Projekt Systementwicklung SS 2017 - Aufgabe 4

Dieses Praktikum besteht aus zwei Teilen. Den Vorbereitungsteil müssen Sie eigenständig fertig stellen und zu Beginn des Praktikums abnehmen lassen. Den Präsenzteil müssen Sie im Laufe des Praktikums erstellen und zum Ende der Praktikumsstunde abnehmen lassen.

Vorbereitungsteil 1

In dieser Aufgabe sollen Sie Ihrem Server Authentifizierung über Benutzername und Passwort beibringen. Greifen Sie dazu z.B. auf

https://www.its.fh-muenster.de/praktika/_aufgaben/

zu und schauen Sie sich im Burp-Proxy an, welche HTTP-Header (`WWW-Authenticate-Header` [0]) der Server schickt, damit der Browser das Popup-Fenster öffnet, in das Sie dann Benutzername und Passwort eintragen. Geben Sie hier den Benutzernamen ‚`test`' und das Passwort ‚`test`' ein und beobachten Sie das Ergebnis im Burp-Proxy. Es erscheint ein neuer Header im HTTP- Request wie folgt:

```
Authorization: Basic dGVzdDp0ZXN0
```

Der hintere Teil ist im base64-Format kodiert (siehe den „Decoder"-Tab in Burpsuite). Dekodieren Sie den Base64- String in Ihrem HTTP-Server und geben Sie die darin verborgenen Daten wie folgt über `printf` auf der Standardausgabe aus:

Benutzer: test
Passwort: test

Sie können hierfür die Base64-Implementierung von https://git.fh-muenster.de/schinzel/PSE2017-Test/blob/master/base64.c verwenden.

Abnahme

Zeigen Sie, dass Ihr HTTP-Server die über Basic-Authentication empfangenen Benutzernamen und Passwörter korrekt auf der Standardausgabe ausgibt. Ungültige Eingaben muss der Server wie ungültige Zugangsdaten behandeln.

Präsenzteil

Ihre Aufgabe ist es jetzt, den über „`Host: intern`“ erreichbaren Teil des DocumentRoot nur für zugelassene Benutzer zuzulassen. Prüfen Sie dazu die vom Browser empfangenen Benutzernamen und Passworte auf Korrektheit. Dazu muss Ihr Server eine vorgegebene „htaccess“-Datei einlesen, die Sie hier herunterladen können: https://git.fh-muenster.de/schinzel/PSE2017-Test/blob/master/htpasswd

In dieser Datei stehen die Benutzernamen und Passworte, die Zugriff auf den internen Bereich haben sollen. Die Passworte sind über den `SHA1`-Hash-Algorithmus [1] „verschlüsselt“ und `Base64`-kodiert [2] und nicht im Klartext lesbar. Das Passwort für den Benutzer ‚`test`‘ ist ‚`testtest`‘ und das Passwort für den Benutzer ‚`test1`‘ ist ‚`test1test1`‘. Die Datei wurde unter anderem mit dem folgenden Befehl erstellt:

```
$ htpasswd -s -c htpasswd test
```

Werten Sie die vom Browser empfangenen Zugangsdaten aus und vergleichen Sie sie mit den Daten aus der htpasswd-Datei. Nur wenn die Daten gültig waren, gibt Ihr HTTP-Server die angeforderten Daten im internen Bereich zurück. Ansonsten antwortet er wie gehabt mit dem Status-Code 401.

Tipp: verwenden Sie die SHA1-Implementierung der OpenSSL-Bibliothek. Stellen Sie sicher, dass Sie die Entwicklerversion von OpenSSL installiert haben (libssl-dev).

Abnahme

Zeigen sie, dass der interne Bereich nur für korrekte Benutzername/Passwort-Kombinationen einsehbar ist und für alle anderen verwehrt bleibt.

[0]: https://de.wikipedia.org/wiki/HTTP-Authentifizierung
[1]: https://de.wikipedia.org/wiki/Sha1
[2]: https://de.wikipedia.org/wiki/Base64