



Silesian
University
of Technology

FINAL PROJECT

Interactive security training platform based on CTF concept

Krzysztof Marek DZIEMBAŁA

Student identification number: 293671

Programme: Control, Electronic, and Information Engineering

Specialisation: Informatics

SUPERVISOR

dr inż. Dominik Samociuk

DEPARTMENT Department of Computer Networks and Systems

Faculty of Automatic Control, Electronics and Computer Science

Gliwice 2023

Thesis title

Interactive security training platform based on CTF concept

Abstract

(Thesis abstract – to be copied into an appropriate field during an electronic submission – in English.)

Keywords

(2-5 keywords, separated with commas)

Tytuł pracy

Interaktywna platforma do nauki bezpieczeństwa wykorzystująca zadania typu CTF

Streszczenie

(Thesis abstract – to be copied into an appropriate field during an electronic submission – in Polish.)

Słowa kluczowe

(2-5 keywords, separated by commas, in Polish)

Contents

1	Introduction	1
2	[Problem analysis]	3
3	Requirements and tools	5
3.1	Functional requirements	5
3.2	Non-functional requirements	7
3.3	Use cases	8
3.4	Tools	8
3.4.1	Core tools	8
3.4.2	Development tools	10
3.5	Methodology of design and implementation	11
3.5.1	Design	11
3.5.2	Implementation	11
4	External specification	15
4.1	Hardware and software requirements	15
4.1.1	Browser	15
4.1.2	Server software	16
4.2	Server installation	17
4.3	Initial configuration	18
5	Internal specification	19
6	Verification and validation	21
7	Conclusions	23
	Bibliography	25
	Index of abbreviations and symbols	29
	Listings	31

List of additional files in electronic submission (if applicable)	35
List of figures	37
List of tables	39

Chapter 1

Introduction

- introduction into the problem domain
- settling of the problem in the domain
- objective of the thesis
- scope of the thesis
- short description of chapters
- clear description of contribution of the thesis's author – in case of more authors
table with enumeration of contribution of authors

Chapter 2

[Problem analysis]

- problem analysis
- state of the art, problem statement
- literature research (all sources in the thesis have to be referenced [3, 2, 4, 5])
- description of existing solutions (also scientific ones, if the problem is scientifically researched), algorithms, location of the thesis in the scientific domain

Mathematical formulae

$$y = \frac{\partial x}{\partial t} \tag{2.1}$$

and single math symbols x and y are typeset in the mathematical mode.

Chapter 3

Requirements and tools

The project development consisted of multiple stages. One of the most important parts was specifying requirements, which then dictated tool selection and the design process.

3.1 Functional requirements

Functional requirements list functionality available in the system. Each of the requirements contains a description detailing the desired behaviour.

1. **Account creation:** Users must be able to register an account in the system. This operation requires username and password submission from an HTML form in a POST request. Registration is allowed only using unique username. If there already exists an account in the system with the same username, the action must be refused. As a result of a successful registration, a document with the username, cryptographic hash of the user's password and a default role "**user**" is inserted into a collection storing user accounts. After the registration succeeds, the user is redirected to the login page.
2. **Signing in:** Users must be able to log into their accounts. Username and password must be sent in a POST request as HTML form data. The operation must fail if there is no account in the database with the provided username or if the password hash does not match the one stored in the database. If there has been no failure, a session is created and the user is redirected to the home page.
3. **Logging out:** Users must be able to log out of their accounts. It is expected that the user is signed in when they log out. This operation destroys the session (if any) and redirects to the home page.
4. **Changing password:** Users must be able to change their account password. New password must be sent in a POST request as HTML form data. User must be logged

in in order to change the password. As a result of this operation, user's password hash in the database is updated.

5. **Listing categories:** Users must be able to see a list of categories that exist in the system. List of categories must link to category pages.
6. **Displaying category:** Users must be able to see category details on a category page. The details should include category name, description and a list of related tasks.
7. **Displaying task:** Users must be able to display task details on task pages. The details should include task name, description, challenge URL, hints (if any), and if the user is logged in, a flag submission form. If the task has been solved by the user, instead of the flag submission form, a question is displayed.
8. **Solving challenge:** Users must be able to submit a form with flag from the task page. This action is allowed only for signed in users. Submitted flag must be verified with the one stored in the database for the given challenge. If the flags match, a success message should be shown to the user and date of solving the challenge by user ought to be saved to the database. Otherwise, a message informing the user about incorrect flag should be presented.
9. **Answering quiz:** User who have solved the main challenge from a task, should be able to to see a question on the task page and be able to answer it. Only signed in users can submit answers. Checkboxes which status indicates whether the user thinks that they are correct must be presented along answers from the database. After the answers are submitted, the quiz should be disabled without a button to submit, checkboxes disabled and reflecting the user's answer and an indication which answers were correct.
10. **Administrator panel:** Users with the "admin" role (administrators) should have access to a separate administration panel. The panel should expose additional functionality related to the system management.
11. **Listing users:** Users with access to the administrator panel should be able to get a list of user account in the system. Each entry must contain information about username and user role. The list should be paginated as there may exist many accounts.
12. **Changing user permissions:** Administrators should be able to grant the "admin" role to other users, as well as change it back to "user".
13. **Deleting user:** Administrators should be able to remove user accounts from the database. It must not be possible to remove own user account this way.

14. **Creating category:** Administrators must be able to create new categories. The categories must have a name and description. The description must support Markdown input.
15. **Editing category:** Administrators must be able to edit the name and description of existing categories.
16. **Creating task:** Administrators must be able to add new tasks to the system. For each task it must be possible to set the name, description (in Markdown), hints, challenge details, question, answers to the question. Each answer must be marked as correct or incorrect.
Challenge details must include:
 - Docker image to pull and start,
 - subdomain used for serving the challenge,
 - flag that the users will try to find,
 - an interval specifying how frequently the challenge container should be regenerated
17. **Starting challenges:** The system must be able to pull challenge images, create and containers and direct connections to specified subdomains into appropriate containers. This must be done automatically during system startup and for each new challenge added when creating new tasks.

3.2 Non-functional requirements

1. **Responsiveness:** UI should properly scale across different display sizes. It must be mobile-friendly.
2. **Accessibility:** There should be no errors in the Accessibility section of a webhint scan.
3. **Visual consistency:** A single set of styling rules, such as colours, fonts and icons should be used across whole user interface.
4. **Page load performance:** The system should have a score of over 90 in PageSpeed Insights report for mobile.
5. **Compatibility:** User interface should work in latest (as of January 2023) versions of Firefox, Firefox ESR, Chrome and Safari browsers for desktops and mobile devices. Basic system functionality, except for the administrator panel, should be available in browsers with JavaScript disabled.

3.3 Use cases

The use case diagram presented on Fig. 3.1 shows actions offered to actors using the system. There are two actors, with different sets of allowed interactions. The actor *User* represents anyone with access to the system. Users with special account role "admin", which allows them to perform operations related to management of the system.

3.4 Tools

The implementation of the project significantly benefited from publicly available tools. Used tools are divided into two classes, depending on the way they were used.

3.4.1 Core tools

The system is built on tools, which are regarded to as *core tools*. These are required for operation and are a part of the system architecture.

Node.js + Express + EJS

Node.js is a JavaScript runtime based on V8 engine. There is an enormous ecosystem built around Node.js with over 1.3 million packages available in the npm registry [1]. The server code runs on Node.js and uses the Express framework for request routing and middleware management. Express is a popular web framework with many features and compatible middleware packages. One of Express' features is template rendering support. The project uses EJS templates, which allows creating HTML templates using embedded JavaScript logic.

MongoDB

MongoDB is a NoSQL document-oriented database capable of storing BSON documents. Because BSON stands for Binary JSON, which in turn is JavaScript Object Notation, it integrates nicely with JavaScript. The MongoDB Node.js driver also supports TypeScript, which helps with suggestions and type checking. During development MongoDB Compass, MongoDB Visual Studio Code extension and mongosh were used. These tools allow database management and, except for mongosh, provide helpful user interfaces.

Docker

Docker is a platform for managing containerised software. Challenges are running as Docker containers and managed using Docker Engine API. For debugging, development

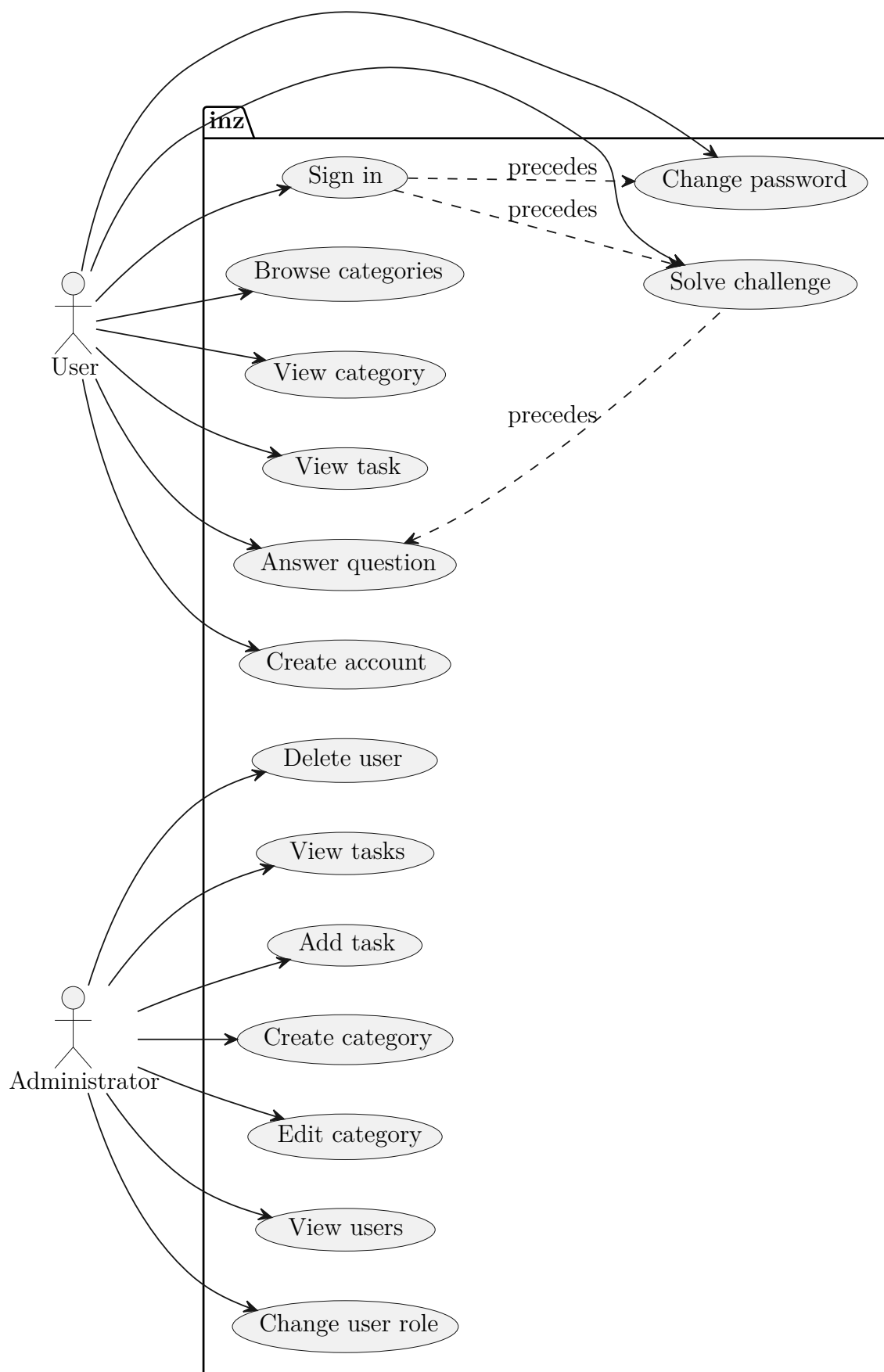


Figure 3.1: Use case diagram

and management standalone Docker tools such as Docker CLI and Docker Desktop can be used.

nginx

To manage multiple domains and subdomain on a single system with one external network interface nginx was used as a proxy. nginx offers multiple functionalities besides proxying. It is also used to serve static files, redirect to HTTPS protocol and terminate TLS connections.

Bootstrap

Bootstrap is a frontend toolkit, which is helpful for designing user interfaces. It provides CSS classes and JavaScript utilities to help with styling and providing interactivity in HTML without the need to write own style sheets and JS scripts.

3.4.2 Development tools

The following tools are in no way required for the systems. These were used to aid development.

Visual Studio Code

Visual Studio Code is a multi-platform code editor that was heavily used for writing the software. It was chosen for multiple reasons, most important of which was familiarity and experience with the tool. This editor supports many languages, especially for JavaScript and related web technologies. Particularly notable is built-in TypeScript support, which can be used with JSDoc comments to improve IntelliSense suggestions. A huge advantage of Visual Studio Code is a broad selection of available extensions.

Git

The project is stored in a Git repository to track changes in the code. The repository is synchronised with GitHub to share it between devices.

ESLint

ESLint is a JavaScript linter, which can be used to detect problems and potential issues in code. It was used with a Visual Studio Plugin, which automatically analysed open files and provided in-editor warnings and suggestions.

Prettier

Prettier is a popular code formatting tool. It was used to maintain a consistent style in JavaScript files. Thanks to Visual Studio Code plugin the tool could be used as a default formatter in the editor. A plugin for ESLint allowed marking improperly formatted code as lint error.

3.5 Methodology of design and implementation

The development process was split into two parts. Before the implementation started the system had to be designed.

3.5.1 Design

The first step in designing the project was defining initial requirements. This resulted in the first (and only) UI concept drawing, which is presented on Fig. 3.2. It was meant to help with defining the exact functionality and the structure of documents in the database. Based on that the structure presented on Fig. 3.3 was created.

After those first ideas were noted, the process of defining the architecture began. The choice of Node.js and Express as a base for the server was easy, as the author had already years of experience with those tools. Similarly, MongoDB was selected as a database server, because of experience and because it can store arrays and objects. To improve experience on low-end devices and enable basic functionality on browsers without JavaScript, server-side rendering was chosen instead of a JavaScript user interface library such as React or Vue. For a template rendering engine two solutions were considered - Handlebars and EJS. Ultimately, EJS was chosen, because of its richer capabilities.

The last problem to solve during the design phase, was coming up with an idea to direct different subdomains to appropriate challenge containers. The simplest solution was using a wildcard DNS record and setting up virtual servers in the proxy (Fig. 3.4). Creation of subdomains could be achieved by creating additional configuration files, which could be automatically picked up by the proxy on reload.

3.5.2 Implementation

The implementation started with setting up a Node.js project with some of the required dependencies and a basic *Hello world* Express server. Additional tools such as Eslint were also set up at the beginning so that they could be used during the development.

The next step was preparing database connection and setting up code for session support. Once the server could handle sessions, related utilities such as message flashing were prepared. Sessions were required to implement authentication, which was done in

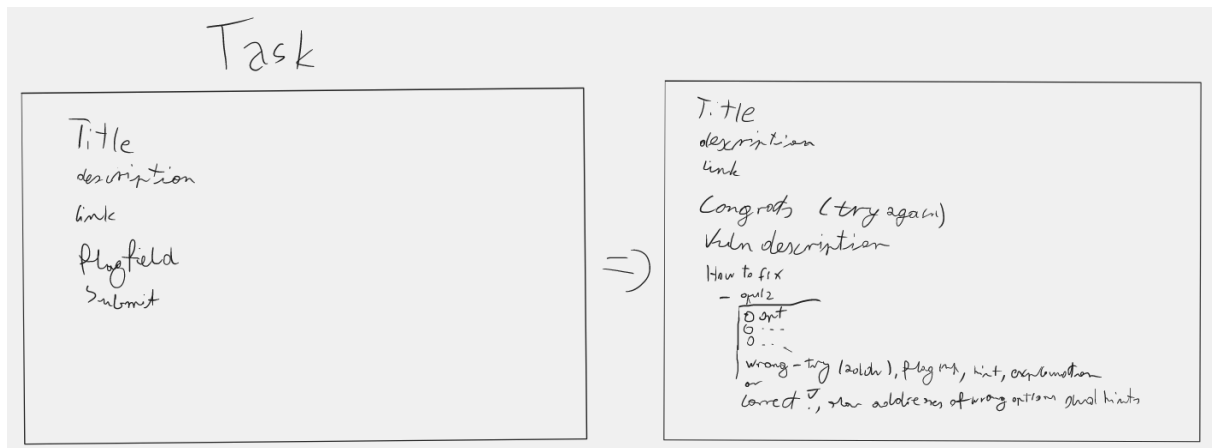


Figure 3.2: Initial task page UI sketch before and after solving the challenge.

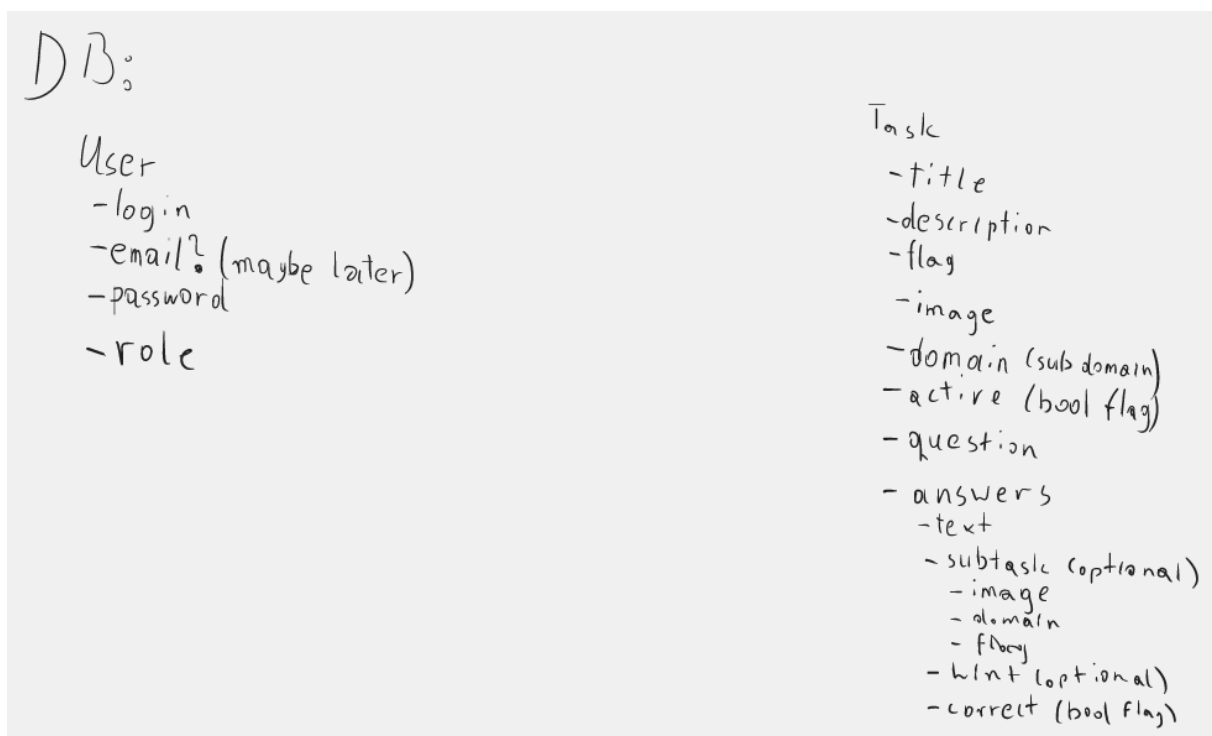


Figure 3.3: Initial design of documents representing users and tasks.

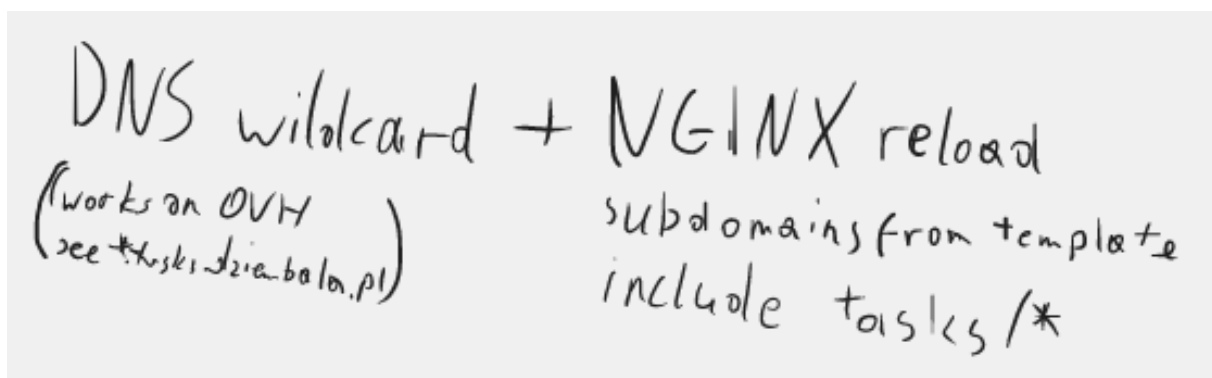


Figure 3.4: Subdomain management design idea.

the next step. The first part of implementing authentication was enabling user account creation, so that it would be possible to test each element as it was developed. With the code responsible for registration ready, logging in could be worked on. In both cases the server logic was prepared first with the UI following right after to test the whole component.

After the authentication was done and there were some simple pages ready, work on styling the interface could begin. This stage of the development was realised at that moment, because there were already pages which could be tested with the styles and could serve as a base for later content.

Before more public pages could be created, an administration panel had to be made in order to insert data for testing. Unlike all other components, this panel required a lot of interactivity and relied on client-side scripting. To facilitate this requirement, the server code exposes REST-like API, which is consumed by scripts running in the browser. The administrator panel started with user management, continued to category management and finished with task creation.

Since some of the inputs supported Markdown, a Markdown parser was integrated on both the server and in browser. To allow for syntax highlighting in code blocks, `highlight.js` was added to the Markdown parser. Syntax highlighting required additional styles, which were available separately in light and dark modes and would not integrate well with Bootstrap's theming. To avoid this problem, a variable-based style sheet with colours from Panda Syntax Light and Dark themes was created with CSS variables set depending on the theme used in Bootstrap.

With the last part of the administration panel, task creation, a system for managing challenge containers had to be prepared. During the implementation of this functionality, the initial database schema shown on Fig 3.3 was recognised as suboptimal and had to be changed.

Finally, user-facing category and task pages were prepared. Because these were template-based and in case of the task page relatively complicated, the user interface and server code were implemented in parallel. As a finishing touch a simple home page was added.

Chapter 4

External specification

- hardware and software requirements
- installation procedure
- activation procedure
- types of users
- user manual
- system administration
- security issues
- example of usage
- working scenarios (with screenshots or output files)

4.1 Hardware and software requirements

Depending on whether one wants to use the user interface via a web browser or host the server themselves there are different requirements for each part.

4.1.1 Browser

The user interface requires a modern browser with JavaScript enabled. It is possible to use the system without JS, but theme switching and dropdowns in the navigation bar will not work.

On desktop the latest stable versions of the following browsers are supported:

- Google Chrome
- Microsoft Edge

- Firefox and Firefox ESR
- Opera
- Safari (macOS only)

On Android and iOS support is restricted to the latest stable versions of:

- Google Chrome
- Firefox
- Safari (iOS only)
- Android Browser and WebView (Android only)

Different and older browsers may work, but compatibility is not guaranteed.

4.1.2 Server software

The server software requires the following external software to be installed:

- Node.js 18.x or newer (not as a snap)
- MongoDB 6.0
- Docker Engine 20.10
- nginx 1.23.2 or newer

Supported operating systems:

- Ubuntu 20.04 or newer (x86-64, arm64)
- macOS 11 (x86-64), 12 or newer (x86-64, arm64)
- Windows 10 1809 or newer (x86-64)
- Windows Server 2019 or newer (x86-64)

It may be possible to run the server on other operating systems and architectures as long as the required software can be installed. These unsupported systems, however, will probably require additional installation steps related to **argon2** package setup.

Warning: Challenge Docker images must be compatible with the server architecture. Images presented in this project support only x86-64.

4.2 Server installation

The process of server software installation and configuration can be summarised in the following steps:

1. Install the required software as described in section 4.1.2.

2. Obtain the code from GitHub:

```
git clone https://github.com/krzysdz/inz.git
```

3. Navigate to the downloaded project directory:

```
cd inz
```

4. Install required npm packages:

```
npm install --omit=dev
```

5. Configure MongoDB as a replica set (tutorial).

6. Configure the DNS to point the main domain and the challenges domain to the server. Example DNS configuration:

```
main-ui.com.      60  IN  A           127.0.0.1
*.challenges.com. 60  IN  CNAME        main-ui.com.
```

7. Obtain TLS certificate for the main domain and the challenges domain. One certificate should cover both domains (the second one with wildcard).

The key and certificate files should be placed in `nginx/certs` and named according to instructions from the `README` file in that directory.

8. Adjust values in the `config.js` file.

9. Start nginx with prefix set to `./nginx` and configuration `nginx/conf/nginx.conf`:

```
nginx -p ./nginx -c ./nginx/conf/nginx.conf
```

10. Set `NODE_ENV` to production:

Bash/dash/zsh/csh:

```
export NODE_ENV="production"
```

Powershell:

```
$env:NODE_ENV="production"
```

11. Start the server:

```
node index.js
```

12. *Optional.* Configure services to automatically start the software. Example configuration for systemd based operating systems:

- (a) Modify the default `mongod.conf` file to specify replica set name as shown on Fig. 1 and enable the mongod service:
`systemctl enable mongod`
- (b) Create a unit file for the proxy. An example is presented on Fig. 2.
- (c) Create a unit file for the main server. An example is presented on Fig. 3.
- (d) Enable and start the services:

```
# Reload systemd configuration to pick up the new services
systemctl daemon-reload
# Enable the services to run at boot
systemctl enable inz-nginx
systemctl enable inz
# Start the server and proxy (required by inz.service)
systemctl start inz
```

4.3 Initial configuration

If setting up the server with a fresh database, an administrator account must be created. To do this, one has to:

- Create a user account (`/auth/register`).
- Set the `role` field of the user document to string `admin`. A Node.js script which does that is presented on Fig. 4.
- Log in into the account again.

Chapter 5

Internal specification

- concept of the system
- system architecture
- description of data structures (and data bases)
- components, modules, libraries, resume of important classes (if used)
- resume of important algorithms (if used)
- details of implementation of selected parts
- applied design patterns
- UML diagrams

Use special environments for inline code, eg `int a;` (package `minted`) . Longer parts of code put in the figure environment, eg. code in Fig. 5.1 . Very long listings—move to an appendix.

```
1 class test : public basic
2 {
3     public:
4         test (int a);
5         friend std::ostream operator<<(std::ostream & s,
6                                         const test & t);
7     protected:
8         int _a;
9
10 };
```

Figure 5.1: Pseudocode in minted.

Chapter 6

Verification and validation

- testing paradigm (eg V model)
- test cases, testing scope (full / partial)
- detected and fixed bugs
- results of experiments (optional)

Table 6.1: A caption of a table is **above** it.

ζ	method						
	alg. 1	alg. 2	alg. 3			alg. 4, $\gamma = 2$	
			$\alpha = 1.5$	$\alpha = 2$	$\alpha = 3$	$\beta = 0.1$	$\beta = -0.1$
0	8.3250	1.45305	7.5791	14.8517	20.0028	1.16396	1.1365
5	0.6111	2.27126	6.9952	13.8560	18.6064	1.18659	1.1630
10	11.6126	2.69218	6.2520	12.5202	16.8278	1.23180	1.2045
15	0.5665	2.95046	5.7753	11.4588	15.4837	1.25131	1.2614
20	15.8728	3.07225	5.3071	10.3935	13.8738	1.25307	1.2217
25	0.9791	3.19034	5.4575	9.9533	13.0721	1.27104	1.2640
30	2.0228	3.27474	5.7461	9.7164	12.2637	1.33404	1.3209
35	13.4210	3.36086	6.6735	10.0442	12.0270	1.35385	1.3059
40	13.2226	3.36420	7.7248	10.4495	12.0379	1.34919	1.2768
45	12.8445	3.47436	8.5539	10.8552	12.2773	1.42303	1.4362
50	12.9245	3.58228	9.2702	11.2183	12.3990	1.40922	1.3724

Chapter 7

Conclusions

- achieved results with regard to objectives of the thesis and requirements
- path of further development (eg functional extension ...)
- encountered difficulties and problems

Bibliography

- [1] Ahmad Nassri. *So long, and thanks for all the packages!* 2020. URL: <https://blog.npmjs.org/post/615388323067854848/so-long-and-thanks-for-all-the-packages> (visited on 19/01/2023).
- [2] Name Surname and Name Surname. *Title of a book*. Hong Kong: Publisher, 2017. ISBN: 83-204-3229-9-434.
- [3] Name Surname and Name Surname. ‘Title of an article in a journal’. In: *Journal Title* 157.8 (2016), pp. 1092–1113.
- [4] Name Surname, Name Surname and N. Surname. ‘Title of a conference article’. In: *Conference title*. 2006, pp. 5346–5349.
- [5] Name Surname, Name Surname and N. Surname. *Title of a web page*. 2021. URL: <http://somewhere/on/the/internet.html> (visited on 30/09/2021).

Appendices

Index of abbreviations and symbols

CTF Capture The Flag

UI User Interface

SQL Structured Query Language

CSS Cascading Style Sheet

HTML HyperText Markup Language

JS JavaScript

Listings

(Put long listings here.)

```
1  if (_nClusters < 1)
2      throw std::string ("unknown number of clusters");
3  if (_nIterations < 1 and _epsilon < 0)
4      throw std::string ("You should set a maximal number of iteration
    ↪ or minimal difference -- epsilon.");
5  if (_nIterations > 0 and _epsilon > 0)
6      throw std::string ("Both number of iterations and minimal epsilon
    ↪ set -- you should set either number of iterations or minimal
    ↪ epsilon.");
```

```
1  # mongod.conf
2
3  # for documentation of all options, see:
4  #   http://docs.mongodb.org/manual/reference/configuration-options/
5
6  # Where and how to store data.
7  storage:
8    dbPath: /var/lib/mongodb
9
10 # where to write logging data.
11 systemLog:
12   destination: file
13   logAppend: true
14   path: /var/log/mongodb/mongod.log
15
16 # network interfaces
17 net:
18   port: 27017
19   bindIp: 127.0.0.1
20
21 # how the process runs
22 processManagement:
23   timeZoneInfo: /usr/share/zoneinfo
24
25 replication:
26   replSetName: rs0
```

Figure 1: Example `/etc/mongod.conf` configuration file. Based on the default config for Debian and Ubuntu

```
1 # /etc/systemd/system/inz-nginx.service
2
3 [Unit]
4 Description=nginx proxy for inz
5 Documentation=https://nginx.org/en/docs/
6 After=network-online.target remote-fs.target nss-lookup.target
7 Wants=network-online.target
8
9 [Service]
10 Type=forking
11 PIDFile=/run/nginx.pid
12 WorkingDirectory=/inz
13 ExecStart=/usr/sbin/nginx -p /inz/nginx -c /inz/nginx/conf/nginx.conf
14 ExecReload=/bin/sh -c "/bin/kill -s HUP $(/bin/cat /run/nginx.pid)"
15 ExecStop=/bin/sh -c "/bin/kill -s TERM $(/bin/cat /run/nginx.pid)"
16
17 [Install]
18 WantedBy=multi-user.target
```

Figure 2: Example unit file for the nginx proxy. Project root is assumed to be /inz.

```
1 # /etc/systemd/system/inz.service
2
3 [Unit]
4 Description=inz server
5 After=network-online.target remote-fs.target nss-lookup.target
6 ↳ mongod.service inz-nginx.service
7 Wants=network-online.target
8 Requires=mongod.service inz-nginx.service
9
10 [Service]
11 Type=simple
12 WorkingDirectory=/inz
13 Environment="NODE_ENV=production"
14 # Remember to change the secret!
15 Environment="SECRET=SECRET"
16 ExecStart=/usr/bin/node /inz/index.js
17 ExecStop=/bin/kill -s TERM $MAINPID
18
19 [Install]
20 WantedBy=multi-user.target
```

Figure 3: Example unit file for the main server. Project root is assumed to be /inz.

```
1 import { MongoClient } from "mongodb";
2 import { DB_NAME, DB_URL } from "./config.js";
3
4 const USERNAME = "administrator_username";
5
6 const client = new MongoClient(DB_URL, { directConnection: true });
7 await client
8     .db(DB_NAME)
9     .collection("users")
10    .updateOne({ _id: USERNAME }, { $set: { role: "user" } });
11 await client.close();
```

Figure 4: A simple Node.js script, which makes the user `administrator_username` an administrator.

List of additional files in electronic submission (if applicable)

Additional files uploaded to the system include:

- source code of the application,
- test data,
- a video file showing how software or hardware developed for thesis is used,
- etc.

List of Figures

3.1	Use case diagram	9
3.2	Initial task page UI sketch before and after solving the challenge.	12
3.3	Initial design of documents representing users and tasks.	12
3.4	Subdomain management design idea.	12
5.1	Pseudocode in <code>minted</code>	20
1	Example <code>/etc/mongod.conf</code> configuration file. Based on the default config for Debian and Ubuntu	32
2	Example unit file for the nginx proxy. Project root is assumed to be <code>/inz</code>	33
3	Example unit file for the main server. Project root is assumed to be <code>/inz</code>	33
4	A simple Node.js script, which makes the user <code>administrator_username</code> an administrator.	34

List of Tables

6.1	A caption of a table is above it.	22
-----	--	----