

New to bug bounty hunting?

Bug Bounty is a term for defining the activity of finding vulnerabilities or exploits in major vendor or web applications. However, the activities referred in this book will focus solely to finding bugs in web applications such as Facebook, Ebay, or Gmail , among other companies that have Bounty programs.

In theory, during a pen testing exercise, organisations such as Google or Facebook should be able to find all major bugs as part of their development life cycle, but even when this is properly done, it does not guarantee that the application will be free from big bugs. Bounty Programs are a way to find those bugs that are not simple to discover and which might required intensive testing with a high doses of creativity.

Our Targets: The vulnerable applications

Pen testers that are willing to spend their free time (yes free time or full time if you want to be a dedicated Bug hunter) into bug bounty hunting, have a deep desire to discover bugs no one has been capable of doing it so far. Most of the bug hunters do this part-time since there is no guarantee you will get paid for the founded bug. The bug you catch has to be 'highly priced' and acknowledged by the organisation in order to get paid good money for.

This daunting activity is definitely not for the faint of heart. It can be very fruitful but also very frustrating. If you are new to bug bounty programs, our advise is to focus on having fun and see this as a great opportunity to learn and become a ninja ZAP user. If you are having fun and learning during this activity, you will enjoyed much more, alone from the fact that maybe, just maybe , there is always a chance you will find a bug worth of some dollar\$.

Eye\$ on the price

Keep in mind that the bugs we are looking for must match the bounty price the application's owner is willing to pay for. For example, Yahoo's bounty program has clear specifications regarding which websites are part of the program and what kind of bugs are eligible. Be sure to read the disclosure agreements related to the bounty program.

Also, make sure to read careful the scope exclusions. Finding bugs in applications that already had a testing cycle is not easy. It can be very disappointing to find out that the bug you found won't receive a bounty, after you spent your entire weekend searching for bugs and declined that offer from that sexy neighbour to join her/him during friday night or have fun with your friends and family. Therefore, have a clear strategy such as:

- Understand the bounty scope
- What kind of vulnerabilities should you focus on finding
- Which web applications fall within the scope

Bug Bounty Arsenal and Training

Swiss knife: Zed Attack Proxy

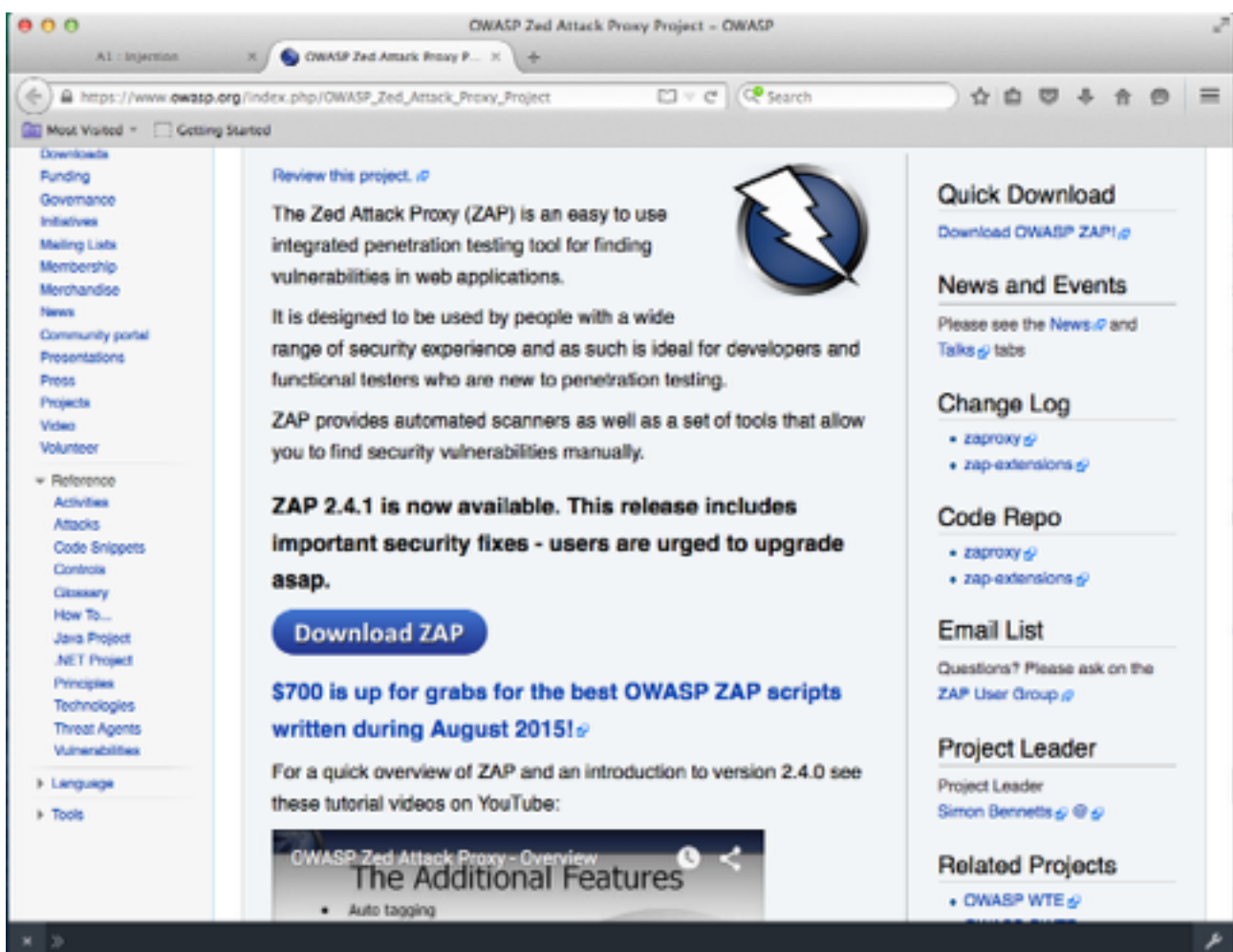
In order to be able to automate our discovery process, we need a couple of tools that help us to monitor and analyse the entire communication between the web application and our browser.

We need to target manipulation of the client 'request' and be able to understand the 'response' of the web server. This process can be complete seen by a Proxy, which acts as an intermediary between the client (our browser) and the web server hosting the application. ZAP is indeed a proxy application, that allows us to see the entire communication between the client (browser) and the web server. ZAP goes beyond that, it allow us to manipulate the entire request before is send to the web server.

ZAP is part of the OWASP projects and is one of the most actively maintained. Its creator Simon Bennets works at Mozilla as a Security Engineer.

There are different commercial and open source tools that do the same, however ZAP as an open source tool, is free and it has some incredible features that allows us to automate the entire process and discover bugs more quickly.

ZAP has a great documentation and is very easy to install. Please refer to ZAP's website: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project for download and installation.



The screenshot shows the OWASP Zed Attack Proxy Project website. The browser address bar displays https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. The page features a navigation menu on the left with categories like Downloads, Funding, Governance, Initiatives, Mailing Lists, Membership, Merchandise, News, Community portal, Presentations, Press, Projects, Video, and Volunteer. The main content area includes a 'Review this project' section with a lightning bolt icon, describing ZAP as an easy-to-use integrated penetration testing tool. It highlights that ZAP 2.4.1 is now available with important security fixes. A prominent blue button labeled 'Download ZAP' is visible. Below this, there is a link to '\$700 is up for grabs for the best OWASP ZAP scripts written during August 2015!' and a video player showing 'OWASP Zed Attack Proxy - Overview The Additional Features'. The right sidebar contains sections for 'Quick Download', 'News and Events', 'Change Log', 'Code Repo', 'Email List', 'Project Leader' (Simon Bennets), and 'Related Projects'.

The Bugs: Top Ten Vulnerabilities

The first step into bug hunting is to master the skill of identifying and understanding the top web vulnerabilities. Most bounty programs pay researchers and hackers to find them. Neal Poole(<https://nealpoole.com>) was a bug hunter before he joined Facebook as security engineer. He has a quite impressive record hunting bugs for companies like Google, Yahoo and Facebook. With bug hunting, not only you get some money but you can also get a new job!

Which are the top vulnerabilities? the OWASP top ten offers an excellent overview of which are these, but if you want to understand them much better, the OWASP testing guide (https://www.owasp.org/index.php/OWASP_Testing_Project) explains in quite detail how to execute the tests and you will be able to see how these vulnerabilities look like.

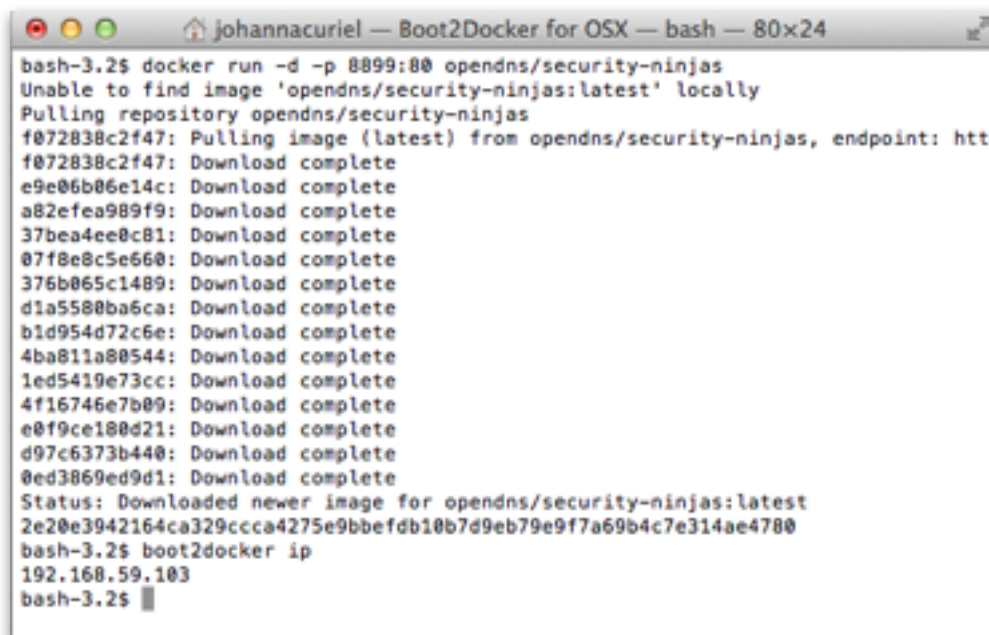
If you are familiar with the top ten that's a good start but is not enough. You need to deep dive into how the vulnerabilities are found and how they behave. The easiest way to do this is by practicing in an already vulnerable application by default. For practicing and studying purpose there are some great vulnerable apps we strongly recommend. Take the OWASP testing guide along with this exercise and you will be a ninja hunter in no time.

OWASP Security Ninjas AppSec Training Program

This open source vulnerable web app was built by Shruti Gupta(https://www.owasp.org/index.php/Category:OWASP_Security_Ninjas_AppSec_Training_Program). It is a great training app because it focuses on the top ten vulnerabilities and it is very easy to install and destroy using docker. Please download and follow the instructions. We are about to begin our hunting adventure.

Open your docker terminal and run 'docker run -d -p 8899:80 opendns/security-ninjas'

Check your boot2docker ip address



```
johannacuriel — Boot2Docker for OSX — bash — 80x24
bash-3.2$ docker run -d -p 8899:80 opendns/security-ninjas
Unable to find image 'opendns/security-ninjas:latest' locally
Pulling repository opendns/security-ninjas
f072838c2f47: Pulling image (latest) from opendns/security-ninjas, endpoint: htt
f072838c2f47: Download complete
e9e06b06e14c: Download complete
a82efea989f9: Download complete
37bea4ee0c81: Download complete
07f8e8c5e660: Download complete
376b065c1489: Download complete
d1a5580ba6ca: Download complete
b1d954d72c6e: Download complete
4ba811a80544: Download complete
1ed5419e73cc: Download complete
4f16746e7b09: Download complete
e0f9ce180d21: Download complete
d97c6373b440: Download complete
0ed3869ed9d1: Download complete
Status: Downloaded newer image for opendns/security-ninjas:latest
2e20e3942164ca329ccca4275e9bbefdb10b7d9eb79e9f7a69b4c7e314ae4780
bash-3.2$ boot2docker ip
192.168.59.103
bash-3.2$
```



And wuala! ready for hunting.

Top Bug #1: Injection

Most of these exercises can be executed without ZAP, but since our goal is to learn uncover and practice with our arsenal favourite tool, we will do this exercises using it

