

PLIS testovanie zraniteľností

Vytvoril: Mgr. Peter Chudý; AXON PRO

Dátum: 15.4.2025

Verzia: 1.0

Na základe objednávky bolo vykonané testovanie vybraných webových a API služieb systému PLIS (Plemenársky informačný systém). Cieľom výkonu testov zraniteľností systému PLIS je identifikovať slabé miesta, ktoré môžu byť zneužívané na kompromitáciu t.j. narušenie integrity, dostupnosti alebo dôvernosti. Ďalším cieľom bezpečnostného testovania je vypracovať odporúčania na elimináciu identifikovaných zraniteľností. Penetračné testy budú vykonávané voči štandardom OWASP.

Testovanie bolo realizované z pohľadu neautentifikovaného používateľa (black-box prístup), bez zásahu do interného prostredia organizácie. Tento dokument sumarizuje rozsah testovania, použitú metodológiu, výsledky automatizovaného skenovania a odporúčania na zlepšenie bezpečnostnej úrovne aplikácie.

1. Rozsah a metóda testovania

Skenovanie prebehlo pomocou nástroja OWASP ZAP, ktorý je určený na automatizované bezpečnostné testovanie webových aplikácií.

Použitá metóda

Penetračné testy realizované technikami tzv. čiernej skrinky, ktorá vychádza z minimálnych znalostí o systéme alebo aplikácii. Je definovaný len rozsah testu, v akom má byť vykonaný. Všetky informácie sú získané analýzou, nedeštruktívnym spôsobom, prostredníctvom sofistikovaných nástrojov a znalostí. Penetračné testovanie infraštruktúry je realizované z pohľadu útočníka, ktorý pristupuje na systémy zadávateľa zo siete Internet.

Testovanie bolo vykonané v nasledovných krokoch:

1. **Crawling (Spidering)** – nástroj prešiel odkazy dostupné na zadaných URL, čím vytvoril mapu dostupných zdrojov.
2. **Pasívna analýza** – bez aktívneho zásahu bola vykonaná kontrola odpovedí servera, hlavičiek a zabezpečenia prenosu dát.
3. **Aktívne testovanie** – vykonané prostredníctvom simulovaných útokov na vstupné body, s cieľom odhaliť známe zraniteľnosti ako napríklad:
 - Cross-Site Scripting (XSS)
 - SQL Injection
 - Open Redirect
 - Nezabezpečené cookies a hlavičky
 - Chyby autentifikácie a prístupových práv

str. 1

Rozsah testovania

Do testovania boli zahrnuté nasledovné URL adresy:

- <https://www.plis.sk>
- <https://www.plis.sk/login.aspx>
- <https://auth.plis.sk>
- <https://auth.plis.sk/plis/org>
- <https://auth.plis.sk/plis/user>
- <https://api.plis.sk>
- <https://api.plis.sk/milk/>
- <https://api.plis.sk/insem/>
- <https://api.plis.sk/lact/>
- <https://api.plis.sk/animalInfo/>
- <https://api.plis.sk/public/brComp>
- <https://api.plis.sk/inbreeding/cows/>
- <https://api.plis.sk/inbreeding/heifers/>
- <https://api.plis.sk/genInfo/cows/>
- <https://api.plis.sk/genInfo/genom/>
- <https://api.plis.sk/linInfo/cows>
- <https://api.plis.sk/animalInfo/bulls>

Obmedzenia

Testovanie prebehlo bez autentifikácie, a teda nezahŕňalo kontrolu interných (autentifikovaných) častí systému. Výsledky tak predstavujú pohľad z perspektívy bežného (neprihláseného) používateľa.

2. Priebeh

Bolo pripravené izolované prostredie s najnovšou verziou OWASP ZAP. Test bol realizovaný vo viacerých kolách v dňoch 18.2.2025, 19.2.2025, 14.4.2024 zo zariadenia s verejnou IP adresou 193.200.9.55. Celkovo bolo identifikovaných 3.515 URL v ktorých boli analyzované HTTP hlavičky, nastavenia cookies, TLS/SSL konfigurácia a podobne. Následne boli simulované bežné útoky na identifikované vstupné URL a REST endpointy. Po skončení testu bol vygenerovaný report vid'. príloha.

3. Sumarizácia výsledkov a odporúčania

V tejto sumarizácii sa zameriame na zraniteľnosti s úrovňou závažnosti High a Medium, ktoré predstavujú najvýraznejšie riziká pre bezpečnosť systému.

Zraniteľnosti kategorizované ako Low alebo Informational nepredstavujú okamžité riziko, avšak môžu signalizovať slabiny v konfigurácii alebo potenciálne vektory útoku v budúcnosti. Ich detailný zoznam je dostupný v detailnom reporte, ktorý je prílohou tejto správy. Odporúčame ich postupne analyzovať a vyhodnotiť podľa interných bezpečnostných štandardov organizácie.

Zraniteľnosť	Risk	Odporúčanie
PII Disclosure	High	Falošné hlásenie „Koeficient príbuznosti – Rodokmeň“ neobsahuje osobné údaje.
SQL Injection SQL Injection – MsSQL SQL Injection - Oracle - Time Based SQL Injection - SQLite	High	Preveriť či je vstup od používateľa validovaný. Pridanie nevyžadovaných atribútov do požiadavky je spracovné bez chybového hlásenia. V testoch sa napríklad ukazuje, že je možné kontrolovať čas vykonania SQL dotazu.
Vulnerable JS Library	High	Ak to je možné aktualizovať JS knižnicu jquery-validation
Absence of Anti-CSRF Tokens Anti-CSRF Tokens Check	Medium	Zvážiť použitie techník na zamedzenie Cross-Site Request Forgery. Prehliadač overeného používateľa môže pristupovať na stránky bez kontextu z aplikácie.
Content Security Policy (CSP) Header Not Set	Medium	Preveriť či web server. resp. load balancer nastavuje v HTTP hlavičke Content-Security-Policy
Multiple X-Frame-Options Header Entries	Medium	Zabrániť duplicitnej hlavičke: X-Frame-Options
Potential IP Addresses Found in the Viewstate	Medium	Falošné hlásenie 4.0.0.0 v odpovedi bolo vyhodnotené ako IP adresa
Secure Pages Include Mixed Content (Including Scripts)	Medium	Upraviť odkazy na JS s použitím SSL http://code.jquery.com/jquery-1.9.1.js http://code.jquery.com/ui/1.10.3/jquery-ui.js
Vulnerable JS Library	Medium	Ak to je možné aktualizovať JS knižnicu jquery

4. Prílohy

PLIS Scanning Report