Dokumentation Sicherheitsanalyse

Levyn Schneider, David Meer, Ramon Rollier, Matthias Baumgartner

Ein Bild, das Text, Grafiken, Grafikdesign, Logo enthält.

Automatisch generierte Beschreibung

Abbildung 1: Titelbild (www.freepik.com)

# Inhaltsverzeichnis

[1. Inhaltsverzeichnis 2](#_Toc168997450)

[2. Abgrenzung Arbeitsbereich 2](#_Toc168997451)

[3. Zielbeschreibung 2](#_Toc168997452)

[4. Vorgehensplanung 2](#_Toc168997453)

[5. Analyse 4](#_Toc168997454)

[Impressum 4](#_Toc168997455)

[Disclaimer 4](#_Toc168997456)

[AGB 4](#_Toc168997457)

[Datenschutzrichtlinien 4](#_Toc168997458)

[Cookie-Consent Banner 4](#_Toc168997459)

[Sicherheitsanalyse des Backends 4](#_Toc168997460)

[Sicherheitsanalyse der Datenbank 4](#_Toc168997461)

[Sicherheitsanalyse des Webapplikation 5](#_Toc168997462)

[6. Umsetzung 6](#_Toc168997463)

[Impressum & Disclaimer 6](#_Toc168997464)

[AGB 6](#_Toc168997465)

[Datenschutzrichtlinien 7](#_Toc168997466)

[Cookie-Consent Banner 7](#_Toc168997467)

[Sicherheitsanalyse des Backends 7](#_Toc168997468)

[Sicherheitsanalyse der Datenbank 8](#_Toc168997469)

[Sicherheitsanalyse des Webapplikation 9](#_Toc168997470)

# Abgrenzung Arbeitsbereich

Wir werden in unserer Analyse nur die Webapplikation und direkte Umsysteme wie Datenbank und Backend anschauen. Wir werden nicht tiefere Schichten wie OS, physikalische, Webserver, Protokoll und Client Sicherheit abdecken.

Ein Bild, das Screenshot, Text, Schrift, Diagramm enthält.

Automatisch generierte Beschreibung

Abbildung 2: Grafik Abgrenzung Arbeitsbereiches

# Zielbeschreibung

Das Ziel unseres Projektes ist es, dass die Webapplikation "Hapinz" alle Datenschutzaspekte des DSGVO und DSG beinhaltet und die Analyse und Verbesserung der Sicherheitsaspekte der Applikation.

Durch das Projekt werden wir uns auch fachlich weiterentwickeln. Unser Ziel ist es, diese Kenntnisse dann auch in der Berufswelt einsetzten zu können.

# Vorgehensplanung

* Analyse
  + Impressum
  + Disclaimer
  + AGB
  + Datenschutzrichtlinien
  + Cookie-Consent Banner
  + Sicherheitsanalyse des Backends
  + Sicherheitsanalyse der Datenbank
  + Sicherheitsanalyse der Webapplikation
* Umsetzung
  + Impressum & Disclaimer
  + AGB
  + Datenschutzrichtlinien
  + Cookie-Consent Banner
  + Sicherheitsanalyse des Backends
  + Sicherheitsanalyse der Datenbank
  + Sicherheitsanalyse der Webapplikation

# Analyse

#### Impressum

Es ist kein Impressum vorhanden, dies ist ein Verstoss gegenüber dem DSG und DSGVO.   
  
Mit dem Impressum soll ein Websitebetreiber seine Identität offenlegen, so dass Besucher Informationen darüber erhalten, wer verantwortlich ist und wie diese verantwortliche Person kontaktiert werden kann.

### Disclaimer

Es ist kein Disclaimer vorhanden, dies könnte gegenüber dem Unternehmen Rechtlich zum Nachteil werden.

### AGB

Es sind keine AGB vorhanden, dies könnte gegenüber dem Unternehmen Rechtlich zum Nachteil werden.

### Datenschutzrichtlinien

Es ist sind keine Datenschutzrichtlinien vorhanden, dies ist ein Verstoss gegenüber dem DSG und DSGVO, da der Nutzer nicht erfahren kann, wie seine Daten gehandhabt werden.

### Cookie-Consent Banner

Es ist kein Cookie-Banner vorhanden. Dies ist kein Verstoss, da die Webapplikation aktuell keine Analyse-Cookies o.Ä. verwendet.

### Sicherheitsanalyse des Backends

Alle Endpunkte sind aktuell durch Autorisierung mittels JWT-Token geschützt. Dies genügt auch bereits für die Sicherheit.

### Sicherheitsanalyse der Datenbank

Die Datenbank ist auf der Cloud Plattform von MongoDB, [MongoDB Atlas](https://www.mongodb.com/products/platform/atlas-database) gehostet. Die Verbindung zwischen Backend und Datenbank erfolgt durch eine Speicherung des Verbindungsschlüssels als Umgebungsvariable, welche eine sichere Verbindung und Speicherung erlaubt.

### Sicherheitsanalyse des Webapplikation

Die Webapplikation ist durch Authentifizierung und Autorisierung mittels einem Session JWT-Tokens geschützt. Bedeutet, Nutzer können bestimmte Seiten nicht sehen oder Funktionen ausführen, wenn sie nicht authentifiziert oder autorisiert sind.

# Umsetzung

### Impressum & Disclaimer

Als erstes haben wir mithilfe von ChatGPT 4o ein Impressum & Disclaimer geschrieben. Danach haben wir, um die Richtigkeit zu gewährleisten, andere Impressen und Disclaimern angeschaut von verschiedenen Webseiten. Dazu haben wir noch ein Tool namens [e-recht24.de](https://www.e-recht24.de/) verwendet, um ganz sicher zu sein. Am Schluss ist dann dieses Impressum mitsamt Disclaimer zusammengekommen:

<https://www.hapinz.com/legal-notice>

### AGB

Für die AGB haben wir uns vollkommen auf ChatGPT verlassen. Wir haben ChatGPT angegeben um was für eine Website es sich handelt und noch zusätzliche Angaben gegeben wie z.B., dass wir Zahlungspflichtige Events haben usw. Wir wissen, dass es nicht die beste Rechtssicherheit gewährleistet, allerdings genügt dies für uns. Am Schluss sind dann diese AGB zusammengekommen:

<https://www.hapinz.com/terms>

### Datenschutzrichtlinien

Für die Datenschutzrichtlinien haben wir den gleichen Weg genommen wie bei den AGB, da es uns die Arbeit erleichtert und wir sowieso keine Experten im Thema Rechtssicherheit einer Website sind. Wir wissen ebenfalls wieder, dass es nicht die beste Rechtssicherheit gewährleistet, allerdings genügt dies wieder für uns. Am Schluss sind diese Datenschutzrichtlinien zusammengekommen:

<https://www.hapinz.com/privacy>

### Cookie-Consent Banner

Da wir Google Analytics für die Konversion-Rate und Nutzungsanalyse verwenden, haben wir von einem meiner älteren Webseite das HTML und JavaScript vom Cookie-Consent Banner kopiert und bei uns eingefügt. Wir haben dann noch das Styling und andere Attribute angepasst. Somit hatten wir am Schluss ein DSG und DSGVO Rechtssicherer simplen Cookie-Consent Banner auf der Webseite.

Ein Bild, das Text, Screenshot, Computer, Software enthält.

Automatisch generierte Beschreibung

Abbildung 3: Codestück, Cookie-Consent Banner

### Sicherheitsanalyse des Backends

Wie in der Analyse bereits beschrieben, sind alle Endpunkte bereits gut geschützt. Dies funktioniert mittels diesem Codestück:

Ein Bild, das Text, Screenshot, Software, Betriebssystem enthält.

Automatisch generierte Beschreibung

Abbildung 4: Codestück, JWT Session Decryption

Ein Bild, das Text, Screenshot, Software, Multimedia enthält.

Automatisch generierte Beschreibung

Abbildung 5: Sicherheitsanalyse des Backends innerhalb des Backends

### Sicherheitsanalyse der Datenbank

Zur Sicherheitsanalyse der Datenbank haben wir nichts geändert. Wir haben uns für die Cloud Plattform von MongoDB, [MongoDB Atlas](https://www.mongodb.com/products/platform/atlas-database), entschieden da dies auch am logischsten erscheint, wenn man eine MongoDB Datenbank hat. Die Verbindung (ob Lokal oder via MongoDB Atlas) funktioniert über dieses Codestück. Wir haben uns entschieden Umgebungsvariabeln zu verwenden, um die Sicherheit und Reinheit des Codes/Programmes zu gewährleisten.

Ein Bild, das Text, Screenshot, Software, Computer enthält.

Automatisch generierte Beschreibung

Abbildung 6: Verbindungsaufbau MongoDB Datenbank

### Sicherheitsanalyse des Webapplikation

Wie in der Analyse bereits beschrieben, sind alle Endpunkte und Seiten bereits gut geschützt. Dies funktioniert mittels diesem Codestück:

Ein Bild, das Text, Screenshot, Schrift, Multimedia enthält.

Automatisch generierte Beschreibung

Abbildung 7: Autorisierung in der Webapplikation

# Abbildungsverzeichnis

[Abbildung 1: Titelbild (www.freepik.com) 1](#_Toc169981174)

[Abbildung 2: Grafik Abgrenzung Arbeitsbereiches 3](#_Toc169981175)

[Abbildung 3: Codestück, Cookie-Consent Banner 8](#_Toc169981176)

[Abbildung 4: Codestück, JWT Session Decryption 9](#_Toc169981177)

[Abbildung 5: Sicherheitsanalyse des Backends innerhalb des Backends 9](#_Toc169981178)

[Abbildung 6: Verbindungsaufbau MongoDB Datenbank 10](#_Toc169981179)

[Abbildung 7: Autorisierung in der Webapplikation 10](#_Toc169981180)

# Quellenangaben

ChatGPT: <https://www.chatgpt.com/>  
e-recht24.de: <https://www.e-recht24.de/>  
Die ältere Website: <https://leys.ch/>