Vorbereitung

[Für diese Aufgabe haben Sie **zwei Termine** Zeit!]

Bereits vor dem Praktikum sollten Sie sich anhand der im Internet verfügbaren Informationen über eine geeignete Programmiersprache informieren und mit deren grundlegenden Anweisungen sowie Datentypen vertraut machen. Geeignet ist z.B.

- Jede gängige Programmiersprachen für das Web

  Bitte sprechen Sie hierfür wegen der nötigen Unterstützung auf dem UBUNTU-Image Herrn Lutz Behnke direkt an!

Außerdem benötigen Sie grundlegendes Wissen über die Konfiguration von:

- Apache – Einbindung eigener Web-Anwendungen

Und Sie müssen herausfinden, wie Passworte sicher auf einem Server hinterlegt werden können, aber eben nicht im Klartext! Und wenn ich sage „sicher“, dann meine ich damit, dass es kein allgemein bekanntes Unsicherheitspasswort wie „123456“ oder so ist sein darf. Außerdem darf kein gemeinsames Passwort verschiedener Benutzer als solches erkannt werden.

Achtung!

Apache verfügt selbst über Möglichkeiten, eine (einfache Art der) Passwortauthentisierung einzurichten, die jedoch für diese Aufgabe **nicht** genutzt werden soll.

Aufgabe 3a: Web-Anwendung mit Benutzerverwaltung

Programmieren Sie in der von Ihnen gewählten Programmiersprache eine Web-Anwendung, die über Ihren Apache-Server zur Verfügung gestellt wird – jeweils unverschlüsselt sowie per HTTPS geschützt ausgehend von „ihrer“ index.html. Das Hauptziel dieser Aufgabe ist es jedoch, die Passworte, die auf dem Server gespeichert werden, vor Angreifern mit lesendem Zugriff auf die Datei zu schützen. Die Anwendung benötigt keine weitere Funktion als die Benutzerverwaltung **existierender** Benutzer, verschwenden Sie also keine weitere Zeit an weitere Details.

Benutzerschnittstelle
Nach dem erfolgreichen Anmelden eines Benutzers mit seinem Passwort kann dieser folgende Funktionen nutzen:

- Ändern des Passwortes
- Ändern der zugehörigen Email-Adresse

Administrationsschnittstelle
Entweder wird das Anlegen neuer Benutzer über die Web-Anwendung für Administratoren (Vorsicht: wie wird dieser Status gespeichert?) ermöglicht oder es gibt ein kleines Kommandozeilenprogramm dafür, dass dem Administrator der Web-Anwendung das Leben einfacher macht, aber auf dem Server ausgeführt werden muss. Unterstützte Funktionen:

- Anlegen eines neuen Benutzers mit neuem Passwort und mit einer Email-Adresse
- Ändern des Passwortes für existierende Benutzer
- Ändern der Email-Adresse für existierende Benutzer
- Löschen eines existierenden Benutzers
- Übersichtsliste anzeigen lassen mit dem Status der Benutzer

Aufgabe 3b: Mitschnitt einer Nutzung des Web-Formulars

Zeichnen Sie mit tcpdump wenige Minuten Netzwerkverkehr auf. Bauen Sie während der Aufzeichnung mindestens eine geschützte und eine ungeschützte Verbindung zu der Web-Anwendung auf dem Projektserver auf, melden Sie sich jeweils an und ändern Sie Ihr Passwort. (Vermeiden Sie unbedingt die Eingabe „richtiger“ Passworte, Dummy-Passworte wie „123456“ reichen vollkommen aus. Warum, wird sicherlich klar werden)

Übertragen Sie nach Abschluss der Aufzeichnung die libpcap-Datei zur weiteren Analyse auf Ihren Arbeitsplatz.

Identifizieren Sie Ihre Verbindung innerhalb der aufgezeichneten Daten und überprüfen Sie die Payload, d.h. die Nutzdaten der übertragenen Pakete, und finden Sie sowohl das alte als auch das neue Passwort – jedenfalls bei der ungesicherten Übertragung – wieder.

Aufgabe 3c: Überprüfung von Email-Adressen

Um die für den Benutzer angegebenen Email-Adressen besser zu überprüfen (ob diese funktioniert und tatsächlich verwendet werden kann), gibt es automatisiert über das Internet nur noch die Email-Kommunikation selbst, die damit genutzt werden kann. Diese ist somit vom Web unabhängig, aber eben immer noch über das Internet verfolgbar und ablauschbar – also selbst nicht ganz sicher. (Sicherer wäre z.B. das Versenden von Nachrichten an das Mobiltelefon, jedoch kann man das so ohne GSM-Gateways schlecht hier im Praktikum realisieren. Anrufen über ein Call-Center wäre auch denkbar, aber ebenfalls sehr unpraktisch).

Realisieren Sie die Erzeugung eines Emailtextes (Ausgabe nur auf der Web-Seite als „Antwort“ beim Click, also nicht per SMTP verschicken), der einen klickbaren, pro Eingabe/Änderung der Email-Adresse eindeutigen, schwer zu ratenden, und nur begrenzte Zeit (30 min) gültigen, Link auf den Projektserver enthält.

Am einfachsten ist die Übergabe des schwer zu ratenden „Anteils“ als Parameter (also sowas wie ...“/team27/activate.php?user=123455&code=xxxxxxx...“). Wird der angegebene Link – also auch aus dem erzeugten Emailtext heraus – geklickt, wird ihre Web-Anwendung angesprochen und der schwer zu ratende „Anteil“ geprüft. Ist dieser gültig und die Zeit noch nicht abgelaufen, wird das als erfolgreiche Überprüfung der Email-Nachricht vermerkt. Sonst gibt es einen Fehler. Ein Fehler wird auch beim wiederholten Klicken des Links angezeigt. Der Status der Überprüfung und ob eine Email-Nachricht „erzeugt“ wurde, die noch nicht bestätigt wurde, soll in der Übersichtsliste für die Administratoren ebenfalls sichtbar sein.

Ändern Sie Ihre Web-Anwendung aus 3a (oder machen Sie die gleich so), so dass jedes Mal, wenn ein Benutzer seine Email-Adresse ändert, ein entsprechender Email-Text erzeugt wird. Auch wenn der Administrator die Email-Adresse eines Benutzers ändert, muss so ein Email-Text erzeugt werden, ebenso beim Anlegen eines neuen Benutzers durch den Administrator. Überlegen Sie sich, warum dieses Vorgehen sinnvoll ist.

Ändern Sie Ihre Web-Anwendung weiterhin so, dass ein neu angelegter Benutzer sich nicht einloggen kann, ohne dass die zugehörige Email-Adresse vorher bestätigt wurde. Zum Testen müssen Sie natürlich dann – weil keine Email verschickt wird, dafür brauchen Sie aber auch nicht auf die Emails zu warten – selbst auf den Link klicken, um die Email-Adresse damit gegenüber dem System zu bestätigen.

Aufgabe 3d: Anfordern eines neuen Passwortes

Immer wieder vergessen Benutzer ihre Passworte. Deswegen können diese sich dann nicht einloggen, und selbst ein neues eingeben. Dies ist sehr kostenaufwändig und muss deswegen vermieden werden.

Erweitern Sie die Web-Anwendung so, dass Benutzer, für die bereits die Email-Adresse bestätigt wurde (warum?), eine Email an diese Adresse anfordern können (wieder simuliert durch die Email-Textausgabe auf der Web-Seite mit gültigen Links). In dieser Email ist ein eindeutiger, schwer zu ratender, und nur begrenzte Zeit (30 min) gültiger, Link auf den Projektserver analog zu Aufgabe 3c zu realisieren. Wird dieser innerhalb des erlaubten Zeitfensters geklickt, kann der Benutzer ein neues Passwort setzen. Sonst gibt es einen Fehler. Überlegen Sie, warum in dieser Email kein neues Passwort mit übertragen werden darf.

Wünsche, das Passwort neu zu setzen, sollen in der Übersichtsliste des Administrators vermerkt werden, solange Sie noch nicht verwendet wurden. Ebenso sollen Passworte, die noch nie verwendet werden, als solche markiert werden.