Cheatography

Metasploit Cheat Sheet

by binca via cheatography.com/44948/cs/13466/

Overview

Most popular exploitation framework and largest Ruby project.

Commonly associated with network explotation but has useful auxiliary modules for web app testing.

Uses modular approach for payloads an exploits allowing for flexibility

Auxiliary modules available for scanning, crawling/spidering and querying web servers; > 150 unique entries in auxiliary/scanner/http.

Especially useful for testing off-the-shelf applications including WordPress, Joomla, Drupal, Oracle DB, SQL Server, SCADA frontends and more.

Seeding Metasploit

Metasploit has two spiders:
auxiliary/crawler/msfcrawler
auxiliary/scanner/http/crawler

But Metasploit's crawlers are not a replacement for ZAP or Burp and instead Metasploit can import results from other tools.

db_import allows Metasploit to ingest the output files of certain tools, parsing them into its own database structure.

db_import -h provides a list of supported files and formats, many tools are included including Acunetix, AppScan, Burp, NetSparker, Nikto, and Wapiti.

WMAP

A web scanning plugin in Metasploit, last updated in 2012 but still useful.

Interfaces with Metaspoit's backend database launching auxiliary and exploit modules related to the web apps results within the database.

Can create custom profiles to run using **wmap_sample_profile.txt** as a template.

Lack documentation.

BeEF and Metasploit

Having a hooked browser allows:
limited system privileges
low persistence
lacks the ability to exploit vulnerabilities
wealth of knowledge about browsing environment

Can configure BeEF to point at **Metasploit RPC listener** to expose Metasploit modules.

Enabling integration:
1. Update config.yml in beef direoctry
2. Configure Metasploit RPC in msfconsole by typing
load msgrpc ServerHost=127.0.0.1
Pass = password
3. Update config.yml in extensions/metasploit directory with info about Metasploit RPC
4. Start BeEF
5. Inject Metasploit

Sqlmap and Metasploit

2-way integration: {{nl}} **Sqlmap.py** can leverage a local **Metasploit** install or use **sqlmap** module within **Metasploit** (less common)

Within Sqlmap, Metasploit is primarily used for shellcode (shell, VNC, Meterpreter)
--os-pwn : leverage Metasploit
--priv-esc: Attempts privilege escalation on Windows
--msf-path: Defines local Metasploit install location

Metasploit and Known Vulnerabilities

Main use in web apps is for known vulnerabilities

Custom application testing can be done with WMAP or auxiliary modules but exploitation is the main purpose.

Exploits against CMS, databases, specified SQLi Flaws, and major vulnerabilities such as ShellShock, Heartbleed, Drupalgeddon

Drupal and Drupalgeddon

One of the most common CMS serving content to end users and providing functionality.

CMS are high-value targets because of their critical purpose.

Drupalgeddon (CVE-2014-3704) and patched on October 15, 2014

Flaw is an unauthenticated SQLi vulnerability present on all Drupal 7 installs.

Successful exploitation provides **data access, remote code execution and local privilege execution**.

Widespread automated exploitation within hours.

Drupal and Drupalgeddon (cont)

Reason for the flaw lies within Drupal's use of prepared statements for SQL queries meant to defend against SQLi.

Drupal includes **expandArguments()** that explodes the arrays but it did not handle specially crafted input properly.

Compounded by Drupal's use of **PHP Data Objects (PDO)**, which employs emulated prepared statements allowing for **multiple queries** as one request.

The result was unfiltered input was passed to **expandArguments()** fnction allowing for an exploit entry point (SELECT pivot to INSERT)

Metasploit and Drupalgeddon

exploit/multi/http/drupal_drupalgeddon is the exploit in msfconsole

The searcher who discovered posted 2 POC:
1. Hijacks an admin session
2. Enabled remote code execution

When Tools Fail

Tools often fail because of **differences in server confgurations, quality issues, some may not be reliable, or results are indeterminate**

Additional testing may reveal an alternative tool or it may require manual exploitation. Researching the vulnerability and exploit may help.

CVE-2014-16010 is a MediaWiki vulnerability with a Metasploit exploit available **exploit/multi/http/media_wiki_thumb** and it uses either a DjVu (default) or PDF. The default fails.

The vulnerability allowed for a PHP backdoor to be uploaded via command execution

The Metasploit module works by manually uploading a PDF