

# Webový aplikační firewall v praxi

Kamil Golombek, Vladimír Kot

V posledních dvou letech se o aplikační bezpečnosti hovoří stále více a množí se titulky typu „SQL Injection Attack Infects Thousands of Websites“. Rok 2008 rozhodně nebude výjimkou, naopak je odborníky označován spíše za rok aplikační bezpečnosti a očekává se zlom a akceptace tohoto nezvratného faktu širší veřejností.

V naší praxi se velmi často setkáváme s případem, kdy klient řeší zajímavé dilema – má podnikovou aplikaci, kterou nemůže jen tak vypnout. Má výsledky bezpečnostních testů a nahlédl tak do „Alenčiny říše za zrcadlem“. Smluvně definované požadavky na bezpečnost bohužel nemá. A jeho dodavatel se netváří, že by byl ochoten „zdarma“ na základě „takzvané reklamace“ něco opravit, eventuálně to prostě není v jeho silách. Máme tady tvrdý oříšek – cenné aktivum, velké riziko, a nedostatečný rozpočet. Řešení existuje, a to ve formě webového aplikačního firewallu.

## Úvod do bezpečnosti webových aplikací

Bezpečnost webových aplikací stručně řečeno znamená implementaci bezpečnostních prvků a opatření ve webových aplikacích samotných. Zkusme zapomenout na odpovědi typu: je to za firewallem, používáme SSL, běží to na bezpečném OS, aplikovali jsme poslední patche, uživatel musí mít heslo. Nic z toho totiž aplikační bezpečnost primárně neřeší. Tyto prvky podporují celkovou bezpečnost řešení, ale nechrání samotnou aplikaci.

Bezpečnost aplikační vrstvy se dnes zpravidla řeší značně intuitivně, nebo vůbec. Reálným dopadem jsou poměrně vážné bezpečnostní chyby v devíti z deseti

v současnosti provozovaných aplikací. Průměrným výsledkem našich testů je, že hodnocené aplikace obsahovaly pět až devět z tzv. top ten (viz tabulka) chyb dle hodnocení projektu OWASP – Open Web Application Security Project. Tento projekt zahrnuje mnoho různých služeb, především Guide to Building Secure Web Applications and Web Services, dále projekt OWASP Top Ten, testovací nástroje, OWASP Web Application Penetration Checklist a mnoho dalších.

## Webový aplikační firewall – WAF

Ze všech dnes hlášených útoků je zhruba sedmdesát procent cíleno na aplikační

vrstvu. WAF – webový aplikační firewall – dodatečně zvyšuje celkovou úroveň bezpečnosti tím, že dokáže zabránit útokům dříve, než zasáhnou vlastní webovou aplikaci. Poskytuje ochranu před velkou škálou útoků, nabízí monitorování HTTP provozu a jeho analýzu v reálném čase. To vše s minimálním, nebo žádným dopadem na existující infrastrukturu.

WAF funguje tam, kde jsou běžné paketové firewally, většina IDS/IPS nebo třeba SSL akcelerátory neúčinné. Může být implementován jako samostatná aplikační brána (forma reverzní proxy), nebo jako modul k webovému serveru (viz obrázek).

V neposlední řadě lze tvrdit, že WAF je cenově velmi dostupné řešení. Říkat „zdarmo“ by bylo nadsazené, protože stále musíte při jeho implementaci vědět, co děláte, a ovládat použitou technologii. V případě open source řešení [www.modsecurity.org](http://www.modsecurity.org) je možné získat licenci zdarma a je na zákazníkovi, jestli si připlatí za komerční podporu.

V dalším textu, pakliže budou zmiňovány nějaké konkrétní vlastnosti WAF, bude vždy uvažován jako příklad ModSecurity.

## Příklady použití WAF

Možnosti využití je mnoho, mezi nejčastější však patří následující:

- detekce/prevence HTTP útoků a logování,
- rychlé řešení existujících chyb – aplikace workaround řešení,
- „hardening“ webových aplikací.

### 1. Detekce anomálií v HTTP provozu, následná ochrana a logování

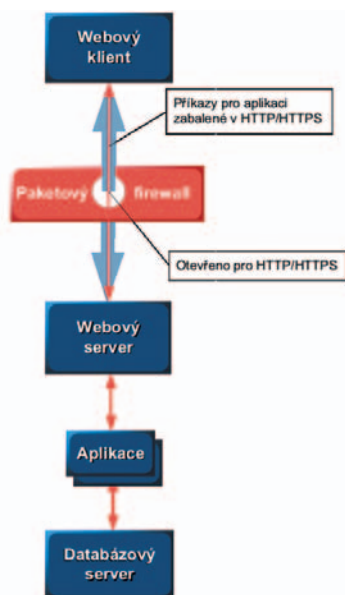
WAF je schopen analyzovat na aplikační vrstvě veškeré náležitosti HTTP protokolu. Je použitelný také pro ochranu tzv. web services. Může analyzovat jak zhlaví, tak tělo dotazů, a to samé platí také pro odpovědi. Proti nejčastějším útokům lze s úspěchem používat dodávaná pravidla, tzv. core rules, pro složitější pravidla je k dispozici jazyk pro definici pravidel. Po vyhodnocení daného pravidla může reagovat jako standardní firewall – od zaholení požadavku přes zobrazení chybového hlášení, přesměrování na tzv. honey-pot až po prosté zalogování události.

### 2. Just-in-time patching

Existují dva základní důvody, proč je nutné, nebo přinejmenším vhodné mít

OWASP Top Ten 2007

A1 – Cross Site Scripting (XSS)	A6 – Information Leakage and Improper Error Handling (Únik informací a neošetřená chybová hlášení)
A2 – Injection Flaws (Chyby na bázi vkládání)	A7 – Broken Authentication and Session Management (Chybná správa sezení a autentizace)
A3 – Insecure Remote File Include (Nezabezpečené vkládání souboru)	A8 – Insecure Cryptographic Storage (Nezabezpečené ukládání)
A4 – Insecure Direct Object Reference (Nezabezpečený přímý odkaz na objekt)	A9 – Insecure Communications (Nezabezpečené komunikace)
A5 – Cross Site Request Forgery (CSRF)	A10 – Failure to Restrict URL Access (Špatná kontrola ACL na URL)



k dispozici rychlé řešení, kterým lze nahradit například bezpečnostní patch nebo nasazení nové verze aplikace. Jedná se o případ, kdy je publikován nový útok a kdy výrobce nebo dodavatel není schopen v krátké časové době připravit a distribuovat opravu. Například v nedávné době populární XSS útoky v rámci PDF souborů. Druhým důvodem je objevení bezpečnostní chyby v rámci vlastní provozované aplikace, kdy může být problém realizovat rychlou nápravu bez důkladnějšího studia chyby. Příkladem může být chyba v administračním rozhraní, které je určené jak pro externí, tak interní uživatele. Dočasným řešením může být povolení této funkce pouze pro interní administrátory, kteří jsou považováni za důvěryhodné, při zachování zbylé funkcionality.

### 3. „Hardening“ webových aplikací

V neposlední řadě může být WAF poslední záchrannou brzdou, pakliže dodavatel, respektive vývojář, prakticky netuší, co znamenají zkratky a termíny jako XSS (cross site scripting) či SQL injection. Validaci dat a jejich jednotné kódování považuje za zbytečné a bezpečnost chápe jako použití SSL protokolu. V tomto případě opravdu není reálné počítat s tím, že by něco dokázal opravit a náhrada aplikace ze dne na den není většinou možná. Neznamená to, že by tímto způsobem šlo docílit stoprocentní bezpečnosti. Pro odstranění chyb v obchodní logice WAF většinou použít nelze.

#### Co dokážou dnešní WAF v základním nastavení?

Protokol HTTP, kterým spolu aplikace komunikují, a HTML jazyk, ve kterém se předávají odpovědi, dovolují velmi širokou škálu možných kódování. Počet možných zápisů jde už u velmi krátkých URL až do řádu milionů. Tato rozmanitost dělá problémy při kontrole vstupu v aplikacích. WAF si dokáží s problémem kódování poradit převodem na definovaný formát a tím ulehčit práci vlastní aplikaci.

Součástí dodávky WAF bývá připravený soubor se základními pravidly. Tato pravidla slouží pro kontrolu anomálií a zachycení útoků proti HTTP protokolu, omezují přístup k různým typům souborů, čímž chrání špatně konfigurované webové servery, zaznamenávají aktivitu různých robotů prohledávajících internet a chrání před útoky známých trojských koní. Existují i speciální pravidla, která vyhodnocují obsah odesílaných webových stránek

a zabraňují tak úniku informací v situaci, kdy dojde k pádu aplikace nebo vypsání neošetřené standardní chybové hlášky. Na rozdíl od klasických paketových firewallů je možné WAF začít používat ihned po vybalení z krabice, podobně jako například antivirové programy. Tedy minimálně v anglickém prostředí, protože české znaky díky často špatnému řešení kódování vytvářejí tzv. false positives.

Pro usnadnění konfigurace jsou WAF vybaveny módem pro učení, který umožňuje sledovat efekt použitých pravidel na procházející provoz, aniž by fakticky docházelo k jeho ovlivňování. ModSecurity používá textový zápis pravidel, podobně jako open source IDS systém Snort. Použití textového zápisu usnadňuje konverzi pravidel a čerpání z denně aktualizované databáze pravidel, jako například projekt Bleeding Edge Threats.

#### Závěr

Proč tedy používat webové aplikační firewally? Webové aplikace jsou v současnosti nasazovány neuvěřitelně nezabezpečené. Takže i když by se vývojáři měli stále pokoušet o kvalitnější a bezpečnější kód, provozovatelé musí něco udělat. Jinými slovy potřebují každou dostupnou pomoc. WAF by měl být klíčovou součástí každé sítě s HTTP provozem. ■

Autoři článku působí ve společnosti BDO IT, která se zabývá poskytováním poradenských služeb v oblasti informačních technologií s důrazem na informační bezpečnost.

Inzerce

## Aplikační testy

BDO provádí kompletní škálu testů na všech úrovních aplikací - od jednoduchých webových prezentací až po internetové bankovníctví či provázané systémy a registry veřejné správy.

Odborníci BDO Vám pomohou prověřit bezpečnost Vašich aplikací s využitím svých několikaletých zkušeností v oboru.

**BDO**

BDO IT a.s.  
Auditorská a poradenská společnost

www.bdo-it.com, tel.: 241 046 111