Burp suite: Top 5 Proffesional extensions

Introduction

When you buy Burp Suite Proffesional edition, it unlocs several possibilites in terms of extensions we can use. Some of the Proffesional edition extensions can be extremly useful for both bug bounty hunters and penters alike so i've taken the time to go through a few of them for you. They are not ranked in any order, these just stand out as 5 extensions i would always have installed.

Active Scan ++

ActiveScan++ extends Burp Suite's active and passive scanning capabilities. Designed to add minimal network overhead, it identifies application behaviour that may be of interest to advanced testers:

- Potential host header attacks (password reset poisoning, cache poisoning, DNS rebinding)
- Edge side includes
- XML input handling
- Suspicious input transformation (eg 7*7 ⇒ '49', \x41\x41 ⇒ 'AA')

- Passive-scanner issues that only occur during fuzzing (install the 'Error Message Checks' extension for maximum effectiveness)

It also adds checks for the following issues:

- Blind code injection via expression language, Ruby's open() and Perl's open()
- CVE-2014-6271/CVE-2014-6278 'shellshock' and CVE-2015-2080, CVE-2017-5638, CVE-2017-12629, CVE-2018-11776

It also provides insertion points for HTTP basic authentication. To invoke these checks, just run a normal active scan. The host header checks tamper with the host header, which may result in requests being routed to different applications on the same host. Exercise caution when running this scanner against applications in a shared hosting environment. These attacks are very invasive and can adjust other people's data unintended.

CSRF scanner

This extension passively scans for CSRF vulnerabilties. It does return a lot of false positives but it beats having to check CSRF manually on every target for every funcationality.

J2EE scanner

Sometimes we encounter J2EE applications in the wild, these require a completly differnt tactic from our usual scanning methods and that's why this extension has been made. It uses new scanning techniques to identify vulnerabilities in J2EE applications that the normal scanner could not.

Test cases:

- Expression Language Injection (CVE-2011-2730)
- JBoss SEAM Remote Command Execution (CVE-2010-1871)
- Java Server Faces Local File Include (CVE-2013-3827 CVE-2011-4367)
- Local File include - /WEB-INF/web.xml Retrieved
- Local File include - Spring Application Context Retrieved

- Local File include - struts.xml Retrieved
- Local File include - weblogic.xml Retrieved
- Local File include - ibm-ws-bnd.xml Retrieved
- Local File include - ibm-web-ext.xmi Retrieved
- Local File include - ibm-web-ext.xml Retrieved
- Local File include - /etc/shadow Retrieved
- Local File include - /etc/passwd Retrieved
- Apache Struts 2 S2-016
- Apache Struts 2 S2-017
- Apache Struts 2 S2-020
- Apache Struts 2 S2-021
- Apache Struts DevMode Enabled
- Apache Wicket Arbitrary Resource Access (CVE-2015-2080)
- Grails Path Traversal (CVE-2014-0053)
- Incorrect Error Handling - JSF
- Incorrect Error Handling - Apache Struts
- Incorrect Error Handling - Apache Tapestry
- Incorrect Error Handling - Grails
- Incorrect Error Handling - GWT
- Incorrect Error Handling - Java
- XML Security - XInclude Support
- XML Security - XML External Entity
- Information Disclosure Issues - Remote JVM version
- Information Disclosure Issues - Apache Tomcat version
- Compliance Checks - web.xml - HTTP Verb Tampering
- Compliance Checks - web.xml - URL Parameters for Session Tracking

- Compliance Checks - web.xml - Incomplete Error Handling
- Compliance Checks - web.xml - Invoker Servlet
- Infrastructure Issue - HTTP Weak Password
- Infrastructure Issue - Tomcat Manager Console Weak Password
- Infrastructure Issue - Tomcat Host Manager Console Weak Password
- Infrastructure Issue - WEB-INF Application Configuration Files Retrieved
- Infrastructure Issue - Status Servlet
- Infrastructure Issue - Snoop Servlet (CVE-2012-2170)
- Infrastructure Issue - Extended Path Traversal Scan
- Infrastructure Issue - JBoss Web Service Enumeration
- Infrastructure Issue - JBoss Admin Console Weak Password
- Infrastructure Issue - JBoss JMX/Web Console Not Password Protected
- Infrastructure Issue - JBoss JMX Invoker Remote Command Execution
- Infrastructure Issue - Jetty Remote Leak Shared Buffers (CVE-2015-2080) found by @gdssecurity
- Infrastructure Issue - Apache Axis2 - Web Service Enumeration
- Infrastructure Issue - Apache Axis2 - Admin Console Weak Password
- Infrastructure Issue - Apache Axis2 - Local File Include Vulnerability (OSVDB 59001)

Reflected parameters

This is ofcourse super useful to test for reflected XSS entry points. This extension monitors traffic and looks for request parameter values (longer than 3 characters) that are reflected in the response. The extension monitors in-scope requests made by the Proxy and Spider tools. You can send reported items to other Burp tools. When sending an item to the Scanner, you can choose to scan all reflected parameters or only one reflected parameter.

Software version reporter

This plugin will report any software version that it encounters, this will help in finding vulnerabilities in certain software versions.