**Analýza Hrozieb a Tvorba Opatrení**

Motošický Ľuboslav

Jan Hofer

# An adversary can spoof the target web application due to insecure TLS certificate configuration

## Analýza Hrozby

Útočník dokáže podvrhnúť cieľovú webovú aplikáciu v dôsledku zlej konfigurácie TLS certifikátu. Ide o závažný problém a vyžaduje vysokú prioritu pre riešenie.

**Priorita**: High

## Navrhované Opatrenia

**Správne nastavenie TLS certifikátu.**

* Kontrola, správnosti nastavenia hodnôt pre certifikát, ako sú platné výdaje, správne doménové názvy a algoritmy šifrovania.

**Aktualizácia a sledovanie certifikátov..**

* Údržba aktuálnosti certifikátov a tatiež monitorovanie ich expirácie.
* Implementácia automatických obnovovaní certifikátov.

**Definícia postupov pre prípady, keď overenie certifikátu zlyhá.**

* Zabezpečenie, aby aplikácia reagovala adekvátne a neumožnila útočníkom neoprávnený prístup

**Kontrola, či je komunikácia s použitím SSL/TLS správne implementovaná v kóde aplikácie.**

Okrem vymenovaných je vhodné zvážiť taktiež zabezpečené skladovanie/uchovávanie certifikátov a kľúčov.

# An adversary can get access to a user's session due to insecure coding practices

## Analýza Hrozby

Hrozba spočíva v poskytnutí možnosti pre útočníka získať prístup k relačnej identifikácii používateľa (session token) v dôsledku zraniteľných programátorských praktík.

**Priorita**: High

## Navrhované Opatrenia

**Ochrana session tokenu.**

* Zabezpečenie dostatočnej ochrany pre session token.
* Zabezpečenie pred neoprávneným prístupom.

*Možnosť použitia moderných techník tokenizácie a zabezpečenia tokenu*

**Aplikácia sanitačných postupov pre vstupné polia.**

**Zabezpečenie, nevyužívania nebezpečných techník vykresľovania/vypisovania.**

**Nevyhnutnosť použitia vhodného kódovania znakov.**

# An adversary can get access to a user's session due to improper logout and timeout

## Analýza Hrozby

Hrozba spočíva v možnosti útočníka získať prístup k relačnej identifikácii používateľa v dôsledku nevhodného spracovania odhlásenia (logout) a nedostatočného nastavenia časového limitu (timeout) relácie.

**Priorita**: High

## Navrhované Opatrenia

**Nastavenie časového limitu aktivity relácie.**

* Nastavenie adekvátneho časového limitu aktivity relácie (session) tak, aby sa automaticky ukončila po určitom čase nečinnosti používateľa.

**Implementácia správneho odhlásenia z aplikácie.**

* Zabezpečenie, aby proces odhlásenia používateľa bol riadne implementovaný a vykonával úplné odhlásenie, čo zahŕňa aj zneplatnenie session tokenu.

Okrem vyššie uvedených je vhodné vykonávať pravidelné sledovanie aktívnych relácií a taktiež ich logovanie.

# An adversary may gain access to sensitive data from uncleared browser cache

## Analýza Hrozby

Útočníkovi hrozba umožňuje získať prístup k citlivým údajom uloženým v mezipamäti webového prehliadača (browser cache), ak tieto údaje nie sú riadne odstránené alebo nezabezpečené.

**Priorita**: High

## Navrhované Opatrenia

**Obmedzenie skladovania citlivých údajov v mezipamäti prehliadača.**

* Proces vymedzenia nastaveniu cachovania pre citlivé alebo dôverné informácie.

**Vynútenie použitia vhodných HTTP Headers.**