Zpráva o bezpečnostní kontrole

Kontrolovaná verze	**1.70**
Datum kontroly	**21. 11. 2026**
Provedení	**Ivo Vaik, autor aplikace, s pomocí jazykového modelu (umělé inteligence)**

> **Jak kontrola vznikla.** Nástroje spustil, zdrojový kód prošel, opravy připravil a tuto zprávu sepsal jazykový model (umělá inteligence) na pokyn autora aplikace. Výsledky na živém webu (Mozilla HTTP Observatory, hlavičky serveru) ověřil autor sám. Jde o vlastní kontrolu s pomocí umělé inteligence, ne o nezávislý audit, penetrační test ani certifikaci. Projekt OWASP kontrolu neprovedl ani nepotvrdil.

Shrnutí

0	0	0	A+
nálezů s vysokou závažností (OWASP ZAP)	neopravených nálezů se střední závažností	známých zranitelností v knihovnách (npm audit)	Mozilla HTTP Observatory, 125/100 bodů

Dokumenty se zpracovávají jen v prohlížeči uživatele. Kontrola nenašla nic, co by umožnilo odeslání dokumentu mimo prohlížeč nebo přístup k datům na serveru. Nalezené nedostatky byly opraveny a opravy ověřeny opakovaným skenem a automatickými zkouškami.

Rozsah a postup

- **OWASP ZAP 2.16.1**: procházení a aktivní sken kopie webu (Apache, PHP) se stejným nastavením jako živý web. Sken proběhl na verzi 1.55; verze 1.56 až 1.70 mění jen pravidla rozpoznávání osobních údajů a vzhled stránky v prohlížeči, serverová část a nastavení serveru jsou beze změny.
- **Mozilla HTTP Observatory** na živém webu anonymio.cz: hodnocení A+, 12 z 12 testů. Ověřit si ho může kdokoli.
- **npm audit** všech přibalených knihoven.
- **Serverová část** (počítadlo, statistiky): prověření celého kódu a 29 automatických zkoušek, všechny prošly.
- **Běh aplikace** se všemi bezpečnostními hlavičkami bez jediného porušení pravidel prohlížeče.
- **Vybrané požadavky OWASP ASVS 4.0.3**, úroveň 1, posouzené po kapitolách (ne úplné posouzení).

Nálezy a opravy

Nález (OWASP ZAP)	Závažnost	Stav	Poznámka
Pravidlo stránky (CSP) povolovalo styly zapsané přímo ve stránce	Střední	Opraveno	Všechny styly jsou v souborech webu (`style-src 'self'`).
Přihlášení do statistik bez tokenu proti CSRF	Střední	Opraveno	Token mají přihlášení, odhlášení i obnova ze zálohy. Statistiky jsou jen pro autora.
Hlavička Server prozrazuje verzi	Nízká	Živý web v pořádku	Jen na zkušebním serveru; živý web uvádí jen „Apache“.

Ostatní nálezy byly jen informativní (záměrné nastavení nebo planý poplach). Při kontrole byly navíc opraveny drobnosti stránky statistik: odhlášení formulářem místo odkazu, odmítnutí podvrženého ID relace, skrytí chybových hlášek PHP a správné slučování zálohy.

Vybrané kapitoly OWASP ASVS 4.0.3 (úroveň 1)

Kapitola	Zjištění	Výsledek
V2 Ověřování	Heslo ke statistikám jako otisk, omezený počet pokusů.	Splněno
V3 Správa relací	Cookie HttpOnly, SameSite=Strict, Secure; nové ID po přihlášení, platnost 8 h, tokeny CSRF.	Splněno

Kapitola	Zjištění	Výsledek
V4 Řízení přístupu	Nastavení a data nejsou z webu dostupná (403).	Splněno
V5 Validace vstupu	Počítadlo i obnova ze zálohy přijmou jen platná data v daných mezích; výstupy ošetřené.	Splněno
V7 Chyby a záznamy	Chybová hlášení PHP se návštěvníkům nezobrazují.	Splněno
V8 Ochrana dat	Dokumenty neopouštějí prohlížeč; na server jdou jen počty.	Splněno
V9 Komunikace	HTTPS s HSTS a přesměrováním.	Splněno
V10 Integrita kódu	Kontrolní součty, soupis knihoven (SBOM), noční kontrola živého webu.	Splněno
V12 Soubory	Soubory se zpracovávají jen v prohlížeči; limity velikosti.	Splněno
V14 Konfigurace	Hlavičky A+, přísné CSP, knihovny bez známých zranitelností.	Splněno

Omezení

- Bez ručního penetračního testu a bez kontroly třetí stranou. Jazykový model se může mýlit.
- Sken OWASP ZAP běžel na kopii webu a nespouští JavaScript; chování aplikace v prohlížeči pokrývají autotest a vlastní testy.
- Zabezpečení serveru a účtu u hostingu zajišťuje poskytovatel.
- Kontrola nehodnotí, jak spolehlivě aplikace rozpozná osobní údaje. Výsledek musí vždy zkontrolovat člověk.

Podrobné výsledky jsou k dispozici na vyžádání. Zranitelnost nebo chybu prosím hlaste na ivo.vaik@gmail.com. · Stav k 21. 11. 2026.