Integrating Burp and File Attacks

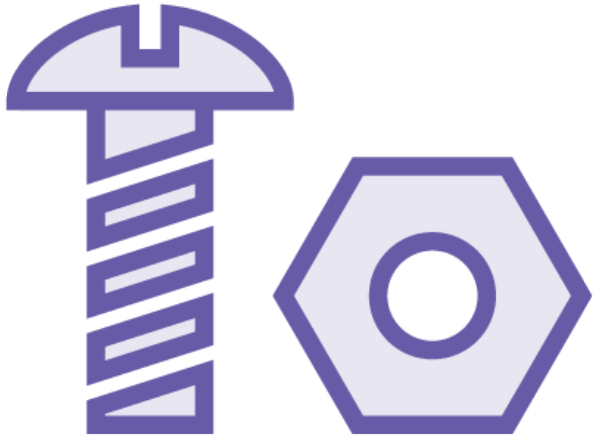
USING BURP WITH 3RD PARTY PENTESTING TOOLS

Sunny Wear
SECURITY ARCHITECT AND PENETRATION TESTER
@SunnyWear www.sunnywear.org

Burp Extenders Explained

Extend the Power of Burp

External tools



Customization

BApp Store

All available extensions:

Some pro-only

Source code available:

https://github.com/PortSwigger

Demo

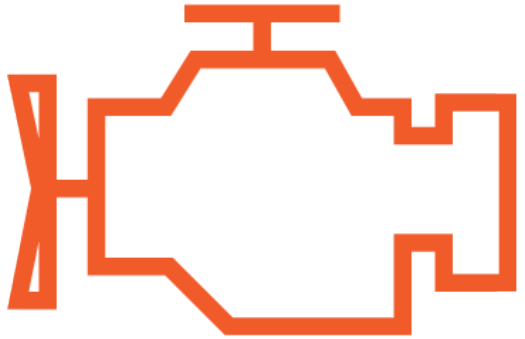
BApp Store introduction

Burp Extenders Sampling

Three Extenders in Our Course

CO2 (SQLMap)

Retire.js



Carbonator

Demo

Install this course's Burp extenders

Burp and File Uploads

Changes to Files with Burp

File extensions

Content-types

Demo

File upload attacks against Juice Shop

Burp and File Downloads

Null Byte Injection

URL-encoded null byte characters (i.e. %00, or 0x00 in hex)

Alter the intended logic allowing unauthorized access

Demo

File download attacks against Juice Shop

Summary

Burp extenders

File upload/download vulnerabilities