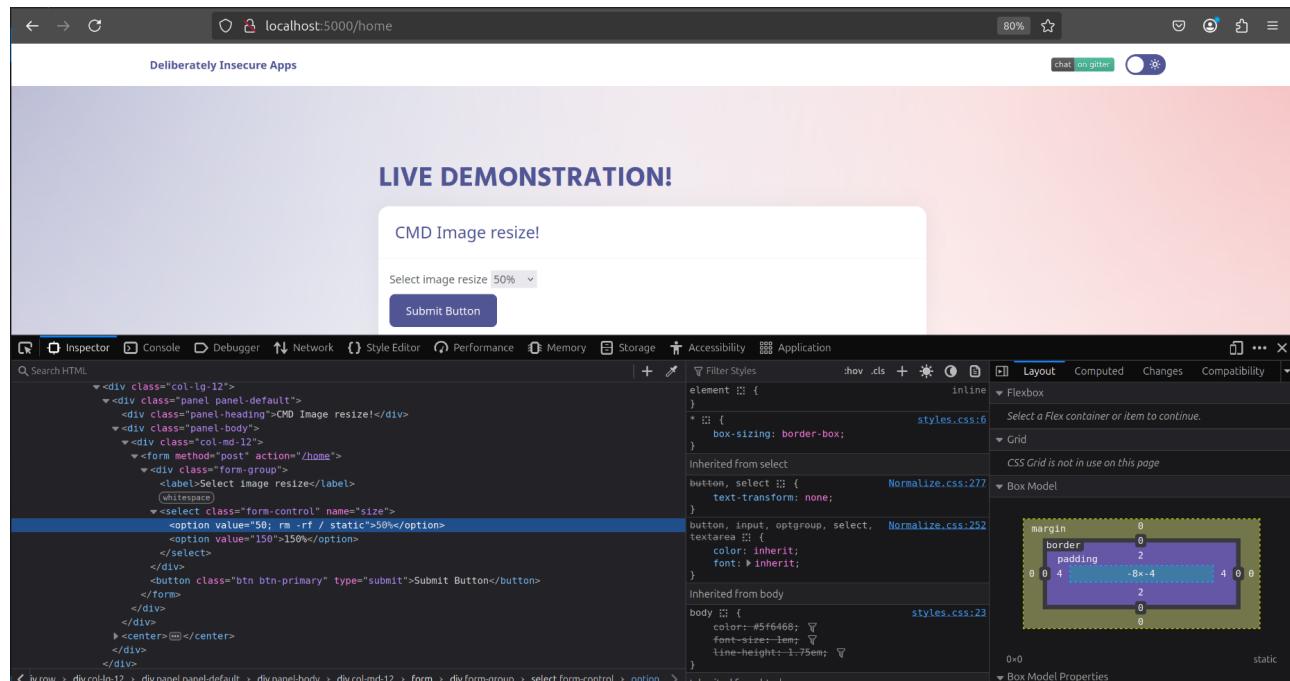
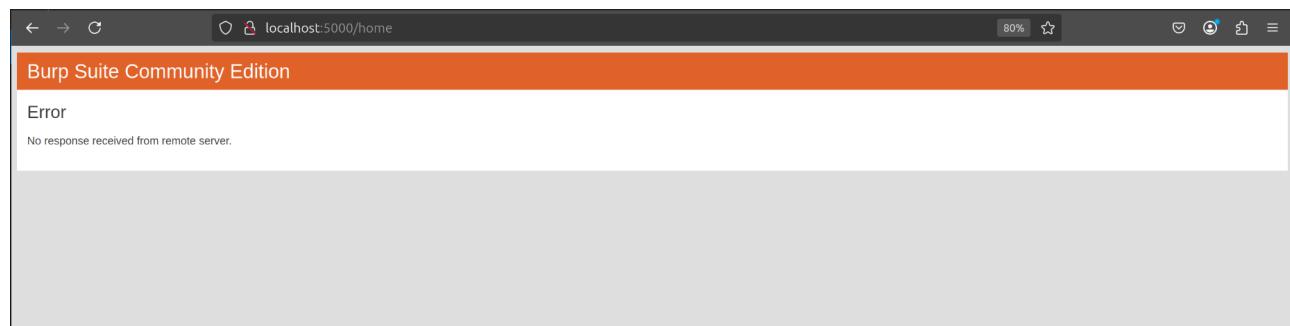
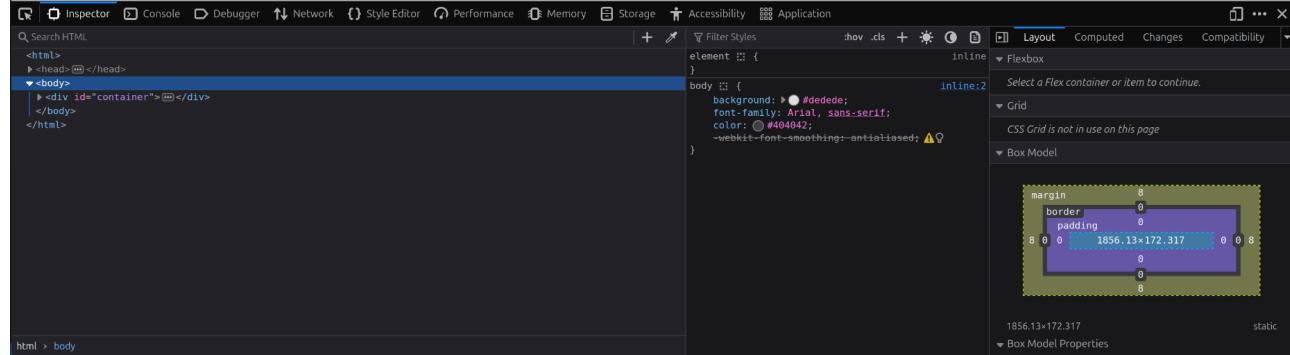
- let's try to inject the following command `50; ls -la /`:



- let's check the terminal (i executed it many times to check the correct syntax):

```
amar@ubuntu:~ 172.17.0.1 - - [04/Mar/2025 12:51:18] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
ls: /%: No such file or directory
-rw-rw-r-- 1 app app 118704 Feb 18 21:46 static/img/bones.png
172.17.0.1 - - [04/Mar/2025 12:51:37] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
sh: ls-al%: not found
172.17.0.1 - - [04/Mar/2025 12:54:40] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
sh: ls-al%: not found
172.17.0.1 - - [04/Mar/2025 12:54:59] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
sh: ls-al%: not found
172.17.0.1 - - [04/Mar/2025 12:55:10] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
sh: ls-al%: not found
172.17.0.1 - - [04/Mar/2025 12:55:36] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
sh: ls-al%: not found
172.17.0.1 - - [04/Mar/2025 12:56:03] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
ls: /%: No such file or directory
static/img/bones.png
172.17.0.1 - - [04/Mar/2025 12:56:14] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
ls: /%: No such file or directory
-rw-rw-r-- 1 app app 118704 Feb 18 21:46 static/img/bones.png
172.17.0.1 - - [04/Mar/2025 12:56:36] "POST /home HTTP/1.1" 200 -
convert: `50' @ error/convert.c/ConvertImageCommand/3272.
ls: /%: No such file or directory
-rw-rw-r-- 1 app app 118704 Feb 18 21:46 static/img/bones.png
172.17.0.1 - - [04/Mar/2025 12:57:56] "POST /home HTTP/1.1" 200 -
```

- let's try to inject a command to recursively remove all files in `/static`:

- A screenshot of a browser developer tools window. The main content area shows a dropdown menu with the option "Select image resize 50%" highlighted. Below it is a "Submit Button". The bottom half of the window is a detailed CSS inspector showing the DOM tree and the computed styles for the selected element. A box model diagram on the right shows the element's dimensions: width 1856.13px, height 172.317px, padding 8px, border 0px, and margin 0px.
- A screenshot of a browser developer tools window. The main content area displays an error message: "Error" and "No response received from remote server.". The bottom half is a CSS inspector showing the DOM tree and the computed styles for the body element. A box model diagram on the right shows the body's dimensions: width 1856.13px, height 172.317px, padding 8px, border 0px, and margin 0px.
- A screenshot of a browser developer tools window. The main content area displays an error message: "Error" and "No response received from remote server.". The bottom half is a CSS inspector showing the DOM tree and the computed styles for the body element. A box model diagram on the right shows the body's dimensions: width 1856.13px, height 172.317px, padding 8px, border 0px, and margin 0px.

- let's check the terminal:

```
ammar@ubuntu:~ ammar@ubuntu:~ ammar@ubuntu:~  
rm: can't remove '/etc/ImageMagick-7/quantization-table.xml': Permission denied  
rm: can't remove '/etc/ImageMagick-7/policy.xml': Permission denied  
rm: can't remove '/etc/ImageMagick-7/coder.xml': Permission denied  
rm: can't remove '/etc/ImageMagick-7/log.xml': Permission denied  
rm: can't remove '/etc/ImageMagick-7/magic.xml': Permission denied  
rm: can't remove '/etc/ImageMagick-7/type-apple.xml': Permission denied  
rm: can't remove '/etc/ca-certificates.conf': Permission denied  
rm: can't remove '/etc/pkcs11/pkcs11.conf.example': Permission denied  
rm: can't remove '/etc/pkcs11': Permission denied  
rm: can't remove '/etc/fonts/fonts.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/90-synthetic.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/51-local.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/60-latin.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/30-metric-aliases.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/69-unifont.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/10-scale-bitmap-fonts.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/65-fonst-persian.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/20-unhint-small-vera.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/50-user.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/README': Permission denied  
rm: can't remove '/etc/fonts/conf.d/65-nonlatin.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/49-sansserif.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/45-generic.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/80-delicious.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/40-nonlatin.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/60-generic.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/10-hinting-slight.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d/45-latin.conf': Permission denied  
rm: can't remove '/etc/fonts/conf.d': Permission denied  
rm: can't remove '/etc': Permission denied  
rm: can't remove '/.dockerenv': Permission denied  
• rm: can't remove '/': Resource busy
```

- baaang! we exposed the whole system structure and its files



- why it's dangerous? because it allows an attacker to execute arbitrary system commands on a server leading to full system compromise, data theft, and destruction of files
- possible mitigations:
 - avoiding executing system commands
 - using parameterized inputs
 - using secure APIs instead of shell execution

