Web Application {Security, Firewall}

Mirko Dziadzka
mirko.dziadzka@gmail.com
http://mirko.dziadzka.de
18.1.2011 / IEEE SB Passau

Alle Abbildungen aus
http://www.heise.de/newsticker/archiv/

Inhalt

- Kurze Einführung in das Gebiet der Web Application Security
  - Welche Probleme gibt es, was kann man dagegen tun
  - Was sind Web Application Firewalls
- Standard-Disclaimer:
  - Ich arbeite für einen WAF Hersteller
  - Ich gebe hier meine Meinung wieder

Wer bin ich?

- Studium Mathe / Informatik
- 93-2003, 2010 Vorlesung Unix + Security
- Seit 12 Jahren im Umfeld
  - Beratung / Entwicklung / Betrieb
  - Security / Scalability / Unix / Netze

Probleme mit HTTP

- HTTP ist das Haupteinfallstor in die Firma, Angriffe über HTTP haben die meisten anderen Angriffsklassen abgelöst
- Angriffe auf den Web-Browser
- Angriff auf den Web-Server bzw. die Web Applikation

Probleme mit HTTP

- Wurde für das ausliefern statischer Dokumente entworfen
- Kein State, keine Session, keine Authentisierung
- Vorhandene Securitymodelle im Browser sind Broken (“same origin policy”)

Angriff auf Webbrowser

- Angriffsvektoren
  - Browser (DOM Implementation , Java-Script)
  - Flash, Java, Image / Video / externe Formate
  - Trustmodell: Der Benutzer vertraut ~~der Webapplikation~~ den Daten, die er via HTTP bekommt

Angriffe auf den Webbrowser

News-Meldung vom 15.01.2010 09:32 « Vorige | Nächste »

Alert! Angriffe auf Google und Co. durch bislang unbekannte Lücke im Internet Explorer

vorlesen / MP3-Download

Ersten Analysen des Antivirenherstellers McAfee zufolge nutzten die vermutlich chinesischen Angreifer bei ihrem Einbruch eine bislang unbekannte Sicherheitslücke im Internet Explorer aus. Die Lücke findet sich in den Versionen 6, 7 und 8 und lässt sich missbrauchen, um über eine manipulierte Webseite Code in einen Windows-Rechner zu schleusen und zu starten. Die Angreifer nutzten dies, um einen Trojaner-Downloader in den angegriffenen Rechner zu schleusen. Der lud wiederum über eine SSL-gesicherte Verbindung weitere Module von einem Server nach, unter anderem eine Backdoor, mit der die Angreifer aus der Ferne Zugriff auf den Rechner hatten. Die Links zu den präparierten Webseiten wurden wohl an ausgesuchte Mitarbeiter in den jeweiligen Firmen per Mail gesendet.

Angriffe auf den Webbrowser

- Was kann man tun?
  - Gehirn einschalten
  - aktuellen gepatchten Browser benutzen
  - Kein Flash, kein Java, kein PDF, ...
  - Firefox: Noscript, Safari: ClickToFlash
  - Browser in Sandbox laufen lassen

Angriffe auf Web Applikationen

- Sehr vielfältig, dass Angriffstor 'Port 80' ist in der Regel offen.
- Klassische Firewall (Port-basiert) hilft hier nicht.
- Klassifizierung der Angriffstypen nach OWASP

OWASP

- Open Web Application Security Project
- http://owasp.org
- OWASP is a ... worldwide ... organization focused on improving the security of application software. Our mission is to make application security visible, so that people ... can make informed decisions about true application security risks.
- Einfluss auf Standards wie PCI-DSS, ...

OWASP TOP 10

- A1: Injection
- A2: Cross-Site Scripting
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object Reference
- A5: Cross Site Request Forgery

OWASP TOP 10

- **A1: Injection**
- A2: Cross-Site Scripting
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object Reference
- A5: Cross Site Request Forgery

OWASP A1: Injection

- "Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data."

OWASP A1: Injection

- In der Regel als SQL Injection
- Fehlende Eingabeüberprüfung bzw. falsches Quoten sorgt dafür, das Nutzereingaben (Daten) als SQL Code interpretiert werden
- Der Bufferoverflow des Web Zeitalters

SQL Injection

- http://broken.com/user?id=42
- $query = "SELECT * FROM user_t WHERE id=$id"
- Angreifer: http://broken.com/user?id=42;UPDATE%20user_t%20SET%20role=admin%20WHERE%20id=23
- Eingabevalidierung!

News-Meldung vom 01.12.2010 14:19

« Vorige | Nächste »

GNU-Server erneut gehackt

vorlesen / MP3-Download

Unbekannte haben sich offenbar Zugang zu einem Server des GNU-Projekts verschafft. Derzeit ist das Web-Interface auf Savannah offline; der Server zeigt nur eine kurze Zusammenfassung des aktuellen Status an.

Der betroffene Savannah-Server der FSF dient als Download- und Entwicklungszentrale für GNU- und andere freie Software. Offenbar gelang es Unbekannten, sich via SQL-Injection eine Liste verschlüsselter Passwörter zu verschaffen. Einige davon ließen sich wahrscheinlich via Brute-Force knacken, sodass die Angreifer Zugriff auf die zugehörigen Projekte erhielten. Dies nutzen sie anscheinend für nicht weiter spezifizierten "Vandalismus". Laut den Betreibern gibt es keine Anzeichen, dass der Root-Account des Servers kompromittiert wurde.

Webseiten-Massenhack richtet sich gegen Online-Spieler

vorlesen / MP3-Download

Die seit rund einer Woche registrierten Massenhacks von Webseiten haben neuesten Analysen zufolge zum Ziel, Online-Gamern die Zugangsdaten für Spiele zu stehlen. Prominenteste Opfer der Hacks waren das Wall Street Journal und die Jerusalem Post.

Bei den Webservern handelt es sich zwar durchgehend um Systeme auf Basis von Microsofts Internet Information Server (IIS) und ASP.NET, den Untersuchungen mehrerer Sicherheitsdienstleister zufolge manipulierten die Angreifer die Webseiten aber offenbar über SQL-Injection-Schwachstellen in den selbst geschriebenen Webanwendungen der Betreiber. Administratoren sollten ihre Systeme auf mögliche Manipulationen überprüfen.

Durch die SQL-Injection-Schwachstelle waren (und sind) die Angreifer in der Lage, eigenen HTML-Code und JavaScript in die Datenbank des Content Management Systems (CMS) zu schreiben. Konkret betteten sie Code ein, der in einem iFrame einen Exploit für eine seit über einer Woche bekannte Lücke im Flash Player nachlädt. Darüber versuchen die Kriminellen, die PCs von Besuchern mit Trojanern zu infizieren. Der hat vermutlich zum Ziel, die Zugangsdaten zu asiatischen Spieleseiten wie aion.plaync.co.kr, aion.plaync.jp und df.nexon.com zu stehlen. Die Lücke im Flash Player ist in Version 10.1 geschlossen.

OWASP TOP 10

- A1: Injection
- **A2: Cross-Site Scripting**
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object Reference
- A5: Cross Site Request Forgery

A2: Cross Site Scripting

- Eine Benutzereingabe wird ohne korrektes Quoting wieder in der HTML Ausgabe benutzt:
  - http://broken.app/?user=foo
  - <html>....<p>Hallo $user<body></html>
  - http://broken.app/?user=<scipt>alert ("huhu");</script>
  - Gerne übersehen werden Fehlerseiten ...

OWASP TOP 10

- A1: Injection
- A2: Cross-Site Scripting
- A3: Broken Authentication and Session Management
- **A4: Insecure Direct Object Reference**
- A5: Cross Site Request Forgery

News-Meldung vom 29.10.2009 10:34 « Vorige | Nächste »

Libri lässt Kundenrechnungen offen im Netz liegen

vorlesen / MP3-Download

Durch eine Lücke im System des Online-Buchhändlers Libri.de war es jedermann möglich, online unautorisiert mehrere tausend Rechnungen von Kunden einzusehen. Das berichtet netzpolitik.org. Zum Abruf genügte es, in der URL der online als PDF hinterlegten Rechnungen einfach die Rechnungsnummer zu variieren – die einfach durchnummeriert waren. Auf diese Weise konnten die Mitarbeiter von netzpolitik.org per Skript in einer halben Stunde rund 20.000 Rechnungen herunterladen.

Die Rechnungen enthielten die Kundenadresse, das Kaufdatum, die gekauften Produkte, Preis, Rechnungsnummer, Kundennummer und die Bezahlweise (jedoch keine Bankdaten) sowie den Partner vor Ort. Libri arbeitet nämlich auch als Dienstleister für viele stationäre Buchhändler und andere Online-Shops. Durch das Herunterladen und Auswerten der Rechnungen ließe sich laut Bericht nachvollziehen, wer welche Bestellungen in der letzten 16 Monaten über Libri getätigt hat.

News-Meldung vom 03.11.2009 11:58 « Vorige | Nächste »

Zugriff auf Rechnungen im Sparkassen-Shop möglich [Update]

vorlesen / MP3-Download

Nach Libri hat nun den Deutschen Sparkassenverlag (DSV) ein Datenschutzproblem mit Kundenrechnungen ereilt. So konnten angemeldete Nutzer die Rechnungen anderer Kunden durch Ändern einer bestimmten ID einsehen. Das berichtet netzpolitik.org.

Anders als bei Libri genügte dazu allerdings nicht das simple Manipulieren der URL im Browser. Vielmehr war das Ändern der ID-Variablen im POST-Request eines Formulars notwendig – das lässt sich aber beispielsweise mit speziellen Web-Proxies oder dem Firefox-Plug-in Firebug bewerkstelligen. Mitarbeiter des Newsdienstes netzpolitik.org hatten auf diese Weise nach eigenen Angaben Zugriff auf fast 350.000 Rechnungen im Sparkassen-Shop.

Fehlerquellen

- Validierung der Eingabe
- Kodierung der Ausgabe
- Zugriffskontrolle
- logische Probleme, Kryptography, ...

Lösungen

- Erst gar keine Fehler einbauen
- Softwareentwicklungskultur, Schulungen, Awareness (auch ein Ziel von OWASP)
- Qualitätssicherung
- ständige externe Reviews

Lösungen

- Fehler finden und entfernen
  - Source Code review
    - per Tool oder manuell
  - Penetration Test
    - per Tool oder manuell
- Tools finden nur bestimmte Probleme, z.B. SQL-Injection aber keine Logik Fehler

Lösungen

- Wenn wir akzeptieren, das Fehler vorhanden sind:
- Ausnutzung der Fehler verhindern, Angriffe vorher abfangen
- Web Application Firewall

Was ist eine WAF?

- OWASP: "eine Schutzlösung auf Webanwendungsebene, die technisch nicht von der Anwendung selbst abhängig ist."
- Eine Komponente, die den Datenverkehr zwischen Browser und Webapplikation untersucht, ggf. ändert oder blockiert.
- Unabhängig von der Applikation
- Kein B2B SOAP Filter

Deployment

- Reverse Proxy / Transparent Proxy
- Plugin in Firewall / Loadbalancer / Webserver
- Plugin in Application Server
- Plugin in Applikation

Funktionalitäten

- Request-Filterung
  - Blacklist - Bekannte Angriffe (ähnlich einem Virenscanner)
- Whitelist - was ist ungefährlich
  - Allgemein
  - Applikations-spezifisch

Funktionalitäten

- Response Filterung
  - Data Leakage (keine KK-Nummern)
  - Fehlermeldungen (Stackdump, SQL Error Meldungen)
  - Nachträgliches erkennen von Angriffen oder Angriffsversuchen
  - Malware Detection

Funktionalitäten

- Sessions
  - Sichere Session zw. Browser und WAF
  - Setzt mehrere Requests in Verbindung
  - Bestimmung gültiger Daten
    - auto-whitelist
    - URLs, Formularfelder, Cookies, ...

Funktionalitäten

- Authentisierung, Autorisierung
  - von Benutzern
    - zentrale Authentisierung, SSO
    - Applikationsunabhängig
  - von IP Addressen

Funktionalitäten

- Normalisierung der HTTP Requests
  - IMHO: Nein, WAF soll Entscheidungen fällen und nicht kaputtes HTTP eines Clients reparieren
- Aber: Sinnvoll, damit WAF und Applikation dieselbe Sicht auf die Daten haben (zum Beispiel bei der Interpretation von Multipart-Mime Headern)

Warum braucht es eine WAF?

- Das kann man doch alles in der Applikation lösen?

- Ja, aber.

  - Applikation nicht änderbar, hot patching, PCI compliance, Zweites Sicherheitsnetz

  - Neue Funktionalität

Administration

- Ziele: Einfachheit und Nachvollziehbarkeit
- Versionierung des Regelwerks, Rollback, Audit-Log (Nachvollziehbarkeit)
- Optional: Granulares User und Rechtekonzept
- Optional: Clustermanagement
- Logview, Statistiken, Reports, Alerting, ...

Regelwerkerstellung

- Mitgelieferte Blacklists a.k.a. Grundschutz
- Hilfe bei der Erstellung von Whitelists passend zu den Applikationen
- Einstellung anderer Funktionalitäten:
  - Cookie Protection, Formular Protection, ...
- Regelwerk testen (wie mache ich das?)

Probleme

- Encoding / Charset
  - Der Browser deklariert nicht(!) in welchem Zeichensatz die reinkommenden Bytes zu interpretieren sind, die Web-App und die WAF müssen raten.
- Die WAF muss an die Applikation angepasst werden.

Probleme

- Interpretation von Standards
  - ~~Multipart-Mime (siehe Beispiel)~~
  - Web ist von Anfang an "schwammig" definiert, die Parser für HTTP sind "programming by example."
  - Es gibt eine Teilmenge des Standards, die von allen gleich verstanden wird.

Probleme

- Die WAF braucht ein Modell der Applikation
  - Applikationen können WAF und WAF-Admin freundlich sein oder nicht
  - korrektes HTML
  - Variablennamen, die etwas aussagen und konsistenz über die ganze Applikation sind
  - URLs die unterscheidbar sind vs. index.php

Probleme

- Das Thema Performance hängt immer vom Regelwerk mit ab.
- Eine WAF ist kein "Ein Klick und ich bin sicher" Gerät, die Konfiguration ist deutlich komplexer als die einer klassischen Firewall.

Performance

- Selber messen! Je nach Deployment, braucht man andere Werte.
- Wie kann ich skalieren wenn meine App um den Faktor 10 mehr Benutzer bekommt? Faktor 100?

Fragen?

Propaganda

- art of defence GmbH in Regensburg sucht:
  - Diplomanden, Praktikanten, Berufseinsteiger, Spezialisten, ...
  - Softwareentwicklung (Python, Java, C, Unix, ...)
  - Pen-Testing / Consulting / Support
  - mail: info@artofdefence.com