

Burp HUNT

Information Security Inc.

Contents

- About Burp
- Introduction to HUNT
- Demo Setup
- Demo
- References

About Burp

- Burp or Burp Suite is a graphical tool for testing Web application security (installed by default in Kali Linux)
- The tool is written in Java and developed by PortSwigger Security



About Burp

- The tool has two versions: a free version that can be downloaded free of charge (Free Edition installed by default in Kali Linux) and a full version that can be purchased after a trial period (Professional Edition)



Introduction to HUNT

- HUNT is a Burp Suite extension to:
 - ▲ Identify common parameters vulnerable to certain vulnerability classes.
 - ▲ Organize testing methodologies inside of Burp Suite.



Introduction to HUNT

- The problems

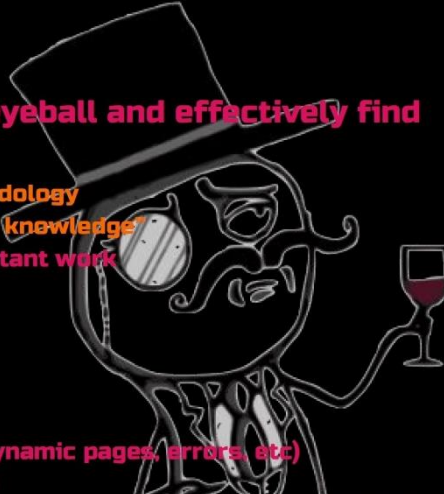
- 1. Increasingly large and complicated Web Applications. Need manual testing. Lots of params.**
- 2. Applications Assessment Training lacks “tribal knowledge” of vulnerability location**
- 3. No in-tool workflow for web hacking methodologies**

Introduction to HUNT

- Current solutions

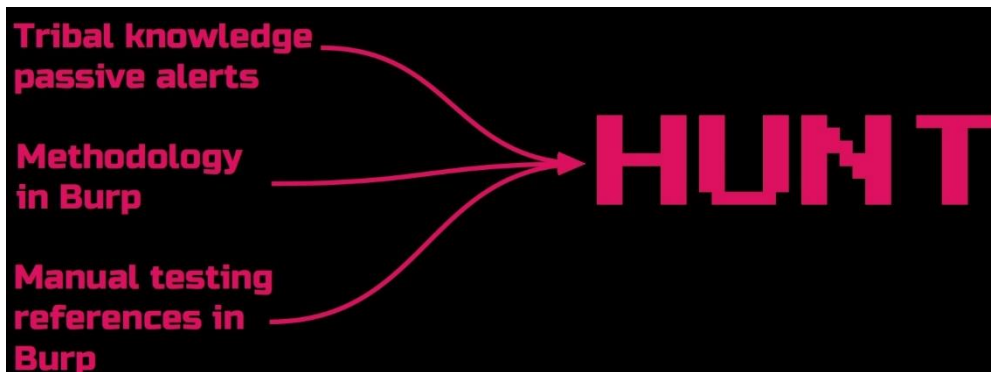
Current Solutions

- 1. Badass hacker who can eyeball and effectively find security bugs**
 - a. May or may not have a methodology
 - b. Definitely has accrued "tribal knowledge"
 - c. Bughunts and/or does consultant work
- 2. Dynamic Scanner**
 - a. Limited test cases (fuzzing)
 - b. Cost prohibitive
 - c. Limited in detection cases (dynamic pages, errors, etc)
 - d. Complex sites are hard (auth)

A cartoon illustration of a man with a large, round face, wearing a black top hat and a monocle over his right eye. He has a thick mustache and is holding a small glass of red wine in his right hand. The illustration is drawn in a simple, sketchy style with white lines on a black background.

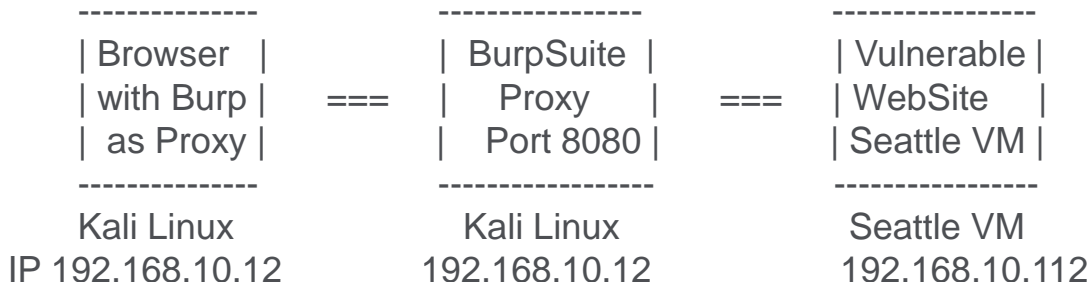
Introduction to HUNT

- HUNT approach



Demo Setup

- Demo configuration



Demo

- BurpSuite Free Edition is installed by default in Kali Linux (2017)



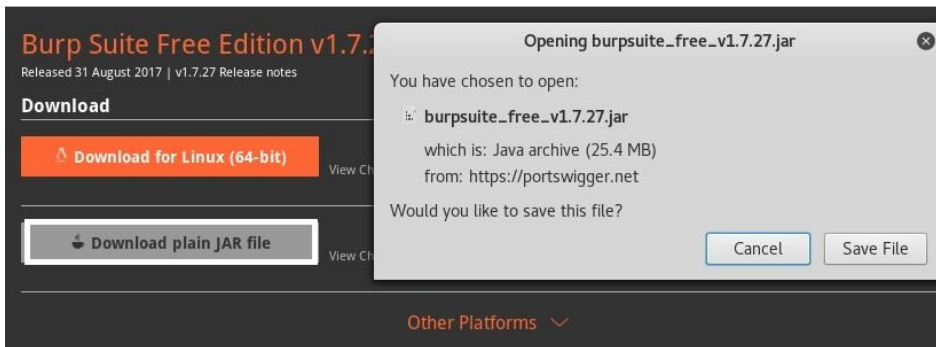
Demo

- Update BurpSuite Free Edition



Demo

- Update BurpSuite Free Edition



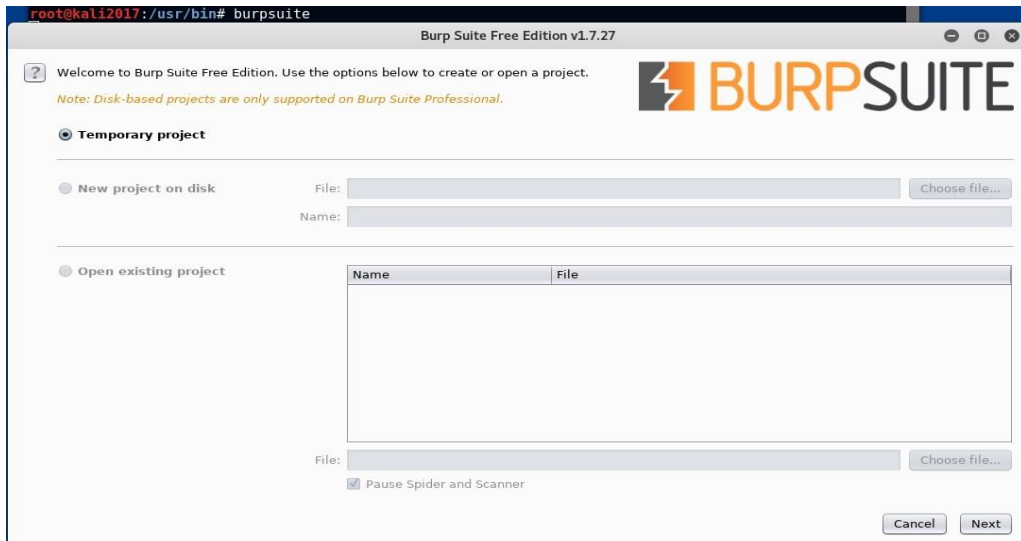
Demo

- Update BurpSuite Free Edition

```
root@kali2017:~/Downloads# cd /usr/bin
root@kali2017:/usr/bin# mv burpsuite burpsuite.old
root@kali2017:/usr/bin# cp /root/Downloads/burpsuite_free_
burpsuite_free_linux_v1_7_27.sh burpsuite_free_v1.7.27.jar
root@kali2017:/usr/bin# cp /root/Downloads/burpsuite_free_v1.7.27.jar burpsuite
root@kali2017:/usr/bin# chmod +x burpsuite
root@kali2017:/usr/bin#
```

Demo

- Start BurpSuite Free Edition



Demo

- HUNT installation on Kali Linux 2017

- ▲ Clone the hunt repo

```
root@kali2017:~# git clone https://github.com/bugcrowd/HUNT
Cloning into 'HUNT'...
remote: Counting objects: 423, done.
remote: Total 423 (delta 0), reused 0 (delta 0), pack-reused 423
Receiving objects: 100% (423/423), 4.65 MiB | 2.77 MiB/s, done.
Resolving deltas: 100% (232/232), done.
```

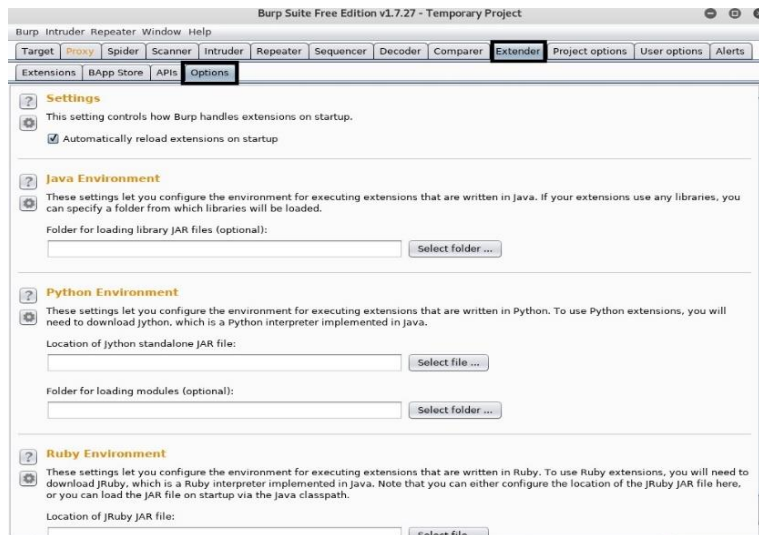
- ▲ Download the jython standalone jar from: <http://www.jython.org/downloads.html>

```
root@kali2017:~# file Jython-standalone-2.7.0.jar
Jython-standalone-2.7.0.jar: Java archive data (JAR)
```

Demo

- HUNT installation on Kali Linux 2017

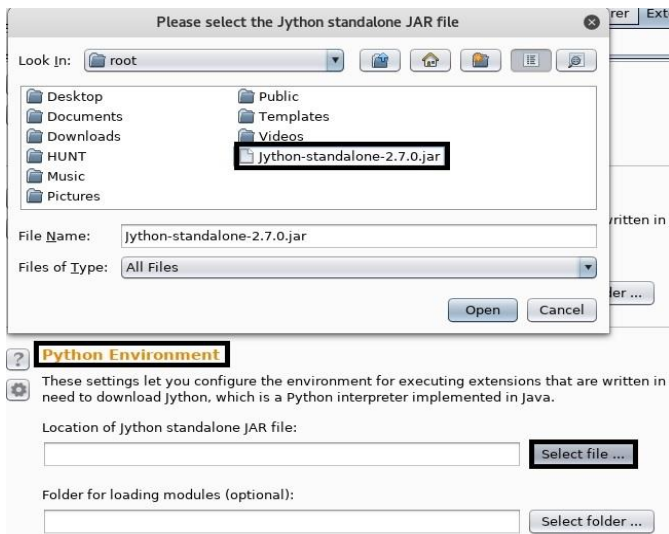
- ▲ Open Burp Suite and Click Extender -> Extender



Demo

- HUNT installation on Kali Linux 2017

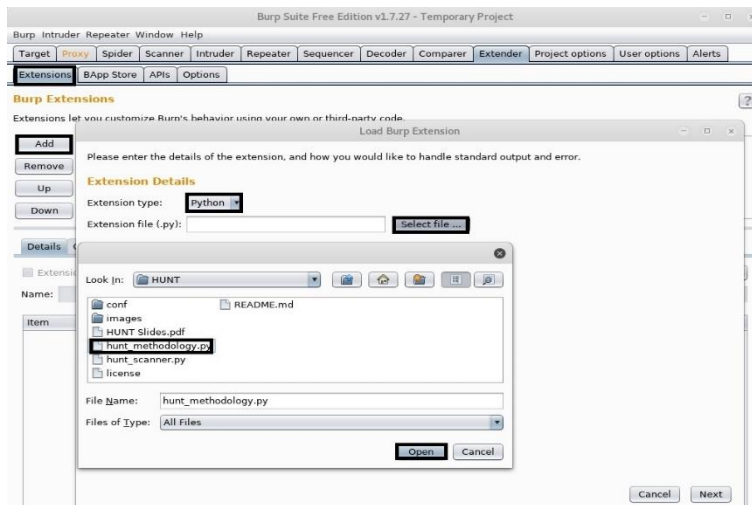
▲ Under Python Environment, click Select file, find the downloaded jython jar and double click it



Demo

- HUNT installation on Kali Linux 2017

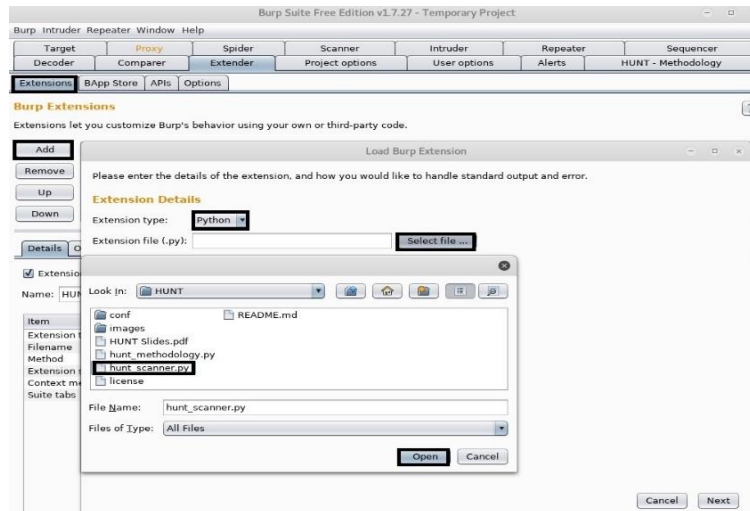
▲ Click Extensions -> Add -> Select file; Find hunt_methodology and add it



Demo

- HUNT installation on Kali Linux 2017

▲ Click Extensions -> Add -> Select file; Find hunt_scanner and add it



Demo

- HUNT installation on Kali Linux 2017

- ▲ Verify the extensions



Demo

- HUNT installation on Kali Linux 2017

- ▲ Setting Target Scope

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. All fields take regex strings. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

Include in scope

Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>	Any	192.168.10.112		

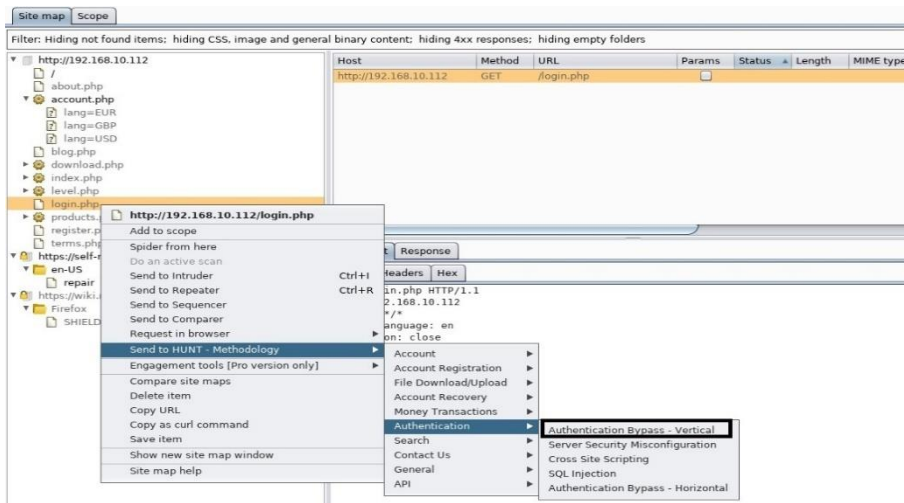
Exclude from scope

Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>	Any			logout
<input checked="" type="checkbox"/>	Any			logoff
<input checked="" type="checkbox"/>	Any			exit
<input checked="" type="checkbox"/>	Any			signout

Demo

- HUNT usage

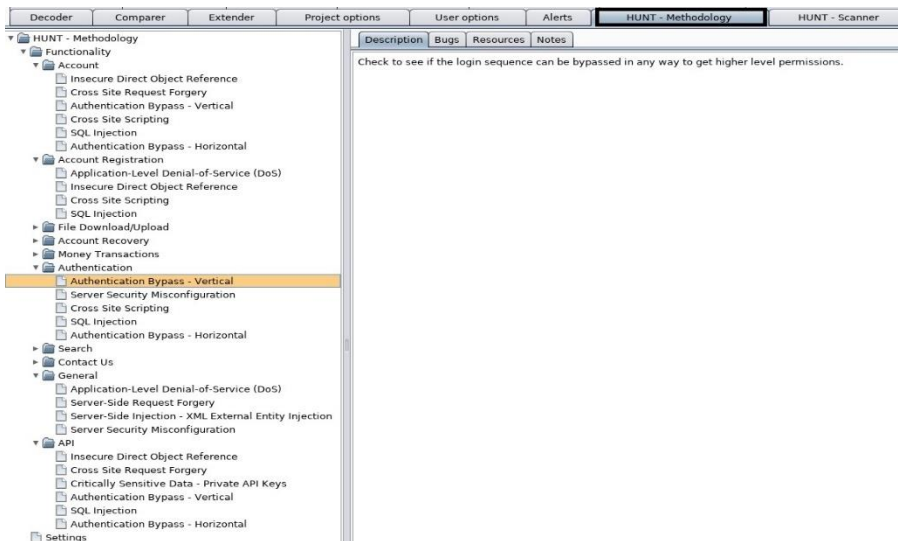
- ▲ Right Click -> Send-To Methodology Section



Demo

- HUNT usage

- ▲ Description



Demo

- HUNT usage

- ▲ Request/Response Tracking

The screenshot displays the HUNT application interface. The top navigation bar includes tabs for Decoder, Comparer, Extender, Project options, User options, Alerts, HUNT - Methodology, and HUNT - Scanner. The left sidebar shows a tree view of the HUNT - Methodology structure, with the 'Authentication Bypass - Vertical' item highlighted. The main panel on the right shows the 'Request' and 'Response' tabs, with the 'Request' tab selected. The request details are as follows:

```
GET /account.php HTTP/1.1
Host: 192.168.10.112
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.10.112/
Cookie: level=1
Connection: close
```


References

- Burp Suite
<https://portswigger.net/burp>
- HUNT Github
<https://github.com/bugcrowd/HUNT>
- Kali Linux
<https://www.kali.org/>
- OWASP
https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- Seattle VM
<https://www.gracefulsecurity.com/vulnvm/>