Was eine WAF (nicht) kann.
Ausgabe 2013

Mirko Dziadzka

http://mirko.dziadzka.de/
@MirkoDziadzka

OWASP Stammtisch München - 19.11.2013

Inhalt

Worum soll es heute gehen

- Meine (subjektive) Meinung
  - was eine WAF können sollte
  - was eine WAF weniger gut kann
- Offen für andere Meinungen und Diskussion

DISCLAIMER

- Ich arbeite für einen WAF Hersteller
- Ich gebe hier meine Meinung wieder
- das ist nicht notwendigerweise auch die Meinung meines Arbeitgebers.

Wer bin ich - Kurzfassung

- Old School Unix Geek, currently interested in
  - IT-Security
  - Software Development
  - Unix
  - Python
  - Distributed Systems

Wer bin ich - Kurzfassung

- 80er: Studium Mathe/Informatik
- 90er:
  - System- und Netzwerkadmin
  - Dozent: Unix und Security
  - Autor: Linux Kernel Programmierung
- ab 1999: Entwicklung + Betrieb im Schweizer Bankumfeld.
  - unter anderem Implementation von Web-Input-Filtern und Authentisierungs-Proxies
- seit 2005 bei art of defence / Riverbed in Regensburg

Was ist eine WAF

Was ist eine WAF

Definition - from the OWASP website [OWASP, 2013]

1. A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation.
2. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection.
3. By customizing the rules to your application, many attacks can be identified and blocked.
4. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

Was ist eine WAF nicht

Definition - Ergänzung von mir

1. unabhängig von der Applikation
2. kein B2B XML Gateway

Grundfunktionalität

Request Validierung

- Blacklist - Bekannte Angriffe
  - meist musterbasiert (in der Regel regex)
  - ähnlich einem Virenscanner
  - teilweise parser basiert ([libinjection, 2012])
- Whitelist - was ist ungefährlich
  - allgemein
  - applikationsspezifisch

Grundfunktionalität

Response Validierung

- Data protection (cookies, ...)
- Data leakage (erkennen von KK Nummern, etc)
- Fehlermeldungen (Stacktrace, SQL-Error)
- Aber auch: nachträgliches Erkennen von Angriffen
- Aber auch: Malware detection (outgoing virus scanner)

Weitergehende Features

Session Handling

- WAF kann eine ganze UserSession verfolgen
- Cookie protection
- Auto learning / auto whitelisting
- control flow enforcement / anti-deep-linking

Weitergehende Features

Authentisierung / Autorisierung

- WAF als zentraler Punkt für single-sign-on
- selbst wenn es die Applikationen nicht unterstützen
- Integration mit verschiedenen Authentication platforms

Weitergehende Features

(Halb)-Automatische Regelwerkerstellung

- Support bei der Erstellung des Regelwerkes
- Lernmodus
- Regelwerk refinement (one click false positive fixing)
- Anbindung an externe Security Scanner
  - Erzeuge Hot-Patching Regeln als Ergebnis von Security Scans

Weitergehende Features

Reaktion auf Angriffe

- Limitierung des Zugriffs auf 'teure' Resourcen
  - Limitierung der login Versuche pro IP und Zeit
- Automatische Reaktion auf Angriffe (IP Blacklist)

Probleme

Input Interpretation

Input Interpretation

- WAF und Applikationen interpretieren den Request.
  - Identisch?
- Standard versus ad-hoc implementation
- Zum Beispiel: multipart header (Beispiel von 2009)

Input Interpretation

Multipart interpretation (standard view)

```
POST /test.php HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (...) Gecko/1234 Firefox/3.5.3
Content-Length: ...
Content-Type: multipart/form-data; boundary=----,xxxx

------,xxxx
Content-Disposition: form-data; name="img";
                                filename= "img.gif"

GIF89a...
------
Content-Disposition: form-data; name="payload1"

...
```

(example from 2009: [Esser, 2009])

Input Interpretation

Multipart interpretation (PHP view)

```
POST /test.php HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (...) Gecko/1234 Firefox/3.5.3
Content-Length: ...
Content-Type: multipart/form-data; boundary=----,xxxx

------,xxxx
Content-Disposition: form-data; name="img";
                                filename= "img.gif"

GIF89a...
------
Content-Disposition: form-data; name="payload1"

...
```

(example from 2009: [Esser, 2009])

Input Interpretation

Andere Interpretationsprobleme

- Zeichensatz (wenn der Browser ihn nicht deklariert)
- kaputtes / fehlendes Encoding
  - Kunde: aber ohne die WAF geht es doch
- Wie und wie oft dekodiert die Applikation die Daten? Was soll denn die WAF jetzt genau unsersuchen?

WAF muss Applikation verstehen

Unbekannte Protokolle

Unbekannte Protokolle

- Die Zeit des standardisierten Encodings geht zu Ende
- AJAX mit XML/JSON waren die ersten Schritte
- Websockets werden noch mehr applikationsspezische Protokolle fahren

WAF muss Applikation verstehen

False Positives

False positives

- Die meisten Anwender werden 'false positives' um jeden Preis vermeiden
- Umsomehr, wenn die Anfragen von Google kommen
- 'kritische' IP Addressen werden auf die whitelist gesetzt

False Positives

ars technica

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

Google crawler tricked into performing SQL injection attacks using decade-old technique

Let the search engine do the dirty work with carefully crafted links.

by **Peter Bright** - Nov 7 2013, 2:05am CET

HACKING 56

Daniel Cid, a developer of a cloud-based firewall/proxy system, was surprised to discover that his product was blocking requests from Google-owned IP addresses. This was unusual, because few websites want to block Web crawlers, as search engines are so important as a method of site discovery. Cid and his colleagues strive to make sure that their product's default rules *don't* block Google.

The Google IP address was determined to be legitimate: the traffic was from a Google Web crawler. It was being blocked because it appeared malicious, like it was an attempt at SQL injection. Further examination of the firewall logs showed other, similar requests from Google IP addresses also being blocked.

(taken from : [ArsTechnica, 2013])

Auswahlkriterien

Brauche ich eine WAF und wenn ja welche?

Auswahlkriterien

Auswahlkriterien für eine WAF

- Da gibts doch was von OWASP ... [OWASP, 2008]
- Einsatzzweck (brauch ich eine und wenn ja welche)
- Management
  - Einzelinstallation oder Cluster
  - Verschiedene Admins, Permission, ...
  - Nachvollziehbarkeit (audit), Rollback
  - logs, stats
  - nice GUI vs. automatisierbarkeit
  - Welche Skillset habe ich bei den Administratoren

Auswahlkriterien

Auswahlkriterien für eine WAF

- Skalierbarkeit
  - cluster with 10x the current machines
  - Amazon Cloud
  - multiple sites with central administration

Weiterführendes

ArsTechnica (2013).

Google crawler tricked into performing sql injection attacks.

http://arstechnica.com/security/2013/11/google-crawler-tricked-into-performing-sql-injection-attacks-using

Esser, S. (2009).

Shocking news in php exploitation.

http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pdf.

libinjection (2012).

https://libinjection.client9.com.

OWASP (2008).

Best practices: Use of web application firewalls.

https://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls.

OWASP (2013).

https://www.owasp.org/index.php/WAF.

Danke für's zuhören

Fragen?