Bezpečnosť webového servera

Špecifikácia projektu

Bc. András Nagy

Predmet: Bezpečnosť v internete

Cvičiaci: Ing. Rudolf Grežo

Cvičenie: Štvrtok 18:00 - 19:50

Obsah

Úvod **3**
Zadanie **4**
Ciele projektu **4**
Metodológia **4**
Harmonogram **5**
Použité pramene **6**

Úvod

Webové servery dnes predstavujú neoddeliteľnú súčasť digitálneho prostredia, keďže umožňujú fungovanie širokej škály online služieb vrátane webových stránok, aplikácií, e-shopov a cloudových riešení.
So stále rastúcim množstvom kybernetických hrozieb a útokov sa však ich bezpečnosť stáva kľúčovou otázkou nielen pre administrátorov a vývojárov, ale aj pre organizácie, ktoré ich využívajú. Nesprávne nastavenie, zastaraný softvér či nedostatočné bezpečnostné opatrenia môžu vytvoriť priestor pre útočníkov, čo môže viesť k úniku citlivých informácií a ďalším bezpečnostným incidentom. Medzi najrozšírenejšie webové servery patria Apache HTTP Server (Apache2) a Nginx.

Bezpečnosť webových serverov je komplexná téma, ktorá zahŕňa viacero aspektov, ako sú správne nastavenie konfigurácie, kontrola prístupu, používanie šifrovacích mechanizmov či detekcia zraniteľností. Medzi najčastejšie bezpečnostné riziká patria [8]:

- **Zastaraný softvér** – Ak webový server nie je pravidelne aktualizovaný, môže obsahovať známe bezpečnostné chyby, ktoré môžu útočníci ľahko zneužiť.
- **Nesprávna konfigurácia** – Slabé alebo nevhodne nastavené predvolené hodnoty môžu umožniť neoprávnený prístup alebo neúmyselne odhaliť citlivé informácie o systéme.
- **Nedostatočné riadenie prístupu** – Slabé prihlasovacie údaje a neadekvátne nastavené oprávnenia môžu viesť k neoprávnenému prístupu k dôležitým údajom.
- **Zraniteľnosti v aplikáciách** – Webové aplikácie bežiace na serveri môžu obsahovať chyby ako SQL Injection alebo Cross-Site Scripting (XSS), ktoré môžu byť zneužité na napadnutie servera a získanie citlivých údajov.

Apache2, vyvíjaný Apache Software Foundation, je jeden z najpopulárnejších webových serverov, využívaný pre svoju stabilitu, flexibilitu a širokú podporu modulov. Vďaka modulárnej architektúre umožňuje rozšírenie funkcionality podľa potrieb – napríklad mod_rewrite na úpravu URL adries alebo mod_security na ochranu pred útokmi [2].

Bezpečnosť Apache2 závisí od správnej konfigurácie. Zastaraný softvér, nesprávne nastavenia oprávnení či nezabezpečená komunikácia môžu viesť k vážnym zraniteľnostiam. Preto je dôležité pravidelne aktualizovať server, implementovať SSL/TLS na šifrovanie dát a obmedziť prístup k citlivým súborom.

Na identifikáciu bezpečnostných slabín sa používajú nástroje ako Nikto, OpenVAS, OWASP ZAP či Acunetix, ktoré pomáhajú odhaliť chyby v konfigurácii a známe zraniteľnosti. Správne nastavenie Apache2 v kombinácii s monitoringom a pravidelným testovaním je nevyhnutné pre bezpečnú a spoľahlivú prevádzku [7].

- **Acunetix** – Komerčný nástroj na automatizovanú detekciu zraniteľností, ktorý umožňuje testovanie webových aplikácií a serverov na širokú škálu bezpečnostných problémov, vrátane SQL Injection, XSS a nesprávnej konfigurácie servera.
- **OpenVAS** – Open-source riešenie pre detekciu zraniteľností, ktoré dokáže identifikovať známe bezpečnostné chyby na serveroch, sieťových zariadeniach a webových aplikáciách.

- **OWASP ZAP (Zed Attack Proxy)** – Nástroj vyvíjaný komunitou OWASP, ktorý slúži na automatizované aj manuálne testovanie bezpečnosti webových aplikácií. Je ideálny na odhaľovanie zraniteľností ako XSS či SQL Injection.
- **Nikto** – Open-source skener určený na identifikáciu známych zraniteľností webových serverov. Skontroluje konfiguráciu, potenciálne nebezpečné súbory a staršie verzie softvéru, ktoré môžu predstavovať bezpečnostné riziko.

Zadanie

V projekte je potrebné skúmať charakteristiku webových serverov a ich funkcie.
Téma zahŕňa:

- Výber webového servera (napr. Nginx, Apache alebo iný).
- Štandardné prevádzkové procedúry a bežné chyby v konfigurácii.
- Zraniteľnosti vybraného (jedného alebo viacerých) webového servera.
- Zvýšenie bezpečnosti prostredníctvom rozširujúcich modulov (napr. mod_security).
- Testovanie zvýšenej bezpečnosti.

Ciele projektu

Hlavným cieľom projektu je analyzovať a implementovať bezpečnostné opatrenia pre webový server s cieľom minimalizovať riziká spojené s jeho prevádzkou. Projekt sa zameria na webový server Apache2. Na identifikáciu zraniteľností, konfiguráciu bezpečnostných mechanizmov a testovanie ich efektivity.

Cieľ 1 - Preskúmať architektúru a bezpečnostné mechanizmy webového servera.

Cieľ 2 - Identifikovať bežné konfiguračné a bezpečnostné zraniteľnosti pomocou automatizovaných nástrojov a/alebo penetračnými testami.

Cieľ 3 - Konfigurovať a implementovať bezpečnostné opatrenia, implementovať rozširujúcich moduloch.

Cieľ 4 - Testovanie implementovaných opatrení, a vyhodnotiť ich s vhodnou interpretáciou.

Metodológia

1. **Analýza literatúry a dostupných zdrojov**: Prieskum existujúcich riešení pre zabezpečenie webových serverov [1] [4].
2. **Konfigurácia a nasadenie serverov**: Inštalácia Apache2 prostredie [3].
3. **Identifikácia zraniteľností**: Skúmanie bezpečnostných hrozieb pomocou automatizovaných nástrojov (vyskúšať viacerých): Acunetix, OpenVAS, OWASP ZAP, Nikto [5].
4. **Implementácia bezpečnostných opatrení [4]**:
    a. Použitie firewallov a WAF (Web Application Firewall)
    b. Nasadenie SSL/TLS

    c. Obmedzenie prístupu a riadenie oprávnení
    d. Hardening konfigurácie
5. **Testovanie bezpečnosti**: Vykonanie penetračných testov a vyhodnotenie ich úspěšnosti [6].
6. **Vyhodnotenie a dokumentácia**: Spracovanie zistení, tvorba odporúčanií.

Harmonogram

1. - 3. týždeň: Prieskum literatúry, konzultácie a vypracovanie špecifikácie projektu.

4. - 5. týždeň: Vypracujem prvý progress report, ktorý sa bude venovať teoretickému úvodu do problematiky, vrátane analýzy zraniteľností a bezpečnostných problémov v Apache2. Tento report bude slúžiť ako základ pre ďalší postup projektu.

6. - 7. týždeň: Vypracuje druhý progress report, ktorý sa bude sústrediť na výber a odôvodnenie použitia nástrojov na analýzu zraniteľností, ako sú Acunetix, OpenVAS, OWASP ZAP a Nikto. Bude sa tiež pripravovať testovacie prostredie.

8. - 9. týždeň: Privravím si tretí progress report, ktorý bude obsahovať predbežné výsledky z testovania Apache2 servera s bezpečnostnými opatreniami, ako sú firewally, WAF a SSL/TLS. Budú vykonané prvé skenovania zraniteľností a testy účinnosti implementovaných opatrení.

10. - 11. týždeň: Vypracujem štvrtý progress report, ktorý bude zameraný na finálne výsledky testovania. Tieto výsledky budú obsahovať hodnotenie efektívnosti bezpečnostných opatrení a rozširujúcich modulov, ako je mod_security, s návrhmi na ďalšie zlepšenie bezpečnosti.

12. týždeň: Odovzdávam záverečnú správu, ktorá bude sumarizovať celý projekt, vrátane výsledkov testovania, odporúčaní na zlepšenie bezpečnosti Apache2 servera a vykonaných experimentov.

Použité pramene

1. WIBOWO, Dega Surono, et al. Apache web server security with security hardening. *Journal of Soft Computing Exploration*, 2023, 4.4: 213-221.
2. LAURIE, Ben; LAURIE, Peter. *Apache: The definitive guide*. " O'Reilly Media, Inc.", 2003.
3. APACHE SOFTWARE FOUNDATION. *Apache HTTP Server* [online]. [cit. 2025-03-03]. Available at: https://httpd.apache.org/
4. Welekwe, A. (n.d.). *Apache web server: Security guide*. Comparitech. Available at: https://www.comparitech.com/net-admin/apache-web-server-security/
5. SHAHID, Jahanzeb, et al. A comparative study of web application security parameters: Current trends and future directions. *Applied Sciences*, 2022, 12.8: 4077.
6. SANTOSO, Joseph Teguh; RAHARJO, Budi. Performance evaluation of penetration testing tools in diverse computer system security scenarios. *JURNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI*, 2022, 13.2: 132-159.
7. AYDOS, Murat, et al. Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University-Computer and Information Sciences*, 2022, 34.9: 6775-6792.
8. Varghese, J. **Web Server Security - Beginner's Guide** [online]. GetAstra, [cit. 2025-03-06]. Available at: https://www.getastra.com/blog/security-audit/web-server-security/