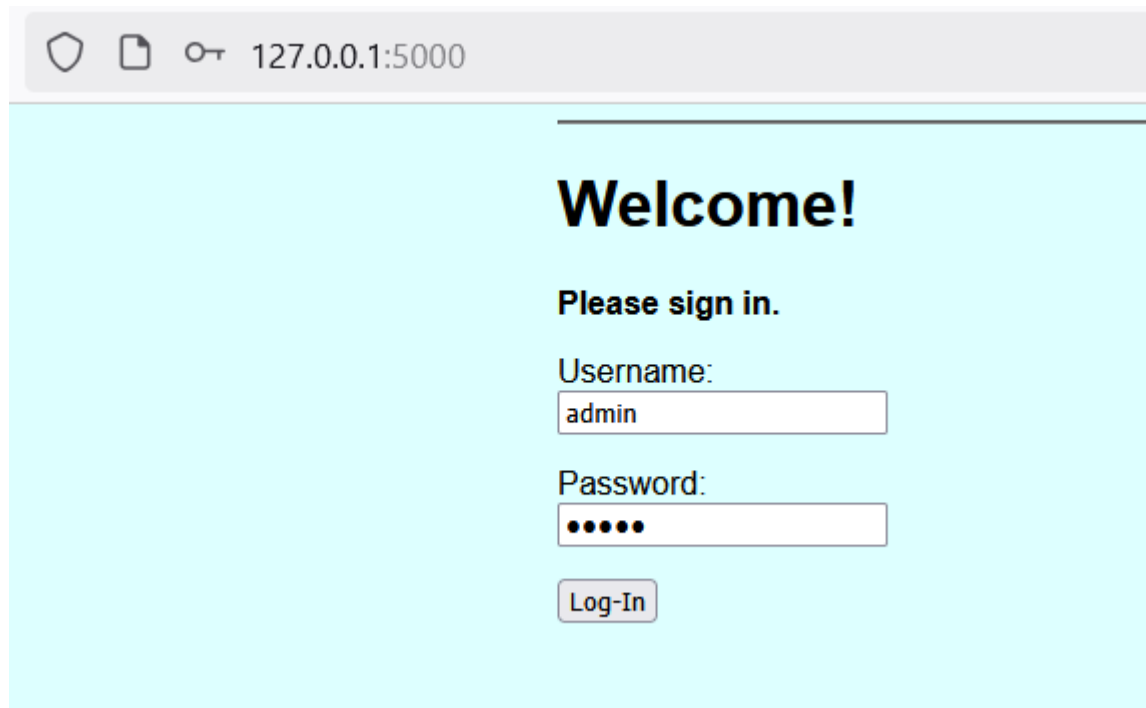


OWASP Top Ten from 2017 from <https://owasp.org/www-project-top-ten/2017/>

Flaw 1, A6:2017-Security Misconfiguration

Default accounts and their passwords are still enabled and unchanged.

Database has pre-defined user names and pass words, like admin/admin, user1/user1.



127.0.0.1:5000

# Welcome!

**Please sign in.**

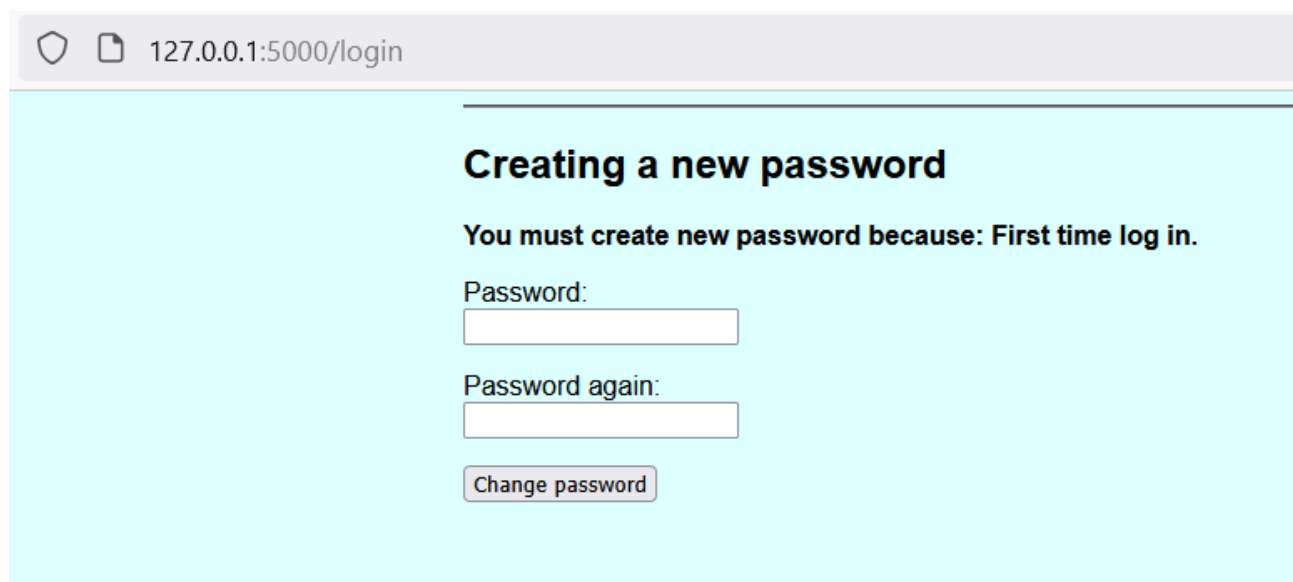
Username:

Password:

One can log in n-times with pre-defined user names and pass words.

After Fix, one must create new pass word after first log-in:

Remove comments from lines: Routes.py #30,31,32



127.0.0.1:5000/login

## Creating a new password

**You must create new password because: First time log in.**

Password:

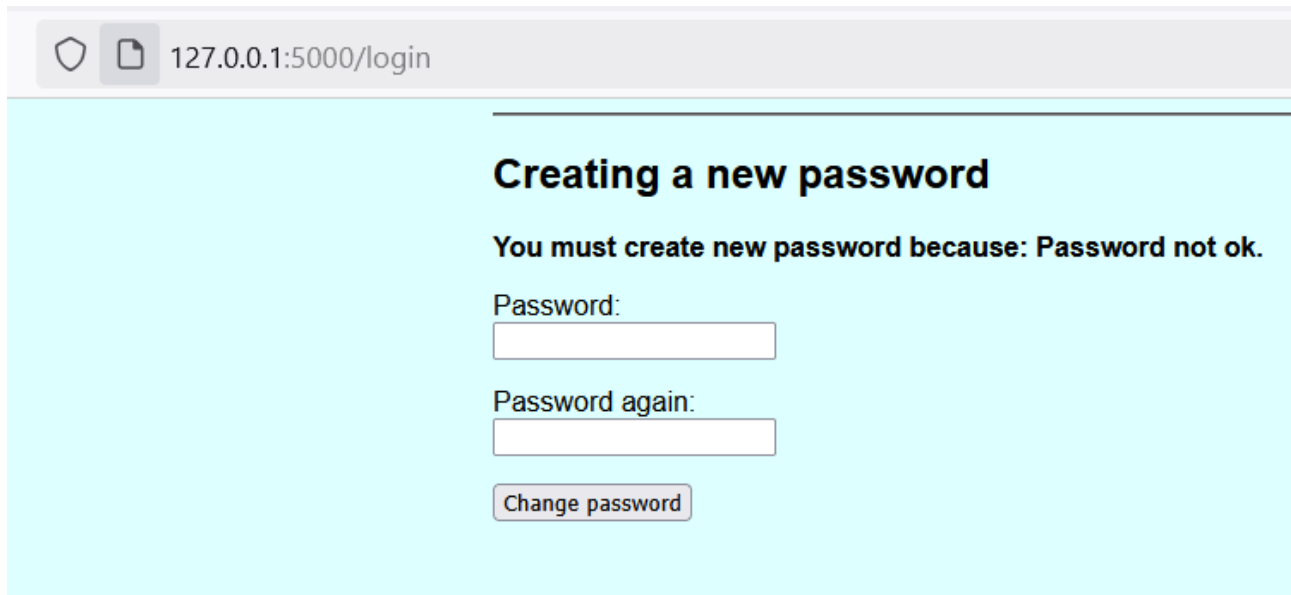
Password again:

Flaw 2, A2:2017-Broken Authentication

Permits weak passwords

Remove comments from lines: Routes.py #33,34,35,54,55

If pass word is too short, less than 8 characters, it is not accepted.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1:5000/login". The page has a light blue background and a white header bar. The main content area is titled "Creating a new password" in bold black text. Below the title, a message states "You must create new password because: Password not ok." in bold black text. There are two input fields for passwords, labeled "Password:" and "Password again:". Below these fields is a button labeled "Change password".

127.0.0.1:5000/login

## Creating a new password

**You must create new password because: Password not ok.**

Password:

Password again:

[Change password](#)

Flaw 3, A1:2017-Injection

SQL Injection

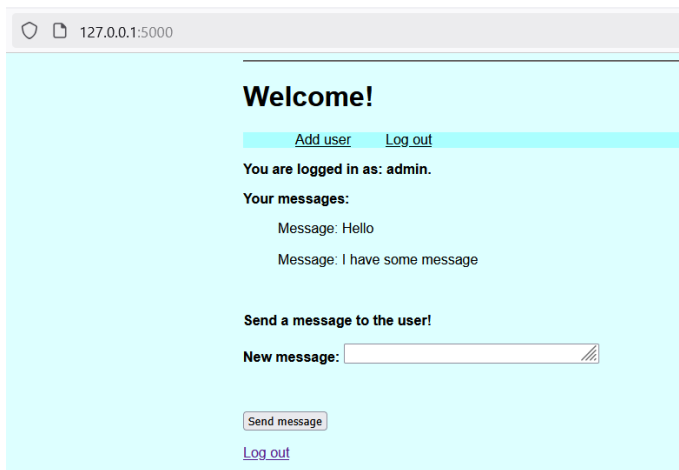
Comment lines: threads.py # 26, 27

Remove comments from lines: threads.py # 29, 30

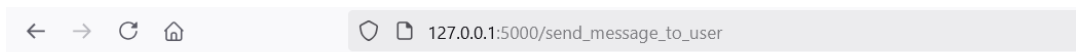
SQL Injection is possible, example message can be found from threads.py # 28

Hello Sir'); DROP TABLE messages;--

will delete messages table.



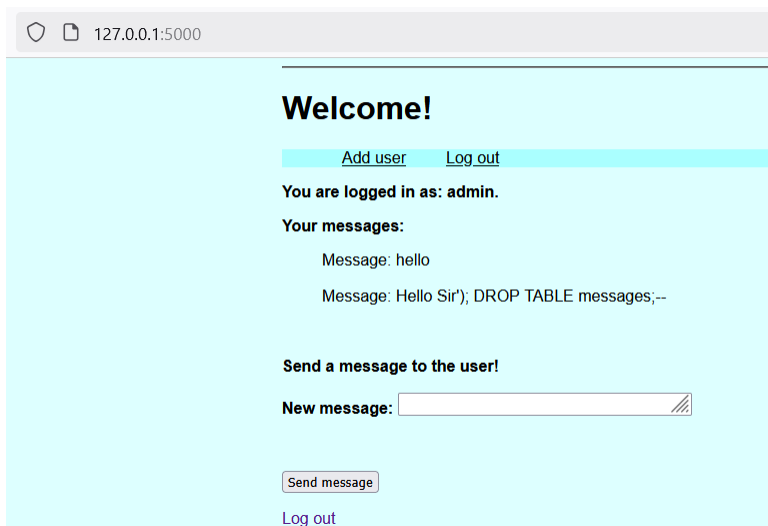
After giving example message:



## Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

All messages will be deleted. After Fix:



Flaw 4, A7:2017-Cross-Site Scripting (XSS)

XSS vulnerability

Comment lines: index.html # 23

Remove comments from lines: index.html # 24

You can test with messages:

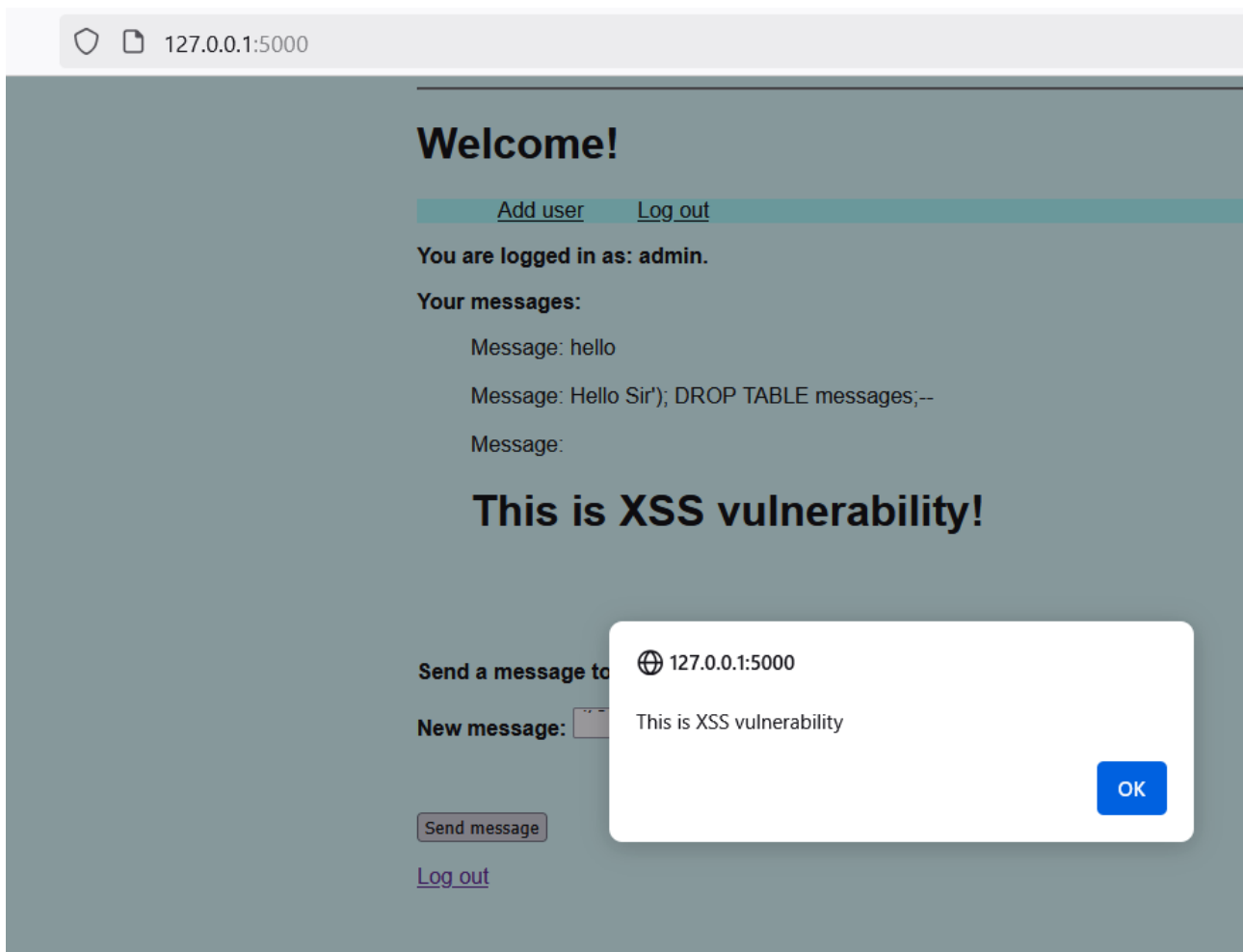
```
<h1><span style="color:black"> This is XSS vulnerability!</span></h1>
```

Or:

```
<script>
```

```
alert("This is XSS vulnerability");
```

```
</script>
```



After fix:

# Welcome!

[Add user](#) [Log out](#)

You are logged in as: admin.

## Your messages:

Message: hello

Message: Hello Sir'); DROP TABLE messages;--

Message: <h1><span style="color:black"> This is XSS vulnerability!</span></h1>

Message: <script> alert("This is XSS vulnerability"); </script>

## Send a message to the user!

New message:

[Log out](#)

Flaw 5, CSRF (CSRF is missing from both lists as it is more rare nowadays due to the more secure frameworks. However, due to its fundamental nature it is allowed as a flaw.)

Remove comments from lines: index.html # 44

Remove comments from lines: routes.py # 14, 15

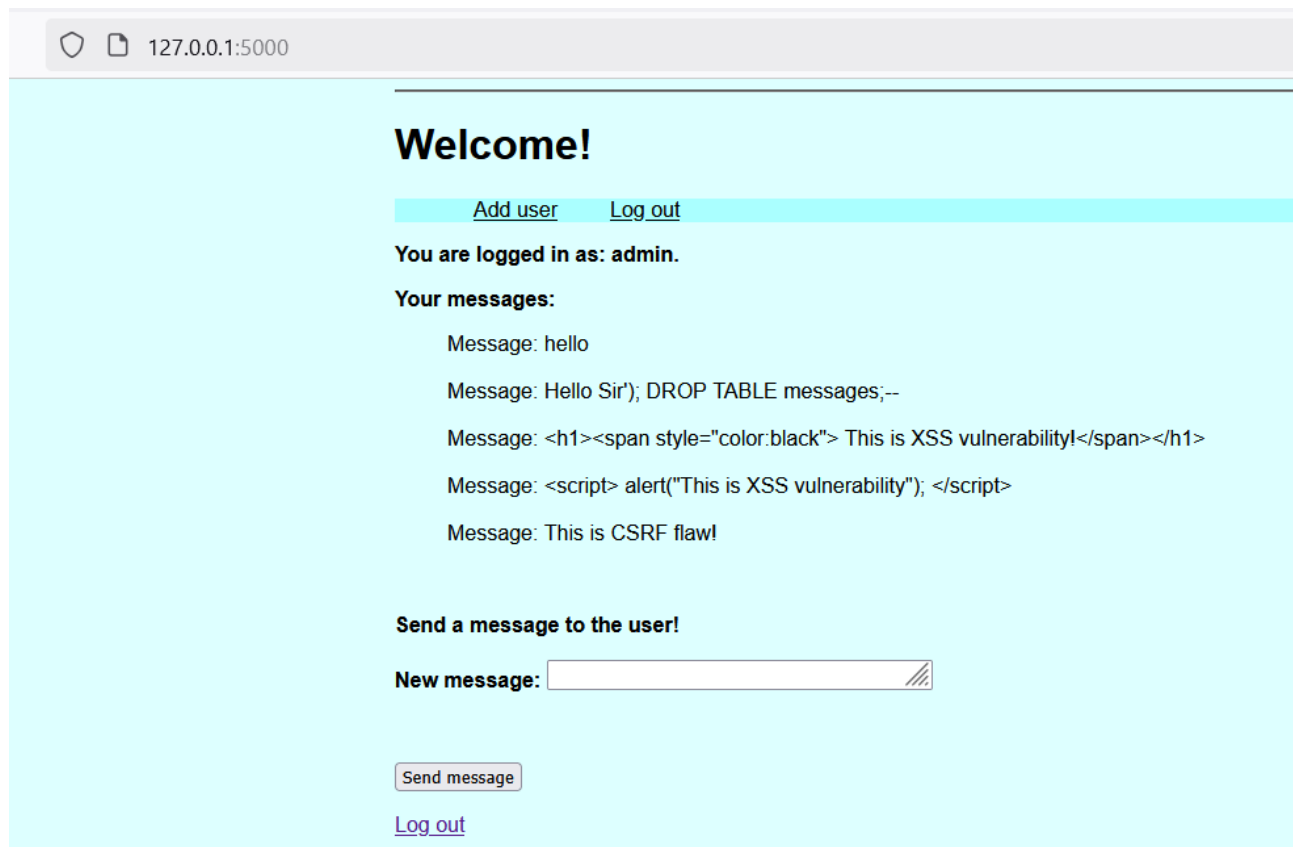
Open: ./templates/CSRF.html



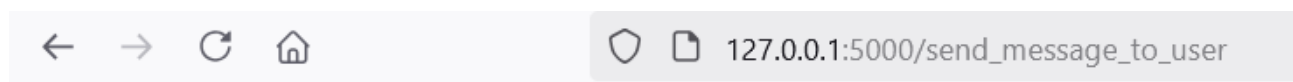
Click here to demo CSRF flaw?

Continue

After clicking Continue:



After fix, clicking Continue:



## Bad Request

The browser (or proxy) sent a request that this server could not understand.