Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze bakalářské práce

Nette Framework z hlediska bezpečnosti proti útokům

Michal Sladký

Souhrn

Bakalářská práce pojednává o technikách, jak předejít bezpečnostním rizikům. Teoretická část se zaměřuje na obecné fungování webových aplikací, poté popisuje výběr nejzávažnějších útoků a ke konci představí Nette Framework, který je použit pro vytvoření zkoumaného prototypu.

Praktická část se týká samotné analýze kódu a analýze zvoleným penetračním testovacím nástrojem a návrhu ochrany sledovaných útoků. Na závěr je zhodnocena schopnost Nette Framework zajistit bezpečnost.

Klíčová slova

webové útoky, web, programování, php, nette, framework

Cíl práce

Cílem práce je návrh obrany proti webovým útokům s využitím Nette Framework. V práci jsou představeny a analyzovány nejčastěji se vyskytující útoky na webové stránky a následně vysvětlena či navržena možná obrana proti nim.

Metodika

Řešení problematiky bakalářské práce je založeno na studiu a analýze odborných informačních zdrojů. Na základě získaných informací jsou vypracovány jednotlivé části práce a vyhodnoceny možnosti Nette Framework a jeho komponent z hlediska ochrany proti útokům. Na základě syntézy teoretických poznatků a výsledků praktické části práce jsou formulovány závěry bakalářské práce.

Obsah práce

V práci je popsána problematika bezpečnosti webových aplikací. Existuje nespočet možností, jak prolomit obranu webových aplikací, proto jsou vybrány pouze ty nejzávažnější útoky, které mohou mít katastrofální dopad v podobě odcizení citlivých dat, finančních prostředků nebo ztráty stávajících, či potenciálních uživatelů.

První kapitola teoretické části charakterizuje způsoby a prostředky, kterými lze vytvořit webová aplikace. Jsou zde popsány technologie klientské strany a strany serveru se zaměřením na prostředí, ve kterém je vytvořen prototyp pro tuto práci.

V další části je představen samotný Nette Framework, který je stavebním kamenem analyzovaného prototypu. Jsou zde informace o částech frameworku, principu fungování a návrhový vzor, kterým se řídí programování aplikací. Část je zejména věnována šablonovacímu systému Latte, který je součástí frameworku.

Poslední kapitola teoretické části se věnuje vybraným webovým útokům. Je použit seznam nejzávažnějších útoků, který vytváří organizace OWASP každé tři roky. Pro tuto práci byl použit poslední zveřejněný, z roku 2013. Každý útok obsahuje kromě principu také příklad použití.

Zmiňovaný prototyp je v praktické části analyzován. Analýza probíhala dvěma způsoby – penetračním testovacím softwarem a osobní analýzou kódu. Následně je navržena ochrana na každý typ ze zaměřených útoků. Samotný návrh má obecné uplatnění a lze tedy použít v jakékoliv jiném vývojovém prostředí.

Závěr

Program OWASP ZAP, pomocí kterého byl proveden sken potenciálních útoků, se osvědčil jako uspokojivý nástroj pro testování menších, či středních webů s menším důrazem na bezpečnost.

Nette Framework se osvědčil jako velmi dobrý nástroj pro vývoj webových aplikací. Často je zmiňováno, že vyznávaným principem Nette Framework je „less code, more security“ (méně kódu znamená více bezpečnosti) a v naprosté většině případů je možné dát tomuto tvrzení za pravdu. Obvyklým způsobem vzniku bezpečnostních děr jsou stovky, či tisíce řádků kódu, ve kterých je téměř nemožné se vyznat. Samotný framework je naprogramován čitelně a jsou k tomu tak vedeni i programátoři.

Ačkoliv jsou bezpečnostní rizika zdůrazňována vývojáři frameworku a komunitou jsou doporučeny co nejjednodušší způsoby implementace kódu při různých situací, není neobvyklé setkat se s takzvaným špagetovým kódem[1]. Už jen vznik těchto nesrozumitelných kódů je důkazem toho, že kvalita a s ní i bezpečnost aplikace závisí zejména na znalosti programátora. Nette Framework je z velké většiny schopen zajistit ochranu automaticky, případně obsahuje takové API, které ochranu zabezpečí. Přesto zůstává zodpovědnost pouze na programátorovi, jestli výsledná aplikace bude, či nebude bezpečná.

[1] Nesrozumitelný, velice rozsáhlý a neudržovaný kód

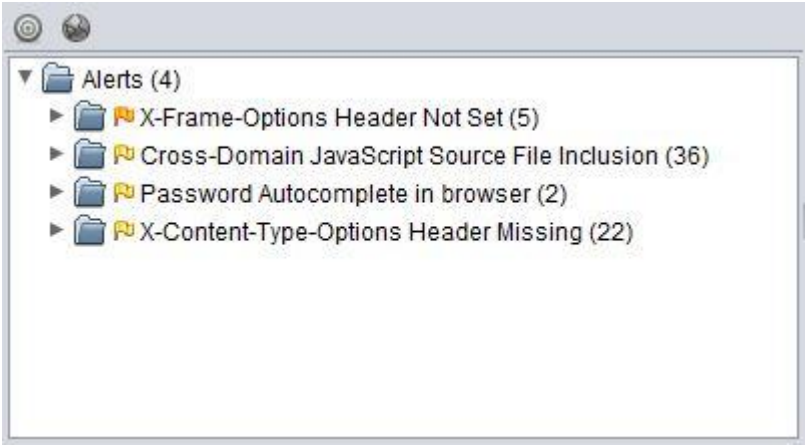
Počáteční stav

Na prototypové akci bylo provedeno automatické skenování pomocí softwaru OWASP ZAP. Jak je vidět na obrázku 1, celkově bylo nalezeno 117 hrozeb, z nichž dva útoky byly označeny jako potenciální XSS a další dva jako SQL Injektování.

Obrázek 1: Seznam potenciálních útoků na webovou aplikaci - zdroj: OWASP ZAP 2.4.3.

Výsledný stav

Po provedení všech zmiňovaných opatření na ochranu byl spuštěn druhý test. Jak je možné vidět na obrázku 2, nejzávažnější hrozby byly odstraněny upravením zdrojového kódu prototypu, případně byly prověřené hrozby označeny jako False Positive.



Obrázek 2 - Seznam útoků po provedení bezpečnostních opatření - zdroj: OWASP ZAP 2.4.3.