UNIVERSITÄT SIEGEN

Lehstuhl IT-Sicherheitsmanagment
Prof. Dr. Kesdogan

Exercise 1: Webfoo

Der Begriff "Internet" wird von vielen Menschen heute synonym zu "Word Wide Web", kurz "WWW" gebraucht. Diese umgangssprachliche Ungenauigkeit offenbart die Wichtigkeit der Webdienste.

Bitte tragt euch in die Mailingliste `ss12-hacker@listserv.uni-siegen.de` ein. Lösungen zu den Übungsaufgaben werden bitte an die Adresse `fischer@wiwi.uni-siegen.de` geschickt. Im Mailheader muss sich müssen sich die Felder "USI-Course: HC12 Exercise X" und "X-Participant: YYYYY" befinden, wobei X durch die Aufgabennummer zu ersetzen ist und YYYYY durch der Nickname, der innerhalb des Kurses verwendet wird. Die Lösung befindet sich in einer einzelnen Datei im Anhang der Mail. Der Anhang ist immer ein tar-Archiv, gegebenenfalls komprimiert. Das Archiv enthält allen Quellcode, Ergebnisse und den oder die Reports. Alle Abgabe-Emails sind PGP/GPG-signiert, wobei nur der Schlüssel verwendet wird, der zu Anfang veröffentlicht wurde.

Reporting

Die Form der Abgabe ist das Security Advisory. Der Report soll sich dabei an den geforderten Teilen des Common Announcement Interchange Format[1] (CAIF) orientieren. Das Format der Abgabe ist jeweils txt (utf-8 oder ascii), XML, oder pdf. Die Einzelnen verwenden dabei die CAIF Bezeichnungen, insbesondere Abschnitt 8. Im Gegensatz zu CAIF sind aber insbesondere "description" und der Punkt "solution" wichtig und nicht optional.

Aufgabe 0: Arbeitsbereitschaft herstellen

1. Drucke den Fingerprint deines PGP-Schlüssels, den du für die Veranstaltung verwenden willst, zusammen mit deinem Nick und deiner Matrikelnummer aus, und gib diesen Ausdruck in Raum H-C 8329/3 ab.

2. Als Arbeitsumgebung empfiehlt es sich einen vorgepackten Werkzeugkoffer[2] zu besorgen (bis man seinen eigenen Koffer packen kann).

3. Generiere einen privaten Schlüssel und eine Zertifikatsanfrage[3]. Letztere sendest du an `fischer@wiwi.uni-siegen.de`. Du erhältst im Gegenzug ein Zertifikat, mit dem du Zugang zum VPN[4].

4. Melde dich mit der Konfiguration, die du erhalten haben wirst im VPN an.

[1] `http://cert.uni-stuttgart.de/projects/caif/`
[2] Die Distribution Backtrack in einer eigenen virtuellen Maschine zum Beispiel.
[3] siehe "PKCS#10 certificate request"
[4] OpenVPN-client gleich installieren

UNIVERSITÄT SIEGEN

Lehstuhl IT-Sicherheitsmanagment
Prof. Dr. Kesdogan

Aufgabe 1: Most insecure Webservice

Unter `http://imshare.itsec-siegen.info` erwartet euch eine Webanwendung, die maximal unsicher programmiert ist. Eure Aufgabe ist es dort mindestens

1. ein Script auf der Webseite zu hinterlassen, dass bei jedem Aufruf der Webseite ein Alarmfenster mit eurem Nicknamen auftauchen lässt.
2. die Datei im Scriptverzeichnis auszulesen, deren Name mit "S" anfängt und mit "T" aufhört. Als ersten Schritt zum üben, könntest du eine Liste aller Nutzer des Webservers erstellen.
3. den Status Administrator des Webservices zu erlangen (bitte nicht alle Nachrichten löschen).
4. einen Link in einer Nachricht unterbringen, der alle Nachrichten löscht, sobald ihn ein Administrator anklickt.
5. logge dich als Nutzer 'p' ein und verfasse als dieser Benutzer einen Post mit deinem Nick im Beschreibungstext.

Stichworte, die euch auf diesem Weg helfen können sind Cross-Site-Scripting (XSS), Path Traversal, Cross-Site-Request-Forgery (CSRF) und HTTP-Header, und ein wenig SQL kann auch nicht schaden. Empfehlenswert ist die Lektüre von `https://www.owasp.org/`.

Die Bewertung wird mit einer gewissen Zeitkomponente bedacht. Nach ungefähr einer Woche werden weitere Informationen zur Implementation geleaked. Natürlich gibt es Bonuspunkte für Advisories, die uns früher erreichen. Ausschlaggebend ist der Eingangsstempel.

Kontakt: `fischer@wiwi.uni-siegen.de`