# Lab 1: Web application Security

## Part 1. Juice Shop Schwachstellen finden

Zu Beginn wurden die erforderlichen Tools Schritt für Schritt installiert. Nachdem die Einrichtung abgeschlossen war, wurde anschließend die Juice Shop Webseite analysiert. Es wurden verschiedene Produkte ausgewählt und die einzelnen Menüpunkte untersucht. Im Anschluss wurden dann die erste Laboraufgabe gestartet. Die Aufgabe war es das Score Board zu finden und anschließend 3 Schwachstellen der Seite zu finden.

## Die Suche nach dem Scoreboard:

Ein Bild, das Screenshot enthält.

Automatisch generierte BeschreibungBeim Durchsuchen der Webseite sind uns verschiedene Unterpunkte aufgefallen. Im Menü haben wir den Punkt „Help getting started“ gefunden. Mit einem Klick auf diesen Menüpunkt hat sich auch schon eine Hilfestellung geöffnet, wie man das Score Board finden kann. Es wurde empfohlen das DevTool mit F12 zu öffnen. Man konnte aber auch durch raten der URL das Score Board finden. Wir ahnten schon was man in der URL ergänzen mussten, aber wollten trotzdem den ausführlichen Weg gehen. Also öffneten wir mit F12 das Devtool. In dem Reiter „Sources“ konnte man verschiedene Javascript Dateien finden und und mit STRG+F die jeweilige Datei durchsuchen. Beim Durchsuchen der „main.js“ Datei mit dem Schlagwort „score“ sind wir beim zwölften Suchergebnis fündig geworden. Hier stand der Punkt (path:"score-board") der uns auf die URL-Lösung brachte. Nach ausprobieren in der URL-Zeile sind wir schließlich auch auf das Scoreboard gestoßen. In der Menüstruktur war nun auch das Scoreboard sichtbar.

Figure 1: Screenshot with author name

## Ein Bild, das drinnen enthält. Automatisch generierte BeschreibungDatenschutzerklärung finden:

Der nächste Schritt bestand darin eine weitere 1-Sterne und zwei 2-Sterne Aufgaben des Scoreboards zu lösen.  
Als 1-Stern Aufgabe wurde die Datenschutzbestimmung des Juice Shops gesucht. Auch hier bekam man wieder eine kleine Hilfestellung. Um die Bestimmungen zu finden wurde zunächst ein neuer Benutzer mit Name und Passwort erstellt. Hier haben wir als Test eine Emailadresse eingegeben mit einem Anbieter, der gar nicht existiert (z.B. @blabla.com). Das hat sogar funktioniert.

Figure 2: Look for curly red lines under your words.

Nachdem der Benutzer erstellt wurde, konnte man die Datenschutzbestimmungen oben rechts über Konto – Datenschutz & Sicherheit finden und lesen.

## Ein Bild, das drinnen enthält. Automatisch generierte BeschreibungPasswortstärke und Adminkonto ermitteln:

Als zwei 2-Sterne Aufgaben wurde die Ermittlung des Admin Passwort- und Benutzername ausgesucht. Für das Ausfindig machen des Benutzernamens wurden die Reviews der einzelnen Produkte untersucht. Schon bereits beim ersten Produkt gab es ein Kommentar des Admins, welchen man anhand der Emailadresse „[admin@juice-sh.op](mailto:admin@juice-sh.op)“ erahnen konnte. Beim Versuch sich mit dieser Emailadresse anzumelden fehlte jetzt nur noch das Passwort. Bei der Passworteingabe erschien ein Hinweis, dass ein sehr einfaches Passwort gewählt wurde. Also versuchten wir zunächst Zahlenfolgen wie 12345 oder 00000. Nachdem es mit der Zahlenfolge nicht funktioniert hat, versuchten wir es weiter mit Text und Zahlen. Schließlich gelang es uns mit dem Passwort „admin123“ uns in das Profil einzuloggen.

Figure 2: Look for curly red lines under your words.

## Some notes on style.

Write in a short, clear and technical style. Use abbreviations carefully. You write text not to be written but to be read. Write for the reader. Use paragraphs and sections to structure your text. Use the correct font styles (just like in this template).

## Submitting your report

Hand in: a) **a PDF file with your lab report** (a single document even for labs with multiple parts) and b**) a ZIP file** (no RAR, no tar.gz, no 7z, … only zip) including all source code.

Not adhering to these rules results in a failure for the non-conforming report.

# Literature

|  |  |
| --- | --- |
| [1] | T. M. Heer, Lab Template, Esslingen: Heer's Pony Books, 2020. |