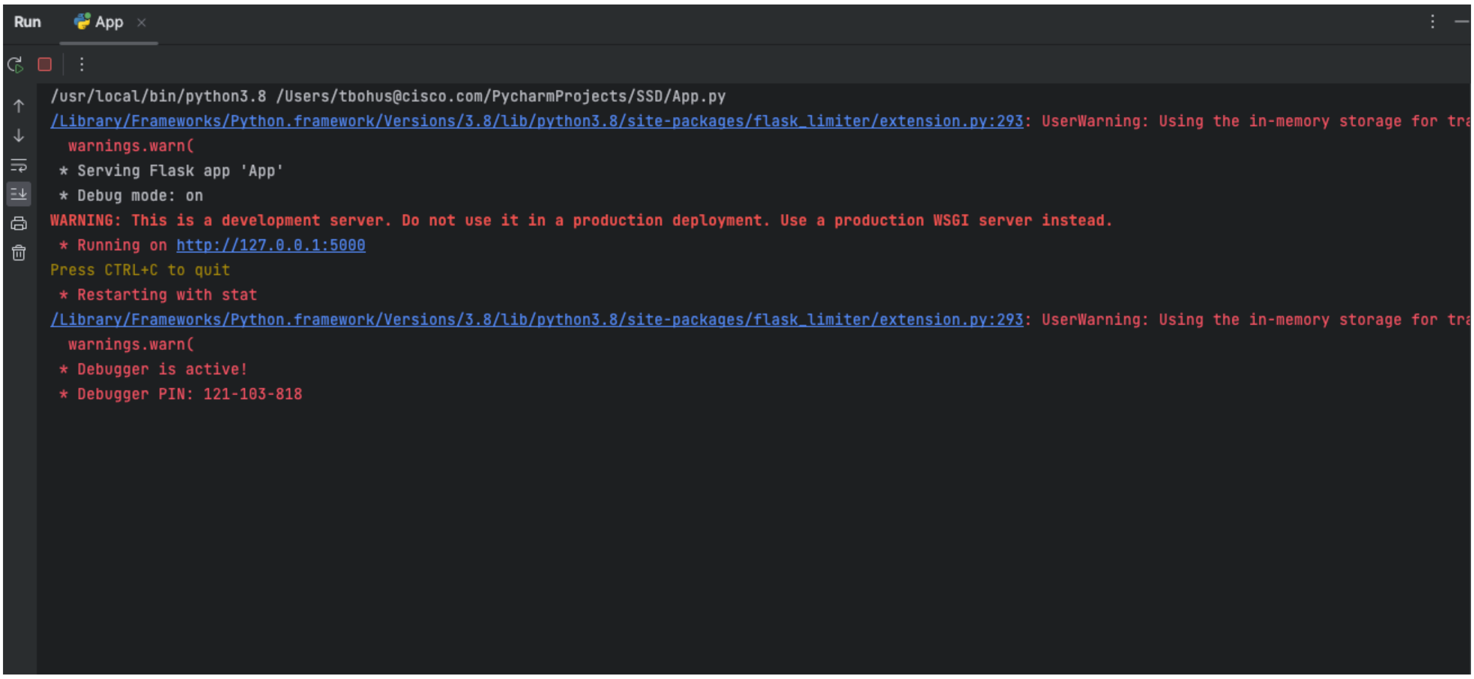
Testing & Output Results

Registration & Login

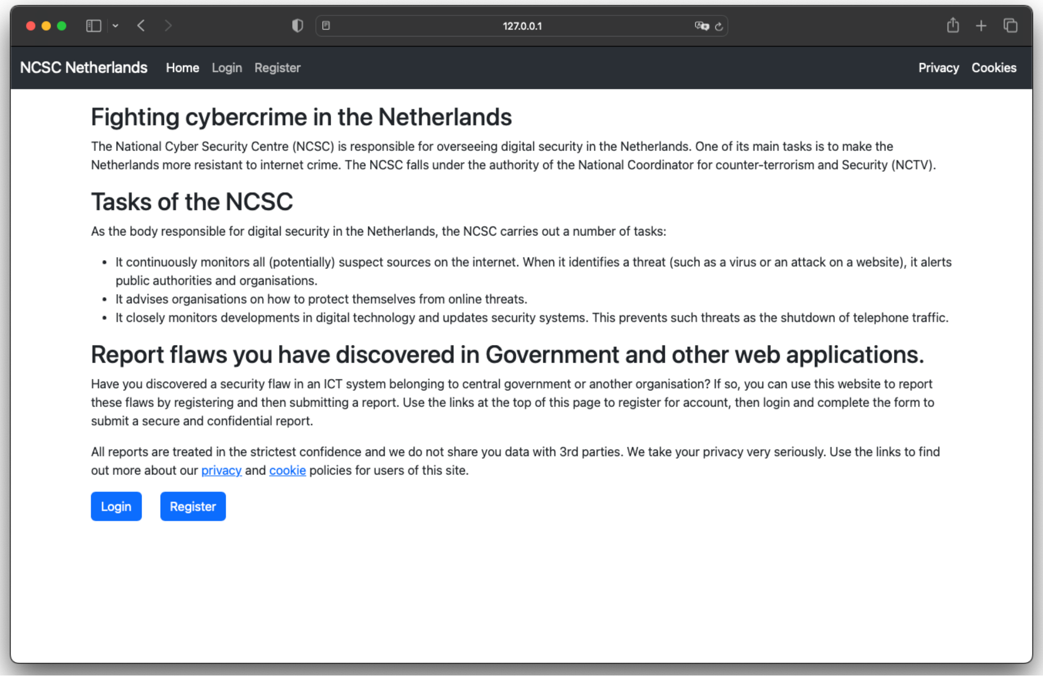
1. After running the code successfully, the user should see the following message, which informs them that the application is up and running using the Flask framework, on their local machine. They can access it by clicking on the IP address directly, or by manually copying it.



```
/usr/local/bin/python3.8 /Users/tbohus@cisco.com/PycharmProjects/SSD/App.py
/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/site-packages/flask_limiter/extension.py:293: UserWarning: Using the in-memory storage for tra
  warnings.warn(
 * Serving Flask app 'App'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/site-packages/flask_limiter/extension.py:293: UserWarning: Using the in-memory storage for tra
  warnings.warn(
 * Debugger is active!
 * Debugger PIN: 121-103-818
```

Figure 1: Application is successfully running

2. After navigating to the application, the user will be presented with the following view, explaining the purpose of the application, as well as having options to either log in or register.



Fighting cybercrime in the Netherlands

The National Cyber Security Centre (NCSC) is responsible for overseeing digital security in the Netherlands. One of its main tasks is to make the Netherlands more resistant to internet crime. The NCSC falls under the authority of the National Coordinator for counter-terrorism and Security (NCTV).

Tasks of the NCSC

As the body responsible for digital security in the Netherlands, the NCSC carries out a number of tasks:

- It continuously monitors all (potentially) suspect sources on the internet. When it identifies a threat (such as a virus or an attack on a website), it alerts public authorities and organisations.
- It advises organisations on how to protect themselves from online threats.
- It closely monitors developments in digital technology and updates security systems. This prevents such threats as the shutdown of telephone traffic.

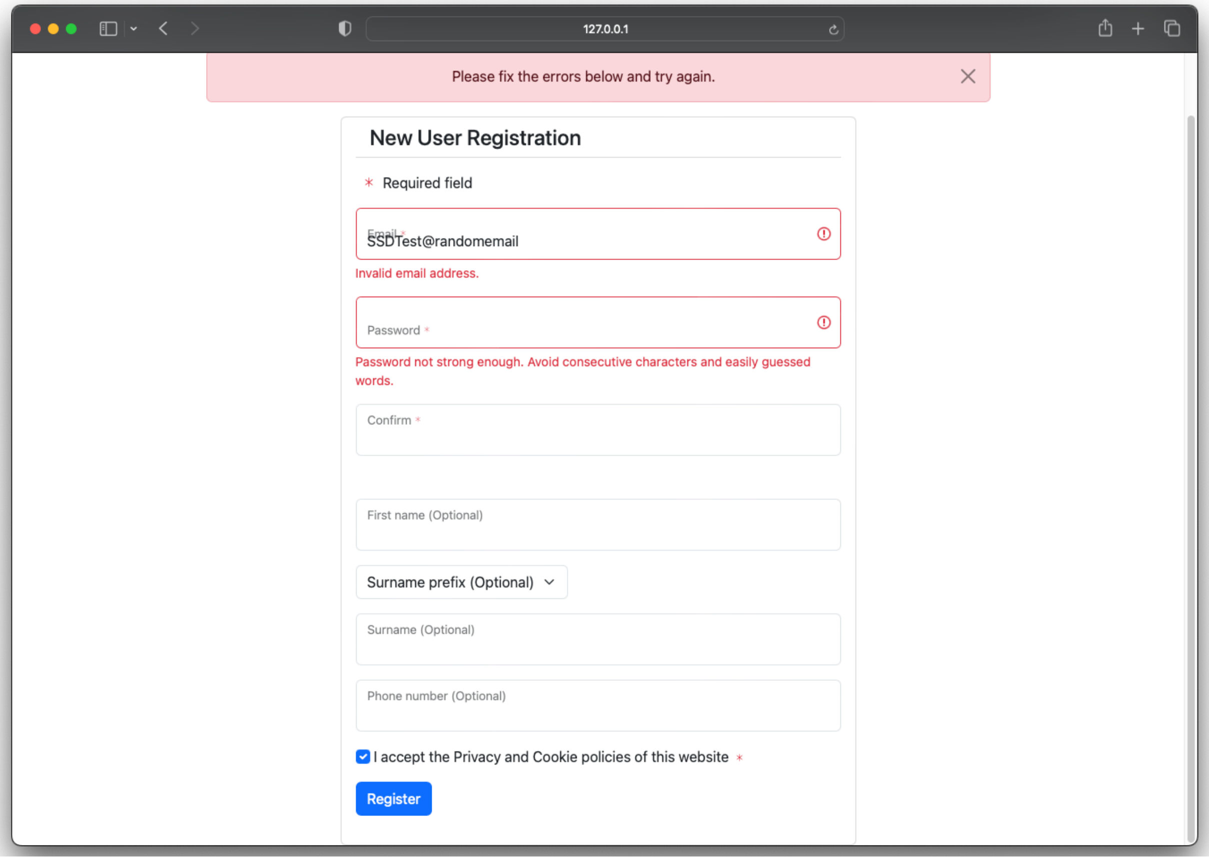
Report flaws you have discovered in Government and other web applications.

Have you discovered a security flaw in an ICT system belonging to central government or another organisation? If so, you can use this website to report these flaws by registering and then submitting a report. Use the links at the top of this page to register for account, then login and complete the form to submit a secure and confidential report.

All reports are treated in the strictest confidence and we do not share you data with 3rd parties. We take your privacy very seriously. Use the links to find out more about our privacy and cookie policies for users of this site.

Figure 2: Application Homepage

3. To register, the user will need to click on “Register” and then provide the required information. As you can see in the screenshot, the e-mail address needs to have a proper format and the passwords must be more complex.



Please fix the errors below and try again.

New User Registration

* Required field

Email * SSDTest@randomemail

Invalid email address.

Password *

Password not strong enough. Avoid consecutive characters and easily guessed words.

Confirm *

First name (Optional)

Surname prefix (Optional)

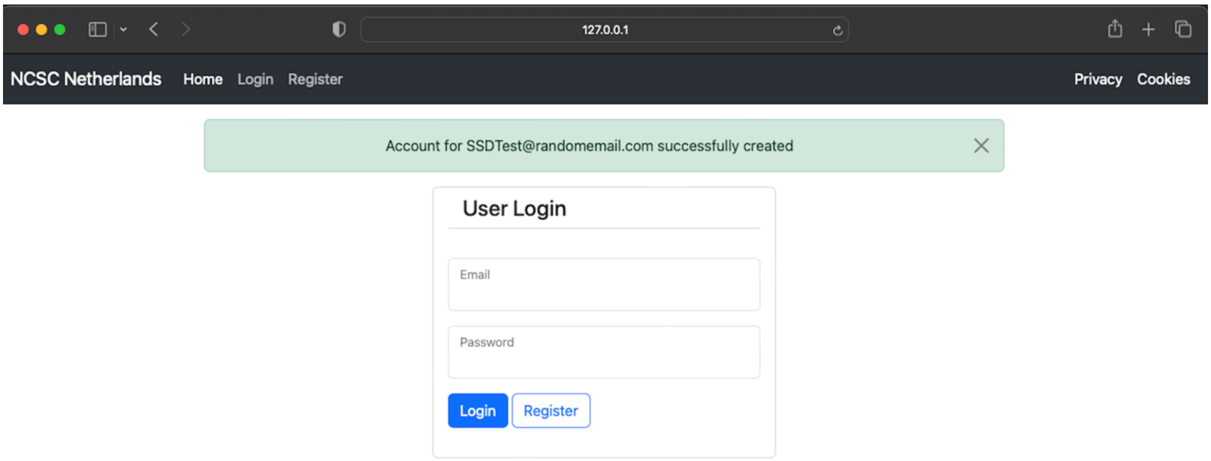
Surname (Optional)

Phone number (Optional)

☑ I accept the Privacy and Cookie policies of this website *

Figure 3: User Registration

4. After the user is registered, their details are populated into the database, and their password is immediately encrypted. They can then log in. Instead of handling clear-text information, we are comparing the hashes of the passwords, which is a more secure way of handling sensitive data. This can be further inspected in the “Enforcing Security” portion of this document.



Account for SSDTest@randomemail.com successfully created

User Login

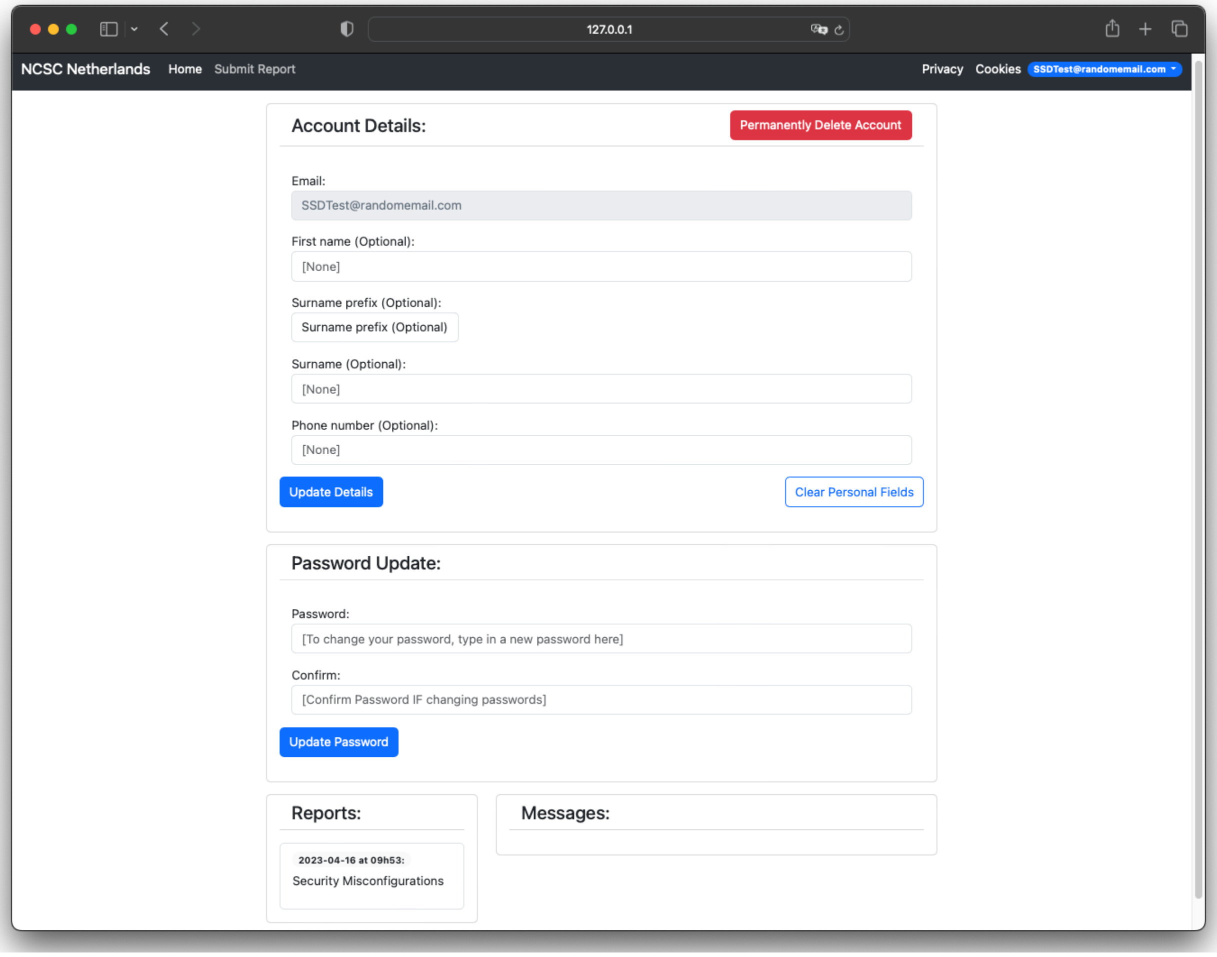
Email

Password

Figure 4: User Login

Account Operations

1. After the user is logged-in, they can modify their personal details, including an e-mail address, name, phone number, as well as their password. The user can also view their submitted security reports.



Account Details:

Email: SSDTest@randomemail.com

First name (Optional): [None]

Surname prefix (Optional): Surname prefix (Optional)

Surname (Optional): [None]

Phone number (Optional): [None]

Password Update:

Password: [To change your password, type in a new password here]

Confirm: [Confirm Password IF changing passwords]

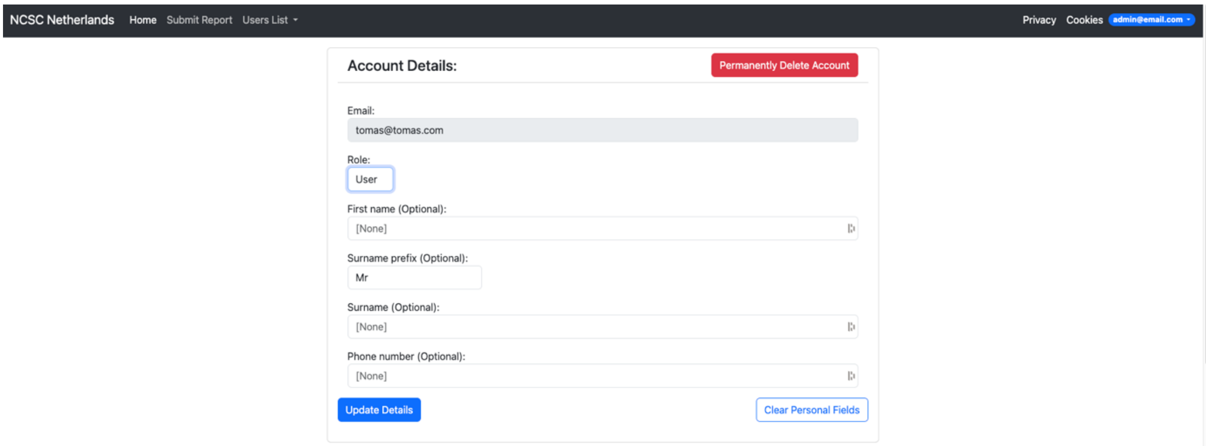
Reports:

2023-04-16 at 09h53:
Security Misconfigurations

Messages:

Figure 5: Account Details

2. As discussed in the README file, an admin user is automatically populated into the database. When logged in as an administrator, the user can change the associated roles with all other registered accounts, effectively making them administrators, too.



Account Details:

Email: tomas@tomas.com

Role: User

First name (Optional): [None]

Surname prefix (Optional): Mr

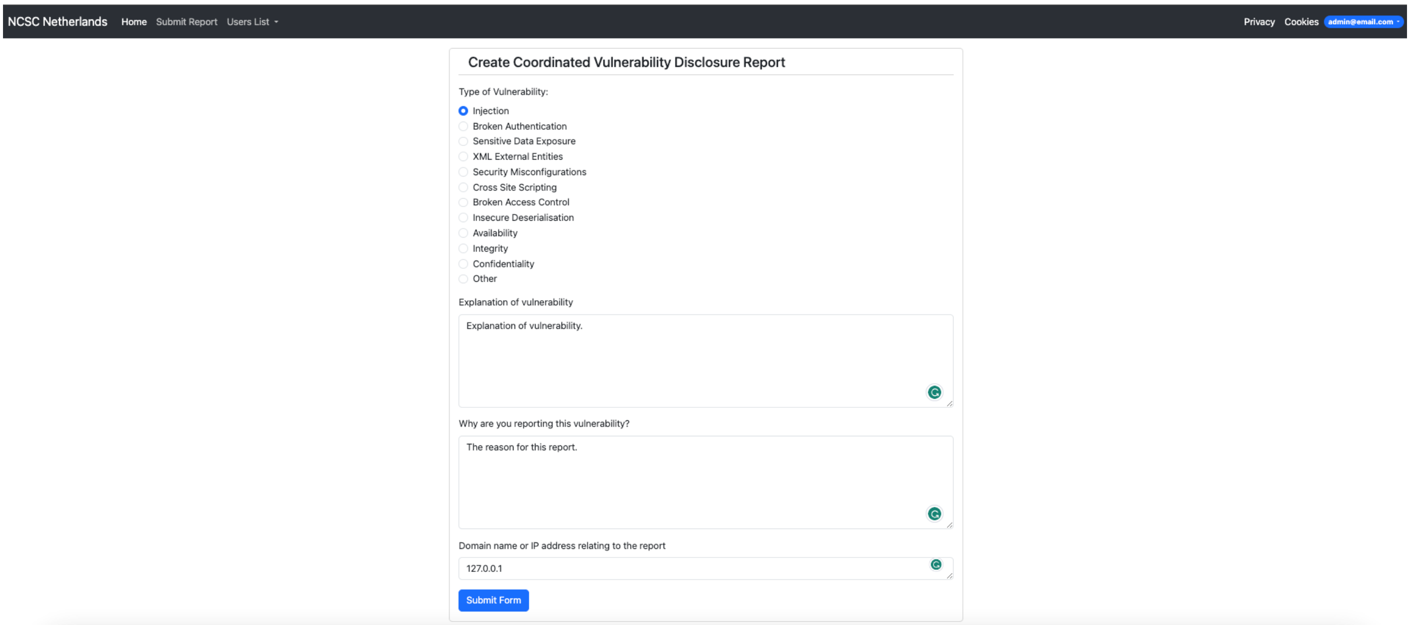
Surname (Optional): [None]

Phone number (Optional): [None]

Figure 6: User Role Change

Submitting, editing, and deleting security reports

1. While the user role can create and edit security reports, only the administrator can delete submitted security reports. The process to create new reports is the same for both roles and is showcased in the following screenshot.



Create Coordinated Vulnerability Disclosure Report

Type of Vulnerability:

● Injection
○ Broken Authentication
○ Sensitive Data Exposure
○ XML External Entities
○ Security Misconfigurations
○ Cross Site Scripting
○ Broken Access Control
○ Insecure Deserialisation
○ Availability
○ Integrity
○ Confidentiality
○ Other

Explanation of vulnerability

Explanation of vulnerability.

Why are you reporting this vulnerability?

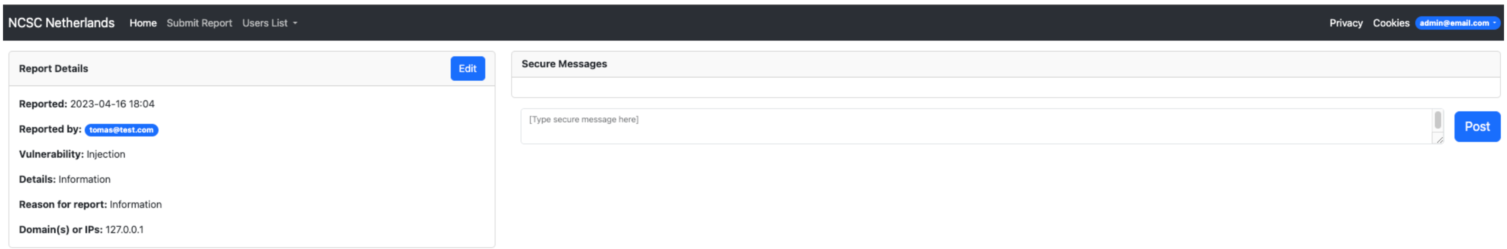
The reason for this report.

Domain name or IP address relating to the report

127.0.0.1

Figure 7: Report Submission

2. The reports can be viewed from the main dashboard, or from the account details page



Report Details

Reported: 2023-04-16 18:04

Reported by: tomas@test.com

Vulnerability: Injection

Details: Information

Reason for report: Information

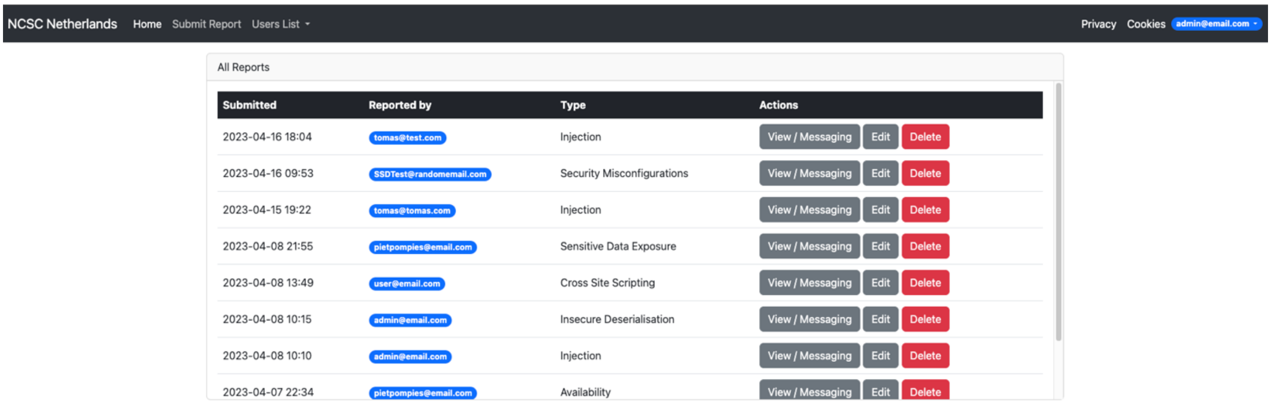
Domain(s) or IPs: 127.0.0.1

Secure Messages

[Type secure message here]

Figure 8: Submitted Report

3. The user can simply click on the report to edit it. All of these reports are viewed by the administrator as per the following screenshot.



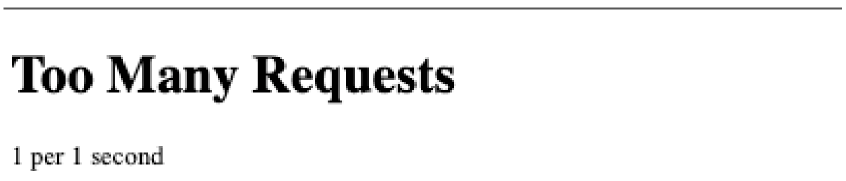
All Reports

Submitted	Reported by	Type	Actions
2023-04-16 18:04	tomas@test.com	Injection	View / Messaging Edit Delete
2023-04-16 09:53	SSDTest@randomemail.com	Security Misconfigurations	View / Messaging Edit Delete
2023-04-15 19:22	tomas@tomas.com	Injection	View / Messaging Edit Delete
2023-04-08 21:55	pietpompies@email.com	Sensitive Data Exposure	View / Messaging Edit Delete
2023-04-08 13:49	user@email.com	Cross Site Scripting	View / Messaging Edit Delete
2023-04-08 10:15	admin@email.com	Insecure Deserialisation	View / Messaging Edit Delete
2023-04-08 10:10	admin@email.com	Injection	View / Messaging Edit Delete
2023-04-07 22:34	pietpompies@email.com	Availability	View / Messaging Edit Delete

Figure 9: Admin Report View

Enforcing Security

1. The application has a built-in limiter provided by the flask_limiter utility, this prevent the user from submitting too many requests and overloading the system.

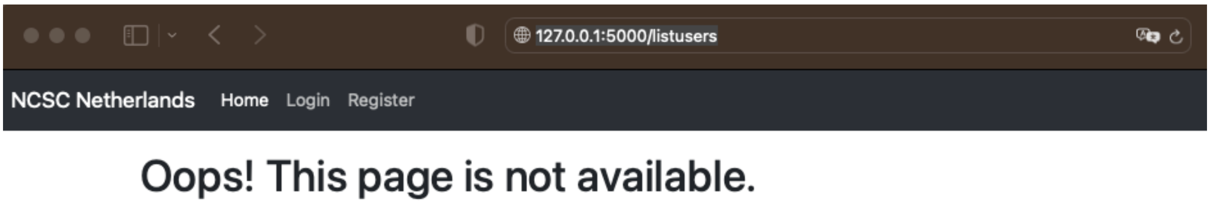


Too Many Requests

1 per 1 second

Figure 10: Request Limiter

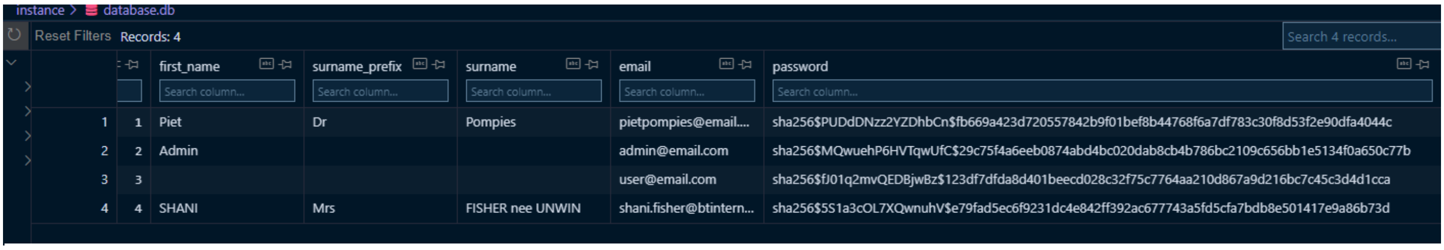
2. If an unauthorized user attempts to access a resource/path directly (by typing /listusers, for example), they will receive a HTTP 403 – Forbidden code, and the following message:



Oops! This page is not available.

Figure 11: Error Page

3. Any sensitive data stored in the database will be encrypted, and only the hashes will be compared. Here is the output from the database showcasing this behaviour:

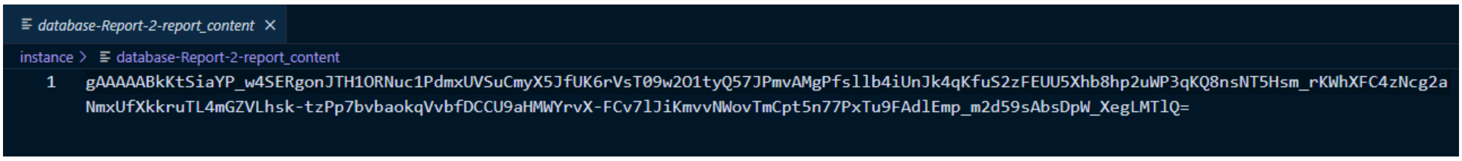


Records: 4

		first_name	surname_prefix	surname	email	password
1	1	Piet	Dr	Pompies	pietpompies@email....	sha256$PUDdDNzz2YZDhbCn$fb669a423d720557842b9f01bef8b44768f6a7df783c30f8d53f2e90dfa4044c
2	2	Admin			admin@email.com	sha256$MQwuehP6HVTqwUfC$29c75f4a6eeb0874abd4bc020dab8cb4b786bc2109c656bb1e5134f0a650c77b
3	3				user@email.com	sha256$fJ01q2mvQEDBjwBz$123df7dfda8d401beecd028c32f75c7764aa210d867a9d216bc7c45c3d4d1cca
4	4	SHANI	Mrs	FISHER nee UNWIN	shani.fisher@btintern...	sha256$5S1a3cOL7XQwnuhV$e79fad5ec6f9231dc4e842ff392ac677743a5fd5cfa7bdb8e501417e9a86b73d

Figure 12: Encrypted Database

4. The reports themselves are also encrypted:

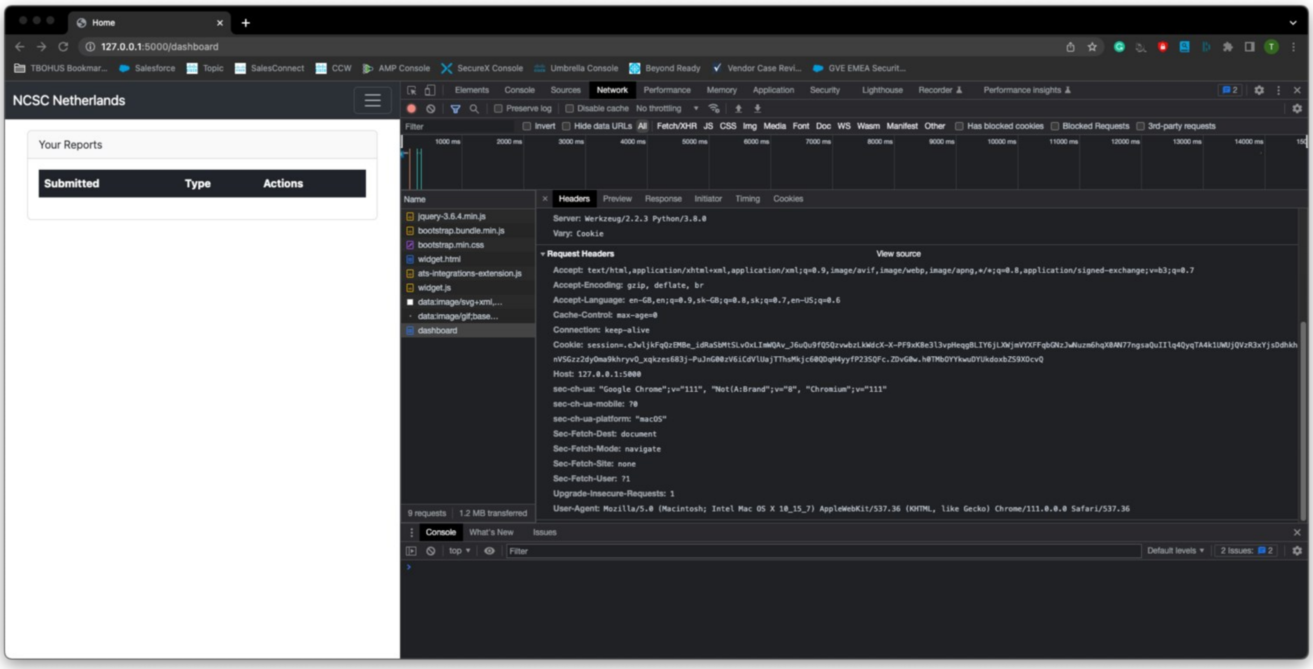


database-Report-2-report_content
instance > database-Report-2-report_content

```
gAAAABkKtSiaYP_w4SERgonJTH1ORNuc1PdmxUVSuCmyX5JfUK6rVsT09w2O1tyQ57JPmvAMgPfsllb4iUnJk4qKfuS2zFEUU5Xhb8hp2uWP3qKQ8nsNT5Hsm_rKWhXFC4zNcg2a
NmxUfXkkruTL4mGZVLhsk-tzPp7bvbaokqVvbfDCCU9aHMWYrvX-FCv7lJiKmvvNWovTmCpt5n77PxTu9FAdlEmp_m2d59sAbsDpW_XegLMTlQ=
```

Figure 13: Encrypted Report

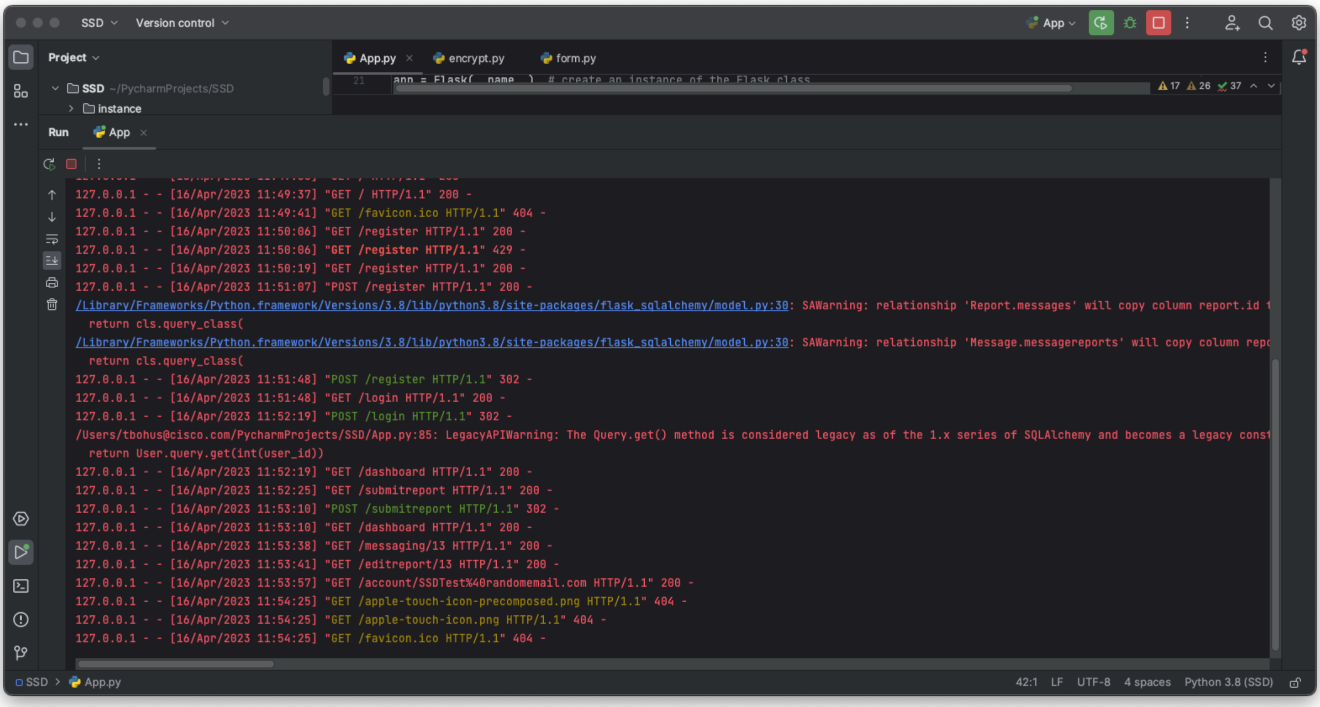
5. The application supports cookies to remember the user's session, this can be confirmed by inspecting HTTP headers provided by the application:



```
Server: Werkzeug/2.2.3 Python/3.8.0
Vary: Cookie
▾ Request Headers                                    View source
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.9,sk-GB;q=0.8,sk;q=0.7,en-US;q=0.6
Cache-Control: max-age=0
Connection: keep-alive
Cookie: session=.eJwljkFqQzEMBe_idRaSbMtSLvOxLImWQAv_J6uQu9fQ5QzvwbzLkWdcX-X-PF9xK8e3l3vpHeqgBLIY6jLXWjmVYXFFqbGNzJwNuzm6hqX0AN77ngsaQuIIlq4QyqTA4k1UWUjQVzR3xYjsDdhkh
nVSGzz2dyOma9khryvO_xqkzes683j-PuJnG00zV6iCdVlUajTThsMkjc60QDqH4yyfP23SQFc.ZDvG0w.h0TMbOYYkwuDYUkdoxbZS9XOcvQ
Host: 127.0.0.1:5000
sec-ch-ua: "Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
```

Figure 14: HTTP Headers

6. All the logs can be viewed in real-time, and with the use of additional mechanisms such as IPS/IDS, potentially malicious attempts can be intercepted as soon as possible based on the traffic pattern.



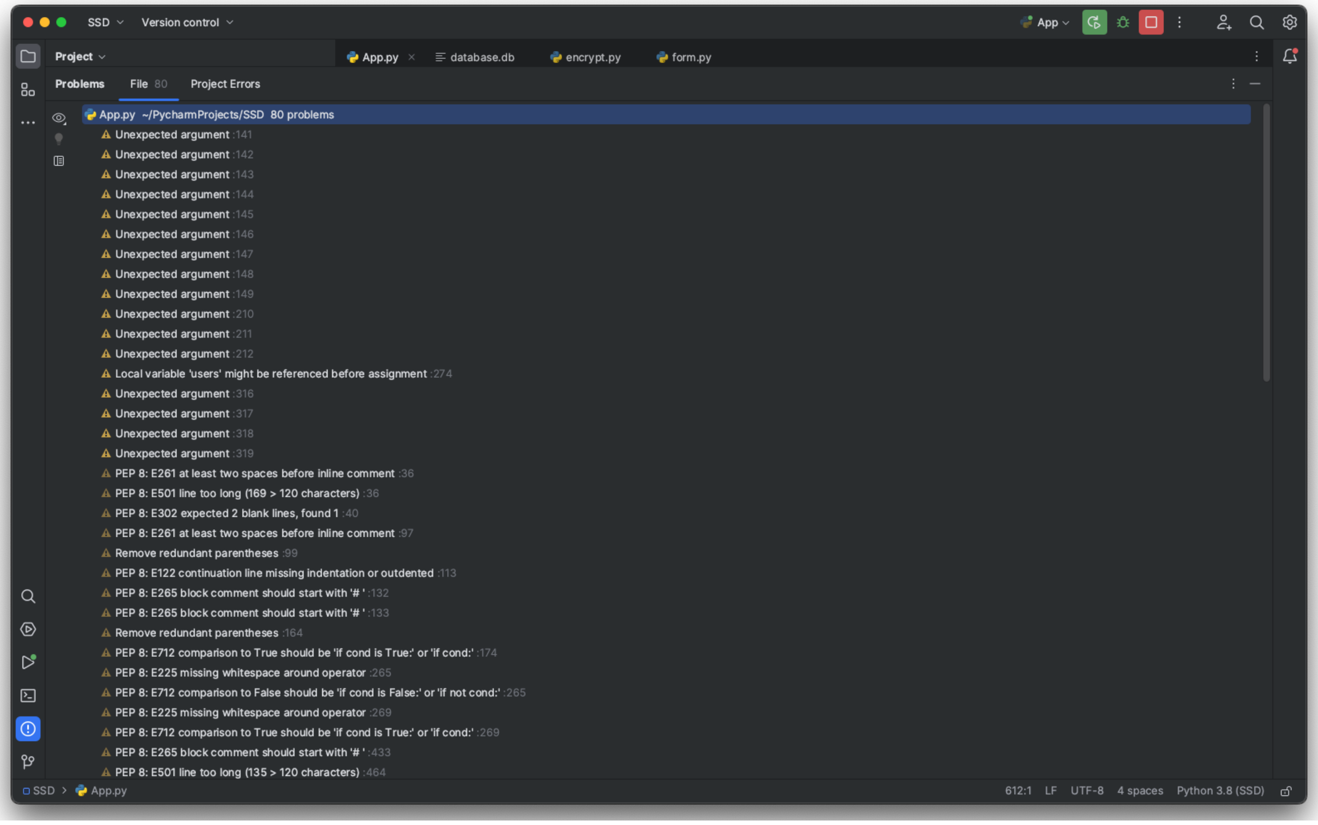
```
app = Flask(__name__)  # create an instance of the Flask class
```

```
127.0.0.1 - - [16/Apr/2023 11:49:37] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:49:41] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [16/Apr/2023 11:50:06] "GET /register HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:50:06] "GET /register HTTP/1.1" 429 -
127.0.0.1 - - [16/Apr/2023 11:50:19] "GET /register HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:51:07] "POST /register HTTP/1.1" 200 -
/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/site-packages/flask_sqlalchemy/model.py:30: SAWarning: relationship 'Report.messages' will copy column report.id t
  return cls.query_class(
/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/site-packages/flask_sqlalchemy/model.py:30: SAWarning: relationship 'Message.messagereports' will copy column repo
  return cls.query_class(
127.0.0.1 - - [16/Apr/2023 11:51:48] "POST /register HTTP/1.1" 302 -
127.0.0.1 - - [16/Apr/2023 11:51:48] "GET /login HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:52:19] "POST /login HTTP/1.1" 302 -
/Users/tbohus@cisco.com/PycharmProjects/SSD/App.py:85: LegacyAPIWarning: The Query.get() method is considered legacy as of the 1.x series of SQLAlchemy and becomes a legacy const
  return User.query.get(int(user_id))
127.0.0.1 - - [16/Apr/2023 11:52:19] "GET /dashboard HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:52:25] "GET /submitreport HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:53:10] "POST /submitreport HTTP/1.1" 302 -
127.0.0.1 - - [16/Apr/2023 11:53:10] "GET /dashboard HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:53:38] "GET /messaging/13 HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:53:41] "GET /editreport/13 HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:53:57] "GET /account/SSDTest%40randomemail.com HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2023 11:54:25] "GET /apple-touch-icon-precomposed.png HTTP/1.1" 404 -
127.0.0.1 - - [16/Apr/2023 11:54:25] "GET /apple-touch-icon.png HTTP/1.1" 404 -
127.0.0.1 - - [16/Apr/2023 11:54:25] "GET /favicon.ico HTTP/1.1" 404 -
```

Figure 15: Debugging Tool

Testing and Code clean-up

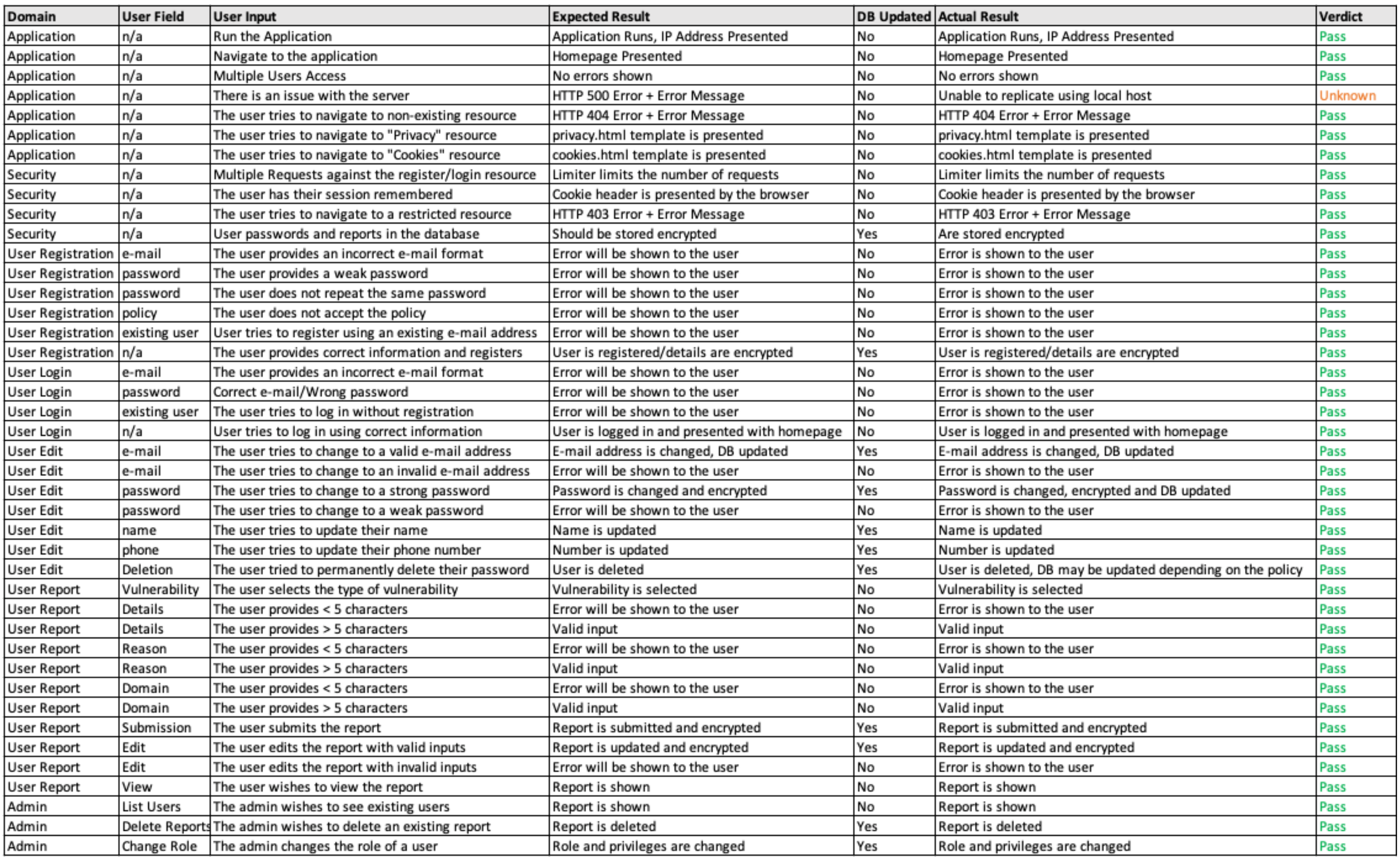
1. Built-in linters inside PyCharm and VS Code were used to test the structure as well as execution of the code. After any errors were resolved, we were left with variable-specific warnings, such as misspelling words (userreports, usermessages, …)



```
App.py ~/PycharmProjects/SSD 80 problems
    Unexpected argument :141
    Unexpected argument :142
    Unexpected argument :143
    Unexpected argument :144
    Unexpected argument :145
    Unexpected argument :146
    Unexpected argument :147
    Unexpected argument :148
    Unexpected argument :149
    Unexpected argument :210
    Unexpected argument :211
    Unexpected argument :212
    Local variable 'users' might be referenced before assignment :274
    Unexpected argument :316
    Unexpected argument :317
    Unexpected argument :318
    Unexpected argument :319
    PEP 8: E261 at least two spaces before inline comment :36
    PEP 8: E501 line too long (169 > 120 characters) :36
    PEP 8: E302 expected 2 blank lines, found 1 :40
    PEP 8: E261 at least two spaces before inline comment :97
    Remove redundant parentheses :99
    PEP 8: E122 continuation line missing indentation or outdented :113
    PEP 8: E265 block comment should start with '# ' :132
    PEP 8: E265 block comment should start with '# ' :133
    Remove redundant parentheses :164
    PEP 8: E712 comparison to True should be 'if cond is True:' or 'if cond:' :174
    PEP 8: E225 missing whitespace around operator :265
    PEP 8: E712 comparison to False should be 'if cond is False:' or 'if not cond:' :265
    PEP 8: E225 missing whitespace around operator :269
    PEP 8: E712 comparison to True should be 'if cond is True:' or 'if cond:' :269
    PEP 8: E265 block comment should start with '# ' :433
    PEP 8: E501 line too long (135 > 120 characters) :464
```

Figure 16: Linter Output

2. Finally all the possible inputs and complications were tested manually, using Google Chrome, as well as Safari, using both existing, newly created as well as admin accounts multiple times. The results of these tests are shown in the below screenshot:



Domain	User Field	User Input	Expected Result	DB Updated	Actual Result	Verdict
Application	n/a	Run the Application	Application Runs, IP Address Presented	No	Application Runs, IP Address Presented	Pass
Application	n/a	Navigate to the application	Homepage Presented	No	Homepage Presented	Pass
Application	n/a	Multiple Users Access	No errors shown	No	No errors shown	Pass
Application	n/a	There is an issue with the server	HTTP 500 Error + Error Message	No	Unable to replicate using local host	Unknown
Application	n/a	The user tries to navigate to non-existing resource	HTTP 404 Error + Error Message	No	HTTP 404 Error + Error Message	Pass
Application	n/a	The user tries to navigate to "Privacy" resource	privacy.html template is presented	No	privacy.html template is presented	Pass
Application	n/a	The user tries to navigate to "Cookies" resource	cookies.html template is presented	No	cookies.html template is presented	Pass
Security	n/a	Multiple Requests against the register/login resource	Limiter limits the number of requests	No	Limiter limits the number of requests	Pass
Security	n/a	The user has their session remembered	Cookie header is presented by the browser	No	Cookie header is presented by the browser	Pass
Security	n/a	The user tries to navigate to a restricted resource	HTTP 403 Error + Error Message	No	HTTP 403 Error + Error Message	Pass
Security	n/a	User passwords and reports in the database	Should be stored encrypted	Yes	Are stored encrypted	Pass
User Registration	e-mail	The user provides an incorrect e-mail format	Error will be shown to the user	No	Error is shown to the user	Pass
User Registration	password	The user provides a weak password	Error will be shown to the user	No	Error is shown to the user	Pass
User Registration	password	The user does not repeat the same password	Error will be shown to the user	No	Error is shown to the user	Pass
User Registration	policy	The user does not accept the policy	Error will be shown to the user	No	Error is shown to the user	Pass
User Registration	existing user	User tries to register using an existing e-mail address	Error will be shown to the user	No	Error is shown to the user	Pass
User Registration	n/a	The user provides correct information and registers	User is registered/details are encrypted	Yes	User is registered/details are encrypted	Pass
User Login	e-mail	The user provides an incorrect e-mail format	Error will be shown to the user	No	Error is shown to the user	Pass
User Login	password	Correct e-mail/Wrong password	Error will be shown to the user	No	Error is shown to the user	Pass
User Login	existing user	The user tries to log in without registration	Error will be shown to the user	No	Error is shown to the user	Pass
User Login	n/a	User tries to log in using correct information	User is logged in and presented with homepage	No	User is logged in and presented with homepage	Pass
User Edit	e-mail	The user tries to change to a valid e-mail address	E-mail address is changed, DB updated	Yes	E-mail address is changed, DB updated	Pass
User Edit	e-mail	The user tries to change to an invalid e-mail address	Error will be shown to the user	No	Error is shown to the user	Pass
User Edit	password	The user tries to change to a strong password	Password is changed and encrypted	Yes	Password is changed, encrypted and DB updated	Pass
User Edit	password	The user tries to change to a weak password	Error will be shown to the user	No	Error is shown to the user	Pass
User Edit	name	The user tries to update their name	Name is updated	Yes	Name is updated	Pass
User Edit	phone	The user tries to update their phone number	Number is updated	Yes	Number is updated	Pass
User Edit	Deletion	The user tried to permanently delete their password	User is deleted	Yes	User is deleted, DB may be updated depending on the policy	Pass
User Report	Vulnerability	The user selects the type of vulnerability	Vulnerability is selected	No	Vulnerability is selected	Pass
User Report	Details	The user provides < 5 characters	Error will be shown to the user	No	Error is shown to the user	Pass
User Report	Details	The user provides > 5 characters	Valid input	No	Valid input	Pass
User Report	Reason	The user provides < 5 characters	Error will be shown to the user	No	Error is shown to the user	Pass
User Report	Reason	The user provides > 5 characters	Valid input	No	Valid input	Pass
User Report	Domain	The user provides < 5 characters	Error will be shown to the user	No	Error is shown to the user	Pass
User Report	Domain	The user provides > 5 characters	Valid input	No	Valid input	Pass
User Report	Submission	The user submits the report	Report is submitted and encrypted	Yes	Report is submitted and encrypted	Pass
User Report	Edit	The user edits the report with valid inputs	Report is updated and encrypted	Yes	Report is updated and encrypted	Pass
User Report	Edit	The user edits the report with invalid inputs	Error will be shown to the user	No	Error is shown to the user	Pass
User Report	View	The user wishes to view the report	Report is shown	No	Report is shown	Pass
Admin	List Users	The admin wishes to see existing users	Report is shown	No	Report is shown	Pass
Admin	Delete Reports	The admin wishes to delete an existing report	Report is deleted	Yes	Report is deleted	Pass
Admin	Change Role	The admin changes the role of a user	Role and privileges are changed	Yes	Role and privileges are changed	Pass

Figure 17: Testing Summary