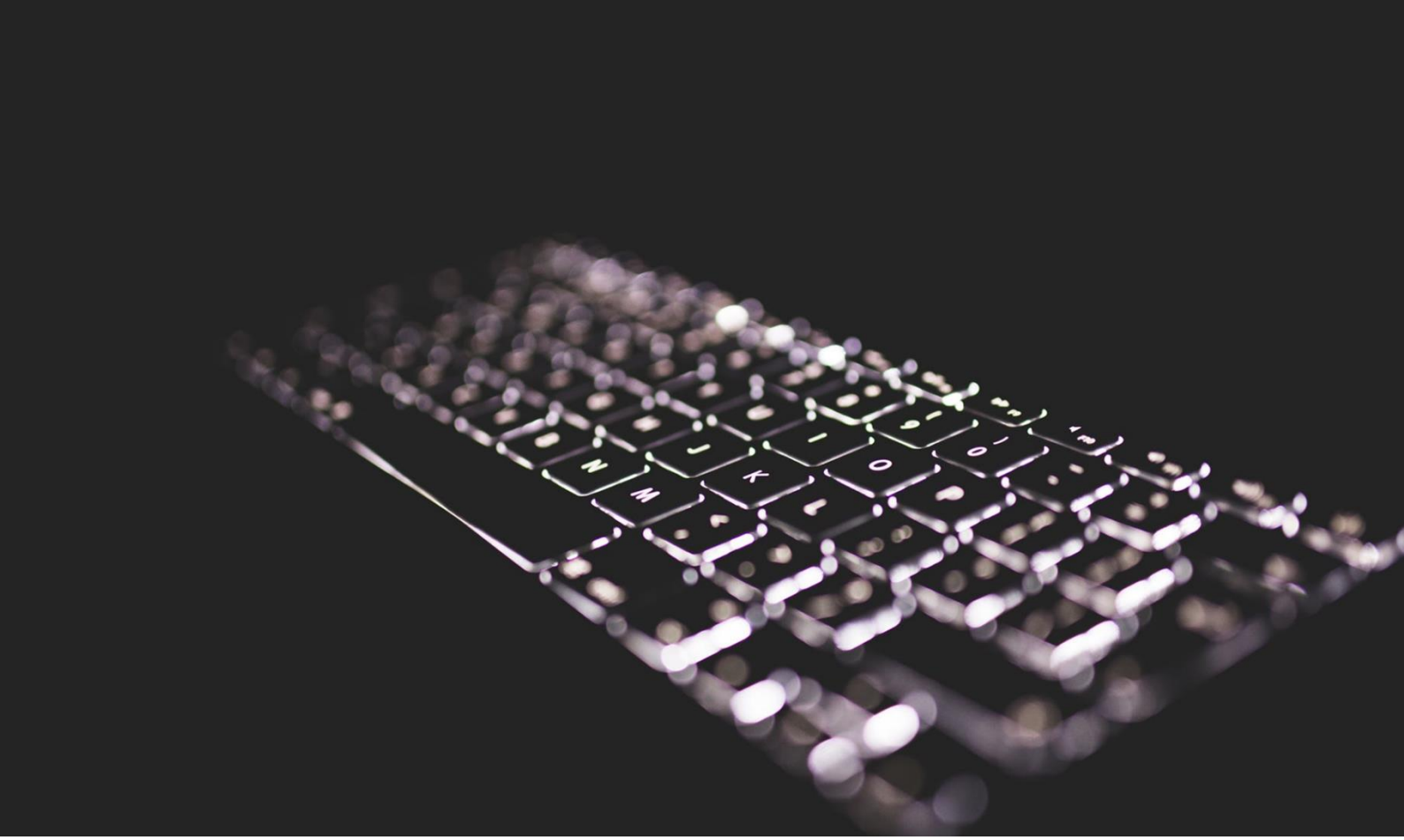

Authentication & Identification failures

Lab Guide

ADPENTEST 08

Inhalt

1 Einführung

1.1 Vorwort

In dieser Laborübung verwenden Sie die Burp Suite, um Kennwort Brute Forcing und drei **Geheime Frage zum Zurücksetzen des Kennworts** Angriffe durchzuführen.

1.2 Laborumgebung

Für diese Übung wird folgendes benötigt:

- Zugang zur **Laborumgebung**
- Eigene **Kali Linux VM** (empfohlen) oder Linux System nach eigener Wahl
- Burp Suite

Im ADPENTEST LAB – Setup Guide befinden sich Hinweise für den Zugriff auf die Laborumgebung. Nach erfolgreicher Verbindung können die Aufgaben in diesem Dokument gelöst werden.

2 Erstellung von Wortlisten

Bruteforce-Kennwort Angriffe benutzen eine Wortliste, die systematisch durchgegangen wird und als Input für die Passwort-Anfrage dient.

Es gibt bereits viele Passwort-Listen, die von Angreifern veröffentlicht wurden.

Für diese Übung steht folgende Wortliste in Kali zur Verfügung: /usr/share/wordlists/fern-wifi/common.txt

3 Bruteforce-Kennwort

Versuchen Sie, das Benutzerkennwort zu bruteforcen :

1. "**admin@secur-shop.com**", ist das Opfer dieses Bruteforce-Angriffs.
2. Verwenden Sie die **Aufgabe 1** generierte Wortliste gegen diesen Benutzer.

Tipps:

Verwenden Sie Burp, um diesen Bruteforce-Angriff durchzuführen.

Vorgehensweise bei der Durchführung der Aufgaben:

- **Burp Bruteforcing**
  - Login-Anfrage mit Burp abfangen. Welches Modul eignet sich am besten für diese Art von Angriff?
  - Senden Sie diese Anfrage an Intruder. Welche Art von Angriff müssen Sie verwenden? Haben Sie eine Payload oder mehrere Payloads?
  - Wählen Sie einen Sniper Angriff und analysieren Sie, welche Dateien Sie als Payload angeben können und welche Felder Sie als Payload haben möchten.
  - Sobald alle Positionen gelöscht sind und nur die Passwort-Payload ausgewählt ist, gehen Sie zum Untermenü Payloads. Was können Sie hier übermitteln?
  - Nach erfolgreicher Wortlistenübermittlung können Sie einen Angriff starten.
  - Analysieren Sie die Ergebnisse, können Sie die Anfragen filtern? Welche Anforderung hat einen anderen Antwortcode und eine andere Textlänge?

4 Optional: Geheime Frage zum Zurücksetzen des Kennworts

Versuchen Sie, das Benutzerkennwort basierend auf der schwachen Funktion zum Zurücksetzen des Kennworts zurückzusetzen:

- Ändern Sie das Benders-Passwort über die Sicherheitsfrage.

Tipps:

Verwenden OSINT, um diese Aufgabe zu lösen.

Vorgehensweise bei der Durchführung der Aufgaben:

- **Zurücksetzen des Benutzerkennworts**

- Interagieren Sie mit der Website und beobachten Sie, wie die Registrierung funktioniert. Gibt es Features, mit welchen Sie das Passwort im Falle eines Passwortverlusts wiederherstellen können?
- Werfen Sie einen Blick auf die Sicherheitsfragen, die von der Website bereitgestellt werden. Sind diese „sicher“? Können sie leicht erraten oder mit Brute Force erraten werden?
- Gibt es etwas im E-Shop, womit Benutzer interagieren können?
- Gibt es im Kommentarbereich Benutzer, die zu viele Informationen bereitstellen?

- **Ändern Sie das Benders-Passwort über die Reset-Funktion**
  - Durchsuchen Sie die Website, wissen Sie, wer Bender ist?
  - Was ist eine Sicherheitsfrage für Benutzer Bender?
  - Führen Sie OSINT durch, um Antworten auf Benders Sicherheitsfrage zu finden.

5 Nachricht

Schreiben Sie einen **Penetration Test Report** über Ihre gefundenen Ergebnisse. Dieser sollte folgende Kapitel beinhalten:

- Einleitung
  - Was wurde gemacht
  - Setup des Labors
- Management Summary
  - Zusammenfassung über gefundene Schwachstellen, Exploits und Vorschläge zur Verbesserung der Sicherheit des Systems
- Ergebnisse im Detail
  - Stellen Sie hier im Detail alle Ergebnisse dar und listen Sie alle Schritte so auf, dass ein technisch versierter Leser alle Schritte nachvollziehen kann. Belegen Sie Schlüsselpunkte mit Screenshots.
  - Screenshots mit Schritten zur Reproduktion des Angriffs und der erfolgreichen Meldung im Browser.

Viel Erfolg!!