

Praktikum 3:

Web Security

DER OWAS JUICE-SHOP

Der OWASP Juice Shop^{1,2} ist eine Open-Source-Webanwendung, die entwickelt wurde, um Sicherheitslücken zu demonstrieren und Sicherheitstrainings zu unterstützen. OWASP steht für Open Web Application Security Project und ist eine weltweite Gemeinschaft, die sich der Verbesserung der Sicherheit von Softwareanwendungen widmet.

Der Juice Shop wurde als absichtlich unsichere Anwendung konzipiert, die auf realen Sicherheitslücken basiert, um ein praktisches Umfeld zum Lernen und Üben zu bieten. Durch die Interaktion mit der Anwendung können Benutzer verschiedene Arten von Sicherheitsproblemen kennenlernen. Das Ziel des Juice Shop besteht darin, Benutzern ein realistisches Szenario zu bieten, in dem sie Sicherheitslücken erkennen, verstehen und beheben können. Dabei wird der Fokus auf Best Practices für sichere Softwareentwicklung und Fehlerbehebung gelegt

Installation

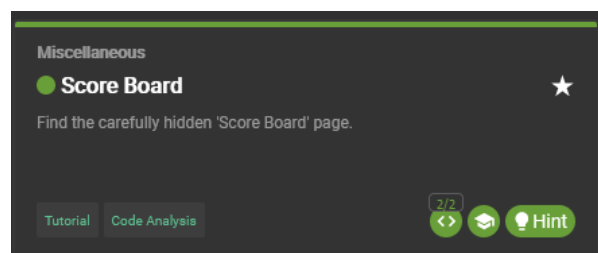
Installieren Sie den OWASP Juice Shop auf ihrem System: <https://pwning.owasp-juice.shop/companion-guide/latest/part1/running.html>

Erste Schritte

Über die Adresse: <http://localhost:3000/#/> können sie den OWASP Juice Shop aufrufen.



Auf dem Score Board (<http://localhost:3000/#/score-board>) werden die verschiedenen Aufgaben, die in dem Shop gelöst werden können, aufgelistet. Aufgaben heißt in diesem Kontext das Schwachstellen gefunden und ausgenutzt werden sollen.

Die Abbildung zeigt beispielhaft die Aufgabe „Score Board, die Sie gelöst haben, wenn Sie oben auf den Link klicken.



¹ <https://github.com/juice-shop/juice-shop>

² <https://owasp.org/www-project-juice-shop/>

- Über den Knopf „Tipp“ („Hint“; ) erhalten Sie wertvolle Hinweise zur Lösung einer jeweiligen Aufgabe
- Für manche Aufgaben steht ein „interaktives Hacking Tutorial“ zur Verfügung (), das Ihnen bei der Lösung der jeweiligen Aufgabe hilft.


AUFGABE 1: CROSS-SITE SCRIPTING

Lösen Sie die XSS-Aufgaben mit 1, 2 und 3 Sternen (<http://localhost:3000/#/score-board?difficulties=1,2,3&categories=XSS>):

- DOM XSS
- XSS Bonus Payload
- Reflected XSS
- API-only XSS
- Client-side XSS Protection

Lösen Sie außerdem die „Coding Challenge“ zu den folgenden Aufgaben:

- DOM XSS
- XSS Bonus Payload
- API-only XSS

Wenn Sie eine Aufgabe gelöst haben können Sie über das entsprechende Symbol () die zugehörige Coding Aufgabe öffnen.

AUFGABE 2: BROKEN ACCESS CONTROL


Lösen Sie die „Broken Access Control“ Aufgaben mit 1,2 und 3 Sternen (<http://localhost:3000/#/score-board?difficulties=1,2,3&categories=Broken%20Access%20Control>):

- Web3 Sandbox
- View Basket
- Admin Section
- Five-Star Feedback
- Forged Feedback
- CSRF
- Forged Review
- Manipulate Basket
- Product Tampering

Lösen Sie außerdem die „Coding Challenge“ zu den folgenden Aufgaben:

- Web3 Sandbox
- Admin Section

- Forged Review
- Product Tampering

Wenn Sie eine Aufgabe gelöst haben können Sie über das entsprechende Symbol () die zugehörige Coding Aufgabe öffnen.


AUFGABE 3: WEITERE INJECTION ANGRIFFE

Lösen Sie die Injection-Aufgaben mit 1, 2 und 3 Sternen (<http://localhost:3000/#/score-board?difficulties=1,2,3&categories=Injection>):

- Login Admin
- Login Jim
- Login Bender
- Database Schema

Lösen Sie außerdem die „Coding Challenge“ zu den folgenden Aufgaben:

- Login Admin
- Login Jim
- Login Bender
- Database Schema

Wenn Sie eine Aufgabe gelöst haben können Sie über das entsprechende Symbol () die zugehörige Coding Aufgabe öffnen.

AUFGABE 4: INPUT VALIDATION

Lösen Sie die „Input-Validation“-Aufgaben mit 1 und 2 Sternen (<http://localhost:3000/#/score-board?difficulties=1,2&categories=Improper%20Input%20Validation>):

- Missing Encoding
- Repetitive Registration
- Empty User Registration
- Admin Registration
- Deluxe Fraud