Exploiting Vulnerabilities in Your Web Application

Sunny Wear
SECURITY ARCHITECT AND PENETRATION TESTER

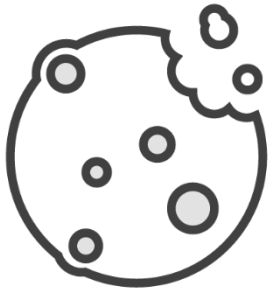
@SunnyWear www.sunnywear.org

Using Burp to Find Common Vulnerabilities

Common Attacks

SQLi

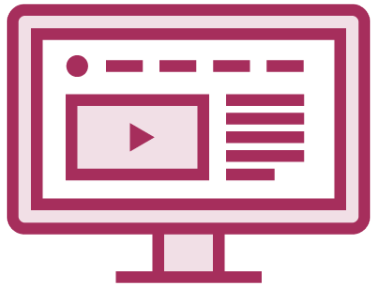
XSS



Cookie/Session Mgmt

Parameter tamper

CSRF



Clickjacking

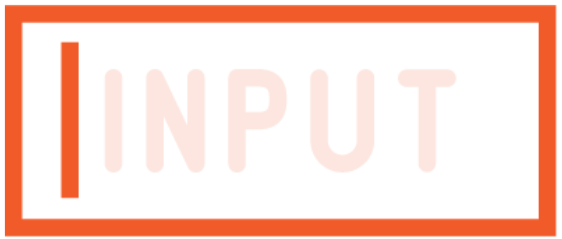
Demo

Juice Shop Challenges

- SQLi
- XSS
- Cookie/session management
- Parameter tampering
- CSRF
- Clickjacking

SQL Injection (SQLi) Attacks

Where to Test



Login forms

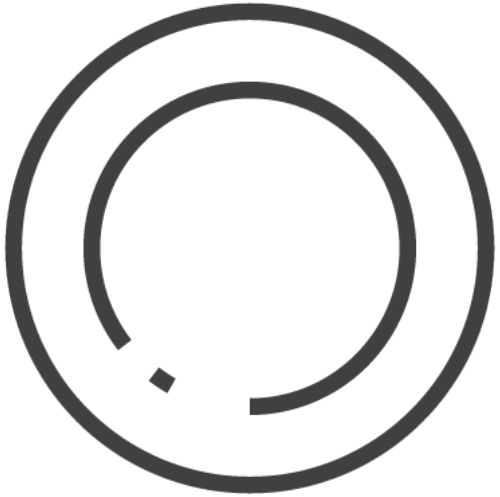
Web forms

Demo

SQLi Attacks against Juice Shop

XSS Injection Attacks

Type of XSS Attacks



Reflected

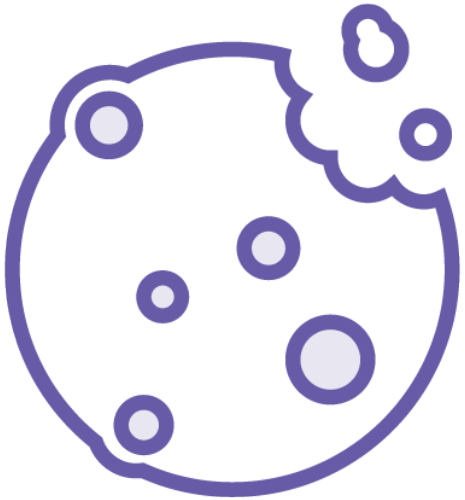
Stored

Demo

XSS Attacks against Juice Shop

Cookie/Session Management Issues

Types of Attacks



Cookie Manipulation

Token Abuse

Demo

Session Mgmt Attacks against Juice Shop

Parameter Tampering

Types of Attacks

URL tampering

JavaScript bypass

Hidden form fields

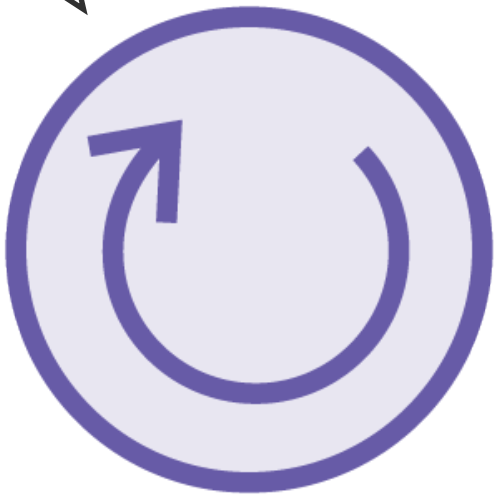
Server-side JSON exploit

Demo

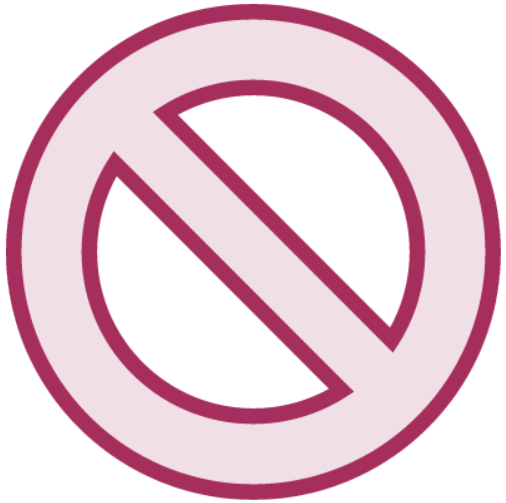
Parameter tamper attacks against Juice Shop

Cross-site Request Forgery (CSRF) Attacks

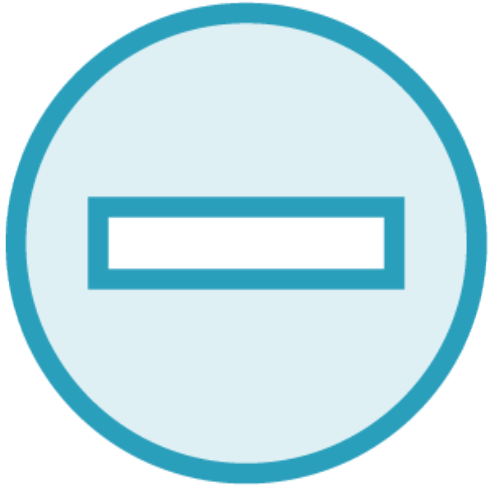
CSRF PoC



Replay Attack Check



Absence of
anti-CSRF token



Absence of
server-side validation

Demo

CSRF attack against Juice Shop

Clickjacking

Demo

Clickjacking attacks against Juice Shop

Summary

Exploitation

Integration with 3rd party tools