Projektdokumentation

Modul: Web Engineering 2

Projektname: Capture The Flag

Kurs: TINF24AI2

Autoren: Sarah Josuweit, Elias Ciuman

Matrikelnummern: 5113643, 6265147

Abgabedatum: 22.06.2025

Inhaltsverzeichnis

1. Technische Dokumentation

Im Rahmen des Moduls “Web Engineering 2” wurde das Projekt “Capture The Flag” entwickelt, um mehrere Rätsel in einer Web-Anwendung zu kombinieren. Die Benutzer sollen sich gegenseitig mit ihren Bestzeiten unterbieten können. Dabei sollen die Benutzer neue Dinge lernen, die mit der Welt der Informatik in Zusammenhang stehen. Darunter fallen unter anderem SQL-Injections, Hex-Farben, Cäsar-Verschlüsselungen, usw.
Die Web-Anwendung decken die Anforderungen, welche im Rahmen des Moduls “Web Engineering 1 und 2” in Form von HTML für die Struktur, CSS für die Darstellung, PHP für die serverseitige Logik und Dynamik sowie einer Datenbankanbindung mit Hilfe einer MySQL-Datenbank gestellt wurden, ab.

Es wurde darauf geachtet eine strukturierte und klare Trennung von Struktur, Darstellung und Logik zu erreichen durch folgende Ordnerstruktur:

capture-the-flag-main/Projekt-CaptureTheFlag

```
├── assets/
│   └── icons/
│       └── flag-fill.svg
│   └── images/
│       ├── combie.png
│       ├── CTFflag_large.png
│       └── CTFflag.png
│   └── style/
│       └── style.css
├── challenges/
│   ├── anagramms.php
│   ├── combie.php
│   ├── encryption.php
│   ├── login.php
│   └── SQL_Injection.php
├── databases/
│   ├── time.php
│   └── users.php
├── index.js
├── index.php
├── modal.php
└── ziel.php
```

- assets/…: Alle nötigen Bilder, Icons sowie das Stylesheet für die Gestaltung der Website
- challenges/…: Separate Dateien für jedes Rätsel
- databases/…:
    - time.php: Aufbau SQL-Verbindung, behandelt Leaderboard
    - users.php: Tabelle für SQL Injection
- index.js: Nötig für Animation auf der Startseite
- index.php: Startseite mit Usernamen-Eingabe und Leaderboard
- modal.php: Vorlage für Hinweisfenster für Rätsel
- ziel.php: Letzte Seite nachdem alle Rätsel gelöst wurden

Verwendete Technologien:

Technologie	*Verwendung im Projekt*
HTML5	Aufbau der Grundstruktur der Website unter Einhaltung der HTML-Standards
CSS3	Styling aller Seiten über ein externes Stylesheet
PHP 8	Datenbank-Anbindungen, Verarbeitung von Formularen(Server-seitig)
MySQL	Speichern von Benutzernamen, Platzierung und Bearbeitungszeiten, sowie Placeholder-User für die SQL-Injection
JavaScript	Animationen auf Startseite, vergrößern des Bildes für bessere Sichtbarkeit
XAMPP	PHP-Entwicklungsumgebung zum lokalen Testen und Nutzen der CTF mit Apache und MySQL

Die Capture The Flag-Anwendung ist übereinstimmend mit HTML5-Standards aufgebaut. Hauptsächlich wurde <form> verwendet, um die verschiedenen Benutzereingaben für die Rätsel zu verarbeiten. <button>-Tags wurden verwendet, um zum einen Hinweise zu den Rätseln anzuzeigen, und zum anderen, um den Nutzer auf die nächsten Rätsel weiterzuleiten. Schließlich wurden - um die Struktur der Webseiten zu gewährleisten - -Container genutzt. Das eigentliche Layout und Styling geschieht über eine einzige externe CSS-Datei. Auf jeder Seite wurde auf eine mittige Anordnung des Seiteninhalts und konsistentes Styling geachtet. Sowohl die Farben als auch die Schriftart wurden gewählt, um dem Spieler eine Retro-Videospiel-ähnliche Ästhetik zu vermitteln.
JavaScript wurde vereinzelt benutzt, um die Spielerfahrung zu verbessern. Hierbei wurde erstens ein Skript hinzugefügt, welches den Text auf der Startseite animiert, zweitens wurde dem Spieler im kombinierten Rätsel die Möglichkeit gegeben, das Bild mit einer versteckten Zahl zu vergrößern und sie somit einfacher zu finden.
PHP Version 8 wurde in diesem Projekt verwendet, um die Benutzereingaben zu überprüfen und zu verarbeiten. Hierbei erfolgen jegliche Benutzereingaben über POST-Requests. Es ist zu beachten, dass bei der SQL-Injection absichtlich auf eine

sichere Übergabe der Eingabeparameter verzichtet wurde, denn die Sicherheitslücke ist Voraussetzung des Rätsels.
Session-Management wurde genutzt, um zu überprüfen, wann ein Spieler erfolgreich alle Rätsel abgeschlossen hat.
Schleifen innerhalb von PHP wurden vereinzelt verwendet, um mehrfach auftretende HTML-Elemente auf einmal zu generieren: beispielsweise in anagramms.php, bei welcher die fünf Aufgabenblöcke untereinander erstellt werden.
Um zu verhindern, dass ein Spieler über die Adressleiste Zugriff auf ziel.php erlangt, wurden mit PHP Teil-Flaggen in jedes Rätsel eingebaut. Ein weiteres wichtiges PHP-Element, welches über alle Rätsel hinweg verwendet wurde, sind Hinweise zu den jeweiligen Rätseln.

Es werden zwei relationale Datenbanken für die Anwendung genutzt:

zeiten
Speichert Nutzernamen und benötigte Zeit zum Lösen aller Rätsel
id
username
start_zeit
end_zeit
dauer

users
Stellt drei Nutzer zur Verfügung, wobei nur der Admin-Account für die SQL-Injection verwendet werden soll
id
username
password

1.1 Serverseitige Logik
Formularverarbeitung:
Die Daten aus den Formularen werden über POST empfangen und validiert.

Session-Management:
Nach dem der User seinen Benutzernamen eingetragen und das Rätsel gestartet hat wird eine Session gestartet, um den Benutzernamen zu behalten um die Timestamps sowie die Teil-Flags für die Überprüfung am Ende zu realisieren, ob der Spieler alle Rätsel erfolgreich abgeschlossen hat

1.2 Datenbankzugriffe

Die Datenbankverbindung erfolgt mit mysqli.
Code-Beispiel: Datenbank erstellen

```
$sql = “CREATE DATABASE IF NOT EXISTS ctf”;
if($conn->query($sql) === TRUE) {
        echo “”;
} else {
        echo “Fehler beim Erstellen der Datenbank”. $conn->error;
```

Zur Erstellung der Datenbank wird das Skript (time.php) verwendet. Dieses wird beim erstmaligen Öffnen der Startseite aufgerufen. In der Datenbank findet man zwei Haupttabellen, wobei eine davon für die Highscore Tabelle verwendet wird (“zeiten”) sowie eine Tabelle “users”. Diese wird verwendet, um Nutzer zur Verfügung zu stellen, mit welchen ein Login durchzuführen ist. Dieser Login geschieht per SQL-Injection in der login.php und ist Teil des Rätsels und ist demnach beabsichtigt.
Die Tabelle “zeiten” besteht aus fünf Feldern: id, username, start_zeit, end_zeit und dauer. Dabei ist das Feld “id” der Primärschlüssel. Sobald der Spieler seinen Usernamen eingetragen hat und auf Rätsel starten klickt, wird der Eintrag in der Tabelle erstellt. Dabei wird in start_zeit ein Timestamp vom aktuellen Datum sowie Uhrzeit verwendet. Am Ende, nach dem der Spieler die Flagge eingesammelt hat, wird in end_zeit eine weiterer Timestamp gesetzt und das Feld “dauer” wird automatisch berechnet und die Sekunden werden eingetragen. Auf der Startseite werden die zehn schnellsten Spieler angezeigt, indem die Dauer in das Format: “HH:MM:SS” umgerechnet wird. Das ganze Skript ist in der Datei “time.php” zu finden.

Die Tabelle “users” wird in dem Skript “users.php” mit den Feldern id, username und password erstellt. Dabei ist “id” der Primärschlüssel. Die Tabelle wird erstellt, sobald der Spieler die Seite der SQL-Injection zum ersten Mal aufruft.
In beiden Fällen wird das Feld “id” durch automatisches Inkrementieren befüllt und beide Tabellen stehen separat, das heißt, sie wurden nicht miteinander verbunden.

Zusammenfassend kann man sagen, dass durch die Aufteilung von Assets, Datenbank-Skripten und Rätsel-Skripten die Übersichtlichkeit und Wartbarkeit gegeben ist, dass beispielsweise Fehler den jeweiligen Rätsel zugeordnet werden können.

2. Benutzerdokumentation

Um die Web-Applikation aufzurufen muss folgendes auf dem Computer installiert sein und beachtet werden:

- XAMPP muss installiert und eingerichtet werden
    - https://www.apachefriends.org/de/index.html
- Wenn XAMPP richtig installiert und das Control Panel gestartet wurde, kann man in diesem den Apache-Web-Server sowie MySQL starten
- Sind die entsprechenden Module grün hinterlegt sind sie richtig gestartet
- Innerhalb des XAMPP-Ordners, welcher sich, je nachdem wo man XAMPP installiert hat, auf dem Computer befindet, beinhaltet den “htdocs”-Ordner. Dort zieht man den Ordner "capture-the-flag-main”, welcher sich im zip-Ordner befindet, hinein.
- Dann folgende URL im Browser öffnen: http://localhost/capture-the-flag-main/Projekt-CaptureTheFlag
    - sollte ein anderer Port verwendet werden, diesen wie folgt in der URL eintragen: http://localhost:*Port*/capture-the-flag-main/Projekt-CaptureTheFlag

Startseite

Beim ersten Besuch der Web-Anwendung landet der Anwender auf der Willkommens-Seite. Auf dieser befindet sich ein Text, der dem Anwender erklärt, dass er vier Rätsel so schnell wie möglich lösen muss, um am Ende eine Flagge, welche das Ziel symbolisiert, einzusammeln. Darunter befindet sich ein Eingabefeld, in welchem der Anwender einen beliebigen Namen eingeben kann. Danach kann er die Rätsel starten. Außerdem befindet sich auf der gleichen Seite eine Tabelle mit der jeweiligen Platzierung des Spielers mit ihrer Zeit für das Absolvieren der vier Rätsel. Dabei werden die zehn schnellsten Spieler angezeigt. Sofern noch keine Zeiten gesetzt wurden, wird der Text “Noch keine Ergebnisse vorhanden” angezeigt.

Auf jeder Seite der einzelnen Rätsel steht dem Spieler der Knopf “Hinweise anzeigen” zur Verfügung, falls dieser Hilfe bei einem Rätsel benötigt.

Anagramme

Hier muss der Spieler fünf verschiedene, aus einer Liste zufällig ausgewählte Anagramme lösen. Die Buchstabenfolge muss also so umgestellt werden, dass das Lösungswort gebildet wird. Dabei ist Groß- oder Kleinschreibung unwichtig.
Es ist zu beachten, dass die Buchstabenfolge und folglich auch das Lösungswort auf Englisch geschrieben sind.
Hat der Nutzer seine Eingaben getätigt, so muss er die Antworten erst überprüfen. Sollte eine oder mehrere Antworten inkorrekt sein, so muss man diese korrigieren. Sind alle Antworten korrekt, so erscheint der Button, der den Spieler zum nächsten Rätsel leitet.

Cäsar-Verschlüsselung

In diesem Rätsel muss der Spieler einen Text entschlüsseln, welcher mit der Cäsar-Verschlüsselung mit dem Schlüssel “3” verschlüsselt wurde. Die Lösung gibt der Spieler dafür in das vorgesehene Textfeld ein. Dabei muss auf keine Groß- oder Kleinschreibung geachtet werden. Danach klickt der Spieler auf den Button “Lösung überprüfen”. Wenn die Lösung des Spielers falsch ist, kann er diese bearbeiten. Wenn diese jedoch richtig ist, erscheint der Button “Nächstes Rätsel”. Wird dieser angeklickt, wird der Spieler zum nächsten Rätsel geleitet.
Die Cäsar-Verschlüsselung funktioniert wie folgt:

- Je nach Schlüssel werden Buchstaben und die jeweilige Anzahl an Stellen verschoben
- Am Beispiel mit dem Schlüssel “3”:
    - A → D
    - B → E
    - C → F
    - …
    - X → A
    - Y → B
    - Z → C

Für das Lösen des Rätsels muss der Spieler demnach die verschlüsselten Buchstaben auf die originalen Buchstaben zurückführen.

SQL-Injection

Nun muss der Spieler ein Login-Feld ohne jegliche vorhandene Anmeldedaten überwinden. Dafür muss SQL-Injection genutzt werden.
Eine SQLi-Sicherheitslücke entsteht, wenn Benutzereingaben direkt in ein SQL-Statement übergeben werden, ohne die Eingaben vorher zu überprüfen und zu bereinigen. Mit gezieltem Nutzen von für SQL spezielle Zeichen wie ‘, – oder # kann der Spieler also so in dem Benutzername-Feld oder auch im Passwort-Feld die Verarbeitung des SQL-Statements manipulieren. Dafür wird entweder der Administrator-Benutzer aus der *users*-Datenbank sowie die richtige Verwendung von SQL-Symbolen benötigt, oder aber ein Statement, welches SQL als immer wahr interpretiert.
Gelingt es dem Nutzer nicht, die SQL-Eingabe zu manipulieren, so erscheint die Meldung “Login fehlgeschlagen :(“ und der Spieler muss wieder zurück auf die Login-Seite. Ist die Injection erfolgreich, erscheint die Meldung “Login erfolgreich!”, sowie ein Button, der zum nächsten Rätsel führt.

Kombiniertes Rätsel

Das kombinierte Rätsel besteht aus drei kleineren Rätsel, welche alle eine Zahl als Ergebnis besitzen. Diese Zahlen muss der User ohne Leerzeichen hintereinander in das Lösungsfeld eingeben (zum Beispiel 123456790).
Das erste Teil-Rätsel ist ein Text, welche die kleinste dreistellige Zahl, die durch 4 und 7 teilbar ist, beschreibt.
Das zweite Rätsel gibt dem Spieler einen Farbcode im Hexadezimalsystem an. Dabei sind die ersten beiden Stellen die Farbe “rot”, die zweite Stelle ist “grün” und die dritte “blau”. Dabei gilt:

- 00 steht dabei für keinen Anteil der jeweiligen Farbe
- FF steht dabei für den vollen Anteil der jeweiligen Farbe
- #FFFFFF ist weiß, #000000 ist schwarz, #FF0000 ist nur rot, …

Der Spieler muss demnach die Farben herausfinden, die Hexadezimalwerte in das Dezimalsystem umrechnen und dann in die Gleichung einsetzen. Das Ergebnis ist der zweite Teil des Codes für die Lösung.
Das dritte Teil-Rätsel ist ein Suchbild. Dort ist eine zweistellige Zahl versteckt, die den letzten Teil des Codes darstellt.

Alle Zahlen zusammen ergeben den Code, welcher am Ende der Seite eingetragen wird. Ist das Ergebnis richtig, dann erscheint der Button “Weiter” welche den Spieler auf die Zielseite bei einem Klick weitergeleitet.

Zielseite

Der Spieler landet, nachdem er alle vier Rätsel gelöst hat, auf der Zielseite. Dort befindet sich der letzte Knopf, der eine Flagge als Symbol besitzt. Wird dieser angeklickt, wird der Spieler zurück auf die Startseite geleitet und bekommt seine benötigte Zeit sowie die aktuelle Platzierung berechnet und angezeigt. Danach können, nachdem ein Username eingegeben wurde, die Rätsel nochmals gespielt werden.

3. Anhang

3.1 ER-Modell der Datenbank ctf