# Lern- und Arbeitsauftrag *LA\_183\_13\_HumanFactor.docx*

|  |  |
| --- | --- |
| Titel | Human Factor |
| Modul | 183 Informatiker/in EFZ |
| Autor / Version | Michael Schneider / V1.0  Birgit Rieder / V2.0 |
| Hilfsmittel: | PR\_183\_HumanFactor.pptx |
| Nachweis |  |
| Sozialform | Einzelarbeit / Partnerarbeit |
| Leistungsziele | 4.5 |

## Ausgangslage

Sie haben den Auftrag, die Webapplikation der BBB Insecure App sicherheitstechnisch zu untersuchen und Sicherheitslücken zu schliessen.

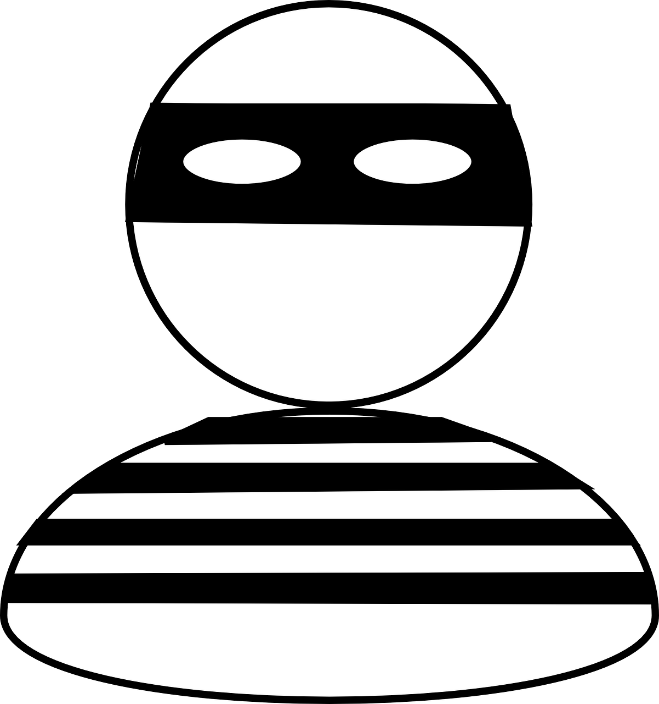


Bild von Clker-Free-Vector-Images auf Pixabay

### Aufgabe 1: Phishing

Lesen Sie «PR\_183\_MenschAlsSicherheitslücke» (auf Moodle) und fassen Sie das Gelernte kurz zusammen.

Phishing ist eine Taktik von Cyberkriminellen, um an vertrauliche Informationen zu gelangen. Dies geschieht durch das Vortäuschen einer vertrauenswürdigen Identität, oft in E-Mails oder auf gefälschten Websites. Ziel ist es, Nutzer dazu zu bringen, sensible Daten wie Passwörter oder Kreditkartendaten preiszugeben. Wachsamkeit, Überprüfung von E-Mail-Quellen und die Nutzung von Sicherheitstools sind entscheidend, um sich vor Phishing zu schützen.

### Aufgabe 2: Installierte Browsererweiterungen

Arbeiten Sie die unter Hilfsmittel erwähnte Präsentation durch.

Erweiterungen für den Browser haben sehr weitreichende Rechte und können ein grosses Sicherheitsproblem darstellen.

1. Was haben Sie für Erweiterungen installiert?

Ich habe Similarweb installiert.  
Ein Bild, das Design enthält.

Automatisch generierte Beschreibung mit geringer Zuverlässigkeit

1. Öffnen Sie den Tab «Netzwerk» in Ihrem Haupt-Browser. Finden Sie Aufrufe, die nicht von Ihnen initiiert wurden? Gibt es Erweiterungen, die «nach Hause» telefonieren?  
     
   Die Aufrufe geschahen erst als ich sie probiert habe.

Ein Bild, das Text, Screenshot, Software, Webseite enthält.

Automatisch generierte Beschreibung

**Aufgabe 3: InsecureApp**

1. Warum wäre es sinnvoll, vor einem Ändern des Passworts das alte Passwort abzufragen?  
   Das alte Passwort abzufragen, bevor es geändert wird, dient zur Sicherheitsüberprüfung und stellt sicher, dass die Änderung autorisiert ist.
2. Implementieren Sie diese Funktion in der InsecureApp. Ergänzen Sie das Formular auf Client-Seite, das Data Transfer Object und die Methode im Controller.
3. Sie legen fest, dass ein Passwort mindestens einen Kleinbuchstaben, einen Grossbuchstaben und eine Zahl beinhalten muss. Ergänzen Sie die View um einen Hinweis auf diese Vorgaben. Ändern Sie den Controller, so dass die neue Passwortrichtlinie sichergestellt wird. Bitte machen Sie den Controller so, dass er alle Verstösse gegen die Vorgaben meldet und nicht einen nach dem Andern während der Änderung des Passwortes. Ein Bild, das Text, Screenshot, Software, Betriebssystem enthält.

   Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot enthält.

Automatisch generierte Beschreibung

## Gütekriterien

Der Lern- und Arbeitsauftrag ist erfüllt, wenn …

* Sie die wichtigsten Erkenntnisse aus der Präsentation zusammengefasst haben.
* Sie die Erweiterungen, die in Ihrem Hauptbrowser installiert sind, aufgelistet haben.
* Sie Netzwerkaktivitäten Ihres Browsers, die von Erweiterungen initiiert wurden, entweder ausgeschlossen oder identifiziert haben.
* Sie begründet haben, wieso es sicherheitstechnisch Sinn macht, dass das alte Passwort bei einer Passwortänderung eingegeben werden muss.
* Sie die BBB InsecureApp um die Eingabe des alten Passwortes bei einer Passwortänderung ergänzt haben.
* Sie bei der BBB InsecureApp eine Passwortrichtlinie inklusive Hinweis für den oder die Benutzer:in implementiert haben.

## Zusätzliche Angaben zum Auftrag

-

## Mögliche Erweiterungsaufträge

Ergänzen Sie den Controller für die Änderung des Passworts dahingehend, dass die letzten 10 Passwörter nicht verwendet werden dürfen.