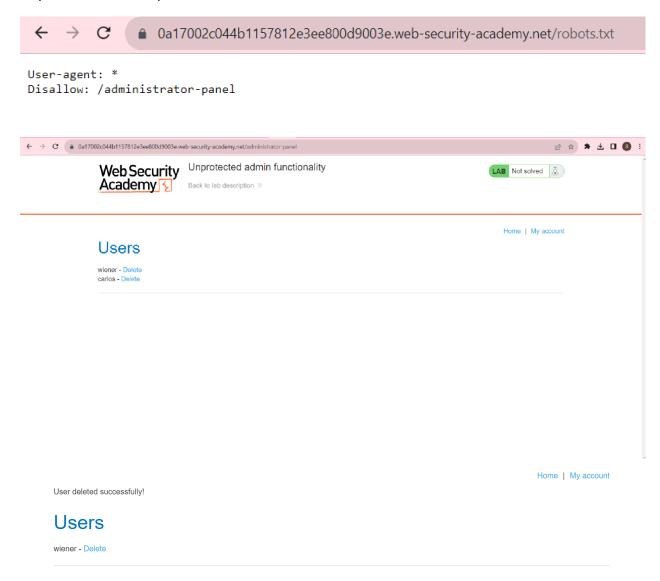
# **Assignment 1**

# **Vulnerability test on websites**

# 1. Broken Access Control

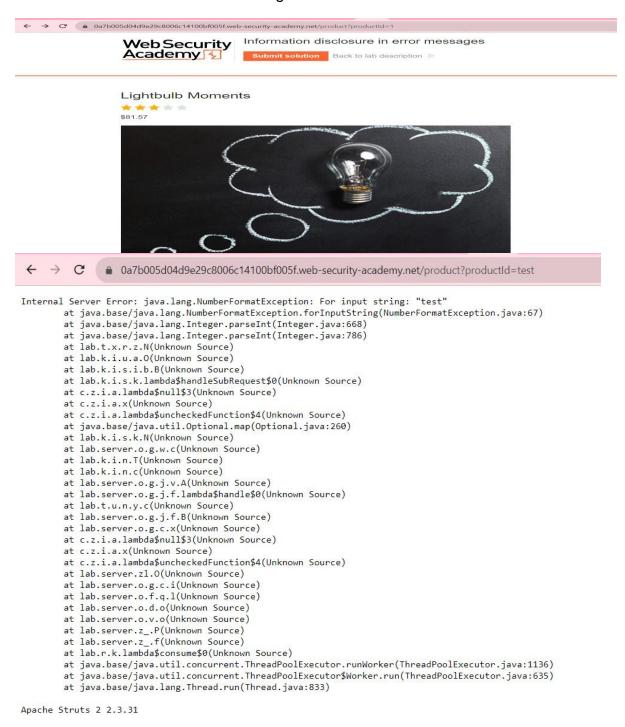
Unprotected admin panel



Once the administrator link is found, there is no access control which makes the application vulnerable.

### 2. Cryptographic failure

Information disclosure in error messages



Version number of the framework is visible in the error message and is not encrypted.

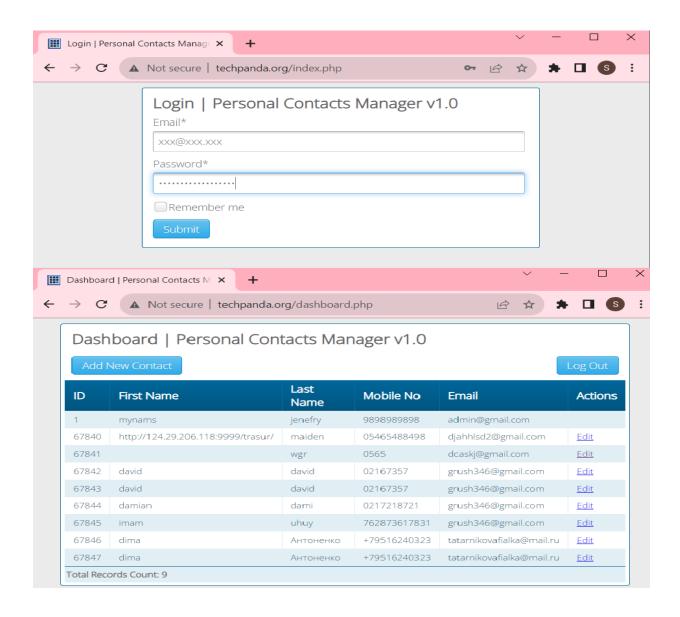
#### 3. Injection

Email: xxx@xxx.xxx

Password: xxx') OR 1 = 1 — ]

SELECT \* FROM users WHERE email = 'xxx@xxx.xxx' OR 1 = 1 LIMIT 1 — '] AND password = md5('1234');

- xxx@xxx.xxx ends with a single quote which completes the string quote
- OR 1 = 1 LIMIT 1 is a condition that will always be true and limits the returned results to only one record.
- — 'AND ... is a SQL comment that eliminates the password part.



### 4. Insecure Design

```
import json

f = open('permissions.json')
employee_roles = json.load(f)

def remove_employee(employee_id, requesting_person):
    # Fetch role from permissions.json where name equals $requesting_person
    role = list(filter(lambda x:x["name"]==requesting_person, employee_roles))[0]['role']

# Only allow the roles 'developer' and 'castle_leader' to delete employees
if role == "developer" or role == "castle_leader":
    print(requesting_person, employee_id)
    cursor.execute("DELETE FROM employees WHERE ID = ?", [employee_id])
```

In the above case, the newly entered developer friend can delete the leader and increase his privilege because of the error in the design.

Here, the privilege of the can be controlled by:

```
"role": ["receive_order", "submit_timecard", "change_permissions", "edit_code",
"add_employee", "remove_employee", ...]
},
{
    "name": "Sir Snake Oil",
    "role": ["receive_order", "submit_timecard", "edit_code", ...]
}

"name": "You",
    "role": [...]
}
]
```

#### 5. Security Misconfiguration

First, Launch Webgoat and navigate to insecure configuration section



We can try out as many options as we can think of. All we need to find the URL of config file and we know that the developers follow kind of naming convention for config files. It can be anything that is listed below. It is usually done by BRUTE force technique.

- web.config
- config
- · appname.config
- conf

