THM TECHNISCHE HOCHSCHULE MITTELHESSEN

Max Stephan

Timon Pellekoorne

MNI Mathematik, Naturwissenschaften und Informatik

Secure Software Engineering (SS 23)

12. Mai 2023 — Übungsblatt 4 — 4

Aufgabe 1 (SQL Injections). Untersuchen Sie verschiedenste Eingabe-Felder im gefakten Forum http://fk-sse.mni.thm.de/forum, ob hier SQL Injections möglich sind und welche Arten von Anführungszeichen im dazugehörigen Query verwendet werden. *Hinweis:* Ein Registrieren im Forum ist nicht nötig.

ACHTUNG Damit man nicht so leicht auf das BB-Forum zugreifen kann, welches ein SQL-Injection ermöglicht, muss man seine eigene IP-Adresse zuerst freischalten.
Hierzu reicht ein Aufruf der Seite http://fk-sse.mni.thm.de/access/. Danach kann man auf http://fk-sse.mni.thm.de/forum zugreifen. Desweiteren ist der Server nur über eine **VPN** (http://vpn.thm.de) Verbindung erreichbar.

Aufgabe 2 (Daten erspähen). Finden Sie heraus, welche Rückgabetypen das SQL-Query mit der Sicherheitslücke hat. Lesen Sie aus den privaten Messages den Message-Text aus, der als Message-Subjekt die ersten 4 Buchstaben/Zahlen Ihrer CAS-Kennung hat. Geben Sie dann den Message-Text im Feedbacksystem ab.
Hinweis: Finden Sie zuvor heraus, auf welchen Quellpaketen das Forum basiert und in welcher Tabelle die privaten Messages gespeichert werden.

Aufgabe 3 (XSS). Suchen Sie sich auf der Seite
https://pwning.owasp-juice.shop/part2/xss.html
eine oder mehrere Aufgaben aus, sodass Sie insgesamt auf 3 Sterne kommen.

Hinweis: Starten Sie dazu den Juice-Shop bei sich lokal und versuchen Sie die XSS Sicherheitslücken zu finden. Eine Anleitung zu Installation finden Sie hier: https://pwning.owasp-juice.shop/part1/running.html

Aufgabe 4 (HTML Sanitization). Schreiben Sie einen JavaScript-Client mit der Möglichkeit eine Eingabe in ein Inputfeld zu schreiben. Bei dem Klick auf einen Button soll die Eingabe auf der Seite ausgegeben werden. Nutzen Sie dafür `element.innerHTML`. Schreiben Sie einen `sanitizer`, sodass trotz der Nutzung des unsicheren Sinks `element.innerHTML` kein XSS möglich ist. Testen Sie ihre Anwendung mit allen gängigen XSS Attacken.