Dokumentation Sicherheitsanalyse

Levyn Schneider, David Meer, Ramon Rollier, Matthias Baumgartner

Hapinz

Abbildung 1: Titelbild (www.freepik.com)

1. Inhaltsverzeichnis

2. 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.

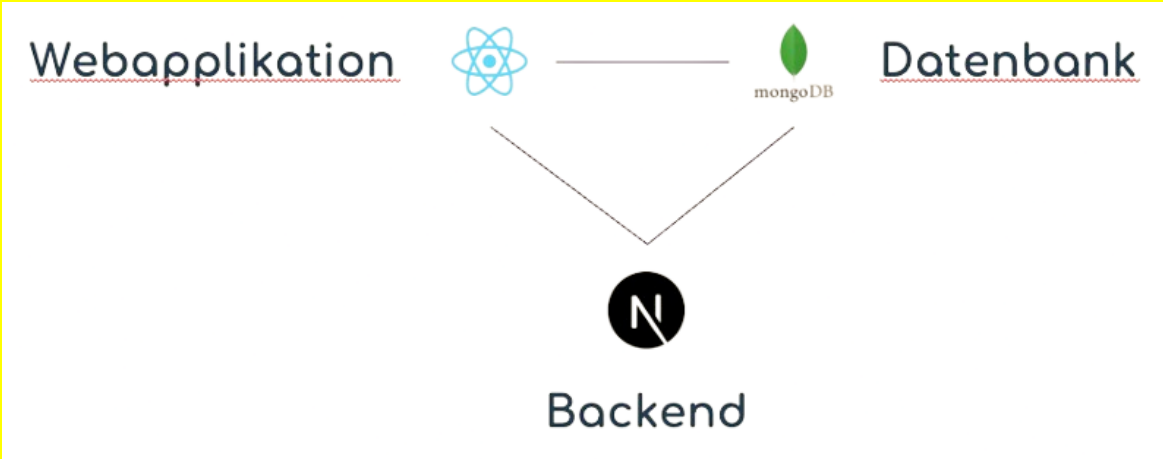


Abbildung 2: Grafik Abgrenzung Arbeitsbereiches

3. 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.

4. 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

5. 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 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.

6. 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 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

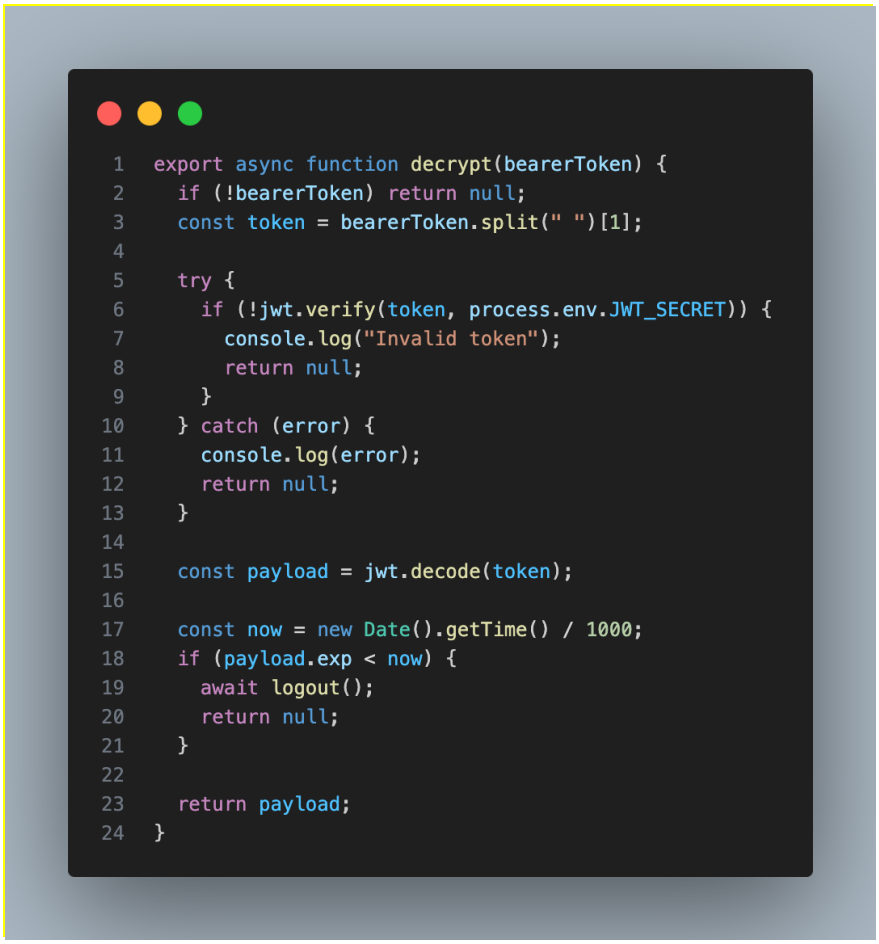
Da wir Google Analytics für die Konversion-Rate und Nutzungsanalyse verwenden, haben wir von einem meiner älteren Webseite das HTML und JavaScript vom Cookie-Consent Banner kopiert und bei uns eingefügt. Wir haben dann noch das Styling und andere Attribute angepasst. Somit hatten wir am Schluss ein DSG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

```tsx
export default function CookieConsent() {
  const [cookieConsent, setCookieConsent] = useState(null);
  const [loading, setLoading] = useState(true);

  useEffect(() => {
    const consent = localStorage.getItem("cookie_consent");
    if (consent === "true") {
      setCookieConsent(true);
      setLoading(false)
    } else if (consent === "false") {
      setCookieConsent(false);
      setLoading(false)
    } else {
      setCookieConsent(null);
      setLoading(false)
    }
  }, []);

  function consent(accept) {
    if (accept) {
      localStorage.setItem("cookie_consent", "true");
      setCookieConsent(true);
    } else {
      localStorage.setItem("cookie_consent", "false");
      setCookieConsent(false);
    }
  }

  if (loading || cookieConsent !== null) {
    if (cookieConsent === true) {
      return (
        <>
          <Script async src="https://www.googletagmanager.com/gtag/js?id=G-4B305JP6DV"></Script>
          <Script>
            {`
            window.dataLayer = window.dataLayer || [];
            function gtag(){dataLayer.push(arguments);}
            gtag('js', new Date());

            gtag('config', 'G-4B305JP6DV');
            `}
          </Script>
        </>
      )
    }
    return null;
  }

  return (
    <div className={`fixed bottom-0 z-50 text bg-background border-2 max-w-md border-border rounded-xl mb-5 mx-8 px-4 py-3
      ${cookieConsent === null ? "block" : "hidden"}`}>
      <p className="text mb-1">Diese Website verwendet Cookies, um Ihnen die bestmögliche Nutzung dieser Website zu ermöglichen.</p>
      <Link href="/privacy" className="text text-primaryText underline">Mehr erfahren</Link>
      <div className="text-end mt-3 w-full flex flex-row gap-3 justify-end">
        <button type="button" className="btn btn-secondary py-1.5" onClick={() => consent(false)}>Ablehnen</button>
        <button type="button" className="btn btn-primary py-1.5" onClick={() => consent(true)}>Annehmen</button>
      </div>
    </div>
  );
}
```

Abbildung 3: Codestück, Cookie-Consent Banner

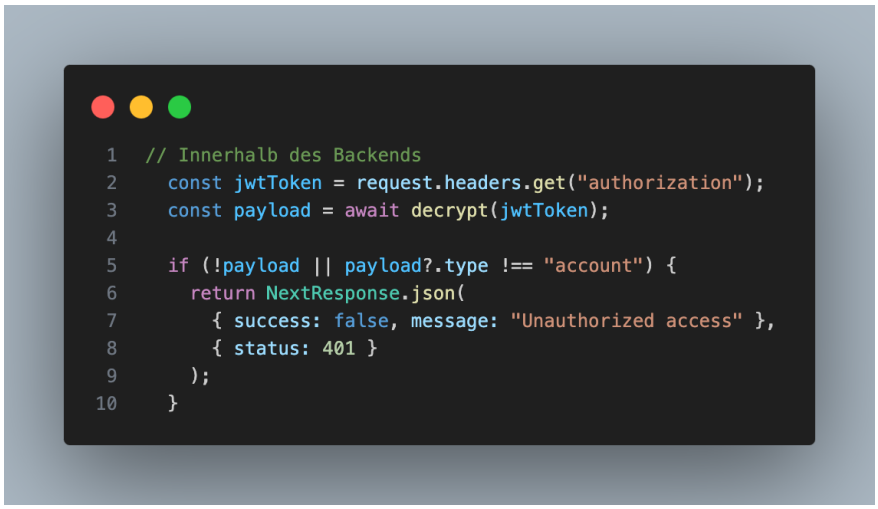
Sicherheitsanalyse des Backends

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



```
export async function decrypt(bearerToken) {
  if (!bearerToken) return null;
  const token = bearerToken.split(" ")[1];

  try {
    if (!jwt.verify(token, process.env.JWT_SECRET)) {
      console.log("Invalid token");
      return null;
    }
  } catch (error) {
    console.log(error);
    return null;
  }

  const payload = jwt.decode(token);

  const now = new Date().getTime() / 1000;
  if (payload.exp < now) {
    await logout();
    return null;
  }

  return payload;
}
```

Abbildung 4: Codestück, JWT Session Decryption



```
// Innerhalb des Backends
  const jwtToken = request.headers.get("authorization");
  const payload = await decrypt(jwtToken);

  if (!payload || payload?.type !== "account") {
    return NextResponse.json(
      { success: false, message: "Unauthorized access" },
      { status: 401 }
    );
  }
```

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, 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.

```
const MONGODB_URI = process.env.MONGODB_URI;

if (!MONGODB_URI) {
  throw new Error("No MONGODB_URI environment variable inside .env.local");
}

// Global is used here to maintain a cached connection across hot reloads in development.
let cached = global.mongoose;

if (!cached) {
  cached = global.mongoose = { conn: null, promise: null };
}

async function dbConnect() {
  if (cached.conn) {
    return cached.conn;
  }

  if (!cached.promise) {
    const opts = {
      useNewUrlParser: true,
      useUnifiedTopology: true,
      bufferCommands: false,
    };

    cached.promise = mongoose.connect(MONGODB_URI, opts).then((mongoose) => {
      return mongoose;
    });
  }
  cached.conn = await cached.promise;
  return cached.conn;
}

export default dbConnect;

```

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:

```
const session = await getSession();

  if (!session || session?.user.type !== "account") {
    redirect("/login");
  }
```

Abbildung 7: Autorisierung in der Webapplikation

7. Abbildungsverzeichnis

8. Quellenangaben

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