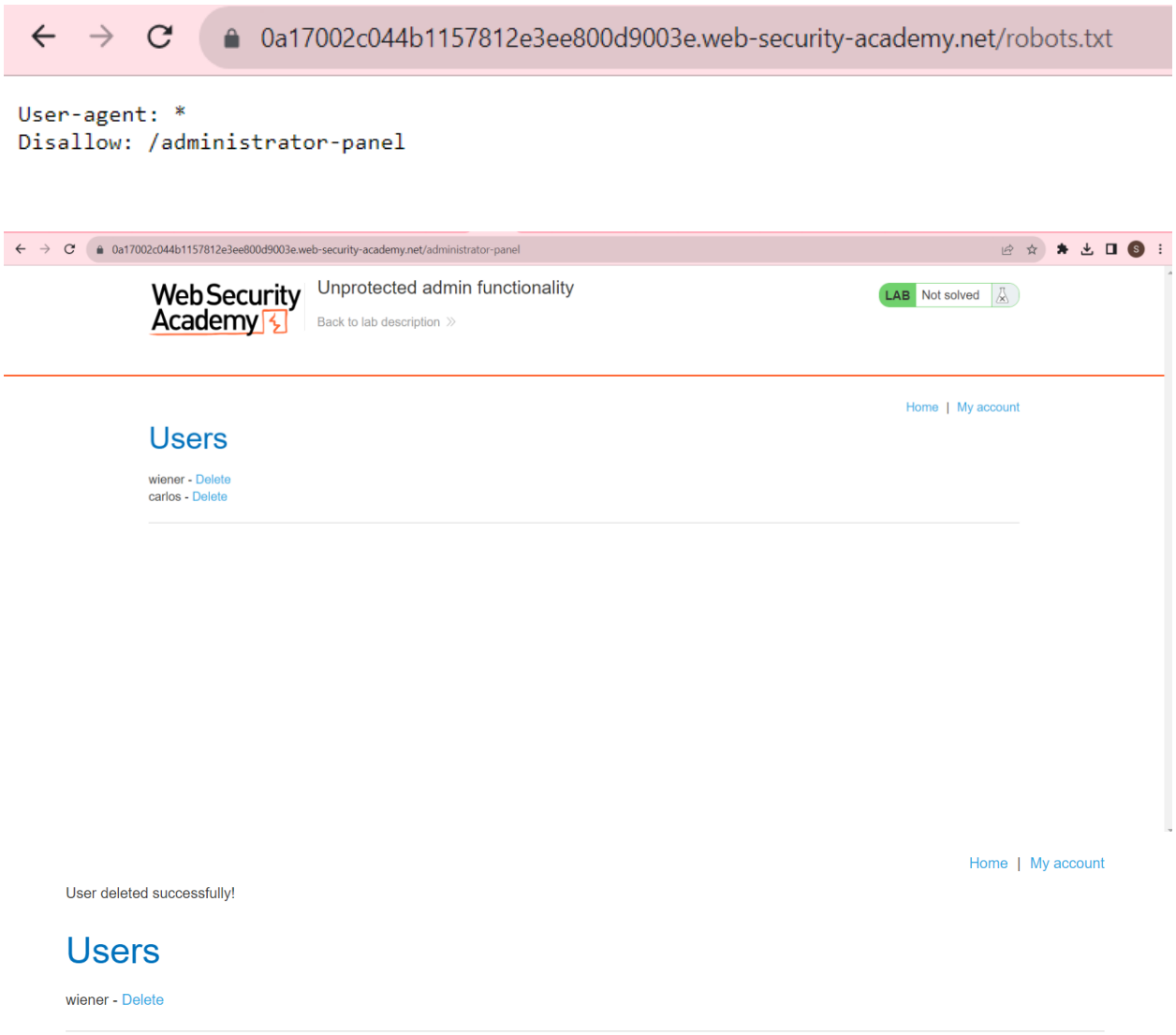
Assignment 1 **Sarika V**

Vulneraility 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


```
Internal Server Error: java.lang.NumberFormatException: For input string: "test"
        at java.base/java.lang.NumberFormatException.forInputString(NumberFormatException.java:67)
        at java.base/java.lang.Integer.parseInt(Integer.java:668)
        at java.base/java.lang.Integer.parseInt(Integer.java:786)
        at lab.t.x.r.z.N(Unknown Source)
        at lab.k.i.u.a.O(Unknown Source)
        at lab.k.i.s.i.b.B(Unknown Source)
        at lab.k.i.s.k.lambda$handleSubRequest$0(Unknown Source)
        at c.z.i.a.lambda$null$3(Unknown Source)
        at c.z.i.a.x(Unknown Source)
        at c.z.i.a.lambda$uncheckedFunction$4(Unknown Source)
        at java.base/java.util.Optional.map(Optional.java:260)
        at lab.k.i.s.k.N(Unknown Source)
        at lab.server.o.g.w.c(Unknown Source)
        at lab.k.i.n.T(Unknown Source)
        at lab.k.i.n.c(Unknown Source)
        at lab.server.o.g.j.v.A(Unknown Source)
        at lab.server.o.g.j.f.lambda$handle$0(Unknown Source)
        at lab.t.u.n.y.c(Unknown Source)
        at lab.server.o.g.j.f.B(Unknown Source)
        at lab.server.o.g.c.x(Unknown Source)
        at c.z.i.a.lambda$null$3(Unknown Source)
        at c.z.i.a.x(Unknown Source)
        at c.z.i.a.lambda$uncheckedFunction$4(Unknown Source)
        at lab.server.zl.O(Unknown Source)
        at lab.server.o.g.c.i(Unknown Source)
        at lab.server.o.f.q.l(Unknown Source)
        at lab.server.o.d.o(Unknown Source)
        at lab.server.o.v.o(Unknown Source)
        at lab.server.z_.P(Unknown Source)
        at lab.server.z_.f(Unknown Source)
        at lab.r.k.lambda$consume$0(Unknown Source)
        at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136)
        at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635)
        at java.base/java.lang.Thread.run(Thread.java:833)

Apache Struts 2 2.3.31
```

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

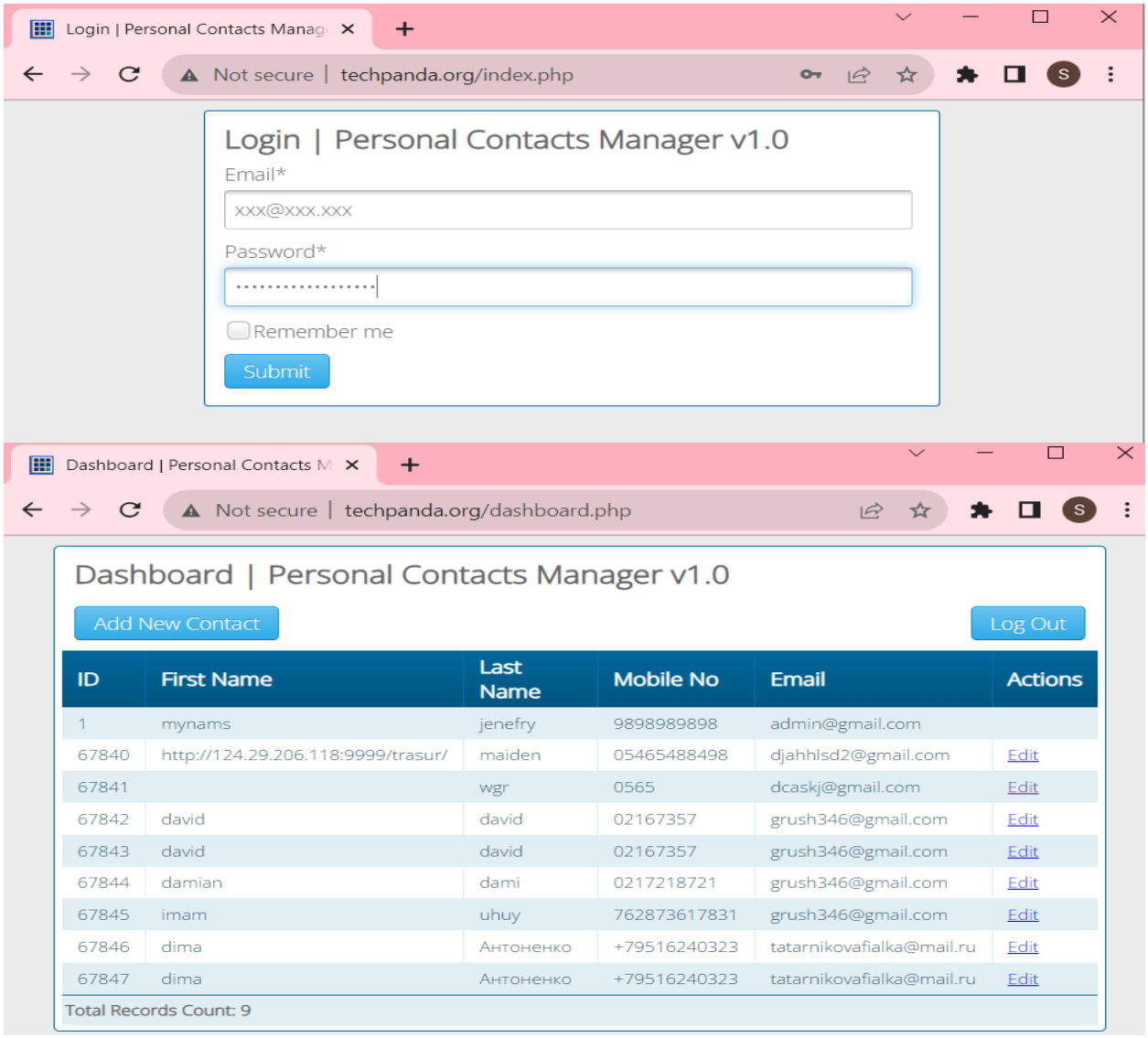
3. Injection

Email: xxx@xxx.xxx

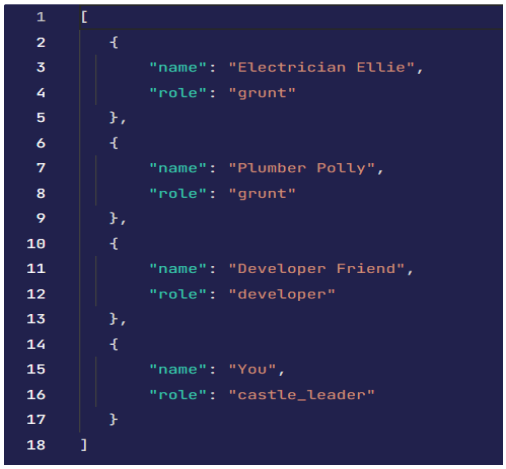
Password: xxx') OR 1 = 1 —]

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



```
[
    {
        "name": "Electrician Ellie",
        "role": "grunt"
    },
    {
        "name": "Plumber Polly",
        "role": "grunt"
    },
    {
        "name": "Developer Friend",
        "role": "developer"
    },
    {
        "name": "You",
        "role": "castle_leader"
    }
]
```

```
[
    {
        "name": "Electrician Ellie",
        "role": "grunt"
    },
    {
        "name": "Plumber Polly",
        "role": "grunt"
    },
    {
        "name": "Developer Friend",
        "role": "developer"
    },
    {
        "name": "Sir Snake Oil",
        "role": "developer"
    }
    {
        "name": "You",
        "role": "castle_leader"
    }
]
```

```
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:

```
[
  {
    "name": "Electrician Ellie",
    "role": ["receive_order", "submit_timecard"]
  },
  {
    "name": "Plumber Polly",
    "role": ["receive_order", "submit_timecard"]
  },
  {
    "name": "Developer Friend",
```

```
    "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


File Edit View History Bookmarks Tools Help
http://localho...&succeeded=yes
http://localhost:8080/WebGoat/attack?Screen=66&menu=1400&succeeded=yes
Most Visited Getting Started Suggested Sites Web Slice Gallery New Tab
* Your goal should be to try to guess the URL for the "config" interface.
* The "config" URL is only available to the maintenance personnel.
* The application doesn't check for horizontal privileges.
* Congratulations. You have successfully completed this lesson.
Welcome to WebGoat Configuration Page
Set Admin Privileges for:
Set Admin Password: