I.　OWASP Juice Shop を通じて Web セキュリティを学ぶ

本章では、OWASP Juice Shop を通じて Web セキュリティについて学ぶ。OWASP Juice Shop は、OWASP（Open Web Application Security Project）が提供する Web アプリケーションであり、脆弱性を含んでいる。この脆弱性を利用して、Web セキュリティについて学ぶことができる。OWASP Juice Shop にはさまざまな脆弱性が含まれており、その中には、SQL インジェクション、XSS（Cross-Site Scripting）、CSRF（Cross-Site Request Forgery）などが含まれている。これらの詳細に踏み入るのではなく、OWASP Juice Shop を通じて CTF の Web の問題をどのように解くか、そして Web セキュリティの概要について紹介する。次の章では、脆弱性を具体的に学んでいく。

i.　OWASP とは

OWASP は Open Worldwide Application Security Project のことで、主に Web アプリケーションのセキュリティ関わる調査や情報共有を行うコミュニティである。中でも OWASP Top 10 は、Web アプリケーションの脆弱性のトップ 10 をまとめたものであり、2024 年 8 月時点では 2021 年版が最新である。OWASP Top 10[1)]は、Web アプリケーションの脆弱性を理解する上で重要な情報源である。

2021 年の OWASP Top 10 は、以下の通りである。ここでは詳細な説明は避けるが、OWASP Top 10 ではこれらの主要な脆弱性の概要や対策が丁寧に記載されているため、Web セキュリティに興味がある方は参照することをお勧めします。

順位	脆弱性名
1	**Broken Access Control**
2	**Cryptographic Failures**
3	**Injection**
4	**Insecure Design**
5	**Security Misconfiguration**
6	**Vulnerable and Outdated Components**
7	**Identification and Authentication Failures**
8	**Software and Data Integrity Failures**
9	**Security Logging and Monitoring Failures**
10	**Server-Side Request Forgery (SSRF)**

1)　https://owasp.org/Top10/ja/

ii. OWASP Juice Shop

それでは、[2]OWASP Juice Shop を見ながら、Web セキュリティについて学んでいこう。OWASP Juice Shop は、OWASP が提供する Web アプリケーションであり、脆弱性を含んでいる。OWASP Juice Shop にアクセスして Start Machine のボタンをクリックすると、Juice Shop が起動する。

1. 偵察

Start Machine ボタンを押すとターゲットマシンの IP アドレスが表示されるので、IP アドレスを使ってターゲットの偵察を行う。まずは、nmap を使ってポートスキャンを行う。

2） https://tryhackme.com/r/room/owaspjuiceshop