

Entwurf und Realisierung eines Capture the Flag Core Systems

Bachelorarbeit

zur Erlangung des Grades *Bachelor of Science*

an der

Hochschule Niederrhein

Fachbereich Elektrotechnik und Informatik

Studiengang *Informatik*

vorgelegt von

Robert Hartings

Matrikelnummer: 1164453

Datum: 21. Juli 2020

Prüfer: Prof. Dr. Jürgen Quade

Zweitprüfer: Prof. Dr. Peter Davids

Eidesstattliche Erklärung

Name: Robert Hartings
Matrikelnr.: 1164453
Titel: Entwurf und Realisierung eines Capture the Flag Core Systems
Englischer Titel: Design and implementation of a Capture the Flag Core System

Ich versichere durch meine Unterschrift, dass die vorliegende Arbeit ausschließlich von mir verfasst wurde. Es wurden keine anderen als die von mir angegebenen Quellen und Hilfsmittel benutzt.

Die Arbeit besteht aus _____ Seiten.

Ort, Datum

Robert Hartings

Inhaltsverzeichnis

1	Einleitung	1
1.1	Motivation	2
1.2	Aufgabenstellung	2
2	Analyse	5
2.1	Lehrveranstaltung IT-Sicherheit	5
2.2	Ausstattung Labor	6
2.3	Versuch „Catch me, if you can“	7
2.4	Systemkomponenten	9
2.4.1	Komponenten des Servers	9
2.4.2	Komponenten des Clients	14
2.5	Schnittpunkte zwischen Server und Clients	15
2.6	Abgeleitete Anforderungen	15
3	Entwurf	17
3.1	Entwurfsziele	17
3.2	Übersicht	19
3.3	Containerisierung	20
3.4	Scanner	21
3.4.1	Verteilte Scanner	22
3.4.2	Zentraler Scanner	22
3.4.3	Scan-Operationen	28
3.5	Webserver	29
3.5.1	Verwendung mehrerer Microservices	30
3.5.2	Fat Webserver	30
3.5.3	Thin Webserver	31
3.5.4	Funktionale Eigenschaften	32
3.5.5	Reverse Proxy	38
3.6	Datenbank	39
3.6.1	Basis-Tabellen	39
3.6.2	Gruppen-Tabellen	40
3.6.3	Flags-Tabellen	42
3.6.4	Service-Tabellen	43
3.6.5	Flagshop-Tabellen	44
3.6.6	Challenge-Tabellen	46
3.6.7	Weitere Tabellen	47

3.7	Webclient	48
3.7.1	SPA vs MPA	48
3.7.2	Mockups	50
3.8	GameClient	54
4	Technologien	55
4.1	Backend	55
4.1.1	Django	55
4.1.2	Flask	56
4.1.3	Wahl des Frameworks	56
4.2	Datenhaltung	56
4.2.1	MySQL und MariaDB	57
4.2.2	PostgreSQL	57
4.2.3	SQLite	57
4.2.4	Wahl der Datenbanksoftware	57
4.3	Frontend	58
4.3.1	Angular	60
4.3.2	React	61
4.3.3	Vue	62
4.3.4	Wahl des Frontend-Frameworks	63
5	Realisierung	65
6	Fazit	67
6.1	Zusammenfassung	67
6.2	Ausblick	67
Anhang		69
1	Installationsanleitung	69
2	Bedienungsanleitung	70

1 Einleitung

Das Thema IT Sicherheit ist besonders in den letzten Jahren relevant geworden. Viele Firmen suchen Fachkundige [it-19], die die bestehenden und neu designten Systeme auf Sicherheitslücken prüfen und Lösungsvorschläge zu deren Behebung präsentieren. Auch werden Experten gesucht, die die im Unternehmen bestehenden Prozesse prüfen und neue zum Umgang mit Sicherheitslücken entwerfen.

Einen Mangel an IT-Sicherheit in privaten und öffentlichen Unternehmen, beziehungsweise ein fehlendes Konzept zur Vorbeugung, Erkennung und Abwendung von Sicherheitslücken sieht man in jüngster Vergangenheit deutlich, nachdem beispielsweise diverse Universitäten wie Gießen [Sch20], Maastricht [WDR19] und Bochum [Ruh20] Ende 2019 Ziele von Hackerangriffen geworden sind. Aber nicht nur Universitäten sind betroffen, so sind neben Gerichten [HHH20], Stadtverwaltungen [BH20] und Krankenhäusern [We119] bereits der Deutsche Bundestag von Hackern angegriffen und kompromittiert worden. [FM20]

In der Studie „Wirtschaftsschutz in der digitalen Welt“ vom 06. November 2019 des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. Bitkom wird die aktuelle Bedrohungslage durch Spionage und Sabotage für deutsche Unternehmen untersucht. Daraus geht hervor, dass im Jahr 2019 von Datendiebstahl, Industriespionage oder Sabotage 75% der befragten Unternehmen¹ betroffen und 13% vermutlich betroffen waren. Die Zahlen dieser Unternehmen ist steigend. Im Jahre 2015 waren „nur“ 51% betroffen und 28% vermutlich betroffen. Die Unternehmen beziffern den Schaden auf 102,9 Milliarden Euro pro Jahr. [BN19]

Dass diese Thematik auch im Lehrbetrieb angekommen ist, sieht man an neu startenden Studiengängen wie dem Bachelorstudiengang Cyber Security Management der Hochschule Niederrhein, der zum kommenden Wintersemester 2020/21 startet. [Hoc20]

Es ist zu erwähnen, dass die Hochschulen sich bereits mit dem Thema auseinandersetzen. So beschäftigt sich an der Hochschule Niederrhein das Institut für Informationssicherheit Clavis besonders mit Themen rund um das Informationssicherheitsmanagement, gestaltet aber auch Inhalte zur Vulnerabilität von (kritischer) Infrastruktur und Hacking. Das Ziel von Clavis ist die Erhöhung der Informationssicherheit von Organisationen im regionalen Umfeld der Hochschule. [Hoc] Auch hat die Hochschule Niederrhein das Thema IT-Sicherheit bereits in ihren Lehrplan für die Studiengänge Informatik und Elektrotechnik am Fachbereich 03 Elektrotechnik und Informatik aufgenommen. So werden dort im fünften Semester in der Veranstaltung

¹Die Grundlage der Studie sind 1070 (2019) und 1074 (2015) befragte Unternehmen

IT-Security grundlegende Kompetenzen zum Thema IT-Sicherheit vermittelt, welche einem allgemeinen Anspruch genügen. [Hoc19]

Begleitend zu dieser Veranstaltung werden drei Versuche im Rahmen des Praktikums durchgeführt. Diese sollen den Studierenden praktische Erfahrungen ermöglichen und ein breites Bewusstsein schaffen, indem die Studierenden sowohl in die Rolle des Angreifers als auch die des Schützers schlüpfen.

Im zweite Versuch namens „Catch me, if you can“ findet ein Vergleichswettbewerb zwischen den teilnehmenden Studierendenteams statt.

Die Aufgabe der Teams besteht darin, festgelegte Programme/Dienste abgesichert bereit zu stellen, geheime Informationen sowohl auf dem eigenen Rechner als auch auf den Rechnern der anderen Teams zu finden und Schwachstellen abzusichern, um so zu verhindern, dass andere Teams an die eigenen geheimen Informationen gelangen. [Sos10, S. 2]

Die geheimen Informationen sind logischerweise Passwörter oder private Bilder und werden durch sogenannte Flags repräsentiert. Eine Flag ist eine generierte Zeichenfolge mit fester Länge.

1.1 Motivation

Neben diversen Meldungen zu erfolgreichen Angriffen auf Unternehmen und öffentliche Körperschaften und durch die Veranstaltung IT-Sicherheit im fünften Semester, besonders herauszuheben ist hier das Praktikum², bin ich auf das Thema IT-Sicherheit aufmerksam gemacht worden.

Die zunehmenden Vorfälle zeigen, dass ein breites Bewusstsein für IT-Sicherheit geschaffen werden muss und das Praktikum hierbei eine wichtige Aufgabe übernimmt.

Das Programm, welches das Praktikum überwacht, ist bereits 10 Jahre alt und bietet Notwendigkeiten der Modernisierung, Überarbeitung und Erweiterung. So gibt es beispielsweise heute bessere Möglichkeiten die Darstellung (Web-Oberfläche) zu realisieren.

1.2 Aufgabenstellung

Das Praktikum wird durch ein Auswertungs- und Überwachungssystem begleitet, welches eine objektiv nachvollziehbare Bewertung vornehmen kann und das die in den Bewertungsprozess eingeflossenen Parameter dokumentiert. [Sos10, S. 2]

²Praktikum ist hierbei mit einer Pflichtübung vergleichbar

Ziel meiner Arbeit ist die Modernisierung und Verbesserung dieses Auswertungs- und Überwachungssystems. Anforderung hierbei war, dass das neue System die gleichen Basisfunktionalitäten, wie das Altsystem erfüllen muss.

In der einführenden Betrachtung (Kapitel 2) wird der aktuelle Stand des Systems, Schnittstellen zwischen Server und Client sowie der Begründung für die Veränderung dargelegt. Aus dieser einführenden Betrachtung werden dann Anforderungen abgeleitet.

Im folgenden Kapitel 3 werden Entwürfe für die verschieden neu designten Komponenten des Servers erstellt.

Anhand der abgeleiteten Anforderungen und des Entwurfs der verschiedenen Komponenten werden im Kapitel 4 verschiedene Technologien diskutiert und passende ausgewählt.

Die Implementierung des Entwurfs mit den gewählten Technologien wird im Kapitel 5 beschrieben.

Eine kritische Auseinandersetzung mit dem Ergebnis dieser Arbeit folgt und es werden Ausichten für mögliche Veränderungen und Erweiterungen gegeben.

Aus diesem Aufbau der Arbeit ergeben sich die folgenden Aufgaben:

- Analyse des vorliegenden Systems
- Analyse der Voraussetzungen
- Ableitung von Anforderungen
- Entwurf der Architektur
- Entwurf der einzelnen Komponenten
- Diskussion einzusetzender Technologien
- Implementierung des Entwurfs
- Bereitstellung von Installations- und Bedienungsanleitung.

2 Analyse

In diesem Kapitel werden die Voraussetzungen im Labor vorgestellt, die derzeitige Implementierung des Auswertungs- und Überwachungssystems beleuchtet und kurz auf einen überwachten Client sowie dessen Schnittstellen zum System eingegangen.

2.1 Lehrveranstaltung IT-Sicherheit

Das Pflichtmodul IT-Sicherheit (ITS) ist in drei Veranstaltungen gegliedert. [Hoc19, S.30]

- Vorlesung (2 Semesterwochenstunden)
- Übung (1 Semesterwochenstunde)
- Praktikum (1 Semesterwochenstunde)

Vorlesung

Die Vorlesung wird im wöchentlichen Turnus angeboten und behandelt grundlegendes Wissen zur IT-Sicherheit unter anderem in den Bereichen Gefährdung, Gegenmaßnahmen, aber auch im Bereich rechtliche Gegebenheiten. Es werden Beispiele aufgezeigt, bei denen die angesprochenen Themen gar nicht oder in einem ungenügenden Zustand umgesetzt worden sind. Die Vorlesung wird von den Veranstaltungen *Übung* (freiwillig) und *Praktikum* (verbindlich) ergänzt.

Übung

Die Übungen sind freiwillig und werden im zweiwöchentlichen Turnus á 2 Stunden angeboten. Diese ermöglichen es den Studierenden, den durch die Vorlesung und das Selbststudium vermittelten Stoff zu vertiefen und zu festigen. Auch können dort praktische Erfahrungen gesammelt werden, von denen die Studierenden unter anderem im Praktikum profitieren können.

Praktikum

Das Praktikum findet im monatlichen Turnus (3x im Semester á 4 Stunden) statt. Es ist in drei Laborversuche untergliedert. Nach Bestehen aller Versuche erhalten die Studierenden ihre Klausurzulassung. Jeder Versuch des Praktikums muss vorbereitet werden, dazu erhalten die Studierenden vor dem Versuch ein Hackit¹. Nur mit erfolgreichem Absolvieren des Hackits ist es möglich, am nächsten Versuch teilzunehmen. [Qua17]

2.2 Ausstattung Labor

Das Praktikum wird im Labor für Echtzeitsysteme (EZS Labor) der Hochschule Niederrhein durchgeführt.

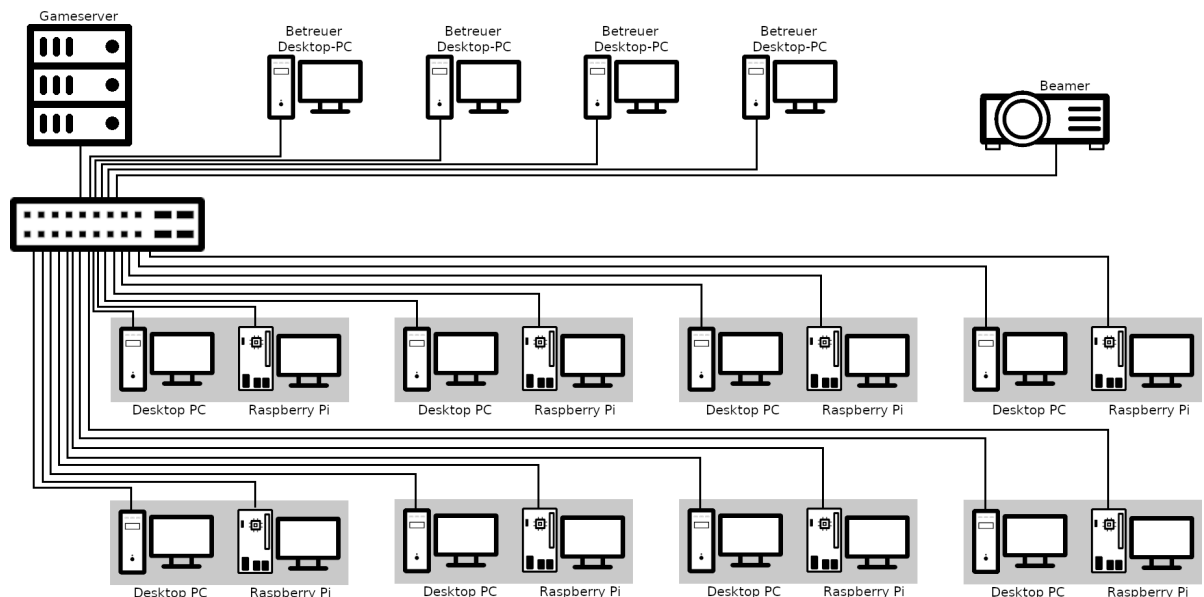


Abbildung 2.1: Übersicht über die Laborausstattung (Netzwerktopologie)

Wie in der Abbildung 2.1 dargestellt, ist das Labor mit acht Gruppenarbeitsplätzen für Studierende sowie Arbeitsplätzen für die Betreuer und Mitarbeiter ausgestattet. Ein Betreuerarbeitsplatz kann zu einem neunten Gruppenarbeitsplatz umfunktioniert werden.

An einem Gruppenarbeitsplatz (in der Abbildung 2.1 grau hinterlegt) können 2 Studierende gleichzeitig arbeiten, da diese mit einem leistungsfähigen Desktop-PC und einem Raspberry Pi² sowie den dazugehörigen Peripheriegeräten (Maus, Tastatur & Monitor) ausgestattet sind.

¹Knobelaufgabe aus dem Bereich IT-Sicherheit / Hacking

²Einplatinencomputer mit der Größe einer Kreditkarte

Als Betriebssystem wird auf den Desktop-PCs Ubuntu³ und auf den Raspberry Pis Raspbian⁴ verwendet.

Auf den Desktop-PCs ist die Software VirtualBox der Firma Oracle installiert. Diese ermöglicht das Virtualisieren eines weiteren Rechners. Diese virtuelle Maschine wird Gast genannt und beheimatet die Dienste und Anwendungen, welche während des Versuchs benötigt werden. Durch die Nutzung der Virtualisierung muss die Software nicht auf dem Wirtssystem installiert werden. So ist dieses auch für andere Versuche im Rahmen der Lehrveranstaltung nutzbar, ohne dass auf Inkompatibilitäten von Softwares der verschiedenen Versuche geachtet werden muss. Auch bietet VirtualBox die Möglichkeit sogenannte Snapshots anzulegen. Ein Snapshot ist eine Momentaufnahme eines aktuellen Systemzustandes. Diese stellt eine Komplettsicherung des Systems dar und es ist möglich, die Systeme auf den gleichen Stand zu bringen. [Ora20c] Dies wird benötigt, um eine Vergleichbarkeit zwischen den Studierenden zu gewährleisten.

Die teilnehmenden Studentengruppen werden in den Softwarekomponenten und in der Auswertung durch die IP-Adresse ihres Gast-Systems identifiziert.

Neben diesen Rechner steht ein Linux Server zur Verfügung, auf welchem das Auswertungs- und Überwachungssystem betrieben wird.

Alle Rechner, auch die Gastsysteme der Studentengruppen, sind untereinander über ein Netzwerkswitch via Ethernet verbunden.

Außerdem steht ein Beamer zur Verfügung, auf dem die aktuelle Spielübersicht dargestellt werden kann.

2.3 Versuch „Catch me, if you can“

Der zweite der drei Versuche „Catch me, if you can“ wird im Rahmen eines Wettbewerbs zwischen den teilnehmenden Studierendenteams ausgetragen. Der Wettbewerb ist an ein Capture the Flag (CTF) angelehnt. Bei einem klassischen CTF erhält der Spieler durch das Lösen von Aufgaben einen bestimmten Text. Dieser wird Flag genannt. Die Aufgaben können das Lösen einer Art Schnitzeljagd, eine einfache Programmierung, aber auch das Hacken mehrerer entfernter Rechner umfassen. Anders als beim klassischen CTF werden bei „Catch me, if you can“ die Flags auf allen teilnehmenden Systemen verteilt. [Tan20] Die Studierenden können diese durch das Analysieren ihres eigenen Gastsystems sowie durch den Angriff auf fremde Gastsysteme erhalten. Besonderheit hierbei sind die Strafpunkte für den Verlust einer Flag an gegnerische Studierendenteams. Wie beim klassischen CTF können die Studierenden Flags und Punkte durch zentrale Aufgaben erhalten.

Der Versuch ist in drei Phasen untergliedert.

³Ubuntu ist eine freie Linux Distribution auf Basis von Debian

⁴Abwandlung von Debian für den Raspberry Pi

1. Vorbereitung
2. Wettbewerb
3. Abschluss

Vorbereitung

Die Studierenden erhalten circa 30 Minuten Zeit, um ihr Gastsystem in Betrieb zu nehmen und sich mit diesem vertraut zu machen. Hierbei sollten die Schwachstellen in den vorhandenen Diensten abgesichert und der Zugriff durch andere Studierende verhindert werden. Während dieser Zeit dürfen die Studierenden andere Systeme nicht angreifen. Auch ist es möglich, in dieser Zeit Flags auf dem eigenen System der Studierenden zu suchen. Da der Ablageort der Flags auf allen Systemen gleich ist, kann diese Information im Spielverlauf einen Angriff schneller Flags einbringen.

Wettbewerb

Die Wettbewerbsphase selbst dauert circa 140 Minuten. In dieser Zeit sind Angriffe auf fremde Gastsysteme erlaubt und ausdrücklich gewünscht. Eine weitere Absicherung ist ebenfalls möglich. Das System sollte auf fremde Aktivitäten hin überwacht werden. Diese Aktivitäten sollten schnellstmöglich unterbunden werden, da die Angreifer Flags entwenden können und so dem Team Strafpunkte einbringen. Auch kann die Zeit für die Lösung von zur Verfügung stehenden Challenges sowie die Nutzung des Flagshops genutzt werden. Der Flagshop sowie die Challenges werden im nächsten Kapitel aufgegriffen.

Abschluss

Nach Ende der Wettbewerbsphase müssen die Studierenden ihre Angriffe einstellen und eine weitere Flagabgabe ist nicht möglich. Die Studierenden erstellen für ihren anzufertigen Versuchsbericht ein Screenshot der Punkteübersicht. Eine Nachbesprechung ist optional und mit maximal 30 Minuten angesetzt.

Während des Wettbewerbs gelten die aufgelisteten Regeln. Es handelt sich hierbei um einen Auszug der für die Bachelorarbeit relevanten Regeln.

- Der Gameserver darf nicht angegriffen werden
- Es dürfen nur die Gastsysteme angegriffen werden
- Das Passwort des Logins *gamemaster* darf nicht zurückgesetzt werden
- Der SSH-Server muss für alle benutzbar sein
- Flags dürfen nicht modifiziert oder gelöscht werden

- Sämtliche Dienste müssen für den Gameserver erreichbar bleiben
- ICMP-Pakete (ping) dürfen nicht blockiert werden.

[Qua17, S.9] [Sos10, S.10-11]

2.4 Systemkomponenten

2.4.1 Komponenten des Servers

Im Folgenden werden die verschiedenen Komponenten des Auswertungs- und Überwachungssystems in der derzeitigen Implementierung untersucht. Dabei werden Rückschlüsse auf Anforderungen gezogen sowie Schwachstellen und Verbesserungsmöglichkeiten herausgearbeitet.

Scanner

Der Scanner prüft in regelmäßigen Abständen die auf den Gastsystemen der Studierenden installierten Dienste und speichert das Ergebnis ab. Die Abstände können beim Starten des Spieles eingestellt werden. Die folgenden Dienste werden pro Team geprüft.

ScanUp Die Aufgabe dieses Scans besteht darin zu prüfen, ob das Gastsystem noch für den Server erreichbar ist. Sollte das Gastsystem nicht erreichbar sein, wird hierfür ein Strafpunkt vergeben. Aus technischer Sicht wird das Linux Kommando *ping* verwendet. Anhand des Rückgabewertes kann nachvollzogen werden, ob der Server das Gastsystem erreichen konnte.

ScanBubble Auf dem Gastsystem läuft ein selbst programmierter Bubble Server, welcher Flags unter Nutzung des Telnet Protokolls bereitstellt. Nachdem eine Flag abgeholt worden ist, stellt der Dienst für eine bestimmte Zeit (Timeout) keine weitere Flag bereit. Der Bubble Server nimmt Anfragen über den Port *12321* für unverschlüsselte Flags und Port *12322* für verschlüsselte Flags entgegen. Die Scan-Operation überprüft, ob eine Telnet Verbindung zu dem Port *12321* möglich ist, in dem die Operation eine Telnet Verbindung öffnet und prüft, ob die Verbindung erfolgreich war.

ScanWebUp Jedes Gastsystem stellt unter Zuhilfenahme eines Apache Web Servers und php-Dateien Webseiten und Daten bereit, welche über einen Web Client abgerufen werden können. Dazu muss auf Port *80* der HTTP- und auf Port *443* der HTTPS-Dienst laufen und erreichbar sein. Dieses verifiziert die Scan-Operation indem sie eine Socket Verbindung zu den Ports *80* und *443* öffnet und das Ergebnis prüft.

ScanSQLInjectUp Dieser Scan prüft, ob die Login-Seite des Teams, auf der die SQL-Injection Schwachstelle implementiert ist, erreichbar und benutzbar ist. Die Operation sendet hierzu eine valide Kombination aus Nutzernamen und Passwort an den Webserver. Das Ergebnis wird dann mit dem erwarteten Resultat verglichen.

ScanSQLInjectSave Ähnlich wie bei der Operation ScanSQLInjectUp (2.4.1) wird geprüft, ob Ergebnis und Erwartung übereinstimmen. Besonderheit hierbei ist, dass statt einer validen Kombination aus Nutzernamen und Passwort eine sogenannte SQL-Injection (wird im Unterabschnitt 2.4.2 genauer erläutert) im Nutzernamen übergeben wird. Sollte die Anfrage alle gespeicherten Nutzerdaten zurückgeben, ohne dass eine Authentifizierung stattfindet, ist die SQL-Injection weiterhin möglich.

ScanXSSSave Diese Scan-Operation prüft, ob die auf dem Gastsystem implementierte XSS Schwachstelle behoben wurde. Dazu wird die Webseite mit präpariertem Inhalt aufgerufen. Auf die Vorgehensweise wird im Unterabschnitt 2.4.2 eingegangen. In der Rückgabe wird geprüft, ob dieser ungefiltert auf der Webseite zu finden ist. Sollte dies der Fall sein, ist die XSS Schwachstelle nicht oder unzureichend von den Studierenden abgesichert worden.

ScanSQLSave Bei diesem Scan wird kontrolliert, ob der Login mit dem auf allen Systemen voreingestellten Passwort *toor* für den SQL-Account *root* möglich ist. Sollte dieser möglich sein, haben die Studierenden dieses unsichere Passwort nicht geändert. Des Weiteren wird geprüft, ob das htaccess Passwort, welches die phpMyAdmin Anwendung schützen soll, geändert worden ist.

ScanFTPSave Auf dem Client System läuft ein FTP Server, welcher ohne Login (Nutzername & Passwort) Daten bereitstellt. Der Scan prüft, ob ein sogenannter Anonymous Login möglich ist, indem eine FTP Verbindung ohne Login aufgebaut wird. Sollte die Verbindung erfolgreich sein, ist der Anonymous Login immer noch möglich.

ScanTelnetSave Ein Telnet Server horcht auf Verbindungen auf Port 23. Da dieser Dienst nicht benötigt wird, soll er durch die Studierenden abgeschaltet oder deinstalliert werden. Die Scan-Operation prüft, ob eine Verbindung mithilfe des Telnet Protokolls auf Port 23 möglich ist. Dazu wird eine Verbindung zu Port 23 aufgebaut und das Resultat geprüft.

Generierung von Flags

Derzeitig erfolgt die Generierung der Flags sowohl auf den Gastsystemen als auch auf dem Auswertungs- und Überwachungssystem. Dies ist notwendig, da ansonsten eine Überprüfung der Gültigkeit der Flags und Verrechnung der Punkte nicht durchgeführt werden kann. Die

Flags werden durch einen Algorithmus generiert. Dieser erzeugt pro Team eine bestimmte Anzahl an Flags.

Dazu wird die Flag mithilfe der Streuwertfunktion (Hashfunktion) MD5 und der Eingabe, einem sogenannten seed, berechnet. Eine Hashfunktion bildet aus einer Eingabe variabler Länge eine Ausgabe mit einer festen Länge. Bei identischer Eingabe wird immer der gleiche Ausgabewert berechnet. Des Weiteren ist es bei einer guten Hashfunktion nicht möglich, von der Ausgabe auf den Eingabewert zu schließen. [MOV96]

Der in der Anwendung genutzte seed setzt sich aus der Verkettung von *Salt*, *IP-Adresse*, dem Wort „*Aufgabe*“ und einem *Zähler* zusammen.

Ein Salt wird benötigt, um den Flags eine Lebenszeit zu geben. In der derzeitigen Implementierung enthält der Salt das aktuelle Jahr sowie das jeweilige Semester. So sind nur Flags des aktuellen Semesters gültig und werden vom Auswertungs- und Überwachungssystem akzeptiert. Einer Verwendung von Flags aus vorherigen Semestern wird somit effektiv vorgebeugt.

Die IP-Adresse stellt hierbei den Bezug zum jeweiligen Team dar.

Der String „*Aufgabe*“ wird als Geheimnis verwendet, um das Fälschen von Flags zu erschweren und bestenfalls zu verhindern.

Damit pro Team mehrere eindeutige Flags generiert werden können, wird ein sogenannter Zähler genutzt. Dieser Zähler ist auf 0 initialisiert und wird pro generierter Flag um eins erhöht, bis die benötigte Anzahl an Flags generiert ist. [Sos10, S.48]

Webserver

Der Webserver stellt die GUI (Graphical User Interface) für die Studierenden und Betreuer dar. Hier kann der aktuelle Punktestand angesehen werden. Auch wird in der GUI dargestellt, welches Team welchen Service abgesichert hat, inklusive der Negativpunkte für nicht abgesicherte Dienste, und wie viele Strafpunkte das jeweilige Team erhalten hat.

Neben diesen Darstellungen befinden sich auf dem Server ein sogenannter Flagshop und diverse Challenges, mit denen Studierende weitere Flags erhalten können.

Die Betreuer haben die Möglichkeit, über die Web-GUI ein neues Spiel anzulegen und das Spiel zu starten oder zu stoppen. Auch kann von dem Spiel ein Backup erstellt werden. Neben diesen Funktionen zur Spielsteuerung können an die Teams Strafen für unfaires oder regelverletzendes Verhalten verteilt werden. Diese nehmen direkten Einfluss auf die Punkte des jeweiligen Teams. Außerdem besteht die Möglichkeit, weitere Benutzer für das Administrationsinterface zu registrieren.

Flagshop Der Flagshop ermöglicht es den Studierenden, weitere Flags mit ihren Punkten zu kaufen. Der Kauf von Flags lohnt sich schon, da die verkauften Flags mehr Punkte bringen als sie kosten. Um einen Einkauf im Flagshop durchzuführen, müssen die Teams vorher einen Account erstellen. Die Registrierung erfragt neben dem benötigten Benutzernamen und Passwort auch für den Flagshop irrelevante Daten ab. Diese ähneln persönlichen Informationen, welche bei den meisten Onlineshops angegeben werden müssen. Das Format, hier die Repräsentation als Zahl oder String sowie die Länge, und die Erforderlichkeit der Daten werden nur im HTML-Formular festgelegt. Durch eine Manipulierung des Formulars kann dieses mit nicht konformen oder nicht vorhandenen Daten abgesendet werden. Für jede der nicht vorhandenen oder nicht konformen Informationen erhält der Studierende eine Flag. Daneben wird die Güte des angegebenen Passwortes anhand von Länge und Anzahl an Sonderzeichen, Groß- und Kleinbuchstaben sowie Ziffern bewertet und mit Flags belohnt.

Nach der Registrierung können die Studierenden sich für ihre Punkte Flags kaufen. Dazu stehen zwei Pakete mit 8 bzw. 6 Flags für den Preis von jeweils 4 Punkten pro Paket zur Verfügung. Dieser Preis kann auf zwei Arten reduziert werden. Einmal müssen sich die beiden Pakete gleichzeitig im Warenkorb befinden und die Identifikationsnummern (ID) dieser müssen auf nicht vorhandene Nummern gesetzt werden. Die Manipulation resultiert in einem reduzierten Preis von 4 Punkten für beide Pakete. Dies ist extra im Flagshop einprogrammiert und soll die Studierenden auf Manipulation von IDs aufmerksam machen. Durch die zweite Art ist es möglich, die Pakete kostenlos zu erhalten. Dazu muss im Warenkorb das sogenannte *hidden input* Feld, in dem der aktuelle Preis des Warenkorbs gespeichert wird, auf 0 gesetzt werden. Dann berechnet der Flagshop für den Kauf einen Preis von 0 Punkten. [Abt16, S. 63]

Ein *hidden input* Feld wird in der Repräsentation eines HTML-Dokumentes nicht angezeigt, kann jedoch durch die Entwicklertools der Browser betrachtet und verändert werden. [w3s]

Auf diese Weise ist es auch möglich, einen negativen Preis festzulegen und dem eigenen Team Punkte zuzuschreiben, da die derzeitige Implementierung nicht prüft, ob der von dem Nutzer eingegebene Preis kleiner als 0 ist, sondern ob dieser gleich 0 ist. Bei richtiger Implementierung würde ein Preis kleiner 0 geprüft und korrigiert.

Challenges Derzeitig sind fünf Challenges implementiert, welche vom System in zufälliger Reihenfolge an interessierte Teams verteilt werden. Eine abgeschlossene oder abgebrochene Challenge, durch das Neuladen der Webseite oder durch das Betätigen der Zurück-Taste, kann nicht wiederholt werden. Eine Challenge kostet 10 Punkte. Nach erfolgreichem Abschließen einer Challenge gibt es 10 Punkte plus eine gewisse Anzahl an Punkten für das Absolvieren der Aufgabe. Die folgenden Challenges sind implementiert. [Abt16, S.19-20]

Aufgabe 1: robots.txt Die Studierenden sollen in dieser Challenge lernen, dass die *robots.txt* Datei keinen Zugriffsschutz darstellt. Diese bittet nur Suchmaschinen, die angegeben Verzeichnisse und Dateien nicht zu indexieren. Aus der *robots.txt* Datei können Informationen zu versteckten Dateien und Verzeichnissen erhalten werden. Die Studierenden sollen über

die *robots.txt* Datei einen vorhandenen Ordner finden. In diesem befindet sich die Lösung zur Challenge.

Aufgabe 2: JavaScript-Login-Bypass Bei dieser Challenge ist das benötigte Passwort zur Lösung der Challenge als Klartext im Quelltext versteckt. Das Verstecken wird derzeit mit einer Meldung wie „Seitenquelltext deaktiviert“ ([Abt16]) und vielen Leerzeilen realisiert. Im Inspector von Firefox Version 78.0.1 und Chromium Version 83.0.4103.116 ist dies nicht möglich, da die Leerzeilen entfernt werden und das Passwort daher oben im Quelltext zu sehen ist.

Aufgabe 3: Form-Modification In dieser Challenge sollen die Studierenden verstehen, dass auch die Werte von Drop-Down-Menüs, Checkboxes und Radio-Buttons durch Manipulation auf nicht vorgegebene Werte geändert werden können. Deshalb müssen Nutzereingaben stets auch serverseitig überprüft werden, da hier die Regeln der Überprüfung nicht durch die Nutzer verändert werden können.

Die Aufgabe besteht darin, einen bestimmten Login-Namen aus einem Drop-Down-Menü auszuwählen. Da der geforderte Name nicht in dieser Liste ist, müssen die Studierenden das HTML Formular so manipulieren, dass er auswählbar ist.

Aufgabe 4: JavaScript-Substrings Das Passwort, welches die Studierenden eingeben müssen, wird clientseitig mithilfe einer JavaScript Funktion geprüft. Damit das Passwort nicht im Klartext im Quelltext steht, wird dieses verschleiert. So werden drei Strings Zeichen für Zeichen verglichen. Sollte ein Zeichen in mindestens zwei der drei Strings übereinstimmen, dann gehört dieses Zeichen zum Passwort. Im Anschluss wird geprüft, ob das generierte Passwort gleich dem ist, das die Studierenden als Passwort gegeben haben.

Aufgabe 5: URL-Hex-Injection Die Studierenden sollen an geheime Informationen in einem Ordner gelangen, welcher nach einem Wert aus dem Hexadezimalsystem (Basis 16 statt Basis 10, wie beim Dezimalsystem) benannt ist. Die Aufgabe soll zeigen, dass Ordner, die nach einem Hexadezimalwert benannt sind, auf diese Art und Weise nicht vor Zugriffen geschützt werden können, da das Präfix Zeichen % für Hexadezimalzahlen selber durch einen Hexadezimalwert dargestellt werden kann.

Abgabe von Flags

Um Flags abgeben zu können, müssen die Studierenden sich mit ihren Zugangsdaten, welche sie durch das Lösen des Hackits erhalten haben, in der Web-GUI anmelden. Dort ist es möglich, in einem Input-Feld eine Flag synchron abzugeben. Das bedeutet, dass nach jeder Abgabe die Webseite neu geladen wird. Des Weiteren ist es nicht möglich, mehrere Flags gleichzeitig abzugeben.

2.4.2 Komponenten des Clients

Da sich die Bachelorarbeit mit der Modernisierung des Auswertungs- und Überwachungssystem beschäftigt, sind nur die für die Bachelorarbeit wichtigen Komponenten des Clients beschrieben.

Webserver des Clients

Auf den Clients wird ein Webserver mit einigen extra implementierten Schwachstellen betrieben. Diese sollen während des Versuches durch die Studierenden behoben werden.

Der Webserver stellt eine Art Kundenbewertungsformular mit implementierter XSS Schwachstelle bereit. In der verwendeten Implementierung wird die Eingabe des Nutzers in das HTML-Dokument geschrieben. Durch die Schwachstelle wird eine Nutzereingabe ungefiltert in das HTML Formular übernommen und potenziell schädlicher Code wird vom Browser verarbeitet. Dieser Code kann dann beispielsweise vertrauliche Informationen, wie Cookies, Session Tokens oder persönliche Daten auslesen und den Angreifern übermitteln. [RG07]

Eine weitere Schwachstelle stellt der sogenannte „Login zum Membersbereich“ mit der implementierten SQL-Injection Schwachstelle dar. Bei einer SQL-Injection versucht ein Angreifer den verwendeten SQL-Befehl so zu erweitern, dass dieser neben der eigentlichen Abfrage an die Datenbank auch einen vom Angreifer vorbereiteten SQL-Befehl ausführt. Die Erweiterung des SQL-Befehls erfolgt, indem die Eingabe, welche in den SQL-Befehl aufgenommen wird, das Zeichen für das Ende des SQL-Befehls inklusive des vom Angreifer intendierten SQL-Befehls enthält. Über diesen Angriff können dann unerlaubterweise Daten ausgelesen werden, aber auch eine Löschung der Daten ist denkbar. [Bac04]

In der verwendeten Implementierung werden der Benutzername und das Passwort ungefiltert in den SQL-Befehl übernommen. Diese Schwachstelle lässt sich erst beheben, wenn die Gruppe die SQL-Injection bei sich selber erfolgreich durchgeführt hat.

Neben diesen Schwachstellen gibt es eine Registrierung für den Flagshop. Diese erfordert einige Eingaben wie Name, Alter, Postleitzahl und vieles mehr. Die Eingaben sind im HTML-Formular als Pflicht markiert und haben eine Vorgabe in der Form. Ein Absenden ist ohne Angabe dieser Daten nicht möglich. Die Studierenden erhalten jedoch für jede nicht getätigte und für jede nicht der Form entsprechenden Angabe Flags nach der Registrierung. Dies ist möglich, da das HTML-Formular durch die Studierenden geändert werden kann und der Server nur die Angaben bezüglich Passwort und Nutzernamen prüft. Diese beiden Angaben werden genutzt, um sich am Flagshop des Servers anzumelden und Flags zu erwerben. (Siehe: *Abschnitt 2.4.1 Flagshop*)

Außerdem stellt der Webserver eine Bildergalerie zur Verfügung. In dieser befinden sich zum Spielstart zwei normal erscheinende Bilder. Entgegen dem Anschein sind in diesen Flags verschleierte. Die Steganografie wird durch die Kombination eines Bildes und eines zip-Archivs erreicht. [Abt16]

2.5 Schnittpunkte zwischen Server und Clients

Der Server und die Clients laufen auf getrennten Systemen. Da die Studierenden Schwachstellen auf ihren Clients beheben sollen, muss das Auswertungs- und Überwachungssystem auf diese Systeme zugreifen. Dadurch lassen sich die folgenden Schnittpunkte begründen.

Der Scanner prüft vom Auswertungs- und Überwachungssystem aus, ob

- das System online
- der Webserver erreichbar
- der Bubble-Server erreichbar
- der Login zum Membersbereich erreichbar und abgesichert
- die Kundenbewertung erreichbar und abgesichert
- ob das SQL Passwort geändert wurde
- ob der FTP Server gegen unautorisierten Zugriff abgesichert und
- ob der Telnet Dienst auf Port 23 abgeschaltet ist.

Des Weiteren verbinden sich die Clients beim Starten mit dem Auswertungs- und Überwachungssystem, um Flags für die Flagshop-Registrierung und -Anmeldung zur Verfügung zu stellen.

2.6 Abgeleitete Anforderungen

Das Auswertungs- und Überwachungssystem muss anhand der vorhergehenden Analyse folgenden Anforderungen genügen:

- Überwachung von mindestens neun Studierendensystemen
- Ermittlung und Sicherung der Zustände von Diensten, welche auf den Studierendensystemen angeboten werden müssen
- Entgegennahme und Prüfung von Flags, inkl. der Verrechnung von (Straf-)Punkten
- Ermittlung und Visualisierung der Teilergebnisse sowie des Gesamtergebnisses
- Informationsvermittlung aller Dienst- und Punkteänderungen durch unter anderem Dienststatusänderung, Flagabgabe und Strafen (fortlaufende Publikation für Studierende und Betreuer)
- Dokumentation aller Events durch Protokollierung der einzelnen Aktionen des Systems
- Bereitstellung von Challenges, damit Studierende sich weiter Punkte erarbeiten können

- Bereitstellung eines (Flag-) Shops, bei dem mehrere Lücken genutzt werden können, um Flags zu erhalten
- Einstellungen des Spiels sollen durch Betreuer geändert werden können
- Verwaltung von Benutzern (Administratoren und Spielern)
- Zugangskontrolle für teilnehmende Studierende durch Prüfung der Hackits
- Sicherung alter Spielstände.

3 Entwurf

Dieses Kapitel beinhaltet die Architektur des Systems sowie den Entwurf der einzelnen Komponenten.

Es wird die Struktur und Zusammensetzung des Systems sowie der einzelnen Komponenten skizziert. Auch werden die Anforderungen und Erwartungen an die verschiedenen Systemkomponenten dargestellt.

Bei einigen Komponenten werden auch Alternativen aufgezeigt, welche auf Grundlage der genannten Entscheidungen im Entwurf nicht verwendet worden sind.

3.1 Entwurfsziele

Bei dem Entwurf des neuen Systems sind neben den in der Analyse beschriebenen Anforderungen auch folgende Ziele beachtet worden:

Beibehaltung der Features Die bereits implementierten Features Flagshop und Challenges sollen auch im neuen System verfügbar sein. Zusätzlich sollen die Studierenden angeregt werden, diese auch aktiv zu nutzen.

Lose Kopplung Zwischen dem Scanner und dem Webserver soll eine lose Kopplung herrschen, damit die Entwicklung der beiden Komponenten unabhängig voneinander fortgesetzt werden kann.

Datenhaltung in Datenbank Die Nutzung einer Datenbank sollte aufgrund zweier Überlegungen angestrebt werden: Erstens sind alle Daten an einem Ort gebündelt, zweitens kann die Berechnung von Punkten an die Datenbank abgegeben werden. Datenbanken sind unter anderem für solche Aufgaben geeignet.

Modernisierung der GUI Das Graphical User Interface soll modernisiert werden, sodass es heutigen Standards entspricht. Auch sollen hierdurch die Verständlichkeit verbessert und die Challenges sowie der Flagshop besser platziert werden.

Einheitliche Programmiersprache Eine einheitliche Programmiersprache sollte, sofern dies möglich ist, genutzt werden. Das erleichtert das Betreiben der Komponenten, da nicht zwei verschiedene Programmiersprachen und/oder Umgebungen installiert werden müssen. Auch erleichtert es die Programmierung, wenn nur eine Person parallel an den Komponenten arbeitet. Die Gefahr von falschen Syntaxen und verschiedenen Konventionen kann dadurch reduziert werden. Sollte die Anwendung durch mehrere Menschen entwickelt und gewartet werden sowie auf verschiedenen Systemen betrieben werden, ist dieses Ziel wichtig.

Module sparsam nutzen Bei der Implementierung der Software sollte, so weit dies notwendig und sinnvoll ist, auf bereits vorhandene Module und Frameworks zurückgegriffen werden. Durch die Minimierung von Abhängigkeiten ist die Wartung von Verwendung der Software durch Dritte leichter möglich. Auch wird die Gefahr von Fehler auslösenden Updates minimiert. Bei der Nutzung von Modulen und Frameworks sollte auf deren Verbreitung und Wartung geachtet werden, damit nicht inaktive Module/Frameworks mit eventuellen Schwächen genutzt werden.

Containerisierung Die Anwendung soll mit möglichst kleinem Wartungsaufwand überall benutzbar sein. Um dies zu gewährleisten, sollte eine Containerisierung genutzt werden. Bei der Nutzung ist darauf zu achten, ob und mit welchen Einschränkungen diese einsetzbar ist.

Ressourcen schonend Um die Ressourcen des Servers zu schonen, sollten die nicht benötigten Komponenten abgeschaltet werden. Hierbei ist der Scanner hervorzuheben, welcher nur während des Praktikums laufen muss.

3.2 Übersicht

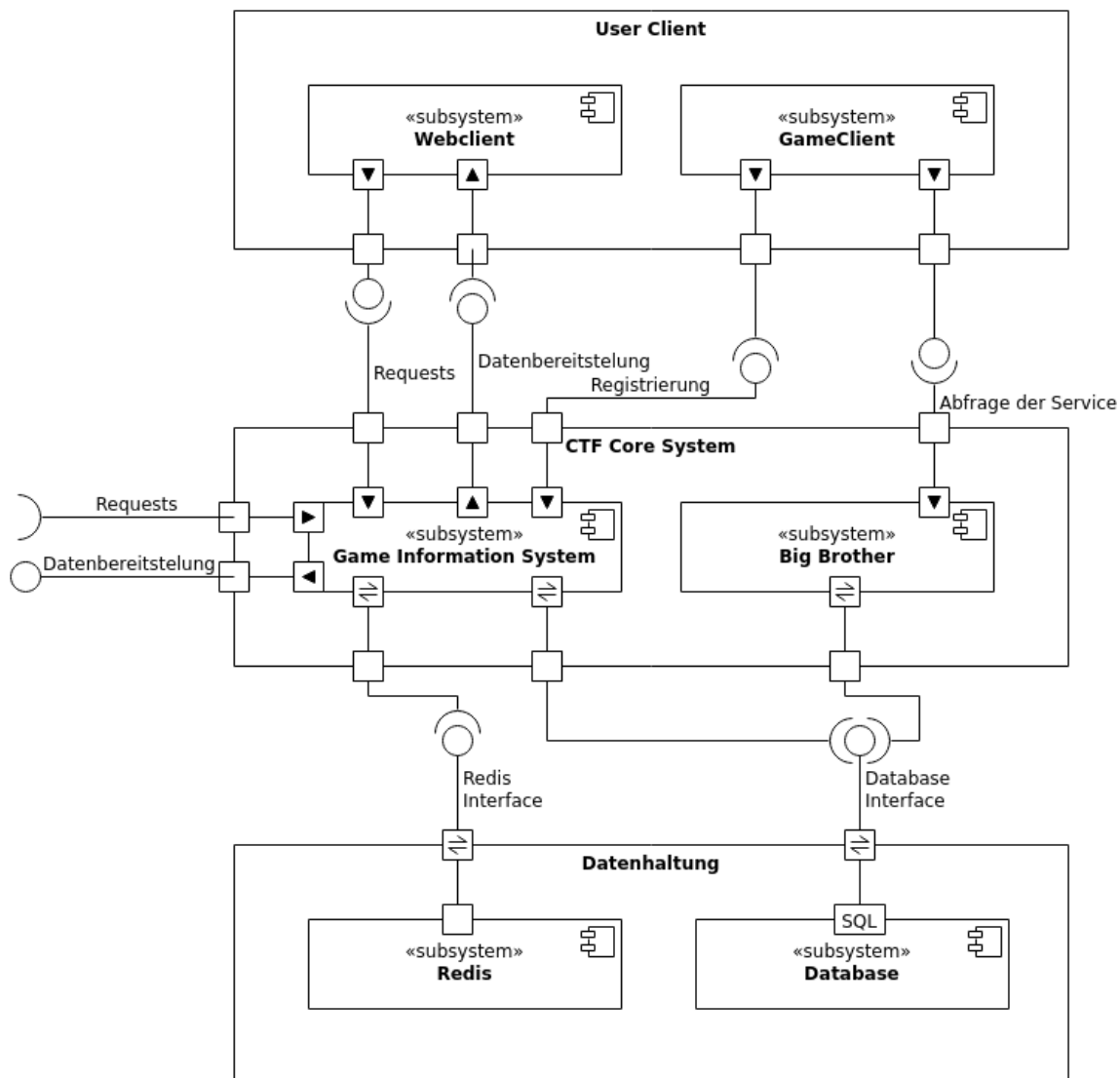


Abbildung 3.1: Übersicht über die Anwendung (Komponentendiagramm)

Die Gesamtheit des Systems (inklusive der User Clients), wie in Abbildung 3.1 zu sehen, lässt sich in drei Ebenen einteilen.

User Client Die erste Ebene *User Client* beinhaltet die auf einem User Client laufenden und für den Versuch relevanten Komponenten.

Bei der Komponente Webclient handelt es sich um einen geläufigen Webbrowser (häufig wird Firefox genutzt), welcher Informationen vom *CTF Core System* abrufen und Daten an dieses

übermittelt. Zu den Informationen gehören beispielsweise die Spielinformationen, der Spielstand aber auch teilnehmende Gruppen und Einstellungen. Der Webclient übermittelt Daten wie gefundene Flags, Lösungen von Aufgaben und Änderungen an Einstellungen.

Die Komponente *GameClient* beinhaltet alle auf dem System für den Versuch installierten Anwendungen. Dazu zählen nicht nur die Dienste mit den Schwachstellen. Auch die clientseitige Spielverwaltungs-Software wird unter dieser Komponente zusammengefasst. Die Spielverwaltungs-Software sorgt für die richtige Konfiguration des User Clients und versteckt die Flags.

CTF Core System Die Ebene des *CTF Core System* besteht aus den Komponenten *Big Brother* und *Game Information System*.

Die Komponente *Big Brother* implementiert einen Scanner, welcher für die Überwachung des *GameClients* mit seinen Schwachstellen zuständig ist. Die Ergebnisse werden in der *Database* für die Bewertung und Dokumentation festgehalten.

Die zweite Komponente *Game Information System* stellt eine Schnittstelle zwischen der Datenbank und den Nutzern dar. Mithilfe dieser können Informationen unter Berücksichtigung von Berechtigungen auf einem einheitlichen Weg aus der Datenbank ausgelesen, verändert und hinzugefügt werden.

Datenhaltung Die Ebene *Datenhaltung* beinhaltet die Komponenten *Redis* und *Database*.

Die Komponente *Redis* ist nach der gleichnamigen Software Redis benannt. Bei Redis handelt es sich auch um eine Datenbank und könnte daher mit in die Komponente *Database* aufgenommen werden; die Trennung erfolgt aber auf der Grundlage der Verwendung innerhalb der Software Architektur. Die Redis-Datenbank wird als Cache verwendet und persistiert die Daten nicht.

Anders als bei Redis werden in der Komponente *Database* die Daten auf eine Festplatte festgeschrieben, um diese persistent nutzen zu können.

3.3 Containerisierung

Bei der Containerisierung wird jeder Container als eine eigene logische Maschine betrachtet. Es können mehrere Container gleichzeitig auf einer physischen Maschine betrieben werden. Die verschiedenen Container laufen unabhängig voneinander und wissen nicht über die Existenz weiterer Container Bescheid. Sollte eine Kommunikation zwischen zwei Container benötigt werden, erfolgt diese über die Netzwerkschnittstelle ähnlich der Kommunikation zwischen Anwendungen, die auf verschiedener physischer Geräte.

Im Gegensatz zur Virtualisierung teilen sich die Container das zugrunde liegende Betriebssystem nicht. Dieses reduziert den Verbrauch von Ressourcen wie CPU und Arbeitsspeicher, da diese nur für die Anwendung und nicht das Betriebssystem benötigt werden.

Containerisierung wird verwendet, um Anwendungen getrennt betreiben zu können. So können verschiedene Versionen einer Software gleichzeitig auf der gleichen physischen Maschine betrieben werden, ohne dass es zu Interferenzen kommt oder dass veränderte Konfigurationen notwendig sind.

Des Weiteren läuft ein Container auf die gleiche Art und Weise unabhängig von der darunter liegenden Hardwarearchitektur. So läuft ein Container auf dem Rechner des Entwickelnden genauso wie ein Container in einem Rechenzentrum. Durch diese Eigenschaft sind die Anwendungen in Containern portabel.

Durch die Isolierungen können Anwendungen keinen negativen Einfluss auf weitere Container nehmen.

Docker wurde erstmalig im Jahr 2013 als Open-Source-Software veröffentlicht und zählt derzeit zu den am weit verbreitetsten Anwendungen für Containerisierung. Es ist der de facto Standard für Containerisierung. [Boe19]

Heutzutage nutzen immer mehr Unternehmen Orchestrierungstechnologien wie Kubernetes oder OpenStack um Container zentral über mehrere physische Maschinen zu verwalten und zu skalieren. [Gav18]

Eine Installation eines Kubernetes Clusters im EZS-Labor ist bisher noch nicht vorhanden. Auch ist eine Installation für diese Bachelorarbeit aufgrund der Kosten-Nutzen-Differenz nicht empfehlenswert.

Anstatt einer Orchestrierungssoftware wird *Docker Compose* genutzt werden. Mithilfe dieses können mehrere Container zu einem Service zusammengefasst und verwaltet werden. *Docker Compose* wird verwendet um die beiden serverseitigen Anwendungen sowie die beiden Datenbanken zu einem Service zusammenzufassen. Auch sorgt es dafür, dass die Container in einem eigenen virtuellen Netzwerk laufen und nur untereinander kommunizieren können. [Doc20]

3.4 Scanner

Im Rahmen des Versuches sollen die Studierenden ihre Systeme auf Schwachstellen untersuchen. Diese ausfindig gemachten Schwachstellen sollen im Anschluss beseitigt werden. Eine Überwachung wird benötigt, um zu prüfen, ob die Studierenden diese Schwachstellen behoben haben. Das Abschalten, beziehungsweise die Verhinderung der Verwendung eines Dienstes, stellt in den meisten Fällen keine Behebung der Schwachstelle dar und wird deshalb ebenfalls geprüft. Um diese Überprüfung zu ermöglichen, wird ein Scanner benötigt, der die Dienste auf

alle teilnehmenden *GameClients* abfragt und auswertet. Die bei der Überprüfung gesammelten Daten werden benötigt, um die Servicepunkte der Gruppen zu berechnen.

3.4.1 Verteilte Scanner

Eine Idee für die Lastverteilung des Scanners ist ein verteilter Scanner. Hierbei wird ein Worker Scanner auf jedem GameClient implementiert, welcher das eigene System überwacht. Ein Master Scanner sammelt die von den Worker Scannern erstellten Ergebnisse ein und speichert diese in einer Datenbank ab.

Der Vorteil des verteilten Scanners ist die Skalierbarkeit, da der Scanner auf dem Server nur von weiteren Scannern die Ergebnisse abholen, jedoch keine Überwachung durchführen muss.

Der verteilte Scanner bringt jedoch auch einige Nachteile mit sich. So muss sichergestellt werden, dass der Scanner auf dem User Client nicht manipuliert worden ist und die Ergebnisse valide sind. Eine solche Überprüfung könnte mithilfe eines „Fingerabdrucks“ geschehen. Jedoch muss dann auch geprüft werden, ob das Programm zur Erstellung des Fingerabdrucks manipuliert worden ist. Des Weiteren muss gewährleistet werden, dass der auf dem Client laufende Scanner dieselben Antworten und Ergebnisse erhält, wie ein fremder Nutzer. Dies ist notwendig, da die überwachten Services weiterhin von anderen Mitspielenden verwendet werden sollen.

Auf Grundlage der Nachteile, des Aufwandes der Implementierung und der ausreichenden Leistung des zentralen Scanners für den aktuellen Anwendungsfall wird ein verteilter Scanner nicht in Betracht gezogen. Die Idee des zentralen Scanners wird weiterverfolgt.

3.4.2 Zentraler Scanner

Die Herangehensweise des zentralen Scanners vermeidet die vorher beschriebenen Nachteile, da dem Ergebnis des Scanners vertraut werden kann und der Scanner zwangsläufig eine externe Sicht auf das System einnimmt. Dem Ergebnis kann vertraut werden, da es auf einem System ohne Einfluss der Mitspielenden berechnet wird.

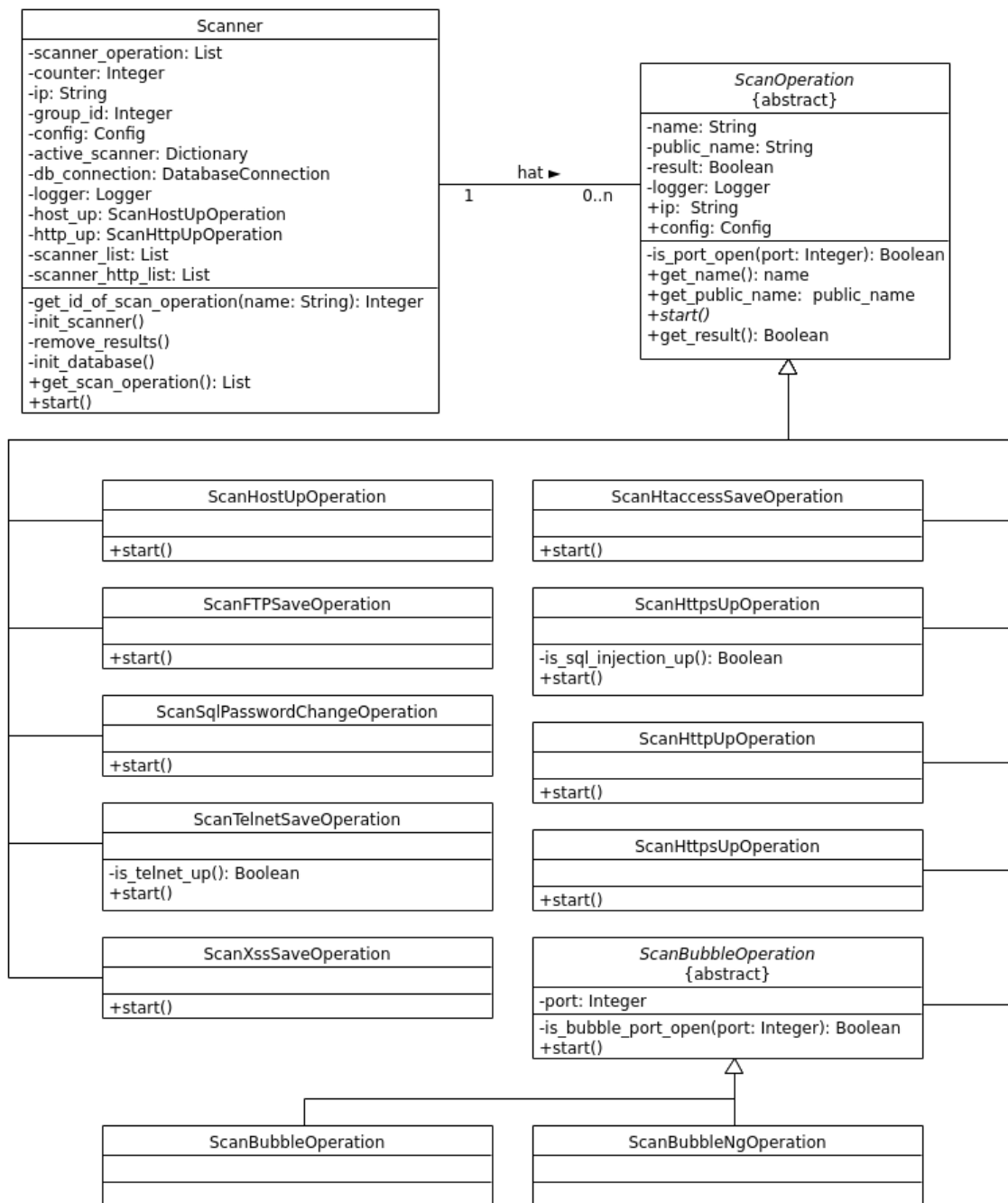


Abbildung 3.2: Klassen der Big Brother Komponente (Klassendiagramm)

Wie in Bild 3.2 erkennbar besteht die Komponente Big Brother aus der Klasse Scanner, der abstrakten Klasse ScanOperation sowie den abgeleiteten Scan-Operationen.

Die Klasse „ScanOperation“ definiert die abstrakte Funktion *start()*. Diese wird von den abgeleiteten Klassen implementiert und ermöglicht das Starten der einzelnen Scan-Operationen.

Ebenfalls speichern alle Scan-Operationen ihr Ergebnis in der privaten Variablen *result*. Mit Hilfe der von der abstrakten Klasse implementierten Funktion *get_results()* kann der Scanner das Ergebnis der Scan-Operation auslesen. Jedes Objekt der Klasse Scanner startet 0 bis n Scan-Operationen abhängig von der Konfiguration beziehungsweise den aktiven Diensten. Des Weiteren stellt die abstrakte Klasse die Funktion *is_port_open* bereit, welche von den Scan-Operationen genutzt werden kann, um den Status eines Ports auf dem fremden System zu prüfen. Ein Objekt der Klasse Scanner kann pro Typ maximal eine Scan-Operation starten und beinhaltet beziehungsweise verwaltet alle Scan-Operationen für ein Game Client.

Um mehrere Game Clients zu überwachen, werden mehrere Objekte der Klasse Scanner benötigt.

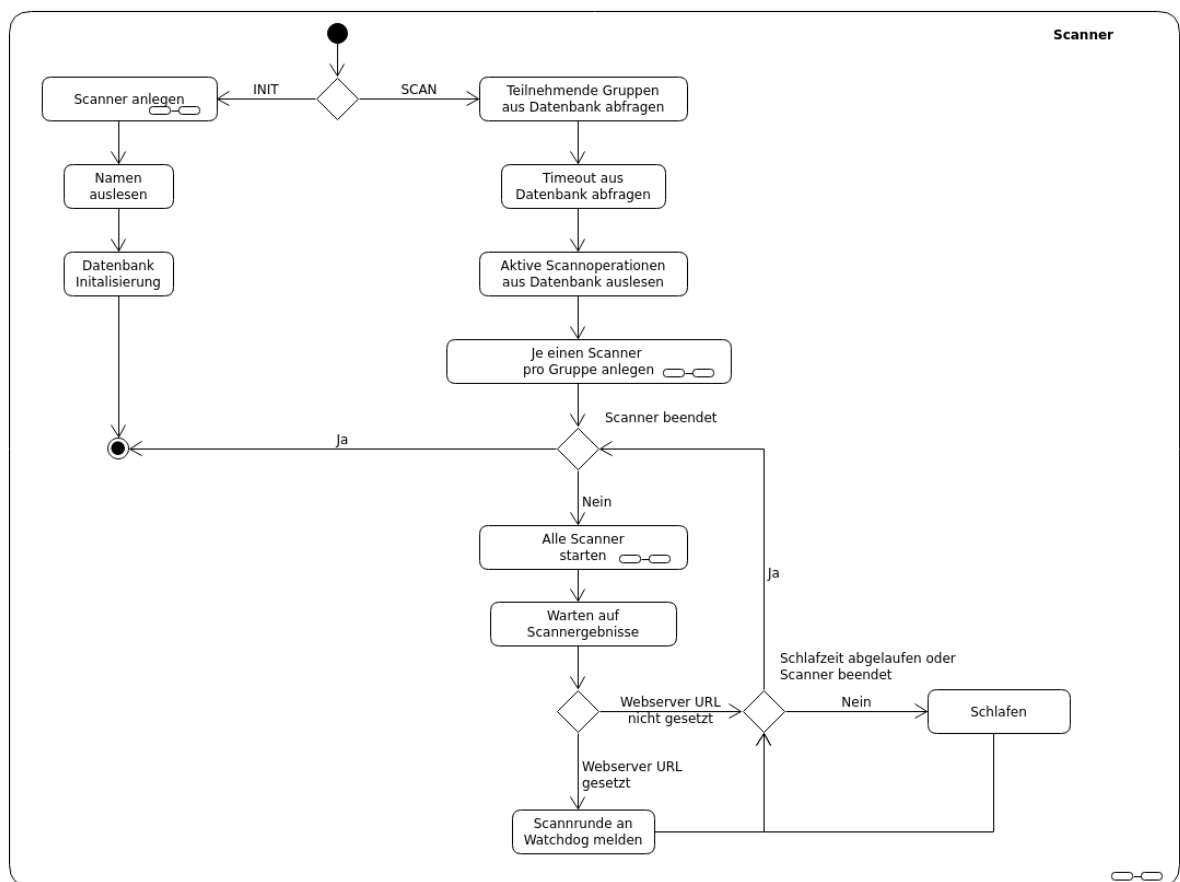


Abbildung 3.3: Ansicht des Scanners (Zustandsdiagramm)

Bei Starten des Scanners wird die zu bearbeitende Aufgabe spezifiziert.

Bekommt der Scanner die Aufgabe „INIT“, soll dieser die Service Datenbank mit den implementierten Scan-Operationen füllen, sodass Administratoren diese an- oder ausschalten können. Um die Service Datenbank zu füllen, wird zunächst ein Dummy der Klasse Scanner angelegt. Aus diesem Dummy Objekt werden von allen Scan-Operationen der Anzeigename

und der interne Name ausgelesen. Nach dem Auslesen alle Operationen werden die erhaltenen Daten gebündelt in die Service Datenbank geschrieben. Danach beendet der Scanner die Verbindung zur Datenbank und endet erfolgreich mit dem Statuscode 0.

Falls die Aufgabe des Scanners „SCAN“ ist, wird der Scan der Game Clients gestartet. Hierzu werden die teilnehmenden Gruppen und das Intervall der Scannerdurchgänge aus der Datenbank ausgelesen. Neben diesem werden die aktiven Scanner aus der Datenbank abgefragt. Sind alle Informationen vorhanden, wird für jede Gruppe ein Scanner Objekt der Klasse Scanner erstellt. Bei der Erstellung werden die aktiven Scan-Operationen sowie die zu überwachende Gruppe übergeben. Das Scanner Objekt legt dann für die benötigten Scan-Operationen die jeweiligen Objekte an.

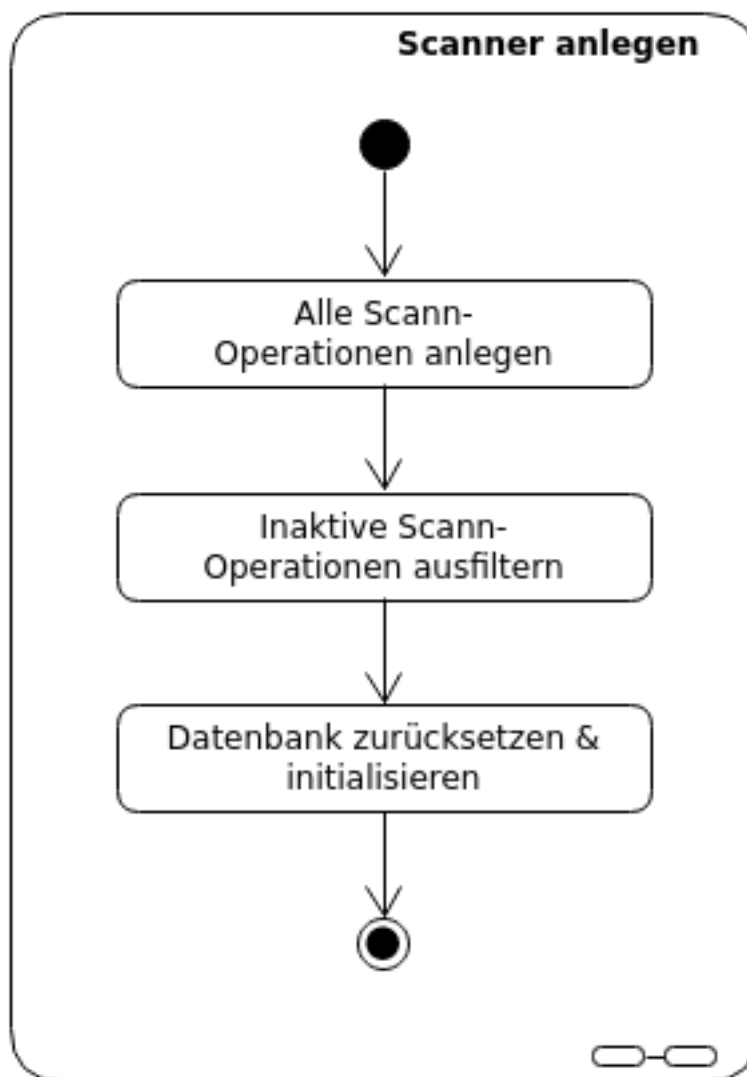


Abbildung 3.4: Erstellung eines Scanners (Zustandsdiagramm)

Nach dem Anlegen aller Scanner wird die Funktion *start()* nebenläufig gestartet. Im Anschluss wird auf das Beenden der gestarteten Funktionen gewartet. Sollten alle abgeschlossen sein, wird geprüft, ob das Durchführen einer Scan-Runde an den Webserver gemeldet werden soll. Ist dies der Fall, wird der Server darüber in Kenntnis gesetzt, dass neue Daten in der Datenbank vorhanden sind. Danach schläft der Scanner bis zum nächsten Durchlauf.

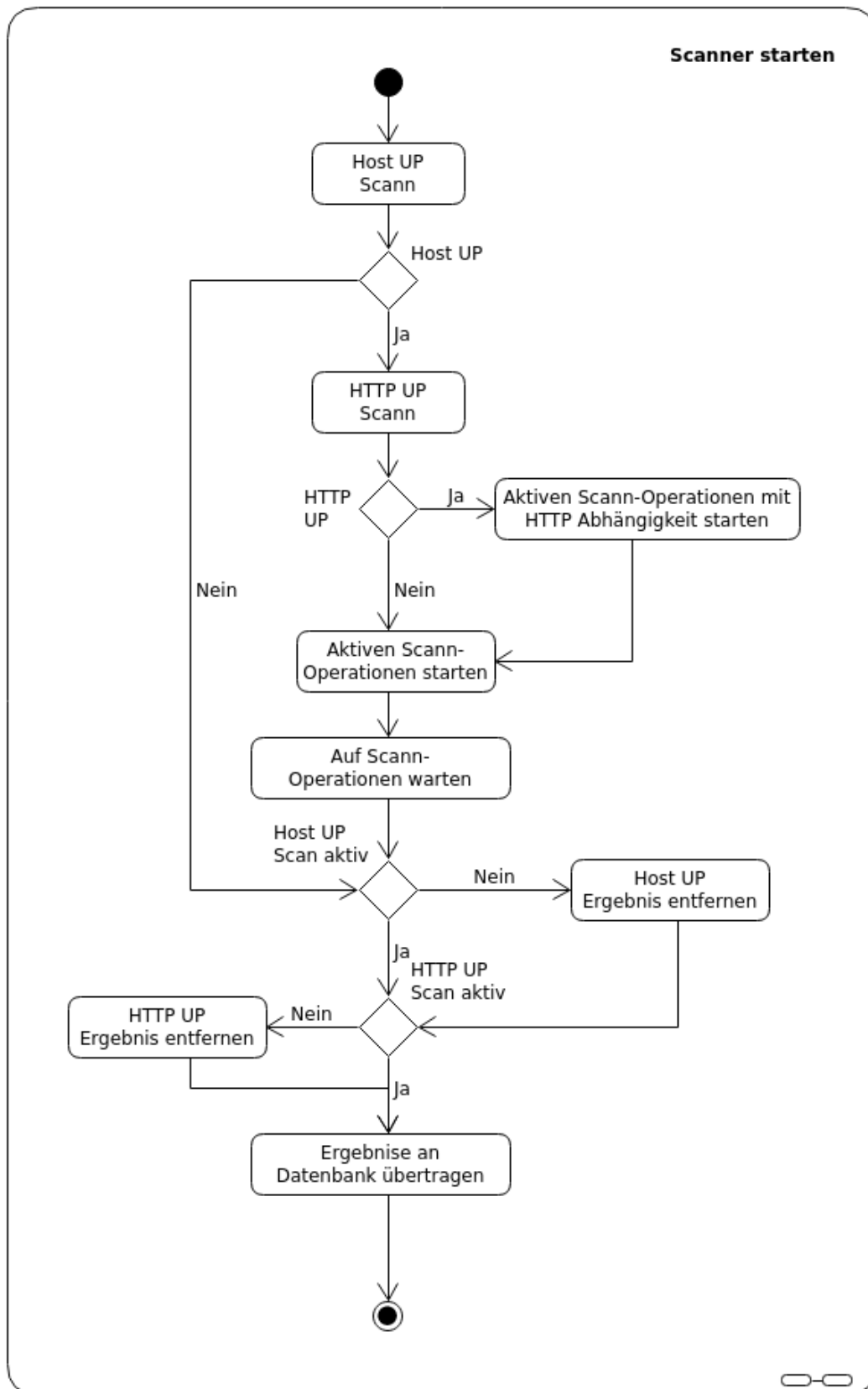


Abbildung 3.5: Starten eines Scanners (Zustandsdiagramm)

Beim Ausführen der Funktion *start()* des Scanners wird zunächst geprüft, ob das entfernte System erreichbar ist. Sollte dies nicht der Fall sein, werden alle nachfolgenden Scan-Operationen nicht durchgeführt, da diese fehlschlagen würden. Im Anschluss wird getestet, ob der HTTP Dienst des entfernten Systems erreichbar ist, da dieser für einige weitere Tests benötigt wird. Ist der HTTP Dienst erreichbar, werden die Scan-Operationen, welche auf dem HTTP Dienst basieren, mit in die Liste der abzuarbeitenden Scan-Operationen aufgenommen. Danach werden alle verbleibenden Scan-Operationen nebenläufig gestartet. Nachdem die Scan-Operationen ihre Aufgabe abgeschlossen haben, sammelt der Scanner alle Ergebnisse ein. Falls die *Host UP Scan-Operation* oder die *HTTP UP Scan-Operation* deaktiviert ist, werden diese aus dem Ergebnis entfernt. Danach übermittelt der Scanner die gesammelten Ergebnisse zur Datenbank und beendet seine Scan-Runde.

3.4.3 Scan-Operationen

Die Scan-Operationen werden nebenläufig abgearbeitet, um so die Dauer eines kompletten Scans zu minimieren. Eine Scan-Operation prüft genau einen Dienst beziehungsweise eine Schwachstelle auf dem entfernten Rechner. Die im alten System implementierten Scans werden in die Scan-Operationen überführt. Deshalb sollen die folgenden Scan-Operationen implementiert werden.

- Host-Up
prüft, ob der entfernte Rechner mit Hilfe von ICMP Paketen erreichbar ist
- Bubble-Up
prüft, ob der Bubble Server erreichbar ist und ob die Telnet Steuerung funktioniert
- BubbleNg-Up
prüft, ob der Bubble NG Server erreichbar ist und ob die Telnet Steuerung funktioniert
- FTP-Save
prüft, ob der FTP Server erreichbar und ob die Nutzung des anonymen Logins unterbunden worden ist
- Htaccess-Save
prüft, ob die Kombination aus Nutzernamen und Passwort des Htaccess Schutzes geändert wurde
- SQL-Injection-Save
prüft, ob die SQL-Injection im Login zum Membersbereich verhindert wurde
- SQL-Password-Save
prüft, ob das lokale Passwort des SQL-Nutzers root geändert wurde

- Telnet-Save
prüft, ob der Telnet Server deaktiviert oder deinstalliert wurde
- HTTP-UP
prüft, ob der HTTP Dienst des entfernten Rechners nutzbar ist
- HTTPS-UP
prüft, ob der HTTPS Dienst des entfernten Rechners nutzbar ist
- XSS-Save
prüft, ob der Cross-Site-Scripting Angriff im Bewertungsformular behoben wurde.

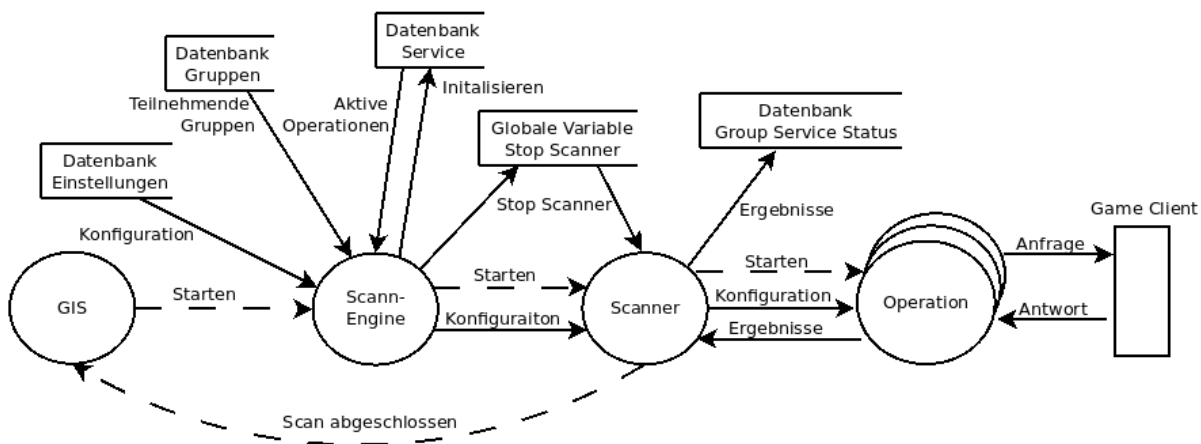


Abbildung 3.6: Datenfluss in der Scanner Komponente (Datenflussdiagramm)

Die im Datenflussdiagramm (Abbildung 3.6) sichtbaren, aber bisher nicht beschriebenen Datenflüsse finden zwischen dem Webserver und dem Scanner oder einer Scan-Operation und dem Game Client statt. Administratoren können über den Webserver den Scanner an- und abschalten. Die Scan-Operationen fragen bei dem Game Client ihren überwachten Dienst beziehungsweise ihre überwachte Schwachstelle an und erhalten eine Antwort zurück. Anhand dieser wird das Ergebnis der Scan-Operationen bestimmt.

3.5 Webserver

Der Webserver bietet die Möglichkeit der Verwaltung des Spiels, der Abgabe von Flags sowie der Durchführung von Käufen im Flagshop und Challenges. Auch können Informationen zum Spiel, wie Einstellungen, Spielstand, Strafen und Teilnehmer abgerufen werden.

3.5.1 Verwendung mehrerer Microservices

Der Webserver kann nach dem Architekturmuster Microservices implementiert werden. Hierbei besteht die Anwendung aus mehreren unabhängig Komponenten, welche, sofern dies notwendig ist, untereinander kommunizieren. Die Komponenten sind so klein wie möglich und können jederzeit durch eine andere Implementierung ausgetauscht werden. [Wol15]

So wären die verschiedenen Komponenten des Webserver (Flagabgabe, Nutzerverwaltung, Spielsteuerung, etc.) unabhängig voneinander und können leichter weiterentwickelt oder ersetzt werden.

Die Verwendung dieses Architekturmusters bedeutet bei der aktuellen Aufgabenstellung zu hohen Aufwand für zu geringen Nutzen.

3.5.2 Fat Webserver

Der Webserver beinhaltet sowohl die Logik als auch die Darstellung. Bei einer Anfrage an den Webserver wird eine Antwort bestimmt und diese dann in eine Vorlage beziehungsweise ein HTML Dokument eingebettet. Danach wird die Antwort zurück an den Nutzer gesendet.

Während der Implementierung des Prototyps und des weiteren Entwurfs hat sich ein Problem mit dem Flagshop Login herausgestellt.

Für die Nutzung des Flagshops ist ein Multi-Login notwendig, da nur am Webserver eingeloggte Nutzer sich mit einem extra angelegten Account am Flagshop anmelden und diesen verwenden dürfen. Dieser Multi-Login ließ sich mit dem im Prototypen implementierten Session basierten Login nicht einfach umsetzen.

So ist für diesen Anwendungsfall ein Stateless Login besser geeignet, da hier die benötigten Informationen vom Client, je nach Anliegen, gesendet werden können.

Die Nutzung des Stateless Logins bietet die Perspektive der Verwendung eines Stateless Webserver sowie eines Thin Webservers. Bei einem Thin Webserver werden nur Daten und keine Repräsentation an dem Client zurückgesendet. So wird die Aufgabe der Darstellung der Daten an den Client übertragen.

Durch die Nutzung eines Thin Servers werden zwei Dinge ermöglicht.

Zum Ersten ist es möglich, den Client und Server unabhängig voneinander zu entwickeln, zu verändern und zu verbessern. Damit kann in Zukunft eine Iteration der Software einfacher geschehen. Zweitens können die Studierenden eigene Clients programmieren, um mit der Anwendung zu interagieren.

3.5.3 Thin Webserver

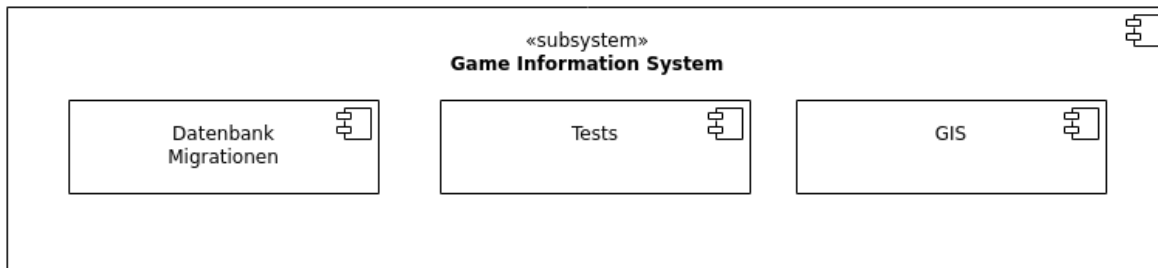


Abbildung 3.7: REST Interface im Überblick (Komponentendiagramm)

Der Server besteht aus der Komponente *Game Information System*, welche wiederum aus drei weiteren Komponenten besteht.

Die Komponente *GIS* implementiert die gesamte Server Logik. In diesem Modul wird der eigentliche Thin Server, über den die teilnehmenden und betreuenden Personen mit der Anwendung interagieren können, implementiert.

In der Komponente Datenbank Migrationen sind Migrationsskripts hinterlegt, welche die Datenbank Iterationen festhalten. Diese Skripts sollen genutzt werden, um die verwendete Datenbanken einfach mit dem benötigten Schema zu initialisieren.

Die letzte Komponente beinhaltet Unit-Tests. Mithilfe der implementierten Unit-Tests kann die Funktionalität der Anwendung bei späteren Änderungen überprüft werden.

Da der Thin Server nur eine Brücke zwischen Nutzer und Scanner oder Datenbank darstellt, kann von einer API (Application Programming Interface) gesprochen werden. Mithilfe dieser API können beispielsweise der aktuelle Spielstand aus der Datenbank ausgelesen und Strafen eingetragen werden.

API

Um bei der Implementierung der API einem Standard / einem Vorgehen zu folgen, wird der de facto Standard für HTTP-APIs Representational State Transfer (REST) verwendet.

Ein RESTful Interface ermöglicht, dass Ressourcen auf dem Webserver eindeutig identifizierbar sind, damit diese als Ziel von Operationen ausgewählt werden können. Des Weiteren werden einheitliche Schnittstellen genutzt. Dazu müssen Standardmethoden und -repräsentationen verwendet werden.

Durch diese Anforderungen bietet das REST Interface die Möglichkeiten, alle zur Verfügung stehenden Ressourcen auf die gleiche Art und Weise zu verwalten. Des Weiteren wird mit dieser Herangehensweise die HTTP Methode GET nicht länger zur Veränderung oder Erschaffung von Ressourcen verwendet, sondern die dafür ausgelegten HTTP-Methoden. Die für die

GET	Auf Ressourcen zugreifen
POST	Neue Ressourcen erzeugen
PUT	Bestehende Ressourcen verändern
DELETE	Vorhandene Ressourcen löschen

Tabelle 3.1: Übersicht über die verwendeten HTTP Methoden

Verwendung benötigten Daten werden auch nicht länger als Parameter der Anfrage beigefügt, sondern im Body der Anfrage übertragen. [Bei14]

Alle Routen werden mit dem Versionspräfix */v1* versehen. Diese Versionierung soll bei späteren Iterationen der API Kollisionen verhindern und die Nutzung der alten Versionen weiterhin ermöglichen.

Bei der Implementierung sollen die zur Verfügung stehenden HTTP Methoden benutzt werden. Das REST-Interface soll auch mit entsprechenden HTTP Codes antworten, um die Antwort und den Erfolg einer Anfrage auch ohne Antworttext interpretieren zu können. Bei der Datenübertragung zwischen Client und Server soll das JavaScript Object Notation (JSON) Format für die Formatierung der gesendeten Daten verwendet werden.

Neben den in Tabelle 3.1 aufgezeigten Methoden gibt es noch weitere HTTP Methoden, welche keine Anwendung in dem zu implementierenden REST-Interface erhalten.

3.5.4 Funktionale Eigenschaften

Login

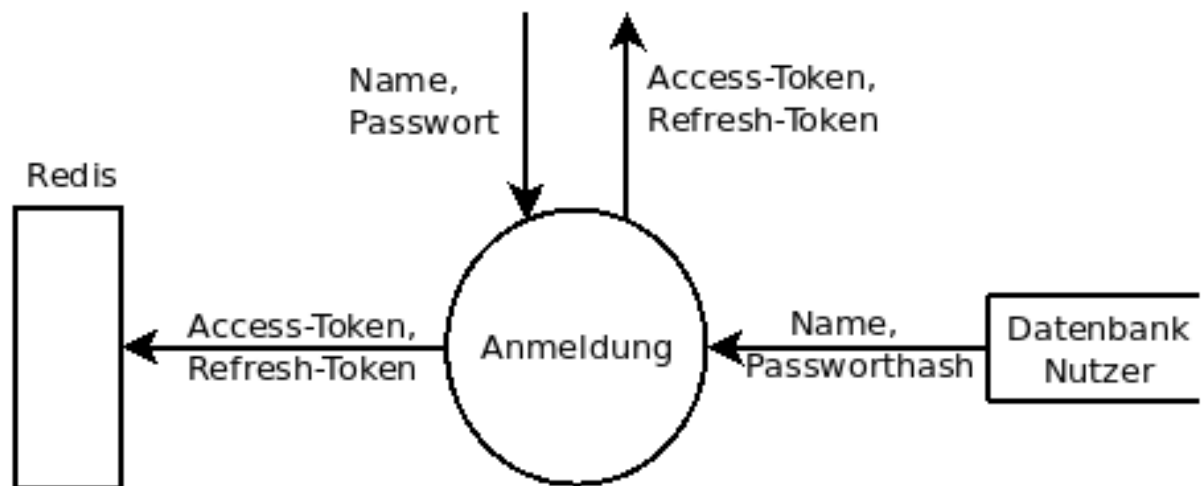


Abbildung 3.8: Datenfluss während eines Logins (Datenflussdiagramm)

Bei einem Login sendet der Nutzende die Kombination aus Nutzernamen und Passwort in seiner Anfrage an den Webserver. Sollte der Nutzernamen und das Passwort mit den in der

Datenbank gespeicherten Informationen übereinstimmen, wird ein Access- und ein Refresh-Token ausgestellt. Wichtig hierbei ist, dass das Passwort in der Datenbank **nur** im gehashten Format vorliegt.

Sollte kein Hackitzugang benötigt werden, muss für die Ausstellung der Tokens kein Nutzername und Passwort angegeben werden.

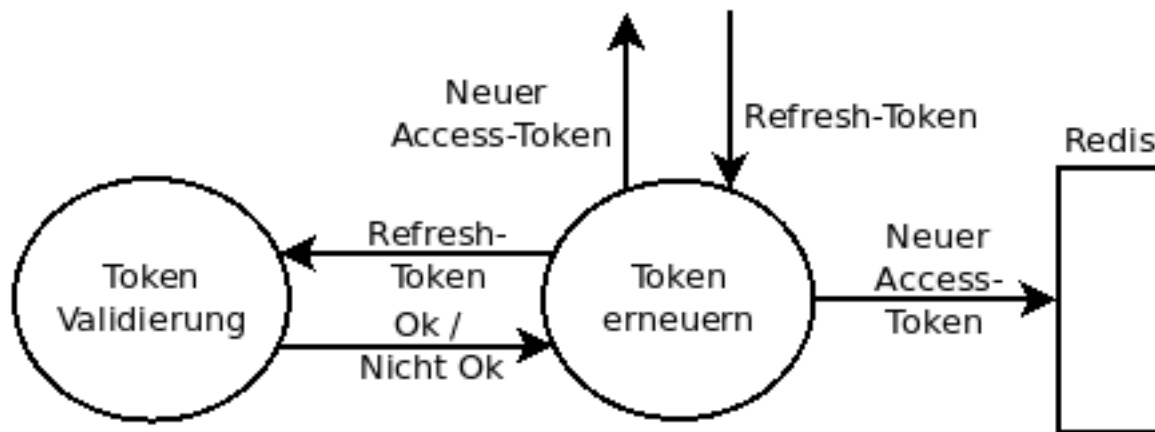


Abbildung 3.9: Datenfluss während eines Logins (Datenflussdiagramm)

Ein Refresh-Token wird ausgestellt, da beide Token eine begrenzte Lebenszeit haben. Der Refresh-Token hat eine längere Lebenszeit und ermöglicht die erneute Ausstellung eines Access-Tokens ohne Angabe eines Nutzernamens und Passwortes.

Des Weiteren werden alle ausgestellten Tokens für die Dauer der Gültigkeit in der Redis-Datenbank gespeichert, um die Tokens bei späteren Anfragen zu validieren.

Authentifizierung

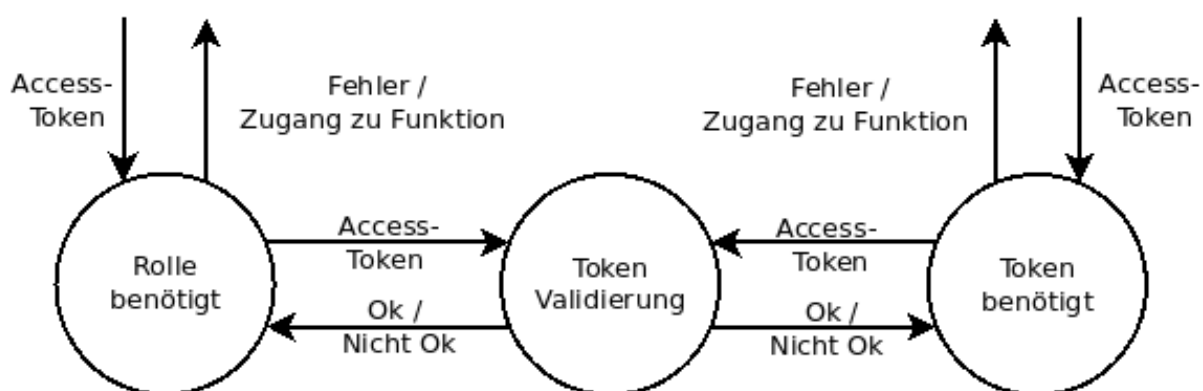


Abbildung 3.10: Datenfluss der Authentifizierung und Autorisierung (Datenflussdiagramm)

Die Authentifizierung des Benutzers wird über die in Abschnitt 3.5.4 erwähnten Tokens realisiert. Die Tokens müssen vom Client bei jeder Anfrage mitgesendet werden und enthalten neben der Nutzerkennung weitere Informationen zu Berechtigungen.

Dies reduziert die Anfragen an die Datenbank. Nachteil hierbei sind langsame Änderungen der Berechtigungen, da die neuen Berechtigungen erst mit dem Erstellen eines neuen Tokens übernommen werden. Da Änderungen an der Berechtigung selten vorkommen, kann dieser Nachteil relativiert werden.

Mit den im Token codierten Berechtigungen kann der Server die Autorisierung der vom Nutzer angefragten Aktion durchführen.

Tokenvalidierung

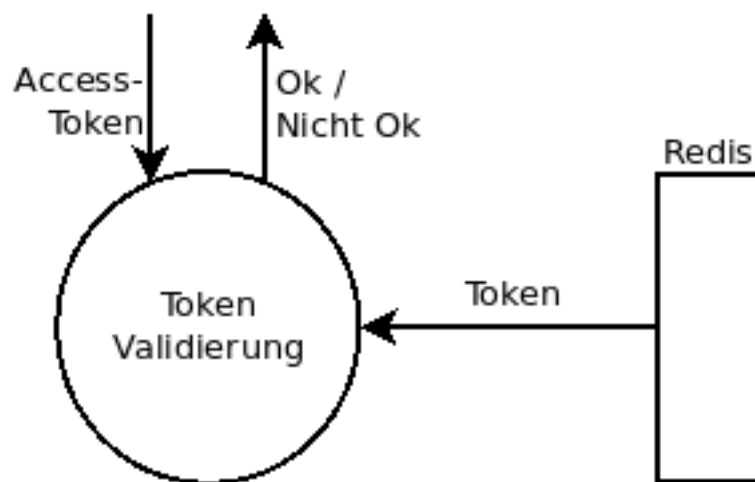


Abbildung 3.11: Datenfluss während der Tokenvalidierung (Datenflussdiagramm)

Für die Authentifizierung und Autorisierung müssen die mitgesendeten Tokens validiert werden. Dazu erhalten diese einen Zeitstempel der Ausstellung und des Ablaufs. Sollte der Nutzer einen Logout durchführen, wird der Token in der Datenbank als Widerrufen markiert.

Registrierung von GameClients

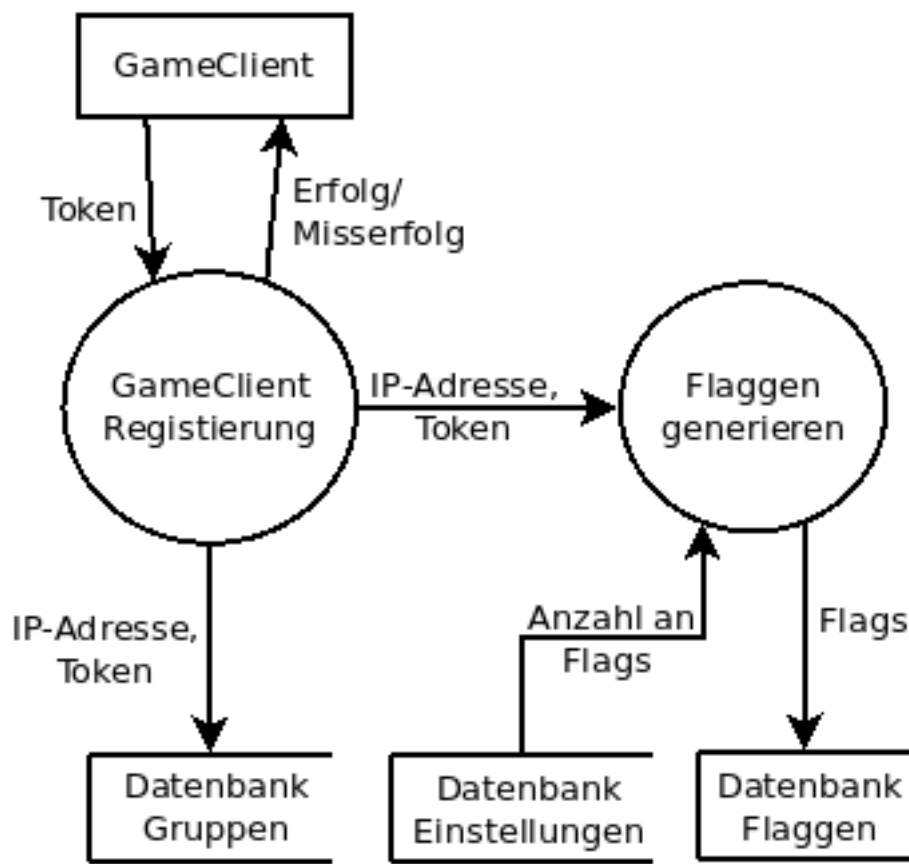


Abbildung 3.12: Datenfluss der Authentifizierung und Autorisierung (Datenflussdiagramm)

Die teilnehmenden GameClients sollen aufgrund der Anforderung nicht länger hartkodiert in der Anwendung vorliegen, sondern dynamisch hinterlegt werden. Deshalb müssen die GameClients sich vor Spielstart registrieren.

Flaggenerierung Durch die benötigte Registrierung ist es möglich, dass der Algorithmus zur Flaggenerierung verändert wird. Diese soll geschehen damit die Flags nicht länger pro Semester, sondern im besten Fall für immer einzigartig sind.

Damit die Flags einzigartig sind, überträgt der GameClient einen Token bei der Registrierung. Dieser wird sowohl vom GameClient als auch vom Server genutzt, um die benötigten Flags zu generieren.

Die Idee, dass die Flaggenerierung nur auf dem Server stattfindet, wurde verworfen, da der Nutzer auf dem Client die Möglichkeit hat die Flags bei der Übertragung abzufangen und abzugeben. Eine Verschlüsselung oder andere Verfahren würden keinen Mehrwert in puncto Sicherheit liefern, da der Nutzer Root-Rechte auf seinem System hat und so auf eventuell vorhandene PGP Keys zugreifen kann.

Flag Abgabe

Da die Flag Abgabe einen Hauptteil des Versuchs darstellt, müssen authentifizierte Spielende die auf dem eigenen oder gegnerischen System gefundene Flags abgeben können.

Das GIS muss die abgegebene Flag auf Gültigkeit prüfen und entweder Offensiv- und Defensiv- oder Discoverpunkte verrechnen. Auch muss sichergestellt werden, dass eine Gruppe eine Flag nur einmal abgeben kann.

Gruppen können alle eigenen Flags sowie gegnerische Flags, welche auf den GameClients verteilt sind, abgeben. Gegnerische Flagshop Flags können nicht abgegeben werden, da diese keine schützenswerten

Des Weiteren muss geprüft werden, ob die Abgabe im Angriffszeitraum geschieht. Andernfalls soll die Abgabe nicht weiter verarbeitet werden und bei einer Abgabe während der Discoverzeit eine Strafe ausgesprochen werden.

Spielsteuerung

Die Betreuenden sollen über das GIS das Spiel steuern können. Dabei müssen sie in der Lage sein, ein Spiel zu starten, zu pausieren und zu beenden. Die Steuerung des Scanners soll an das Spiel gekoppelt werden, aber auch eigenständig funktionieren.

Des Weiteren sollen die Betreuenden Strafen an Gruppen, welche die Regeln gebrochen haben, Strafen verteilen. Hier muss die Gruppe, der Grund der Bestrafung sowie die Anzahl der Strafpunkte übermittelt werden.

Nutzerverwaltung

Administrierende und Betreuungspersonal sollen die Möglichkeit erhalten, neue Nutzer anzulegen, zu bearbeiten und zu löschen. Wichtig hierbei ist, dass das Betreuungspersonal nur Nutzer der Rolle Spieler verwalten können.

Des Weiteren ist ein Import der Spielerzugänge zu realisieren, damit die generierte Zugänge einfach übernommen werden können.

Spielstände

Die abgespeicherten Spielstände sollen über das GIS abrufbar sein. Hierzu soll zuerst eine Liste der verfügbaren Spielstände inklusive des Datums der Speicherung an den Anfragenden übermittelt werden. Mit dieser Liste kann der benötigte Spielstand ermittelt und im nächsten Schritt angefragt werden.

Dieser detaillierte Spielstand beinhaltet die Punkte aller teilnehmenden Gruppen, die überwachten Schwachstellen und Dienste sowie den Spielstatus.

Steuerung der Services

Die betreuenden Personen des Versuchs, sollen die Möglichkeit erhalten einzelne Scan-Operationen zu (de-)aktivieren ohne, dass eine Änderung an der Software vorgenommen werden muss. Des Weiteren soll die Gewichtung der einzelnen Services jederzeit änderbar sein.

Einstellungen

Die betreuenden Personen sollen die Einstellungen des Spiels verändern können. Die Spieleinstellungen sollen als key-value-Paar vorliegen. Zu den Einstellungen zählen beispielsweise die Anzahl der generierten Flags pro Gruppe, aber auch, ob ein anonymer Login für die Rolle *Player* vorgesehen ist.

Notizen

Den betreuenden Personen soll es möglich gemacht werden permanente Hinweise zu geben. Des Weiteren sollen sie in der Lage sein bestehende Hinweise zu bearbeiten oder zu löschen.

Studierende können die verfassten Notizen einsehen, um Hinweise oder Anweisung zum Versuch zu erhalten.

Flagshop

(todo: Bild)

Der Flagshop muss die Verwaltung von Flagshop-Nutzern und Flagshop-Paketen sowie einen Kauf der Flagshop-Pakete ermöglichen.

Flagshop-Nutzer können durch die teilnehmenden Teams erstellt werden. Für die Erstellung werden Flags an die Gruppe verteilt. Betreuende Personen können ebenfalls für Gruppen Flagshop-Nutzer erstellen. Des Weiteren ist es ihnen möglich, bestehende Flagshop-Nutzer zu ändern und zu löschen.

Außerdem müssen Flagshop-Pakete durch die Betreuenden verwaltet werden. Die Erstellung von Flagshop-Paketen soll nur vor einem Spielstart möglich sein, damit die richtige Anzahl an Flags bei der Registrierung eines GameClients erzeugt werden kann. Die Flagshop-Pakete sollen neben den Kosten und dem Namen auch die Anzahl der erwerbbaaren Flags enthalten.

Studierende können Flagshop-Pakete erwerben. Besonderheit hierbei soll sein, dass diese einen Preis mitsenden und so die Flagshop-Pakete für einen anderen Preis als angegeben erwerben können.

Challenges

(todo: Bild)

Die Studierenden müssen Informationen zu Challenge sowie deren Ablageort abrufen können. Des Weiteren müssen sie die Challenge abschließen können. Hierfür sollen die Challenges am Ende ein Passwort mitteilen, welches ebenfalls in der Datenbank vorhanden ist. Die Studierenden können dieses Passwort dann als Beweis der Lösung der Challenge an das GIS übermitteln.

Die Challenges werden entweder mit der SPA ausgeliefert oder sollen von einem Webserver zur Verfügung gestellt werden. Sie werden nicht über das GIS verteilt, da dies als API nur Daten und keine Ressourcen an den Client übermittelt.

3.5.5 Reverse Proxy

Für das Betreiben wird auf den bereits im EZS Labor verwendeten Apache HTTP-Server zurückgegriffen. Durch die Entscheidung bleibt dieser als einziger Einstiegspunkt für Anfragen zuständig. So kann die Protokollierung der Anfragen sowie die Verschlüsselung der Verbindung an die Webserver Software abgegeben.

Der Reverse Proxy muss bei der Weiterleitung der Anfrage an das GIS die eigentliche IP-Adresse der Anfrage mitteilen(todo: replace mitteilen). Dies wird benötigt, um die zugehörige Gruppe, bei der Registrierung und dem Login zu bestimmen. Die originale IP-Adresse der Anfrage soll in einen HTTP Header gespeichert werden.

In einen HTTP Header können Server und Client zusätzliche Informationen zur Anfrage oder Antwort beifügen. [cM20a]

Um einen Spoofing-Angriff zu erschweren und das Vertrauen in den Header mit der IP-Adresse zu erhöhen, soll ein weiterer Header mit einem Geheimnis gesetzt werden. Anhand dieses Geheimnisses kann das GIS entscheiden, ob die Anfrage über einen vertrauenswürdigen Proxy weitergeleitet oder ob ein Spoofing-Angriff durchgeführt worden ist. Die Erweiterung wird benötigt, da die Anwendung auch ohne einen Reverse Proxy betrieben werden kann. In diesem Anwendungsfall kann die angreifende Person sich als Proxy für eine andere Gruppe ausgeben.

Bei einem Spoofing-Angriff versendet die angreifende Person Anfragen für andere IP-Adressen und erhält die Antwort. So kann diese im Namen anderer agieren und den Angegriffenen beispielsweise Minuspunkte verschaffen.

3.6 Datenbank

Im Gegensatz zur bestehenden Anwendung wird auf eine relationale Datenbank anstatt auf Dateien zurückgegriffen. Das Vorgehen resultiert unter anderem aus der gestiegenen Datenmenge. Eine NoSQL Datenbank wird nicht benötigt, da sich die Daten in Schemen untergliedern lassen. Die Nutzung einer Datenbank stellt sicher, dass sich die Daten an einer zentralen Stelle befinden und nicht über die Anwendung verstreut sind. Auch wird eine mögliche Redundanz von Daten verhindert, da in Datenbanken mit Relationen gearbeitet werden kann. Durch die AKID-Eigenschaft (im eng. ACID - Atomarität, Konsistenz, Isolation und Dauerhaftigkeit) der Datenbanken wird sichergestellt, dass Daten in der Datenbank vollständig und konsistent sind. Ferner sind die Abfragen auf eine Datenbank besser optimiert, als Abfragen auf eine Datei. (todo: quelle hinzufügen)

Des Weiteren ist es möglich, die Punktberechnung in der Datenbank unter Zuhilfenahme von Views durchzuführen.

3.6.1 Basis-Tabellen

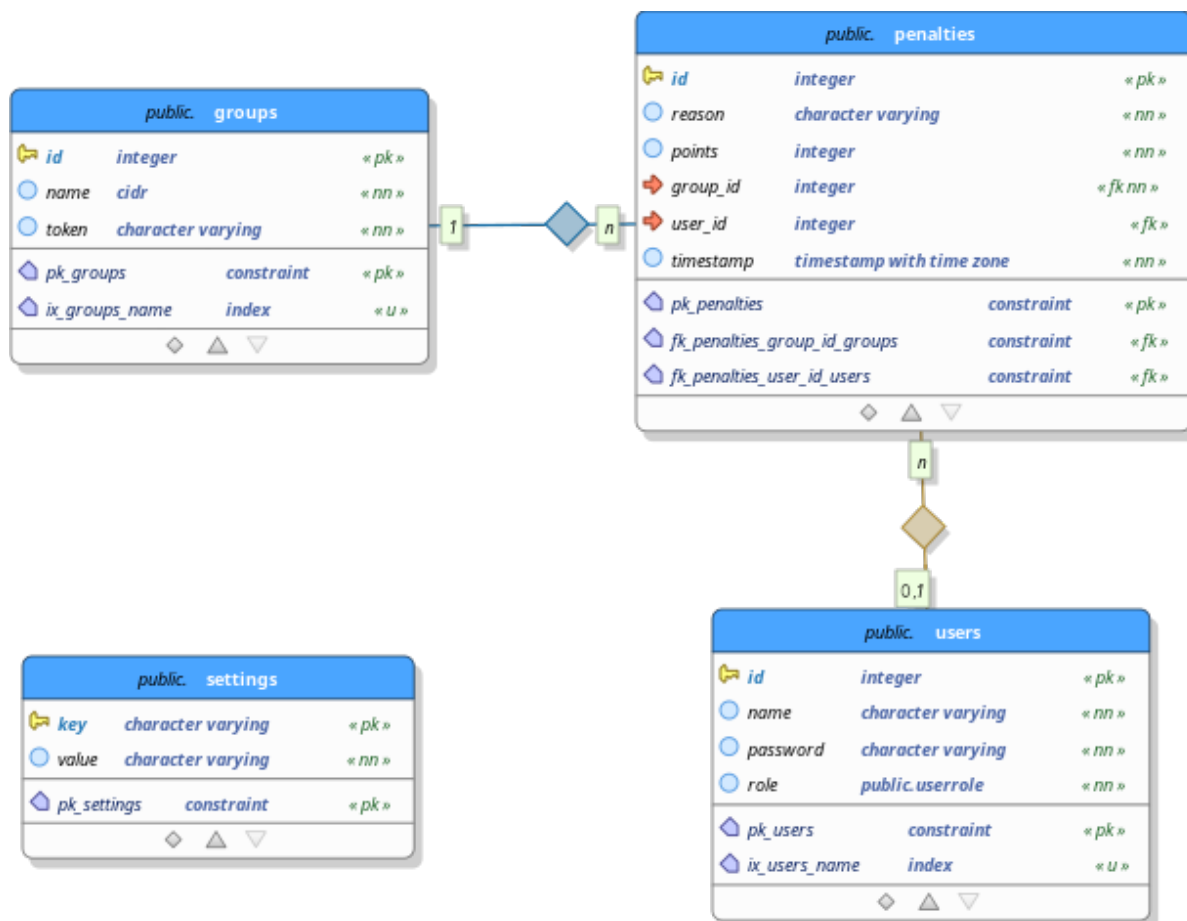


Abbildung 3.13: Ansicht der Basis-Tabellen (ER-Diagramm)

In der Abbildung 3.13 ist neben der alleinstehenden Tabelle *settings* die Tabelle *users* sowie die n:m-Beziehung zwischen *users* und *groups* dargestellt. Die n:m-Beziehung wird über eine Referenztabelle (*penalties*) mit einer 1:n-Beziehung zwischen *groups* und *penalties* und einer 0,1:n-Beziehung zwischen *users* und *penalties* modelliert. In der n:m-Beziehung werden die ausgesprochenen Strafen gespeichert. Jede Gruppe kann von mehreren Betreuern oder dem System mehrmals verwahrt werden.

Einstellungen

Die *settings*-Tabelle beinhaltet Einstellungen des Spiels als key-value Paar. Hierbei sind beide Spalten strings und der key einzigartig. Zu den Einstellungen gehören beispielsweise das Scan-Intervall, die Anzahl der Flags pro Team sowie das Ende der Discover- und Attackzeit.

Nutzer

In der Tabelle *users* sind die Log-In Informationen der Administratoren, Betreuer und Spieler hinterlegt. Da der Login aus Nutzernamen und Passwort besteht, werden die Spalten *name* und *password* benötigt. Auch muss anhand des Nutzernamens eindeutig auf einen Account geschlossen werden, deshalb ist die Spalte *name* als unique gekennzeichnet. Die Rolle des Nutzers wird mithilfe eines Enums (*role*) (Liste von benannten Werten) definiert.

Strafen

Die durch das System oder die Betreuer verteilten Strafen werden in der Tabelle *penalties* gespeichert. Dazu wird neben dem Grund der Strafe (*reason*), dem Zeitpunkt der Bestrafung (*timestamp*) und auch die Anzahl an Strafpunkten (*points*) festgehalten. Damit Gruppen von einem Betreuer öfters bestraft werden können, ist der Primärschlüssel des Eintrages die ID der Strafe.

3.6.2 Gruppen-Tabellen

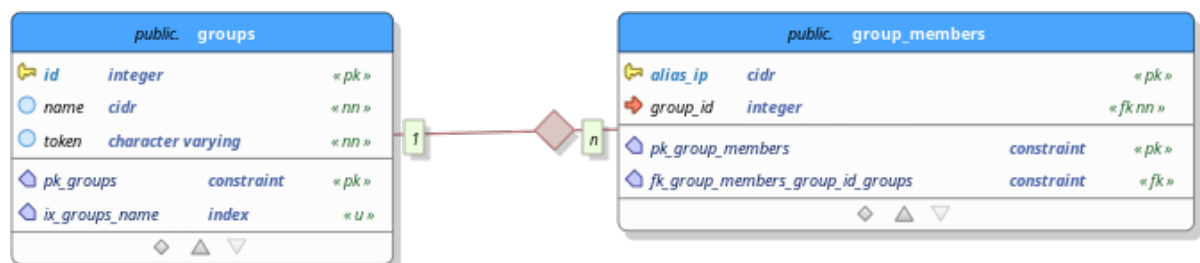


Abbildung 3.14: Ansicht der Gruppen-Tabellen (ER-Diagramm)

Wie in Abbildung 3.14 zu sehen existiert zwischen der Tabelle **groups** und **group_members** eine 1:n-Beziehung. Dies bedeutet, dass eine Gruppe mehrere Mitglieder haben kann, aber jedes Mitglied nur genau in einer Gruppe vertreten sein kann.

Gruppe

In der Tabelle **groups** werden alle teilnehmenden GameClients vermerkt. Jede Gruppe besitzt eine eindeutige *ID* und einen eindeutigen *Namen*. Der *Name* der Gruppe repräsentiert die IP-Adresse des GameClients und ist nach der *Classless Internet Domain Routing (CIDR)* Konvention abgelegt. Des Weiteren besitzt die **groups** Tabelle die Spalte *token*. In dieser wird der individuelle Token, welcher zur Flaggenerierung benötigt wird, abgespeichert. Dies ist nötig, damit der Server dieselben Flags wie der GameClient generieren kann und die Betreuer die Korrektheit verifizieren können.

Gruppenmitglieder

Die Tabelle **group_members** beinhaltet alle IP-Adressen, welche im Namen einer Gruppe agieren dürfen. Dafür wird die IP-Adresse im Feld *alias_ip* und die vertretende Gruppe als Referenz im Feld *group_id* gespeichert. Da das Feld *alias_ip* als Primärschlüssel verwendet wird, kann jede IP-Adresse nur genau eine Gruppe vertreten.

3.6.3 Flags-Tabellen

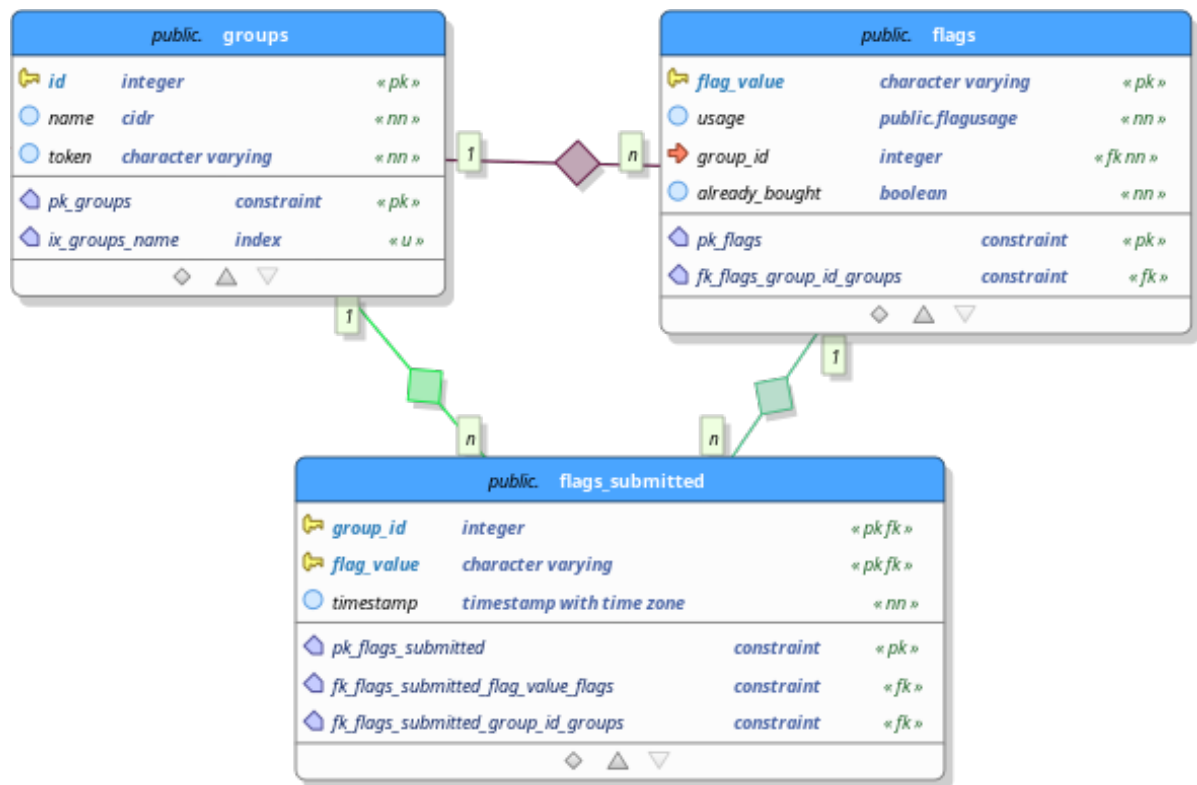


Abbildung 3.15: Ansicht der Flags-Tabellen (ER-Diagramm)

In der Abbildung 3.15 ist die 1:n-Beziehung zwischen den Tabellen **groups** und **flags** erkennbar. Dieses hat zur Folge, dass eine Gruppe mehrere Flags besitzen kann, jedoch eine Flag immer genau zu einer Gruppe gehört. In der Abbildung ist weiter die n:m-Beziehung zwischen **groups** und **flags** abgebildet. Diese wird in eine Verknüpfungstabelle namens **flags_submitted** mit zwei 1:n-Beziehung zerlegt. Diese Tabelle enthält die abgegebenen Flags.

Flags

Die während eines Spiels generierten und benötigten Flags werden in der Tabelle **flags** abgelegt. Hierzu wird der Wert einer Flag als string in der Spalte **flag_value** festgehalten. Des Weiteren wird die Nutzungsart unter Zuhilfenahme eines Enums und die Gruppenzugehörigkeit als Referenz gespeichert. Außerdem wird in der Spalte **already_bought** als bool vermerkt, ob diese Flag bereits im Flagshop erworben worden ist. Diese Spalte besitzt nur Relevanz für die dementsprechenden Flagshop Flags.

Abgegebene Flags

Die durch die Studierenden abgegeben Flags werden in der Tabelle *flags_submitted* eingetragen. Auch wird der Zeitpunkt der Abgabe mitgespeichert, um eventuelle Betrugsversuche aufzudecken. Die Spalten *group_id* und *flag_value* bilden zusammen den Primärschlüssel. Dieses ermöglicht, dass jede Gruppe jede Flag abgeben kann. Die Mehrfachabgabe einer Flag durch eine Gruppe wird so auch unterbunden.

3.6.4 Service-Tabellen

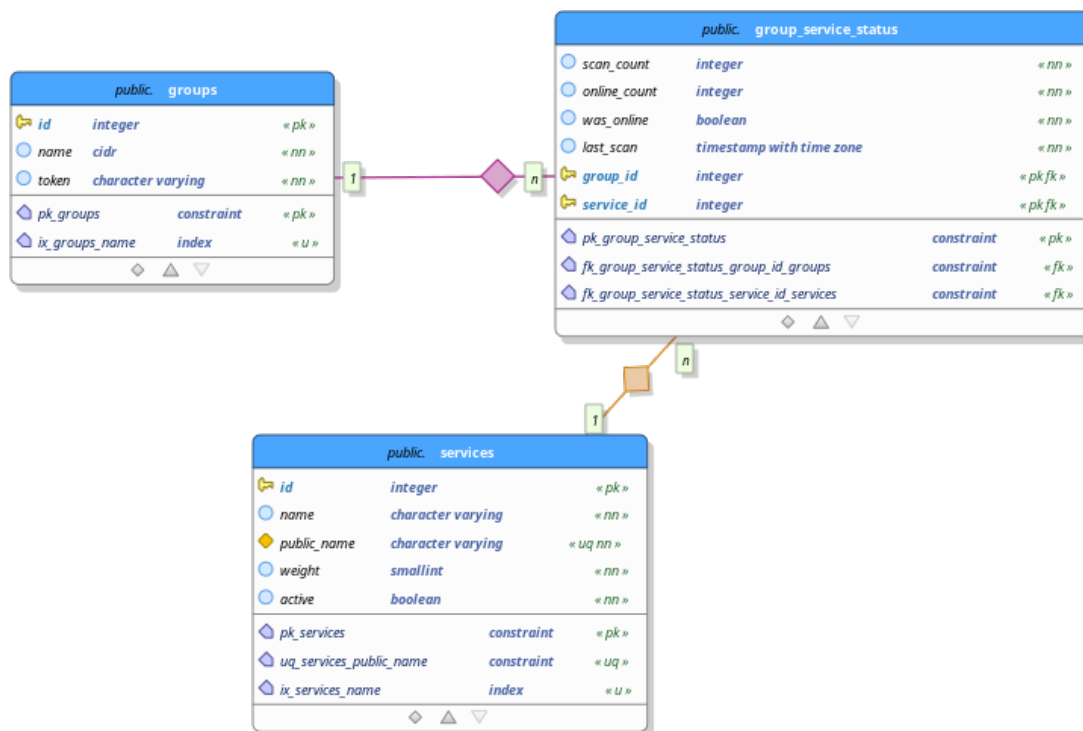


Abbildung 3.16: Ansicht der Service-Tabellen (ER-Diagramm)

In der Abbildung 3.16 ist die *services*-Tabelle sowie die n:m-Beziehung zwischen *groups* und *services* zu sehen. Diese wird als Referenztabelle (*group_service_status*) mit zwei 1:n-Beziehungen dargestellt.

Services

In der *services*-Tabelle sind alle vom Big Brother überwachten Dienste und Schwachstellen eingetragen. Jeder dieser Einträge besteht aus einer eindeutigen ID, dem internen Namen der

Operation (*name*), dem angezeigten Namen (*public_name*) und der Gewichtung im Gesamtergebnis (*weight*). Auch kann die Überprüfung der Schwachstelle mithilfe des bool-Wertes *active* an- oder abgeschaltet werden.

Servicestatus der Gruppen

In der Referenztabelle **group_service_status** wird das Ergebnis der Überprüfung der Schwachstellen und Dienste jeder Gruppe abgespeichert. Dazu wird für die Kombination aus Gruppe und Service ein Eintrag angelegt und die Anzahl der Scans in *scan_count* und die Anzahl der erfolgreichen Scans in *online_count* gespeichert. Des Weiteren wird der Zeitpunkt des letzten Scans in *last_scan* und der Erfolg des letzten Scans in *was_online* festgehalten. Erfolgreich bedeutet in diesem Kontext, dass die Studierenden die überwachte Schwachstelle ausgebessert und den überwachten Dienst erreichbar gehalten haben.

3.6.5 Flagshop-Tabellen

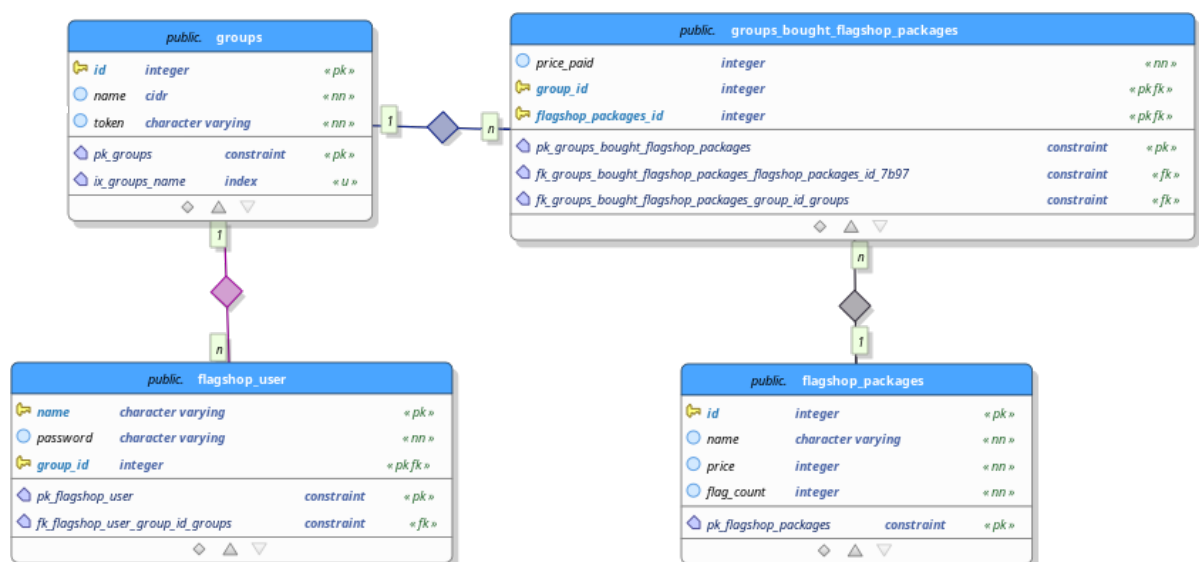


Abbildung 3.17: Ansicht der Flagshop-Tabellen (ER-Diagramm)

Die Abbildung 3.17 stellt die 1:n-Beziehung zwischen den Tabellen **groups** und **flagshop_user** dar. Das heißt, dass jeder Gruppe mehrere Flagshop Benutzer zugehörig sein können, jeder Benutzer aber genau einer Gruppe angehört. Des Weiteren wird die n:m-Beziehung zwischen **groups** und **flagshop_packages** als Referenztabelle (**groups_bought_flagshop_packages**) mit zwei 1:n-Beziehung dargestellt. Diese beinhaltet die gekauften Flagshop-Pakete pro Team.

Flagshop Nutzer

Für die Nutzung des Flagshops müssen die Gruppen einen oder mehrere Flagshop-Nutzer anlegen. Diese werden in der Tabelle *flagshop_user* abgelegt. Hierfür werden neben der erstellenden Gruppe (*group_id*) auch das Passwort (*password*) und der Name (*name*) abgespeichert. Der Primärschlüssel wird aus der Gruppe und dem Namen gebildet. So ist der Nutzernamen für die Gruppe eindeutig. Mehrere Gruppen können aber Nutzeraccounts mit demselben Namen anlegen.

Flagshop Pakete

Die Betreuer und Administratoren können Flagshop Pakete anlegen, die von den Studierenden gekauft werden können. Diese werden in der Tabelle *flagshop_packages* abgelegt und erhalten Informationen zum Preis (*price*) und der Anzahl der erhaltenen Flags (*flag_count*). Auch muss ein Name für das Paket über das Feld *name* angegeben werden.

Gekaufte Flagshop Pakete

Die von den Gruppen gekauften Flagshop Pakete werden in der Tabelle *groups_bought_flagshop_packages* abgespeichert. Auch wird im Feld *price_paid* der beim Kauf gezahlte Preis festgehalten, da die Studierenden den Preis eines Flagshop Paketes beim Kauf reduzieren können. Jedes Paket kann genau einmal von jeder Gruppe gekauft werden, da sich der Primärschlüssel aus Gruppe (*group_id*) und Paket (*flagshop_packages_id*) zusammen setzt.

3.6.6 Challenge-Tabellen

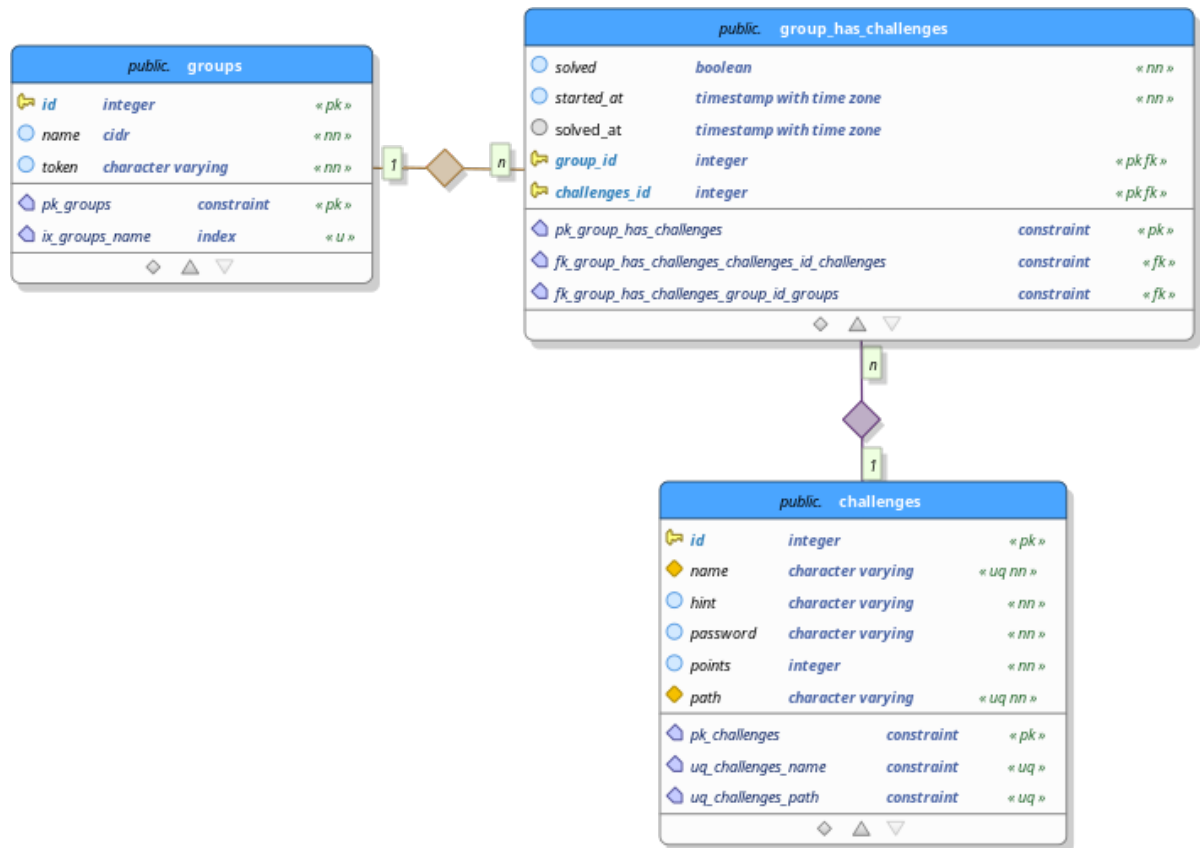


Abbildung 3.18: Ansicht der Service-Tabellen (ER-Diagramm)

In der Abbildung 3.18 ist die **Challenge** Tabelle und die n:m-Beziehung zwischen den Tabellen **groups** und **challenges** zu sehen. Diese Beziehung ist als Verknüpfungstabelle (**group_has_challenges**) mit zwei 1:n-Beziehung realisiert.

Challenges

Die **challenges** Tabelle beinhaltet alle Challenges, welche von den Studierenden gelöst werden können. Jede Challenge besitzt eine eindeutige ID. Neben dieser werden für jede Challenge ein Titel in **name**, ein Hinweis in **hint**, das zum Lösen benötigte Passwort in **password**, die Anzahl der Punkte in **points** und der Pfad, über den die Challenge abgerufen werden kann, gespeichert.

Gestartete / Abgeschlossene Challenges

Alle angefangenen und abgeschlossenen Challenges werden in der Tabelle **group_has_challenges** abgespeichert. Es werden das Startdatum (*started_at*) der Challenge, der Status des Abschlusses (*solved*) und bei erfolgreicher Absolvierung der Challenge das Enddatum (*solved_at*) gespeichert. Durch die Zusammensetzung des Primärschlüssels aus Challenge und Gruppe kann jede Gruppe jede Challenge genau einmal starten und absolvieren.

3.6.7 Weitere Tabellen



Abbildung 3.19: Ansicht der weiteren Tabellen (ER-Diagramm)

Wie in Abbildung 3.19 erkennbar, besitzen die Tabellen keine Abhängigkeiten und Verbindungen zu anderen. Im Folgenden werden die Tabellen für die Logs, die Notizen und die alten Spielstände vorgestellt.

Logs

Um die Aktionen innerhalb der Anwendung nachverfolgen zu können, werden diese in die **logs** Tabelle geschrieben. Jeder Eintrag besteht aus einer ID, einem Enum, in dem der Typ der Aktion festgehalten wird (*action*), einem Zeitpunkt (*timestamp*) und dem Inhalt der Aktion *data*.

Innerhalb der **logs** Tabelle werden nur die Aktionen des derzeit aktivierten Spiels gespeichert. Neben diesen werden auch noch die Aktionen des letzten Spiels in der Tabelle **logs_old** gespeichert. Sollte ein Spiel beendet werden, werden die Aktionen des alten Spiels mit den neuen Aktionen überschrieben.

Notizen

In der Tabelle **notes** soll den Betreuern und Administratoren die Möglichkeit geboten werden, Notizen und Hinweise zum Rahmen und zur Durchführung des Versuches zu geben. Diese Notizen können durch die Studierenden eingesehen werden. Dafür werden Titel und Inhalt jeweils in einem string gespeichert. Um einzelne Notizen abrufen zu können, erhalten diese eine eindeutige ID.

Alte Spiele

Die Tabelle **backups** soll alle alten Spielstände speichern. Dazu wird jedem Backup eine eindeutige ID zugewiesen und der Zeitpunkt des Erstellens wird in *created_at* abgespeichert. Die Informationen zu einem Spiel sind im JSON Format in der Spalte *data* abgelegt.

3.7 Webclient

3.7.1 SPA vs MPA

Multi Page Applications Multi Page Applications, kurz MPA, ist die klassische Architektur für Webanwendungen. Bei dieser Architektur wird für jeden Request (Anfrage) an den Webserver eine neue Seite inklusive Ressourcen wie Cascading Style Sheets (CSS)¹, JavaScript und Bildern geladen. Dieses kann an einem Beispiel verdeutlicht werden.

Auf einer Shop-Seite befinden sich 10 Produkte inkl. Bild und Kurzbeschreibung. Wird ein Produkt ausgewählt, sendet der Client einen Request / eine Anfrage an den Webserver. Der Webserver antwortet mit allen Ressourcen (siehe oben), welche für das Produkt benötigt werden. Der Client stellt dann aus den Ressourcen die Ansicht dar und das Produkt inklusive der Details ist für den Nutzer zu sehen.

Der Vorteil von MPAs ist die einfacherer Optimierbarkeit für Suchmaschinen, das sogenannte SEO (Search Engine Optimization). Ein gutes SEO Rating sorgt dafür, dass die Webseite bei Suchmaschinen weit oben zu finden ist. Dies ist besonders für Webseiten und Shops wichtig, die um Kunden konkurrieren. Anzuführen sind hier diverse Webshops und Zeitungen.

¹Beinhalten Regeln für die Darstellung von unter anderem Webseiten

Single Page Applications Die Single Page Applications, kurz SPA, stellt das genaue Gegenteil von MPA dar. Bei SPA besteht die Anwendung aus genau einem HTML-Dokument, dessen Inhalt bei Bedarf dynamisch nachgeladen wird. Dafür findet ein asynchroner Datenaustausch zwischen Client und Server statt, bei dem benötigte Ressourcen wie Bilder, JavaScript und CSS ausgetauscht werden. Durch dieses Verfahren wird sichergestellt, dass gleiche Elemente oder Ressourcen nicht erneut heruntergeladen werden müssen. Bei Änderungen werden nur Teile des DOMs² ersetzt und neu gerendert.

Die Interaktion mit dem DOM oder auch Virtual DOM kann selbst entwickelt werden. Jedoch ist hierbei zu raten, auf bereits bestehende Frameworks wie Angular (Entwickelt unter der Leitung vom Angular Team bei Google), React (Entwickelt unter der Leitung von Facebook) oder Vue (Evan You und Core Team) zurückzugreifen.

Der große Vorteil von SPAs ist die Geschwindigkeit der Anwendung, da hier nur einzelne Teile ausgetauscht werden müssen. SPAs bieten außerdem den Vorteil, dass die Entwicklung von Front- und Backend entkoppelt wird. Das heißt, dass die Programmierenden des Front- und Backends weitestgehend unabhängig voneinander arbeiten können.

Die SEO Optimierung gestaltet sich schwieriger, da es sich um eine dynamische Anwendung handelt. Zur Nutzung von SPA muss im Browser JavaScript verfügbar und aktiviert sein.

Zusammenfassung Vor- und Nachteile

	SPA	MPA
Vorteile	<ul style="list-style-type: none"> • Sehr schnell, dank dynamischem Nachladen • Entkoppelung zwischen Front- und Backend • Effizientes cachen von Daten 	<ul style="list-style-type: none"> • MPA Architektur ist ausgereift • MPAs sind entwicklerfreundlich, da ein kleiner Technologiestack benötigt wird • Ältere Browser werden unterstützt • SEO ist einfacher zu implementieren
Nachteile	<ul style="list-style-type: none"> • JavaScript muss im Browser verfügbar sein • Alte Browser werden nur teilweise unterstützt • Herausfordernde SEO Implementierung 	<ul style="list-style-type: none"> • Anwendung sind weniger performant als MPAs • Front- und Backend haben eine starke Kopplung

²Das Document Object Model repräsentiert die Webseite als Baumstruktur

Abbildung 3.20: Vor- und Nachteile SPA/MPA

Für die Entwicklung der Anwendung entscheide ich mich für die Verwendung einer SPA. Dies geschieht unter den Gesichtspunkten der Entkopplung zwischen Front- und Backend, der Performance der Anwendung und der Zukunftssicherheit, die meiner Meinung nach für SPA besteht. Die Nachteile vom SPA betreffen meine Anwendung nur wenig. So ist auf den Rechnern im Labor ein moderner Webbrowser installiert und in diesem JavaScript aktiviert. Auch handelt es sich um eine interne Anwendung, bei der die SEO Optimierung keine Rolle spielt. [Mel20]

3.7.2 Mockups

Für das Layout der Oberfläche wird die Designsprache Material Design von Google verwendet, da dieses konkrete Gestaltungsregeln vorgibt und einen Styleguide zur Verfügung stellt. Material Design wurde im Jahr 2014 vorgestellt und in Apps von Google verwendet. Besonders die Optimierung der Benutzerfreundlichkeit steht im Vordergrund. Eine Besonderheit des Material Design ist, dass physikalische Gesetze beachtet werden und die Inhalte für eine Priorisierung auf einer virtuellen z-Ebene verschoben werden. [kul17]

Den Prinzipien des Dark Theme von Material Design wird gefolgt, da die bestehende Anwendung bereits nur im Dark Mode vorhanden ist. Des Weiteren werden Anwendungen derzeit häufig mit Dark Mode als Default Theme veröffentlicht und bestehende Anwendungen ohne Dark Mode erhalten diesen. [Col20]

Das Dark Themes trägt zur Verbesserung der visuellen Ergonomie bei, was zu einer Reduktion der Belastung der Augen führt. Des Weiteren wird bei OLED-Bildschirmen die Batterieleistung geschont. [Goo]

Damit die Icons zum Design der Seite passen und aus einer Charge stammen, werden Icons von Material Design Icons³ verwendet. Hier sind die offizielle Icons sowie Icons von der Community, die dem Material Design folgen, vorhanden.

³<https://materialdesignicons.com/>

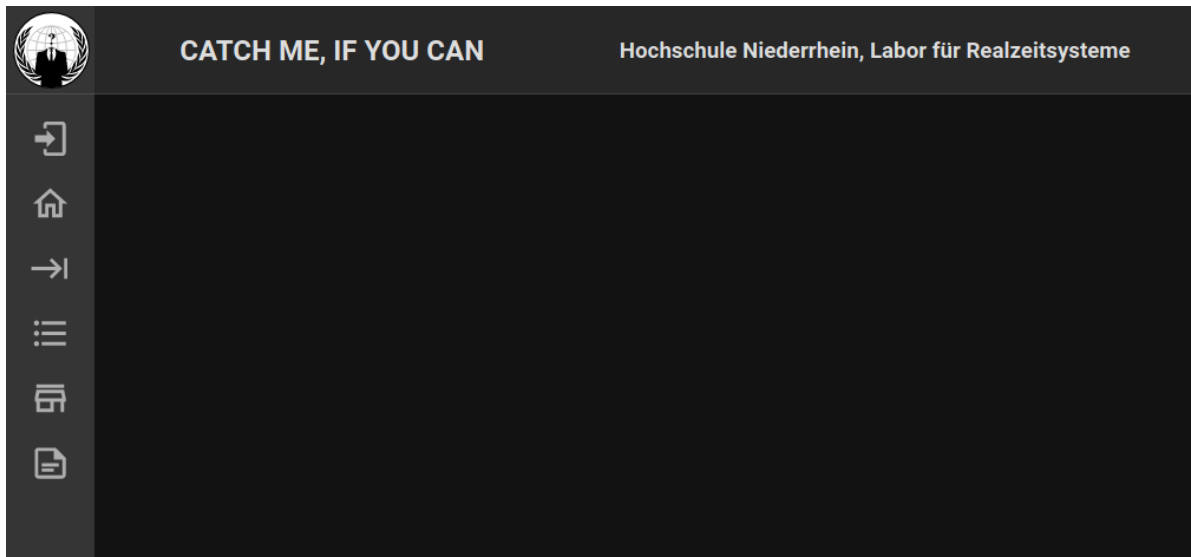


Abbildung 3.21: Grundlayout der Weboberfläche (Mockup)

Das Grundlayout ist wie in Abbildung 3.21 abgebildet in drei Bereiche, Header, Navigation und Content, eingeteilt.

Der Bereich des Headers ist im oberen Teil erkennbar. Dort ist ein Logo, derzeitig noch das Logo aus der alten Anwendung, eine Überschrift sowie ein Untertitel platziert. Über die Überschrift und den Untertitel können die verschiedenen Seiten (Admin-, Spieler-, Flagshop- und Challengeseite) unterscheidbar gemacht werden.

Die Navigation ist auf der linken Seite erkennbar und als Sidebar mit Icons realisiert. Diese beinhaltet Verweise zu den Unterseiten. Sollte ein Eintrag der Navigation aktiv sein, wird dieser mithilfe der im Material Design vorgesehenen Farbe hervorgehoben.

Der Rest der Seite ist der Content Bereich. Dieser wird dynamisch mit dem anzuzeigenden Inhalt gefüllt.

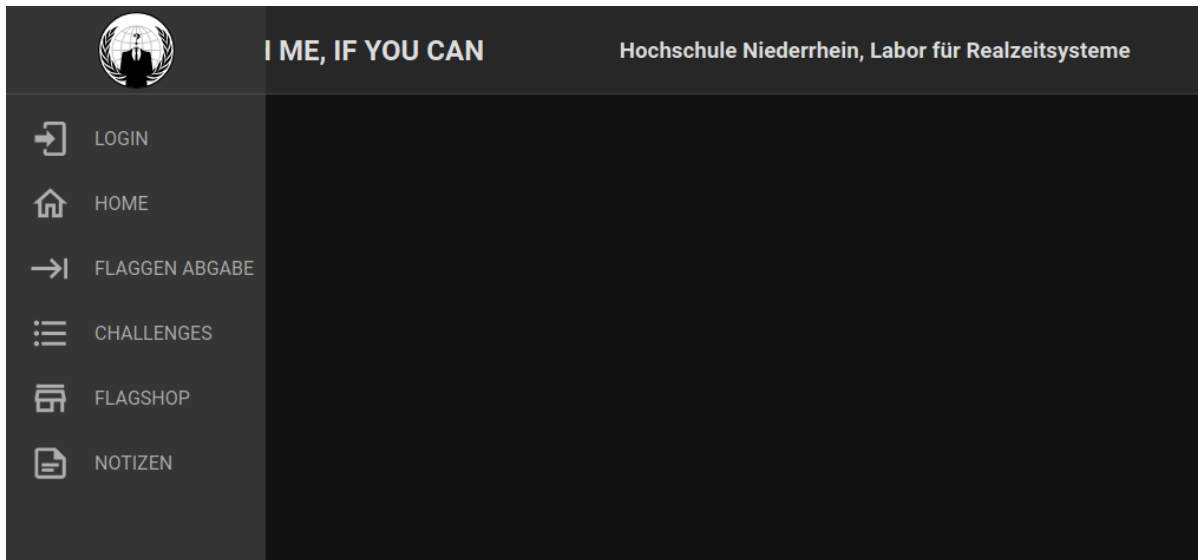


Abbildung 3.22: Ausgeklapptes Menu beim hovern(Mockup)

Damit die Navigation verständlich wird, gibt es wie in Abbildung 3.22 zu erkennen neben den Icons auch beschreibenden Text. Dieser Text wird angezeigt, wenn der Nutzer mit der Maus über die Sidebar hovers. Bei dem Hovern wird die Sidebar über den Content ausgefahren und überdeckt diesen.

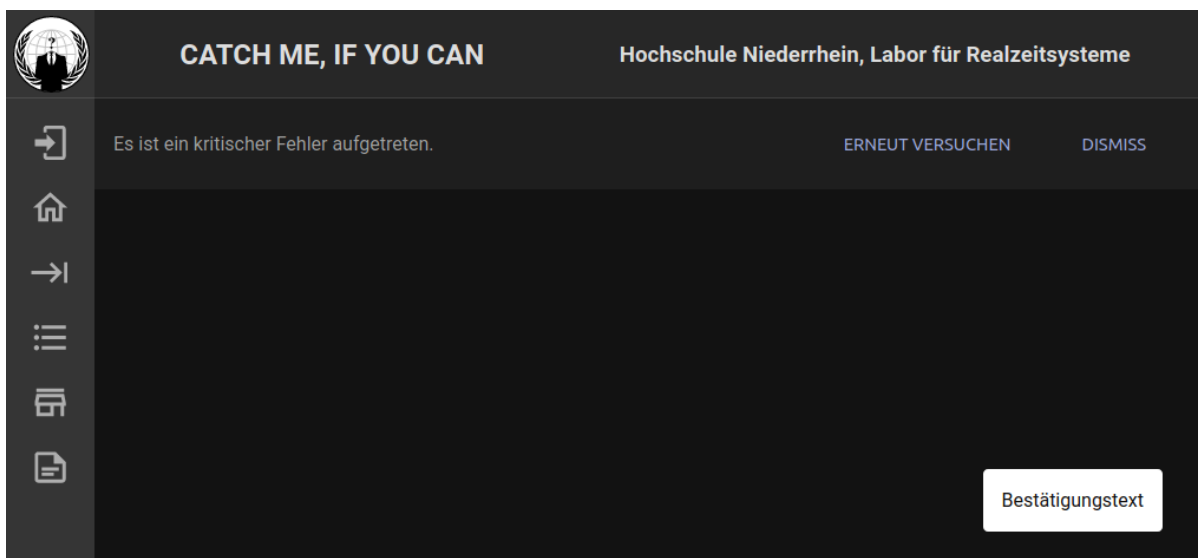


Abbildung 3.23: Fehlernachrichten (Mockup)

Sollte der Nutzer über Ereignisse informiert werden, stehen zwei Möglichkeiten zur Verfügung.

Wenn das Ereignis wichtig ist, wird ein Banner verwendet. Dieser Banner besteht aus drei Elementen, einem Element für die Nachricht und zwei Buttons. Der linke der beiden ermöglicht es dem Nutzer eine Aktion direkt auszuführen. Dies kann unter anderem eine Weiterleitung zu einer bestimmten Seite sein, über die der Nutzer weitere Informationen erhält. Über den anderen Button kann der Banner ausgeblendet werden. Es wird maximal ein Banner zeitgleich angezeigt.

Die andere Möglichkeit den Nutzer zu informieren, ist die sogenannte Snackbar. Diese wird verwendet, wenn die Benutzererfahrung nicht unterbrochen werden soll und keine Benutzereingabe benötigt wird. Die Snackbar wird am unteren rechten Rand platziert und verschwindet im Gegensatz zum Banner nach einer definierten Zeit automatisch. Wenn möglich wird auch hier maximal eine Snackbar gleichzeitig verwendet.

Interaktives Scoreboard										
Team	Uptime	Bubble	Web-Up	XSS-Safe	FTP-Safe	Telnet-Safe	SQLInject-Safe	phpMyAdmin	Challenges	Flagshop
192.168.87.11	-20 (100%)	-2 (6%)	0 (100%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.12	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.13	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.14	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.15	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.16	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.17	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.18	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-
192.168.87.19	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-2 (0%)	-	-

Strafen			
Team	Zeitpunkt	Strafpunkte	Begründung
192.168.87.11	18:52	10	Flaggen während der Disovertime abgegeben
192.168.87.11	18:52	10	Flaggen während der Disovertime abgegeben

Abbildung 3.24: Ansicht des Spielstandes (Mockup)

In Abbildung 3.24 ist ein Teil der Ansicht des Interaktiven Scoreboards inklusive der Strafen abgebildet. Die Ansicht ist in das Grundlayout der Anwendung (Abbildung 3.21) eingebettet. Die Tabelle wird durch eine hellere Farbe dargestellt, da eine Verschiebung auf der z-Achse im Dark Theme nicht funktioniert. Damit die Zeilen in der Tabelle besser erkennbar sind, ist jede zweite Zeile hervorgehoben.

Dienste, die beim letzten Scan den gewünschten Zustand hatten, werden mit einem kontrastarmen grün dargestellt. Im Gegensatz zu der vorhandenen Anwendung wird auf eine rote Darstellung der Dienste, bei unerwünschtem Zustand, verzichtet. Einzig die Gesamtpunkte werden im negativen Bereich rot dargestellt.

3.8 GameClient

Der GameClient bleibt durch diese Bachelorarbeit unberührt. Es ist jedoch eine Änderung an ihm vorzunehmen, damit er mit dem *Game Information System* kompatibel ist. Am Spiel können nur noch Gruppen teilnehmen, die ihre Teilnahme gegenüber dem GIS bekunden. Bei dieser Anmeldung erwartet das GIS einen Token, der bei der Generierung der Flags verwendet wird.

In der derzeitig implementierten Startgame Routine findet durch den GameClient keine Bekundung der Teilnahme statt, somit wird auch kein Token übermittelt.

Auch muss die Hashfunktion zur Generierung an die im GIS verwendete Funktion angepasst werden, damit die generierten Flags vergleichbar bleiben. In der derzeitigen Implementierung wird der Hash-Algorithmus *sha512* angewendet, kann jedoch einfach auf *md5* revidiert werden.

4 Technologien

4.1 Backend

Bei der Entwicklung des Webservers wird auf ein Backend-Webframework zurückgegriffen. Das erleichtert die Entwicklung und Wartung der Webanwendung, indem Werkzeuge und Bibliotheken zur Verfügung gestellt werden, die allgemeine Aufgaben übernehmen. Zu diesen allgemeinen Aufgaben gehört das Verarbeiten von HTTP Anfragen, das Erstellen von HTTP Antworten und das Weiterleiten von Anfragen an die entsprechende Funktion. Bei der Implementierung der Logik müssen alle diese allgemeinen Aufgaben nicht mehr beachtet werden.

Um die Weiterentwicklung durch Studierende des Bachelor Informatik der Hochschule Niederrhein zu gewährleisten, werden nur Webframeworks, die eine Programmierung in C, C++, Python oder JavaScript vorsehen, in Betracht gezogen, da eben diese an der Hochschule Niederrhein gelehrt werden. Derzeitig sind neben Frameworks wie Spring (Java), Ruby on Rails (Ruby) und Laravel (PHP), die nicht in den Vergleich aufgenommen werden, Django (Python), Flask(Python) und Express(Node.js/JavaScript) verbreitet. [cM20b]

In der Lehrveranstaltung *Web-Engineering* wird die Entwicklung mehrere Backend-Server unter Zuhilfenahme von Python durchgeführt. Deshalb werden im folgenden nur Django und Flask betrachtet.

Anschließend wird ein Framework gewählt, mit dem der Backend-Server realisiert werden soll.

4.1.1 Django

Django folgt der sogenannten *Batteries Included* Philosophie.

Bei dieser werden vielseitige Standardbibliotheken mit ausgeliefert, sodass ein Nutzer keine oder nur wenige separate Pakete herunterladen muss. [Kuc]

Django liefert unter anderem Module für Caching, Logging, Versenden von E-Mails, RSS-Feeds, Pagination, Security und der automatischen Generierung von Administrationsseiten. [Dja] Durch den *Batteries Included* Ansatzes funktionieren die Komponenten reibungslos untereinander und sind mit dem Kern kompatibel. Des Weiteren sind die Dokumentationen der verschiedenen Module zentral an einem Ort verfügbar.

Django wurde von einem Team entwickelt, das ursprünglich Zeitungs-Websites erstellt und verwaltet hat. Dieses Team hat die gemeinsame Codebasis abstrahiert und in ein Framework überführt. Daher ist Django besonders gut, aber nicht nur, für Nachrichtenseiten und Content Management Systeme (CMS) geeignet. [cM19]

4.1.2 Flask

Im Gegensatz zu Django ist Flask ein Mikroframework und verfolgt die *Batteries Included* Philosophie nicht. Bei einem Mikroframework ist der Kern einfach, aber erweiterbar gestaltet und es gibt wenige bis keine Abhängigkeiten zu externen Bibliotheken. Dieser Ansatz überträgt der programmierenden Person mehr Verantwortung aber auch mehr Freiheiten. So trifft Flask beispielsweise nicht die Entscheidung, welche Datenbank genutzt werden soll. [Pal10b]

Wie bei Django (Unterabschnitt 4.1.1) werden zwei Module bei der Installation von Flask mit geladen. Zum einen wird auf das Modul *Werkzeug* zurückgegriffen, um eine ordnungsgemäße WSGI-Anwendung zu ermöglichen. Zum anderen wird Jinja2 mitgeliefert, da die meisten Anwendungen eine Template-Engine benötigen. Flask will eine solide Grundlage für alle Anwendungen sein, bei der die entwickelnde Person viele Freiheiten genießt. [Pal10a]

4.1.3 Wahl des Frameworks

Das Mikroframework Flask wird zur Implementierung des Webservers genutzt. Die Anwendung wird in Python geschrieben und kann daher durch Studierende weiterentwickelt werden, ohne dass diese sich in eine neue Programmiersprache einarbeiten müssen. Des Weiteren werden viele Module von Django nicht benötigt. Sie stellen einen Overhead dar. Auch handelt es sich bei der zu entwickelnden Software um eine vergleichbar kleine Anwendung. Es würden nur wenige Vorteile von Django genutzt. Flask kann mit Hilfe von Community Modulen bei Bedarf erweitert werden.

4.2 Datenhaltung

Es gibt eine Vielzahl von verschiedenen relationalen Datenbankmanagementsystemen, die alle einen ähnlichen Funktionsumfang mitbringen.

Im Folgenden werden nur die kostenlos nutzbaren und am weitesten verbreiteten Datenbanken dargestellt. Zu dieser Liste zählen MySQL (Oracle), PostgreSQL (PostgreSQL Global Development Group), MariaDB (MariaDB Foundation) und SQLite (Dwayne Richard Hipp). [DB-]

Im Anschluss an die Darstellung wird die Wahl der Datenbank für die Anwendung begründet.

4.2.1 MySQL und MariaDB

MySQL ist das beliebteste Open-Source SQL Datenbankmanagementsystem, das im Jahr 1995 veröffentlicht worden ist. Dieses ist als Client/Server Architektur implementiert, kann aber auch in eingebetteten Systemen verwendet werden. [Ora20a] MySQL ist in C / C++ geschrieben und kompatibel mit vielen Programmiersprachen, darunter auch Python. Des Weiteren ist es auf diversen Plattformen einsetzbar und für große Datenmengen optimiert. [Ora20b]

MariaDB ist eine Abspaltung von MySQL. Sie resultierte aus der bevorstehenden Übernahme von MySQL durch Sun Microsystems unter der Führung von Oracle. [ION20]

4.2.2 PostgreSQL

PostgreSQL ist frei verfügbar und ohne Lizenzierung nutzbar. Es wurde als universitäres Projekt an der University of California at Berkeley Computer Science Department gestartet. Es sind neben den SQL92 und SQL99 Standard auch einige eigene Erweiterungen implementiert. [BB]

Nach Angaben der Entwickler ist „PostgreSQL [...] heute die fortschrittlichste Open-Source-Datenbank, die es gibt.“ ([The20])

4.2.3 SQLite

Im Gegensatz zu den bereits vorgestellten Datenbanken handelt es sich bei SQLite um eine serverlose Datenbank, die nicht aufgesetzt oder verwaltet werden muss. SQLite speichert die Daten in einer gewöhnlichen Datei, welche kopiert und verteilt werden kann. [SQL]

4.2.4 Wahl der Datenbanksoftware

Die PostgreSQL Datenbank wird den Alternativen vorgezogen, da es für den Anwendungsfall keine nennenswerten Unterschiede zwischen den Datenbanken gibt. Die erhöhte Komplexität von PostgreSQL im Vergleich zu SQLite kann durch die Nutzung eines Dockerimages reduziert werden. Des Weiteren haben sich die Studierenden mit der PostgreSQL Datenbank in der Veranstaltung *Datenbanksysteme* beschäftigt und im EZS-Labor besitzen bereits Mitarbeiter Kenntnisse von PostgreSQL.

4.3 Frontend

Für die Realisierung des Frontends sollte aus den in Kapitel 3 genannten Gründen auf ein bestehendes Framework zurückgegriffen werden. In der Betrachtung werden die drei beliebtesten JavaScript Frameworks, laut einer Stackoverflow (Frage- und Antwortseite für Programmierende) Umfrage, diskutiert. Die Umfrage, bei der circa 65.000 Menschen teilgenommen haben, wurde im Februar 2020 durchgeführt. [Sta20]

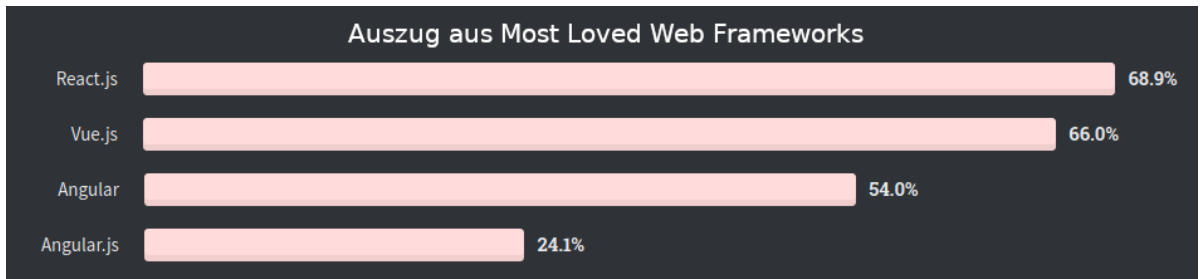


Abbildung 4.1: Weiterverwendung des benutzten Webframeworks (Screenshot) [Sta20]

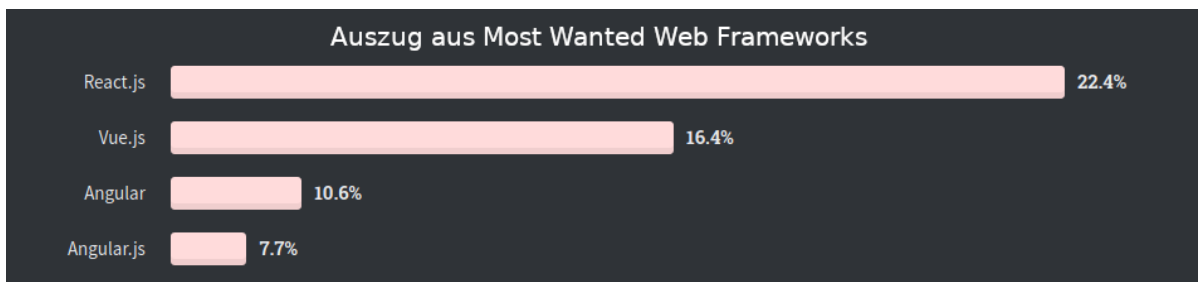


Abbildung 4.2: Interesse an einem neuen Webframework (Screenshot) [Sta20]

In der Abbildung 4.1 ist zu sehen, wie viele Prozent der Entwickelnden, welche bereits mit der Technologie arbeiten, ein Interesse bekundet haben diese für weitere Projekte zu nutzen. React.js führt diese Liste mit 69 % an. Darauf folgt Vue.js dicht mit 66 %. Bei Angular sieht dieses etwas anders aus, hier bekunden nur 54 % ein Interesse. Im Gegensatz dazu wollen ~25 % der Befragten den Vorgänger Angular.js weiter nutzen.

Die Abbildung 4.2 zeigt in Prozent, wie viele der Entwickelnden ein Interesse an der Technologie haben, bisher aber noch nicht mit dieser gearbeitet haben. Auch hier ist React.js mit ~22 % führend. Etwas abgeschlagen mit ~16 % folgt Vue.js. Dahinter reihen sich Angular mit ~11 % und Angular.js mit 8 % ein.

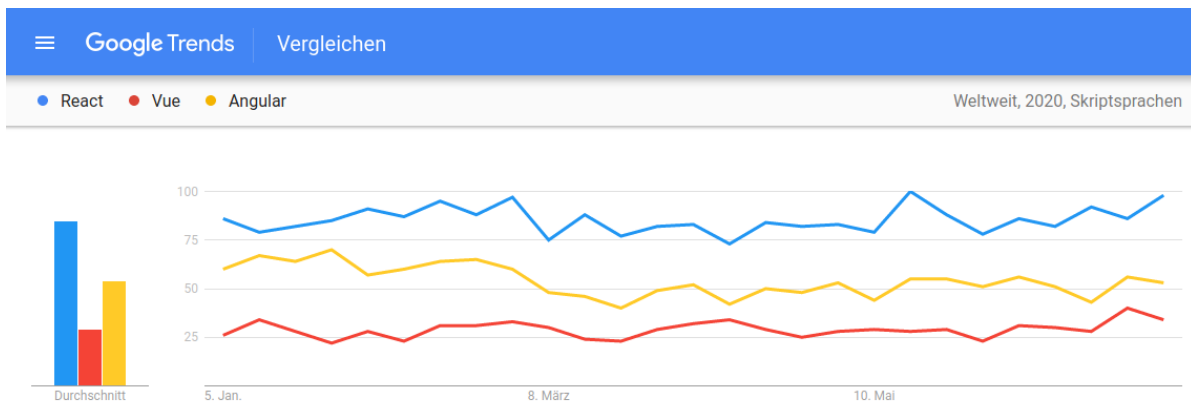


Abbildung 4.3: Google Trends (Screenshot) [Goo20b]

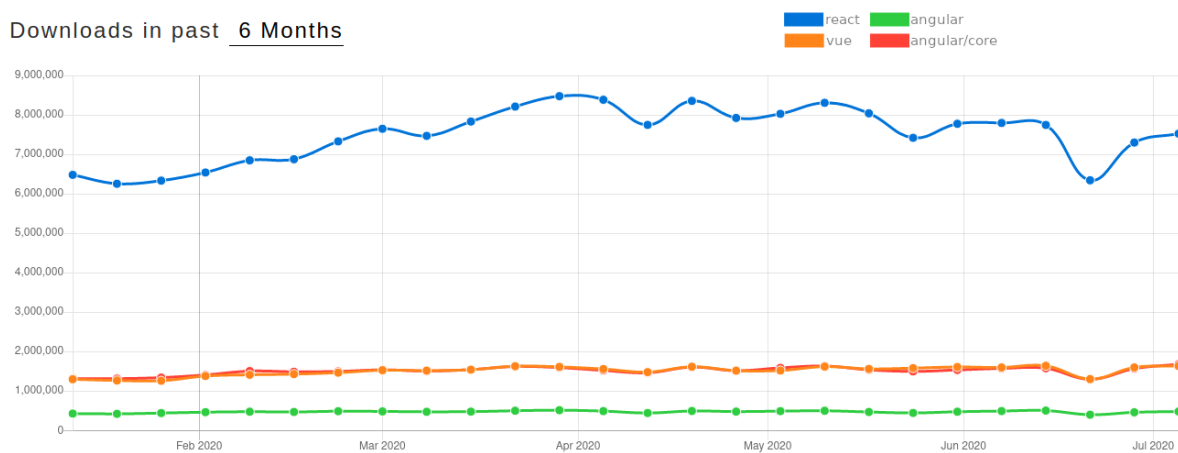


Abbildung 4.4: NPM Trends (Screenshot) [Pot20]

Die Google Trends in Abbildung 4.3 zeigen das normalisierte Interesse an einem Begriff vom Januar 2020 bis Anfang Juli 2020. Das Interesse wird von Google stichpunktartig anhand von Google Suchanfragen bestimmt. [Goo20c]

In der Abbildung 4.4 werden die wöchentlichen Downloads pro Framework grafisch dargestellt. In dieser ist erkennbar, dass Vue.js und Angular ungefähr gleich oft heruntergeladen werden. Generell ist eine Stagnation der Frameworks erkennbar, einzig bei React.js schwanken die Downloadzahlen zwischen 6,5 und 8,5 Millionen. Derzeitig scheinen sich die Downloads bei ungefähr 7 Millionen pro Woche eingependelt zu haben.

Durch die Abbildung 4.1, Abbildung 4.3 und Abbildung 4.4 lässt sich schlussfolgern, dass React.js derzeitig das beliebteste und auch verbreitetste Framework ist. Das unbeliebteste Framework der Auswahl scheint Angular.js zu sein. Anhand der Grafiken fällt eine klare Positionierung von Vue.js und Angular zwischen React und Angular.js schwer.

Im Folgenden sollen die Frameworks genauer betrachtet werden, um eine Nutzung unter anderem anhand des Funktionsumfangs, der Mächtigkeit sowie der Komplexität zu beurteilen.

4.3.1 Angular

AngularJS wurde von einem Google Mitarbeiter (Misko Hevery) als Seitenprojekt gestartet. Das Nebenprojekt wollte er nutzen, um interne Webanwendungen einfacher zu entwickeln. Nachdem einige interne Anwendungen mit diesem Projekt erstellt worden sind, wurde AngularJS im Jahr 2010 als Open-Source-Projekt veröffentlicht. Es fand sowohl in Unternehmensprojekten als auch in Projekten der Open-Source Community Anwendung.

Einige Jahr nach der Veröffentlichung, begann sich die Landschaft der Webentwicklung durch Weiterentwicklungen und neue Standards in JavaScript zu verändern. Neben dieser Veränderung ist das Team an die Grenzen gestoßen, welches die Verbesserung des Frameworks anging. Dieses führte dazu, dass AngularJS über die Zeit an Modernität verlor.

AngularJS war beim Entwurf nie für Mobile oder Unternehmensanwendungen gedacht. So entschied sich das Team bei Google mit der Entwicklung der Version 2 einen Neuanfang zu wagen und Angular 2 für solche Anwendungsfelder zu entwerfen.

Um Verwirrungen zu vermeiden, wurde das bis dahin bekannte Angular in AngularJS umbenannt und die neue Version Angular 2 genannt. Des Weiteren folgt die Versionierung von Angular seit Version 2 dem Semantic Versioning Prinzip bei dem die Versionsnummer in „MAJOR.MINOR.PATCH“ ([Pre]) untergliedert wird.

In der Anfangsphase von Angular 2 war es umständlich ein neues Projekt anzulegen, die Build-Größen waren vergleichsweise groß. So erarbeitete sich Angular den Ruf sperrig zu sein. Neben diesem wurde in Version 2 die Sprache von JavaScript zu TypeScript(Obermenge von JavaScript) umgestellt, welches andere Syntaxen und neue Konzepte zur Folge hatte. [Gav18]

Am 24.06.2020 erschien Angular2 in der Version 10.0.0 [Goo20a] und zählt wie bereits vorher dargestellt zu den beliebtesten Frontend-Frameworks.

Im Folgenden wird nur das aktuell beworbene Angular2 dargestellt und Angular genannt.

Bei der Entwicklung von Angular wurde auf Konsistenz, Produktivität, Wartbarkeit, Modularität und frühzeitige Fehlererkennung gesetzt.

Angular 2 basiert auf Komponenten und Diensten, welche alle identische Strukturen besitzen. Auch gibt Angular vor, wie wiederverwendbarer Code angelegt wird, sodass hierfür keine Code Styles notwendig sind. Des Weiteren erhält die Angular Dokumentation einen Style-Guide. So müssen die Unternehmen keinen eigenen Style-Guide erstellen, was eine Zeitersparnis darstellt. Durch diesen konsistenten Aufbau wird auch eine bessere Wartbarkeit gewährleistet.

Durch die Konsistenz, die gegebenen Style-Guides und den wiederverwendbaren Code steigt die Produktivität, da die Entwicklenden eingeschränkter sind und nicht überlegen und bewerten müssen, ob das aktuell angewandte Vorgehen richtig ist.

Die Wartbarkeit der geschriebenen Anwendung profitiert von der Konsistenz und den Style Guides, da so jeder der involviert ist, den Code leichter nachvollziehen und verändern kann. Derzeitig ist durch das große Interesse der Community sowie der internen Nutzung bei Google, die Wartbarkeit des Frameworks gesichert.

Bei Angular wird der Code in einzelne Module organisiert. Durch die Nutzung dieses modularen Systems können diverse Teams an ein und derselben Anwendung arbeiten, ohne sich gegenseitig zu behindern.

Die frühzeitige Fehlererkennung wird durch die Nutzung von TypeScript ermöglicht. TypeScript bietet im Gegensatz zu JavaScript Unterstützung für Typen. Die Nutzung der Typen ist in TypeScript nicht vorgeschrieben, aber dringend zur Fehlererkennung empfohlen. Des Weiteren ermöglicht das Angular-CLI eine einfache Methode um Unittests und End-zu-End-Tests durchzuführen, so können Fehler entdeckt und behoben werden. [Wah17]

Diese Vorgaben führen zwar zu einer besseren Wartbarkeit und einer konsistenten Anwendung, schränken aber zeitgleich Entwickler ein. Um eine konsistente Anwendung zu erhalten, ist das Gerüst unflexibel.

Da Angular in Unternehmensanwendungen verwendet werden soll, ist es komplex und benötigt so eine gewisse Einarbeitungszeit. Diese steile Lernkurve muss durch neue Programmierende bewältigt werden. [Ven18]

4.3.2 React

Im Jahr 2010 startete React als Port von XHP (PHP-Erweiterung, welche XSS Angriffe vorbeugen sollte) bei Facebook. Da XHP Probleme mit dynamischen Webanwendungen nicht löste, bat ein Facebook Software-Engineer um Zeit, damit er XHP unter zur Hilfenahme von JavaScript in den Browser bringen könne. [Daw14]

Anfänglich wurde React noch unter „BSD + patents“ lizenziert. Diese Lizenz gewährte eine Nutzungslizenz und eine Patentlizenz, solange von einer Klage gegen Facebook bei möglichen Patentverletzungen abgesehen wird. Am 25. September 2017 wurde die Lizenz nach Kritik zu „MIT“ gewechselt. [Kri17] [Lar17] Die MIT-Lizenz ist eine sehr restriktiv arme Lizenz und gibt die Erlaubnis zur Veränderung, Modifikation und Nutzung ohne Kosten. Des Weiteren beinhaltet diese keine Copyleft. Bei einem Copyleft muss das Ergebnis der Entwicklung, welches die Software mit Copyleft nutzt, unter derselben Lizenz angeboten werden. [Weh20]

React besteht aus Komponenten und nutzt eine Syntaxerweiterung von JavaScript namens JSX um JavaScript und HTML zusammenzuführen. Die JSX-Datien müssen vor der Auslieferung an den Client in JavaScript transformiert werden. Reacts Komponenten sollten möglichst klein sein und nur eine Aufgabe erledigen. Diese führt zu einer besseren Test- und Wartbarkeit sowie einem besseren Verständnis der Anwendung.

Auch nutzt React einen sogenannten Virtual DOM (Document Object Model). Die Nutzung des vDOM ermöglicht es Anwendungen auf dem Server zu rendern. Neben diesem können

Unterschiede zwischen DOM und vDOM erkannt werden. Dadurch muss nicht mehr die gesamte Seite sondern nur die veränderte Komponente neu gerendert werden. Dieses führt zu einer besseren Performance. [Bez15]

Um beispielsweise eine SPA Anwendung in React zu entwickeln muss auf Drittanbieter Anwendungen zurückgegriffen werden oder die entsprechenden Funktionen müssen selber programmiert werden, da diese nicht in React enthalten sind. Dieses stellt entweder Zeitaufwand oder Abhängigkeiten von weiteren Entwicklern dar.

4.3.3 Vue

Vue.js wurde durch einen damaligen Mitarbeiter von Google (Evan You) entworfen und entwickelt, nachdem er viel mit Angular gearbeitet hatte. Er wollte nur einen ganz kleinen Teil aus Angular nutzen. So begann er zunächst nur für sich, veröffentlichte aber im Februar 2014 Version 1.0.0 auf GitHub.

Das Projekt gewann auf GitHub Beliebtheit und die Community beteiligte sich. Die ersten Plugins wurden erschaffen und es bildete sich ein Core Team.

Vue liefert im Gegensatz zu den anderen vorgestellten Frontend-Frameworks nur das Data Binding und die Möglichkeit Komponenten zu programmieren im Kern mit. Zusätzlich benötigte Funktionen können bei Bedarf als Module geladen werden. Dies macht Vue zu einem spezialisierten aber auch universell nutzbaren Framework. Es ist nicht so universell nutzbar wie Angular aber auch nicht so spezialisiert wie React. [Teu18a]

Die Dokumentation von Vue ist leicht verständlich und die Community hilft schnell bei Fragen. Anwendungen in Vue sind in eine hierarchische Struktur von kleinen Komponenten untergliedert. Dies soll ermöglichen, dass die Komponenten und so das gesamte System besser zu verstehen sind. Redundanz ist dort zulässig, wo diese benötigt wird. Komponenten erhalten neben dem reinen HTML auch CSS und JavaScript und sollen atomar sein. Das heißt, dass diese alleine und ohne Bindungen zu einer Komponente in einer höheren liegenden Ebenen (logisch gesehen) nutzbar sind. Durch diesen Ansatz ist die Software übersichtlicher, was zu einer besseren Test- und Wartbarkeit führt.

Damit diese Trennung nicht nur in der Software, sondern auch auf der Dateiebene passiert, nutzt Vue hierfür die sogenannten Single File Components. Diese Dateien enden mit der Dateiendung `.vue` und sind erst nach einer „Kompilierung“ nutzbar. Eine Single File Component trennt HTML, CSS und JavaScript auf, sodass dieses übersichtlich betrachtet werden kann. [Teu18b]

Ein Nachteil von Vue ist, dass es von keiner großen Firma entwickelt/unterstützt wird, welche die Entwicklung vorantreibt und die Verbreitung erhöht. Des Weiteren werden Angular und React intern selber genutzt, sodass das Framework eine langfristige Nutzung hat. Aber seit circa 2016 nutzen immer mehr Unternehmen Vue. Hier sind beispielsweise GitLab (2016, [Sch16]), Laravel und Nintendo zu nennen. [tec18]

4.3.4 Wahl des Frontend-Frameworks

Für das Frontend sollte entweder Vue oder React genutzt werden, da diese einsteigerfreundlicher sind. Angular wird auf Grund der Komplexität und des Umfangs des zuschreibenden Frontends nicht in Betracht gezogen. Sowohl für Vue als auch für React sprechen ausreichend Gründe.

Vue ist schlanker und noch etwas leichter zu erlernen als React, da hier nur Kenntnisse in JavaScript, CSS und HTML benötigt werden. Bei React werden noch zusätzliche Kenntnisse in JSX benötigt.

Für React spricht die Verbreitung und damit größere Community, welche bei Problemen konsultiert werden kann. Auch ist es wahrscheinlicher das Problemstellungen bereits auf Frage-Antwort Plattformen wie StackOverflow behandelt worden sind.

Schlussfolgernd sollte für das Frontend React genutzt werden, da hier eine größere Community bei Fragen zur Verfügung steht.

5 Realisierung

6 Fazit

6.1 Zusammenfassung

6.2 Ausblick

Im Folgenden wird ein Ausblick auf mögliche Veränderungen und Erweiterungen gegeben.

Implementierung Webseite

Die angedachte Single Page Applikation konnte aus Zeitgründen nicht in dieser Bachelorarbeit implementiert werden. Die Webseite kann anhand des hier vorgestellten Entwurfs und der diskutierten Technologie in einer weiteren Bachelorarbeit aufgegriffen werden. Hierbei sollte in jedem Fall ein eigener Vergleich aktueller Technologien sowie eine kritische Auseinandersetzung mit der in dieser Arbeit vorgeschlagenen Idee durchgeführt werden. Es ist aber auch möglich die Idee einer SPA zu verwerfen und eine klassische Multi Page Applikation, welche dann die API nutzt, zu entwickeln.

Implementierung weiter Scan-Operationen

Durch den modularen Aufbau der Scanners ist es leicht möglich neue Scan-Operationen zu implementieren. Dieses kann genutzt werden, um auf dem Client weitere Schwachstellen und / oder Dienste zu implementieren, welche dann durch Big Brother überwacht und durch die Studierenden behoben oder online gehalten werden müssen. Herr Abts hat in seiner Bachelorarbeit¹ Ideen für Schwachstellen im Kapitel Ausblick genannt.

Veränderungen in der Anwendung

In der derzeitigen Implementierung wird zum Parsen einer Anfrage der im verwendeten Modul Flask-RESTful implementierte *reqparse (request parser)* verwendet. Dieser soll mit der Flask RESTful Version 2.0.0 entfernt werden und müsste daher gegen beispielsweise Marshmallow² oder den Flask internen Anfragen-Parser getauscht werden. Es besteht derzeit keine

¹Abt16.

²<https://marshmallow.readthedocs.io/en/stable/>

Dringlichkeit, da Flask-RESTful am 6. Februar 2020 erst in der Version 0.3.8 erschien. Sollte die Anwendung nicht weiterentwickelt werden, ist auch keine Änderung notwendig, da dann die Flask-RESTful Version unverändert bleibt.

Dummy Client

Im Versuch werden bei Bedarf GameClients gestartet, welche nicht durch die Studierenden geschützt werden. Diese Dummy Clients werden als zusätzliches Angriffsziel benötigt und werden derzeit gleichwertig behandelt. Eine mögliche Änderung wäre, dass bei dem Dummy Client ein bool-Wert in der Datenbank bei der Registrierung gesetzt wird. Dieser Wert sorgt dafür, dass der GameClient nicht vom Scanner überwacht wird und in der Weboberfläche gesondert dargestellt wird.

Tokengenerierung für Flags

Es ist zu prüfen, ob der Token nicht auf dem Server generiert werden sollte und dem Client nur mitgeteilt wird. Bei der jetzigen Implementierung teilt der GameClient dem Server den Token mit, mit dem die Flags generiert werden sollen. Wenn die Studierenden es schaffen diesen Token in der Mitteilung an den Server zu verändern, kann dieser auf einen Token gesetzt werden, bei dem die generierten Flags aus alten Versuchen bekannt sind.

Auch kann eine historische Tabelle aller genutzten Tokens in der Datenbank angelegt werden, um sicherzustellen, dass jede Gruppe einen historisch einzigartigen Token hat. Damit ist gewährleistet, dass Flags aus alten Terminen nicht verwendet werden können.

Lokale Webseiten überarbeiten

Die auf dem Client betriebenen Webseiten sollten nach der Implementierung der vom Server ausgelieferten Webseite an das Design angepasst werden. Dieses erzeugt ein einheitliches Bild und verdeutlicht den Zusammenhang zwischen der lokalen Webseite und dem Versuch.

Die Challenge- und Shopseiten und -verweise können entfernt werden, da diese auf der vom Server ausgelieferten Webseite platziert werden sollten. Passiert dieses nicht, müssen sie weiterhin vom GameClient ausgeliefert werden. Damit die bereitgestellte API des Servers verwendet wird, ist dann eine Änderung der Seiten auf dem GameClient notwendig.

Flagshop Flags

Es ist zu überlegen, zu bewerten und zu prüfen, ob eine Abgabe gegnerischer Flagshop Flags sinnvoll ist. Sollte die Abgabe sinnvoll sein, muss die implementierte Limitierung rückgängig gemacht werden.

Anhang

1 Installationsanleitung

Beide Programme sind unter Zuhilfenahme des Versionsverwaltungssystems *git* entwickelt worden und liegen derzeit auf der GitLab Instanz des Gemeinschaftslabors Informatik (GLI) des Fachbereiches Elektrotechnik und Informatik der Hochschule Niederrhein. Sie sind im zugangsbeschränkten Repository *Its2*, erreichbar über <https://gl.kr.hsnr.de/ezslabor/abschlussarbeiten/its2>, abgelegt.

Um die Anwendung nutzen zu können, muss das Repository heruntergeladen werden. Dazu kann dieses als zip- oder tar-Archiv mithilfe der Weboberfläche oder unter Verwendung von *git clone* heruntergeladen werden. Die Methode *git clone* ist zu bevorzugen, da so Änderungen leichter herunter- oder hochgeladen werden können.

```
$ git clone https://gl.kr.hsnr.de/ezslabor/abschlussarbeiten/its2.git
```

Listing 6.1: git clone (bash)

Zur einfachen Nutzung der Anwendung ist im Repository neben einer *docker-compose.yaml* Datei auch ein *Makefile* angelegt. Die *docker-compose.yaml* Datei sorgt sich um das Zusammenspiel sowie die Konfiguration der einzelnen Container. Falls die Dockerimages für Big Brother oder GIS nicht vorhanden sein sollten, werden diese automatisch erzeugt. Dieses funktioniert nur, wenn die Ordner- und Dateistruktur nicht verändert wird.

In der *docker-compose.yaml* Datei ist darauf zu achten, dass Docker Socket in die Anwendung übergeben wird, da ansonsten die Steuerung des Scanners fehlschlägt.

Im *Makefile* sind drei Befehle (*init*, *start*, *stop*) hinterlegt, welche zur einfachen Nutzung von *docker-compose* beitragen sollen.

Der Befehl *init* führt eine Initialisierung der Anwendung aus. Dazu wird der bash Befehl (6.2) im REST-Interface Container ausgeführt wird. Dieser sorgt dafür, dass die Datenbank durch die hinterlegten Migrationen auf den benötigten Zustand gebracht wird. Danach wird ein Nutzer mit dem Namen *admin*, der Rolle *admin* und dem Passwort *admin* angelegt. Über diesen Benutzer können weitere Accounts angelegt werden. Der Account kann nach der Erstellung eines weiteren Administrator-Accounts gelöscht werden.

```
$ pipenv run flask db downgrade base &&  
  pipenv run flask db upgrade &&  
  pipenv run flask user create admin --role admin \  
    --password admin
```

Listing 6.2: Initialisierung REST-Interface (bash)

Danach wird der Scanner gestartet und die Initialisierung der Service-Datenbank wird ausgeführt. Nachdem alle Services eingetragen worden sind, beendet sich der Container und der letzte *docker-compose* Befehl (6.3) wird ausgeführt. Dieser sorgt dafür, dass alle Container und Netzwerke, welche durch *docker-compose* angelegt worden sind, entfernt werden.

```
$ docker-compose down
```

Listing 6.3: Aufräumen mit docker-compose down (bash)

Nach der Initialisierung ist die Anwendung einsatzbereit und kann über *make start* und *make stop* gestartet und beendet werden.

Bei *start* werden alle Container angelegt und im Hintergrund gestartet. Danach wird der Scanner Container beendet. Dies ist notwendig, damit das GIS, diesen starten, pausieren und stoppen kann.

Bei *stop* wird nur der Befehl *docker-compose down* ausgeführt, welcher die oben beschriebene Wirkung hat.

Sollten die Anwendungen einzeln verwendet oder installiert werden, muss die Dokumentation der jeweiligen Anwendung konsultiert werden.

2 Bedienungsanleitung

Das Game Information System ist ein RESTful Interface und kann daher mit einem REST-Client angesprochen werden. Dazu kann die entworfene SPA Anwendung implementiert werden. Es können aber auch Programme wie cURL („Werkzeug zur Übertragung von Daten von oder zu einem Server“ ([cURL])) oder Insomnia¹ verwendet werden. Insomnia wurde während der Entwicklung genutzt.

Über einen REST-Client können dann, alle implementierten Routen (??) angesprochen werden. Für die Authentifizierung muss ein Access-Token über die Login-Schnittstelle abgeholt werden und in den nächsten Anfragen mitgesendet werden.

In der Dokumentation des GIS wird auch auf die implementierten Routen eingegangen. Dort kann nachgeschaut werden, ob eine Authentifizierung notwendig ist, welche Daten mitgesendet werden müssen und wie die Antwort aufgebaut ist.

¹<https://insomnia.rest/>

Abbildungsverzeichnis

2.1	Übersicht über die Laborausstattung (Netzwerktopologie)	6
3.1	Übersicht über die Anwendung (Komponentendiagramm)	19
3.2	Klassen der Big Brother Komponente (Klassendiagramm)	23
3.3	Ansicht des Scanners (Zustandsdiagramm)	24
3.4	Erstellung eines Scanners (Zustandsdiagramm)	25
3.5	Starten eines Scanners (Zustandsdiagramm)	27
3.6	Datenfluss in der Scanner Komponente (Datenflussdiagramm)	29
3.7	REST Interface im Überblick (Komponentendiagramm)	31
3.8	Datenfluss während eines Logins (Datenflussdiagramm)	32
3.9	Datenfluss während eines Logins (Datenflussdiagramm)	33
3.10	Datenfluss der Authentifizierung und Autorisierung (Datenflussdiagramm) . .	33
3.11	Datenfluss während der Tokenvalidierung (Datenflussdiagramm)	34
3.12	Datenfluss der Authentifizierung und Autorisierung (Datenflussdiagramm) . .	35
3.13	Ansicht der Basis-Tabellen (ER-Diagramm)	39
3.14	Ansicht der Gruppen-Tabellen (ER-Diagramm)	40
3.15	Ansicht der Flags-Tabellen (ER-Diagramm)	42
3.16	Ansicht der Service-Tabellen (ER-Diagramm)	43
3.17	Ansicht der Flagshop-Tabellen (ER-Diagramm)	44
3.18	Ansicht der Service-Tabellen (ER-Diagramm)	46
3.19	Ansicht der weiteren Tabellen (ER-Diagramm)	47
3.20	Vor- und Nachteile SPA/MPA	49
3.21	Grundlayout der Weboberfläche (Mockup)	51
3.22	Ausgeklapptes Menu beim hovern(Mockup)	52
3.23	Fehlernachrichten (Mockup)	52
3.24	Ansicht des Spielstandes (Mockup)	53
4.1	Weiterverwendung des benutzten Webframeworks (Screenshot) [Sta20] . . .	58
4.2	Interesse an einem neuen Webframework (Screenshot) [Sta20]	58
4.3	Google Trends (Screenshot) [Goo20b]	59
4.4	NPM Trends (Screenshot) [Pot20]	59

Tabellenverzeichnis

3.1	Übersicht über die verwendeten HTTP Methoden	32
-----	--	----

Listings

6.1	git clone (bash)	69
6.2	Initialisierung REST-Interface (bash)	70
6.3	Aufräumen mit docker-compose down (bash)	70

Literatur

- [Abt16] Benjamin Abts. „Überarbeitung und Erweiterung eines Client- / Server-Systems zur Durchführung von IT-Sicherheitsschulungen (Capture the Flag)“. Bachelor Arbeit. Hochschule Niederrhein, Juni 2016. 85 S.
- [Bac04] Daniel Bachfeld. *Giftspritze*. 6. Jan. 2004. URL: <https://www.heise.de/security/artikel/Giftspritze-270382.html> (besucht am 06.07.2020).
- [BB] Cornelia Boenigk und Ralf Burger. *Was Ist PostgreSQL? | PostgreSQL*. URL: <http://postgresql.de/was-ist-postgresql> (besucht am 10.07.2020).
- [Bei14] Hans Dieter Beims. *Web-Applikationen / REST*. Revision 2. 10. Dez. 2014.
- [Bez15] Roberto Bez. *JavaScript: Einführung in React*. 12. Juni 2015. URL: <https://www.heise.de/developer/artikel/JavaScript-Einfuehrung-in-React-2689175.html> (besucht am 15.07.2020).
- [BH20] Valerie Barsig und Jana Haase. *Cyber-Attacke auf das Potsdamer Rathaus*. 22. Jan. 2020. URL: <https://www.pnn.de/potsdam/hacker-nutzten-sicherheitsluecke-cyber-attacke-auf-das-potsdamer-rathaus/25462398.html> (besucht am 16.05.2020).
- [BN19] Achim Berg und Michael Niemeier. „Wirtschaftsschutz in der digitalen Welt“. In: (11. Juni 2019), S. 13.
- [Boe19] Eric Boersma. *Containerization: A Definition and Best Practices Guide - Plutora.Com*. 8. Juli 2019. URL: <https://www.plutora.com/blog/containerization-best-practices> (besucht am 18.07.2020).
- [cM19] MDN contributors und Mozilla. *Django Introduction*. 30. Nov. 2019. URL: <https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/Introduction> (besucht am 09.07.2020).
- [cM20a] MDN contributors und Mozilla. *HTTP Headers*. 27. Apr. 2020. URL: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers> (besucht am 08.07.2020).
- [cM20b] MDN contributors und Mozilla. *Server-Side Web Frameworks*. 3. Juni 2020. URL: https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Web_frameworks (besucht am 08.07.2020).

- [Col20] Clifford Colby. *Windows 10 Dark Mode Is Here. Turn It on Now*. 15. Feb. 2020. URL: <https://www.cnet.com/how-to/windows-10-dark-mode-is-here-turn-it-on-now/> (besucht am 19.07.2020).
- [cUR] cURL. *Curl - How To Use*. URL: <https://curl.haxx.se/docs/manpage.html> (besucht am 15.07.2020).
- [Daw14] Chris Dawson. *JavaScript's History and How It Led To ReactJS*. 25. Juli 2014. URL: <https://thenewstack.io/javascripts-history-and-how-it-led-to-reactjs/> (besucht am 15.07.2020).
- [DB-] DB-Engines. *DB-Engines Ranking*. URL: <https://db-engines.com/en/ranking> (besucht am 09.07.2020).
- [Dja] Django. *Django Documentation | Django Documentation | Django*. URL: <https://docs.djangoproject.com/en/3.0/> (besucht am 09.07.2020).
- [Doc20] Docker Inc. *Overview of Docker Compose*. 15. Juli 2020. URL: <https://docs.docker.com/compose/#features> (besucht am 18.07.2020).
- [FM20] Florian Flade und Georg Mascolo. *Cyberangriff auf Bundestag: Haftbefehl gegen russischen Hacker*. 5. Mai 2020. URL: <https://www.tagesschau.de/investigativ/ndr-wdr/hacker-177.html> (besucht am 16.05.2020).
- [Gav18] Dave Gavan. *The History of Angular*. 25. Mai 2018. URL: <https://medium.com/the-startup-lab-blog/the-history-of-angular-3e36f7e828c7> (besucht am 14.07.2020).
- [Goo] Google. *Dark Theme*. URL: <https://material.io/design/color/dark-theme.html#usage> (besucht am 19.07.2020).
- [Goo20a] Google. *Angular - Angular Versioning and Releases*. Version 10.0.4-local+sha.9cf78d5701. 2020. URL: <https://angular.io/guide/releases> (besucht am 14.07.2020).
- [Goo20b] Google. *Google Trends*. 13. Juli 2020. URL: <https://trends.google.com/trends/explore?cat=733&date=2020-01-01%202020-12-31&q=React,Vue,Angular> (besucht am 13.07.2020).
- [Goo20c] Google. *Häufig Gestellte Fragen Zu Google Trends-Daten - Google Trends-Hilfe*. 2020. URL: https://support.google.com/trends/answer/4365533?hl=de&ref_topic=6248052 (besucht am 13.07.2020).
- [HHH20] Simon Hurtz, Jan Heidtmann und Max Hoppenstedt. *Hacker-Angriff auf Gericht massiver als bislang bekannt*. 28. Jan. 2020. URL: <https://www.sueddeutsche.de/digital/berlin-kammergericht-hacker-angriff-emotet-1.4775305> (besucht am 16.05.2020).
- [Hoc] Hochschule Niederrhein. *Flyer Institut Clavis*. URL: https://www.hs-niederrhein.de/fileadmin/dateien/Institute_und_Kompetenzzentren/Clavis/Flyer_Institut_Clavis__5_.pdf (besucht am 16.05.2020).

- [Hoc19] Hochschule Niederrhein. *Modulhandbuch Vollzeit BA Informatik*. 9. Dez. 2019. URL: https://www.hs-niederrhein.de/fileadmin/dateien/FB03/Studierende/Bachelor-Studiengaenge/PO2013/modul_bi.pdf (besucht am 16.05.2020).
- [Hoc20] Hochschule Niederrhein. *Hackern die rote Karte zeigen - Neuer Studiengang Cyber Security Management*. 7. Feb. 2020. URL: https://www.hs-niederrhein.de/startseite/news/news-detailseite/?tx_news_pi1%5Bnews%5D=18990&cHash=e849d260ecd92cf53fc9c98f6dc9edaa (besucht am 16.05.2020).
- [ION20] IONOS. *MariaDB vs. MySQL*. 10. März 2020. URL: <https://www.ionos.com/digitalguide/hosting/technical-matters/mariadb-vs-mysql/> (besucht am 10.07.2020).
- [it-19] it-daily.net. *IT-Security-Experten Werden Händeringend Gesucht - It-Daily.Net*. 3. März 2019. URL: <https://www.it-daily.net/analysen/20773-it-security-experten-werden-haenderingend-gesucht> (besucht am 16.05.2020).
- [Kri17] Raúl Kripalani. *If You're a Startup, You Should Not Use React (Reflecting on the BSD + Patents License)*. 21. Nov. 2017. URL: <https://medium.com/@raulk/if-youre-a-startup-you-should-not-use-react-reflecting-on-the-bsd-patents-license-b049d4a67dd2> (besucht am 15.07.2020).
- [Kuc] A.M. Kuchling. *PEP 206 – Python Advanced Library*. URL: <https://www.python.org/dev/peps/pep-0206/> (besucht am 09.07.2020).
- [kul17] kulturbanause-Team. *Material Design – Die Designsprache von Google*. 26. Dez. 2017. URL: <https://blog.kulturbanause.de/2016/01/material-design-die-designsprache-von-google/> (besucht am 19.07.2020).
- [Lar17] Quincy Larson. *Facebook Just Changed the License on React. Here's a 2-Minute Explanation Why*. 28. Sep. 2017. URL: <https://www.freecodecamp.org/news/facebook-just-changed-the-license-on-react-heres-a-2-minute-explanation-why-5878478913b2/> (besucht am 15.07.2020).
- [Mel20] Ian Melnik. *Single Page Application (SPA) vs Multi Page Application (MPA): Pros and Cons - Merehead*. 17. Apr. 2020. URL: <https://merehead.com/blog/single-page-application-vs-multi-page-application/> (besucht am 04.06.2020).
- [MOV96] Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone. *Handbook of Applied Cryptography*. 1 edition. Boca Raton: CRC Press, 16. Dez. 1996. 780 S. ISBN: 978-0-8493-8523-0.
- [Ora20a] Oracle Corporation. *MySQL :: MySQL 8.0 Reference Manual :: 1.3.1 What Is MySQL?* 2020. URL: <https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html> (besucht am 10.07.2020).

- [Ora20b] Oracle Corporation. *MySQL :: MySQL 8.0 Reference Manual :: 1.3.2 The Main Features of MySQL*. 2020. URL: <https://dev.mysql.com/doc/refman/8.0/en/features.html> (besucht am 10.07.2020).
- [Ora20c] Oracle Corporation. *Oracle® VM VirtualBox® User Guide*. Version 6.1.10. 5. Juni 2020. URL: <https://www.virtualbox.org/manual/UserManual.html#features-overview> (besucht am 06.07.2020).
- [Pal10a] "Pallets. *Design Decisions in Flask — Flask Documentation (1.1.x)*. 2010. URL: <https://flask.palletsprojects.com/en/1.1.x/design/#design> (besucht am 09.07.2020).
- [Pal10b] Pallets. *Foreword — Flask Documentation (1.1.x)*. 2010. URL: <https://flask.palletsprojects.com/en/1.1.x/foreword/> (besucht am 09.07.2020).
- [Pot20] John Potter. *React vs Vue vs Angular | Npm Trends*. 13. Juli 2020. URL: <https://www.npmtrends.com/react-vs-vue-vs-angular-vs-@angular/core> (besucht am 13.07.2020).
- [Pre] Tom Preston-Werner. *Semantic Versioning 2.0.0*. URL: <https://semver.org/lang/de/> (besucht am 14.07.2020).
- [Qua17] Jürgen Quade. *Praktikum IT-Security*. Revision 2. 25. Sep. 2017.
- [RG07] Christiane Rütten und Tobias Glemser. *Sicherheit von Webanwendungen*. 25. Jan. 2007. URL: <https://www.heise.de/security/artikel/Sicherheit-von-Webanwendungen-270870.html> (besucht am 06.07.2020).
- [Ruh20] Ruhr24. *Hacker-Angriff legt IT-Systeme der Uni Bochum lahm - Klausuren ausgefallen*. 7. Mai 2020. URL: <https://www.ruhr24.de/ruhrgebiet/bochum-rub-uni-hacker-angriff-webmail-moodle-news-universitaet-systeme-it-studierende-13753554.html> (besucht am 16.05.2020).
- [Sch16] Jacob Schatz. *Why We Chose Vue.js*. 20. Okt. 2016. URL: <https://about.gitlab.com/blog/2016/10/20/why-we-chose-vue/> (besucht am 14.07.2020).
- [Sch20] Dennis Schirmacher. *Uni Gießen nähert sich nach Hacker-Attacke wieder dem Normalbetrieb*. 1. Juni 2020. URL: <https://www.heise.de/newsticker/meldung/Uni-Giessen-naehert-sich-nach-Hacker-Attacke-wieder-dem-Normalbetrieb-4628715.html> (besucht am 16.05.2020).
- [Sos10] Alexander Sosna. „Konzeption und Realisierung eines modular aufgebauten Auswertungs- und Überwachungssystems zur Durchführung von IT-Sicherheitsschulungen.“ Bachelor Arbeit. Hochschule Niederrhein, Juni 2010. 98 S.
- [SQL] SQLite. *Features Of SQLite*. URL: <https://www.sqlite.org/features.html> (besucht am 10.07.2020).

- [Sta20] Stack Exchange. *Stack Overflow Developer Survey 2020*. The survey was fielded from February 5 to February 28. Feb. 2020. URL: <https://insights.stackoverflow.com/survey/2020/#technology-most-loved-dreaded-and-wanted-web-frameworks> (besucht am 13.07.2020).
- [Tan20] Aaron Tan. *What Is CTF and How to Get Started!* 7. Mai 2020. URL: <https://dev.to/atan/what-is-ctf-and-how-to-get-started-3f04> (besucht am 06.07.2020).
- [tec18] techuz. *Top 9 Websites Built Using Vue.JS Front-End Framework*. 30. Aug. 2018. URL: <https://www.techuz.com/blog/top-9-websites-built-using-vue-js/> (besucht am 14.07.2020).
- [Teu18a] Marc Teufel. *Vue.Js Tutorial: Einführung in Das JavaScript-Framework*. 23. Juli 2018. URL: <https://entwickler.de/online/javascript/tutorial-vue-js-einfuehrung-579851571.html> (besucht am 14.07.2020).
- [Teu18b] Marc Teufel. *Vue.Js Tutorial: So Entwickelt Man Komponenten Mit Vue.Js*. 25. Juli 2018. URL: <https://entwickler.de/online/javascript/einfuehrung-vuejs-vue-579851816.html> (besucht am 14.07.2020).
- [The20] The PostgreSQL Global Development Group. *PostgreSQL: Documentation: 12: 2. A Brief History of PostgreSQL*. 2020. URL: <https://www.postgresql.org/docs/current/history.html> (besucht am 10.07.2020).
- [Ven18] Ventzke Media. *Angular vs. React 2020 - Ein Vergleich Der Bibliotheken*. 5. Juni 2018. URL: <https://www.ventzke-media.de/blog/angular-vs-react-vergleich.html> (besucht am 14.07.2020).
- [w3s] w3schools. *HTML Hidden Input*. URL: https://www.w3schools.com/tags/att_input_type_hidden.asp (besucht am 06.07.2020).
- [Wah17] Dan Wahlin. *Die 5 wesentlichen Vorteile von Angular und TypeScript - Blog - t2informatik*. Ins deutsche Übersetzt von t2informatik am 19.01.2019. 26. Aug. 2017. URL: <https://t2informatik.de/blog/softwareentwicklung/die-5-wesentlichen-vorteile-von-angular-und-typescript/> (besucht am 14.07.2020).
- [WDR19] WDR. *Cyberattacke: Hackerangriff auf Universität Maastricht legt Wissenschaftsbetrieb lahm*. 27. Dez. 2019. URL: <https://www1.wdr.de/nachrichten/rheinland/hacker-angriff-uni-maastricht-100.html> (besucht am 16.05.2020).
- [Weh20] Cornelia Wehner. *Software unter MIT Lizenz rechtssicher verwenden*. 2. Apr. 2020. URL: <https://www.haerting.de/neuigkeit/software-unter-mit-lizenz-rechtssicher-verwenden> (besucht am 15.07.2020).

- [Wel19] Bianca Wellbrock. *IT-Sicherheit im Krankenhaus: Hack bringt Krankenhäuser zum Stillstand* - PSW GROUP Blog. 10. Sep. 2019. URL: <https://www.psw-group.de/blog/it-sicherheit-im-krankenhaus-hack-bringt-krankenhaeuser-zum-stillstand/7175> (besucht am 16.05.2020).
- [Wol15] Eberhard Wolff. *Microservices: Grundlagen flexibler Softwarearchitekturen*. 1., Auflage. Heidelberg: dpunkt.verlag GmbH, 1. Okt. 2015. 386 S. ISBN: 978-3-86490-313-7.

A