Report k ročníkovému projektu: Podporný systém na analýzu rizík pre webové aplikácie a služby

Úvod

Hlavným cieľom tohto projektu bolo vytvoriť webovú aplikáciu, ktorá slúži ako podporný systém na analýzu rizík v oblasti kybernetickej a informačnej bezpečnosti. Projekt bol zameraný na implementáciu metodiky IT-Grundschutz od nemeckého BSI (Bundesamt für Sicherheit in der Informationstechnik), konkrétne na modul APP.3.1 Web Applications and Web Services. Táto aplikácia umožňuje používateľom identifikovať zraniteľnosti, hrozby, a navrhnúť opatrenia na minimalizáciu identifikovaných rizík.

Postup práce

1. Zber informácií:
Väčšinu času projektu som venoval štúdiu a analýze rôznych zdrojov. Primárne som sa zameral na:

- IT-Grundschutz Compendium: Tento rámec poskytol štruktúrovaný prehľad zraniteľností, hrozieb a návrhov opatrení pre webové aplikácie a služby.
- OWASP (Open Web Application Security Project): Použitý na doplnenie informácií o najčastejších útokoch a spôsoboch ochrany webových aplikácií.
- NIST a ISO/IEC 27001, ktoré podporili proces identifikácie hrozieb a opatrení.

2. Príprava obsahu:
Na základe získaných informácií som vytvoril:

- Zoznam zraniteľností pre webové aplikácie a služby, doplnený o vysvetlenia z IT-Grundschutz.
- Pre každú zraniteľnosť som identifikoval možné hrozby a navrhol vhodné opatrenia.

3. Vývoj webovej aplikácie:
V záverečnej fáze projektu som tieto informácie implementoval do webovej stránky, ktorá obsahuje:

- **Zoznam zraniteľností**: Každá zraniteľnosť je popísaná, vrátane hrozieb a návrhov opatrení.
- **Interaktívne prvky**: Používatelia môžu zobraziť podrobné vysvetlenia, hrozby a opatrenia pre každú zraniteľnosť.
- **Dynamický obsah**: Použitím HTML, CSS a JavaScriptu som zabezpečil dynamickú prezentáciu informácií.