Wie überprüfe ich die Sicherheit meiner Website?

Intention

Dieses Pattern beschreibt gängige Methoden, die verwendet werden, um die Sicherheit einer Website zu testen.

Problemstellung

Um die Sicherheit des eigenen Computers zu gewährleisten verwenden viele einen Virenscanner. Selbiges kann natürlich auch auf einem Webserver verwendet werden. Webserver bieten, je nach Konfiguration, unterschiedlich viele Angriffsvektoren die ausgenutzt werden können. Daher müssen viele Punkte bei der Überprüfung der Sicherheit, der eigenen Seite und des Servers, auf dem die Seite liegt, beachtet werden.

Szenario

Die Sicherheit der eigenen Seite muss überprüft werden, um den Websitebesuchern eine gute und sichere Surferfahrung zu bieten.

Lösung

- Prüfen ob die Seite eine verschlüsselte Kommunikation anbietet
    - Mehr Informationen hierzu findet man im Pattern: „**Wie verschlüssele ich die Kommunikation mit meiner Website?**“.
- Viren- und Malware-Scanner über die Dateien auf dem Server laufen lassen, vor allem, wenn es Seitenbenutzern erlaubt ist eigene Dateien hochzuladen. Einige Webhoster bieten ein Zusatzservice an, die diesen Punkt abdecken.
- Überprüfung der MD5-Prüfsummen bei Software die auf dem Server installiert werden soll.
- Verwendung eines ScanTools um die Sicherheit und Features der Seite von einem Drittanbieter testen zu lassen
    - Nach einem Scan werden mögliche Angriffsvektoren und Sicherheitsprobleme aufgezeigt. Oftmals wird beschrieben worin Probleme liegen und wie man diese lösen kann.
- Namen der URL / Domain überprüfen
    - Wenn Websitebesucher beim Eingeben der *URL* häufig Fehler machen, sollte man den Namen unter Umständen überdenken. Dies könnte bei Namen passieren, die ähnlich zu anderen bekannten Seiten sind.

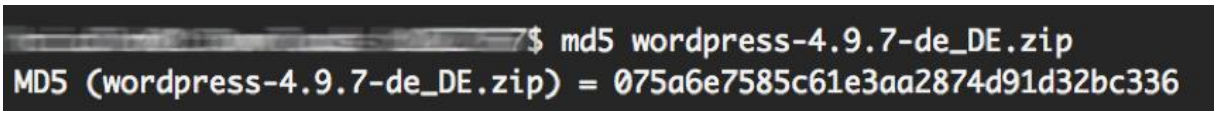
- Cyberkriminelle verwenden oft ähnlich geschriebene Webadressen für Phishing. Im Falle von amazon.com gab es beispielsweise die Variante amaz0n.com (man beachte, dass hier eine Null statt dem Buchstaben „o“ verwendet wird). Diese Seite kann auf eine Seite verweisen, die zwar ähnlich aussieht, jedoch dazu genutzt wird Daten zu stehlen oder *Schadcode* zu verbreiten.
- Auf *Punycode* Domains achten:
  - https://www.xudongz.com/blog/2017/idn-phishing/
  - https://www.golem.de/news/domain-erneut-angriff-ueber-punycode-domains-demonstriert-1704-127353.html

Beispiele

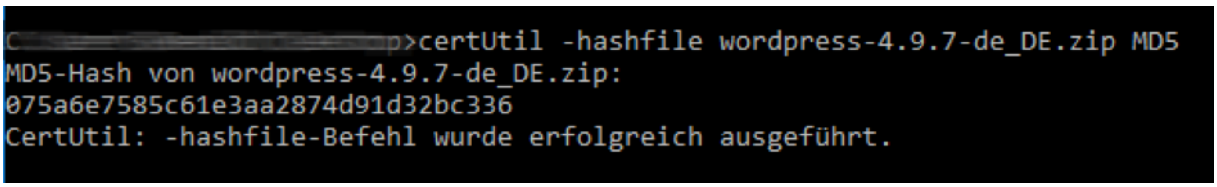
Checken von Prüfsummen (anhand von MD5)

Es gibt verschiedene Arten von Prüfsummen. In diesem Beispiel gehen wir auf die MD5 Prüfsumme einer WordPress Installationsdatei ein. Beim Klicken auf MD5 erscheint folgende Prüfsumme: **075a6e7585c61e3aa2874d91d32bc336**. Nachdem die Datei heruntergeladen wurde, kann man mit folgendem *Kommandozeilenbefehlen* die Prüfsumme der Datei anzeigen lassen.

macOS



Windows



Wenn die Prüfsumme der Datei mit der Prüfsumme von der WordPress Seite identisch ist, kann man sicher gehen, dass diese nicht verändert wurde und damit ist die Datenintegrität gewährleistet. Mehr Informationen zum Überprüfen von verschiedenen Prüfsummen (Checksums) in einer UNIX-Umgebung findet man hier: https://itsfoss.com/checksum-tools-guide-linux/.

Ähnlich geschriebene URLs erwerben
Um Phishing mit ähnlich aussehenden Seiten sowie ähnlich geschriebenen URLs zu erschweren, würde es Sinn machen ähnlich geschriebene Domains zu kaufen und diese dann auf die eigene Seite verweisen zu lassen. Ein Beispiel dafür ist gogle.com, diese URL verweist auf google.com.

Sicherheitscheck der Mozilla Foundation für beliebige Websites
Nach Eingabe der URL und einiger Optionen werden sicherheitsrelevante Konfigurationsdaten anzeigt.

- https://observatory.mozilla.org

SSL-Labs führt eine **tiefe Analyse der Website-Konfiguration für jegliche SSL-Webserver** im Internet aus. Es wird vom Anbieter darauf hingewiesen, dass dieser Service rein zur Information dient und nicht für kommerzielle Zwecke verwendet wird.

- https://www.ssllabs.com/ssltest/
- https://www.virustotal.com/de/
- https://www.htbridge.com/websec/

Wichtig: Es wird darauf hingewiesen die Nutzungs- und Datenschutzbedingungen der jeweiligen Anbieter zu beachten.

Referenzen

https://www.heise.de/ix/meldung/Mozilla-bringt-kostenlosen-Sicherheitstest-fuer-Websites-3306197.html
https://security.stackexchange.com/questions/245/does-a-webserver-need-an-antivirus-software-installed

Keywords

Sicherheit, Integrität, ScanTool, Malware