Modelování hrozeb pro KOS a Progtest

Owner: Michal Filip
Reviewer:
Contributors: Eva Skaunicova
Date Generated: Tue Oct 14 2025

Executive Summary

High level system description

Zjednodušená verze školní infrastruktury pro provozování služeb KOS a Progtest

Summary

Total Threats	6
Total Mitigated	1
Total Open	5
Open / Critical Severity	0
Open / High Severity	1
Open / Medium Severity	0
Open / Low Severity	0
Open / TBD Severity	4

Diagram infrastruktury

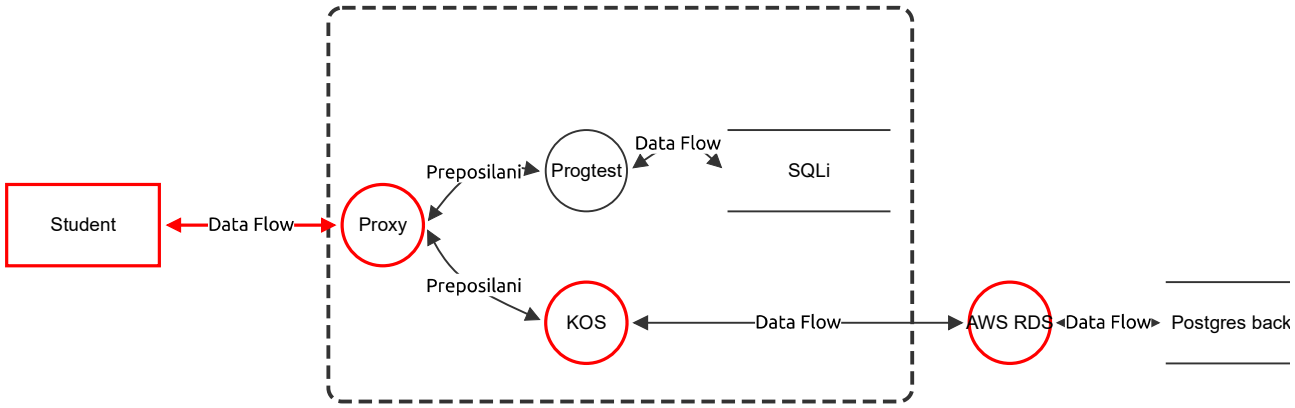

Diagram infrastruktury

Data Flow (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
3	Únik hesel	Information disclosure	TBD	Open		Komunikace prochází veřejným inrentem přes protokol HTTP, který není šifrovaný a umožňuje MITM, či jiné způsoby odposlechu např hesel.	Pro veškerou komunikaci používat HTTP s TLS pro zajištění šifrování a zabezpečení obsahu.

Progtest (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
4	Připsání uložených dat	Tampering	TBD	Mitigated		Nahraný program pro testování může obsahovat škodlivý kód, který po spuštění přepíše data v SQLi databázi, nebo může otevřít backdoor do serveru.	Spouštět programy v sandbox prostředí, kontrolovat oprávnění spouštěných programů a pravidelně revidovat nastavení aplikace.

KOS (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Přihlášení se jako admin	Elevation of privilege	High	Open		Pomocí XSS nebo jiné techniky např. z OWASP TOP 10 se přepnout na administrátorský účet.	Kontrolovat kód, zda neumožňuje známé zranitelnosti. Omezit práva uživatelů a rozdělit je mezi více různých účtů pouze podle toho, jaké funkce může daná role potřebovat.

Proxy (Process)

Description: Squid server

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	Přetížení serveru	Denial of service	TBD	Open		Jediný proxy server pro všechny aplikace vytváří single point of failure, kde pokud dojde k přetížení při vyšším provozu jedné aplikace znepřístupní to i ty ostatní.	Pro každou aplikace používat samostatnou reverse proxy.

Student (Actor)

Description: Žák připojující se do systému v rámci školní potřeby.

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	Krádež hesel	Spoofing	TBD	Open		Uživatel si uložil přihlašovací údaje do prohlížeče. V rámci spuštění viru byly ukradeny i daná hesla a následně použita pro přihlášení se do portálů školy.	Proškolení uživatelů ohledně ukládání hesel do prohlížeče. Používání MFA nebo FIDO klíčů misto hesel.

AWS RDS (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
2	Únik studentských informací	Information disclosure	TBD	Open		Jelikož se pro komunikaci používá veřejný endpoint, při útoku či chybě na něm můžou uniknout i osobní data studentů.	Pro posílání a ukládání osobních dat používat privátní endpoint.