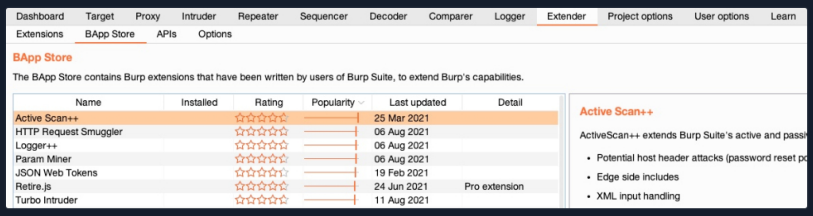
Extensions

Both Burp and ZAP have extension capabilities, such that the community of Burp users can develop extensions for Burp for everyone to use. Such extensions can perform specific actions on any captured requests, for example, or add new features, like decoding and beautifying code. Burp allows extensibility through its `Extender` feature and its BApp Store, while ZAP has its ZAP Marketplace to install new plugins.

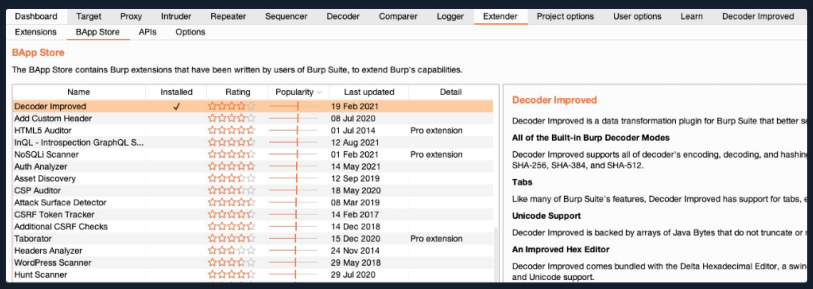
BApp Store

To find all available extensions, we can click on the `Extender` tab within Burp and select the `BApp Store` sub-tab. Once we do this, we will see a host of extensions. We can sort them by `Popularity` so that we know which ones users are finding most useful:



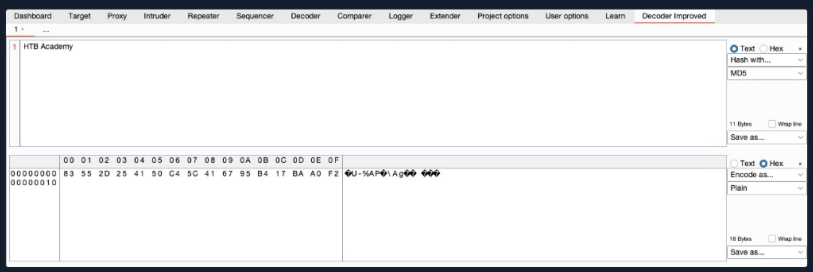
Note: Some extensions are for Pro users only, while most others are available to everyone.

We see many useful extensions, take some time to go through them and see which are most useful to you, and then try installing and testing them. Let's try installing the `Decoder Improved` extension:



Note: Some extensions have requirements that are not usually installed on Linux/macOS/Windows by default, like `Jython`, so you have to install them before being able to install the extension.

Once we install `Decoder Improved`, we will see its new tab added to Burp. Each extension has a different usage, so we may click on any extension's documentation in `BApp Store` to read more about it or visit its GitHub page for more information about its usage. We can use this extension just as we would use Burp's Decoder, with the benefit of having many additional encoders included. For example, we can input text we want to be hashed with `MD5`, and select `Hash With>MD5`:



Similarly, we can perform other types of encoding and hashing. There are many other Burp Extensions that can be utilized to further extend the functionality of Burp.

Some extensions worth checking out include, but are not limited to:

.NET beautifier	J2EEScan	Software Vulnerability Scanner
Software Version Reporter	Active Scan++	Additional Scanner Checks
AWS Security Checks	Backslash Powered Scanner	Wsdler
Java Deserialization Scanner	C02	Cloud Storage Tester
CMS Scanner	Error Message Checks	Detect Dynamic JS
Headers Analyzer	HTML5 Auditor	PHP Object Injection Check
JavaScript Security	Retire.JS	CSP Auditor
Random IP Address Header	Autorize	CSRF Scanner
JS Link Finder		

Cheat Sheet

Table of Contents

Getting Started
Intro to Web Proxies
Setting Up

Web Proxy
Proxy Setup
Intercepting Web Requests
Intercepting Responses
Automatic Modification
Repeating Requests
Encoding/Decoding
Proxying Tools

Web Fuzzer
Burp Intruder
ZAP Fuzzer

Web Scanner
Burp Scanner
ZAP Scanner
Extensions

Skills Assessment
Skills Assessment - Using Web Proxies

My Workstation

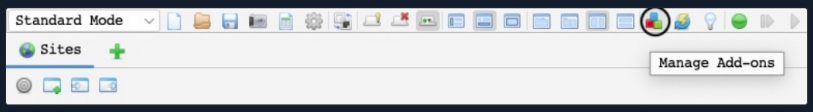
OFFLINE

Start Instance

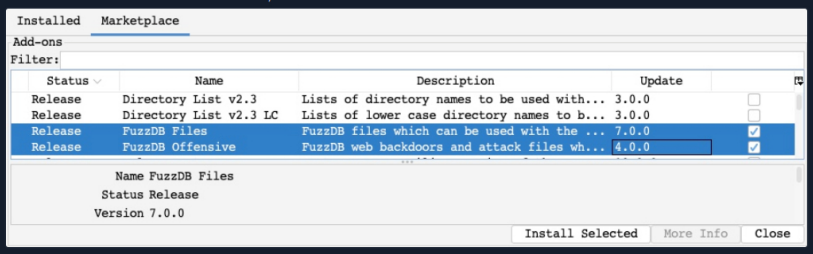
∞ / 1 spawns left

ZAP Marketplace

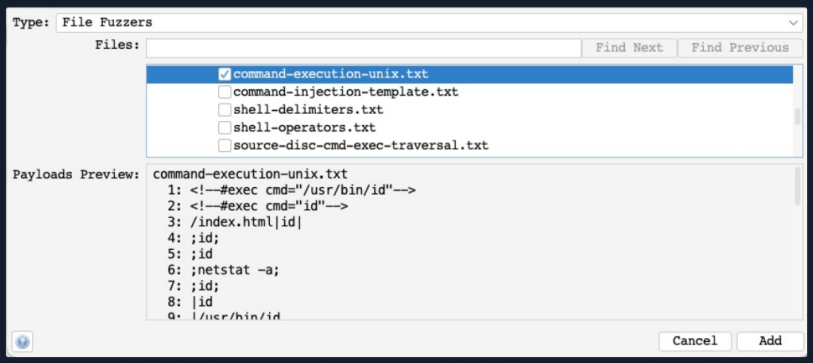
ZAP also has its own extensibility feature with the `Marketplace` that allows us to install various types of community-developed add-ons. To access ZAP's marketplace, we can click on the `Manage Add-ons` button and then select the `Marketplace` tab:



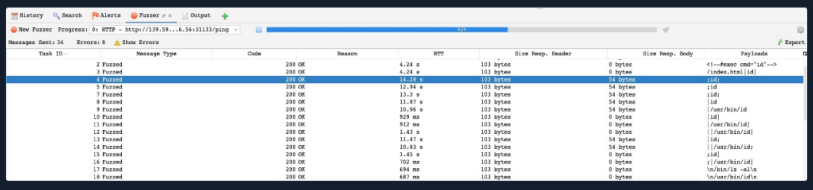
In this tab, we can see the different available add-ons for ZAP. Some add-ons may be in their `Release` build, meaning that they should be stable to be used, while others are in their `Beta/Alpha` builds, which means that they may experience some issues in their use. Let's try installing the `FuzzDB Files` and `FuzzDB Offensive` add-ons, which adds new wordlists to be used in ZAP's fuzzer:



Now, we will have the option to pick from the various wordlists and payloads provided by FuzzDB when performing an attack. For example, suppose we were to perform a Command Injection fuzzing attack on one of the exercises we previously used in this module. In that case, we will see that we have more options in the `File Fuzzers` wordlists, including an OS Command Injection wordlist under (`fuzzdb>attack>os-cmd-execution`), which would be perfect for this attack:



Now, if we run the fuzzer on our exercise using the above wordlist, we will see that it was able to exploit it in various ways, which would be very helpful if we were dealing with a WAF protected web application:



Try to repeat the above with the first exercise in this module to see how add-ons can help in making your penetration test easier.

Closing Thoughts

Throughout this module, we have demonstrated the power of both Burp Suite and ZAP proxies and analyzed the differences and similarities between the free and pro versions of Burp and the free and open-source ZAP proxy. These tools are essential for penetration testers focused on web application security assessments but have many applications for all offensive security practitioners as well blue team practitioners and developers. After working through each of the examples and exercises in this module, attempt some web attack-focused boxes on the main Hack The Box platform and other web application security-related modules within HTB Academy to strengthen your skillsets around both of these tools. They are must-haves in your toolbox alongside Nmap, Hashcat, Wireshark, tcpdump, sqlmap, Ffuf, Gobuster, etc.