Webové aplikačné brány

Richard Németh

Zámer

V tomto projekte sa budem venovať webovým aplikačným bránam, známym aj pod skratkou WAF (Web Application Firewall), ktoré slúžia na ochranu webových stránok pred rôznymi kybernetickými útokmi. V úvode sa zameriam na históriu týchto brán, ich vznik, zakladateľov a prvotné použitia. Okrem teoretickej časti si ukážeme aj štatistiky používania WAF a najznámejšie prípady, kde tieto systémy úspešne ochránili aplikácie pred útokmi. Na druhej strane sa pozrieme aj na prípady, kedy došlo k prelomeniu ochrany, a aké boli dôsledky pre napadnuté systémy. Cieľom tejto časti je poskytnúť ucelený pohľad na to, kde WAF exceluje a kde môže zlyhať.

Webové aplikačné brány nie sú všemocné a nedokážu zabrániť všetkým možným útokom. V tomto projekte sa preto zameriam aj na ich technické fungovanie. Opíšem, ako WAF systémy analyzujú prichádzajúce požiadavky, ako identifikujú podozrivé správania a akým spôsobom reagujú na zaznamenané útoky. Kľúčové je pochopiť, kedy takáto brána zaeviduje útok a aké má možnosti reakcie – od jednoduchého zablokovania požiadavky až po detailné logovanie aktivít útočníka pre ďalšiu analýzu. Taktiež si ukážeme niekoľko spôsobov, ako môžu WAF systémy reagovať na rôzne typy kybernetických hrozieb.

Ďalej si porovnáme rôzne možnosti nasadenia WAF brán, vrátane ich výhod a nevýhod. Existuje mnoho produktov na trhu, ktoré ponúkajú rôzne riešenia ochrany webových aplikácií, od komerčných až po open-source verzie. V rámci projektu plánujem podrobne porovnať aspoň dva až tri open-source WAF systémy, konkrétne NAXSI, ModSecurity a Shadow Daemon. Okrem toho sa zameriam aj na analýzu kódu týchto open-source systémov. Preštudujeme si niektoré dôležité a zaujímavé časti kódu, ktoré sú zodpovedné za ochranu aplikácií a vysvetlíme si, ako fungujú.

V ďalšej fáze projektu si ukážeme, že WAF nemôže odolať všetkým útokom, a preto je dôležité kombinovať ho s ďalšími bezpečnostnými opatreniami. Budeme testovať rôzne druhy útokov na našom serveri, na ktorom budú nasadené rôzne WAF systémy. Nasadíme si domáci Linux server, na ktorý nainštalujeme webovú aplikáciu, kde budeme simulovať reálne scenáre útokov. Úmyselne nahráme staršiu verziu WAF, o ktorej vieme, že obsahuje zraniteľnosti, aby sme mohli tieto slabiny využiť na prienik do systému.

Na vytvorenej aplikácii budeme testovať viacero typov útokov, pričom každý útok bude mať špecifický cieľ a použijeme rôzne nástroje na jeho simuláciu. Pri Injection útokoch, použijeme nástroj SQLMap, ktorý nám umožní automaticky zisťovať a zneužiť zraniteľnosti v databázových dopytoch. Tento útok nám umožní získať prístup k citlivým údajom v databáze. Výsledky budeme sledovať cez záznamy v logoch databázy a samotného WAF, kde uvidíme, či WAF útok detegoval a či zabránil vykonaniu nelegitímnych SQL dopytov.

Pri Cross-Site Scripting (XSS) útokoch budeme používať nástroj OWASP ZAP, ktorý umožňuje simulovať vloženie škodlivého kódu do webovej aplikácie. Cieľom XSS je vykonanie skriptov na strane klienta (v prehliadači), čo môže viesť k krádeži cookies, session tokenov alebo iných citlivých údajov.

Pri útoku Sensitive Data Exposure sa zameriame na to, ako aplikácia pracuje s citlivými údajmi, ako sú heslá alebo osobné údaje. Použijeme nástroje ako Burp Suite na zachytenie komunikácie medzi klientom a serverom, aby sme zistili, či sú dáta prenášané v nezašifrovanej podobe, alebo či aplikácia používá zastarané šifrovacie algoritmy. Tieto zraniteľnosti budú sledované v zachytených HTTP požiadavkách a odpovediach, kde budeme hľadať nezašifrované citlivé údaje.

Pri Broken Authentication budeme testovať, či je možné obísť autentifikačný systém aplikácie. Na tento účel využijeme Metasploit Framework, ktorý nám umožní simulovať útoky na prihlásenie, ako napríklad brute-force útoky.

Pre Cookie Poisoning budeme skúšať modifikovať cookies odosielané medzi klientom a serverom, aby sme zmenili užívateľské oprávnenia alebo získali prístup k citlivým častiam aplikácie. Na modifikáciu cookies využijeme OWASP ZAP alebo Burp Suite, pričom budeme analyzovať, či aplikácia správne overuje integritu cookies a či WAF zachytí pokusy o manipuláciu s údajmi.

Každý útok bude dôkladne monitorovaný nielen v logoch aplikácie a servera, ale aj prostredníctvom WAF systému, ktorý by mal zaregistrovať a reagovať na podozrivé aktivity. To nám poskytne prehľad o tom, ako účinná je ochrana, ktorú WAF poskytuje, a kde sú ešte slabiny, ktoré môžeme zlepšiť.

Po úspešnom prelomení ochrany si vysvetlíme, čo útočník môže urobiť, keď získa prístup k systému, a zároveň sa budeme venovať aj opačnej strane – ako sa brániť po úspešnom útoku a aké kroky je potrebné podniknúť na zmiernenie škôd. Po tomto experimente si upravíme pravidlá v našom WAF systéme, aby lepšie reagoval na zistené útoky, a pokúsime sa systém napadnúť opäť. V závere projektu aktualizujeme WAF na novšiu verziu a zistíme, či sú tieto aktualizácie schopné lepšie odolať rovnakým typom útokov.

Záverom si vysvetlíme, ako WAF zapadá do širšieho bezpečnostného konceptu, konkrétne do modelu OSI, a porovnáme WAF s inými bezpečnostnými systémami, ako sú IPS (Intrusion Prevention System) a NGFW (Next-Generation Firewall). Tento projekt poskytne komplexný pohľad na vývoj, fungovanie a efektivitu WAF systémov v reálnych podmienkach.

Časový harmonogram

- Progress report 1: Plánujem mať vypracovanú spomínanú teóriu a preštudované znalosti ohladne WAF, spolu so všetkými porovnaniami. Rozpísaný postup nasadenia WAF na vytvorený server aj s postupom rozbehnutia samotného servera.
- Progress report 2: Preštudujeme a vysvetlíme si konkrétne nástroje za pomoci, ktorých neskôr vykonáme útoky. Taktiež prejdeme si konkrétne útoky na náš server a pozrieme sa na následky týchto útokov. Vyskúšame spomínané útoky na rôznych bránach a budeme meniť nastavenia WAF.

Použité zdroje:

https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF

https://www.imperva.com/learn/application-security/what-is-web-application-firewall-waf/

https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

https://www.f5.com/glossary/web-application-firewall-waf