Module Trainers and Authors

Jason Haddix
@jhaddix
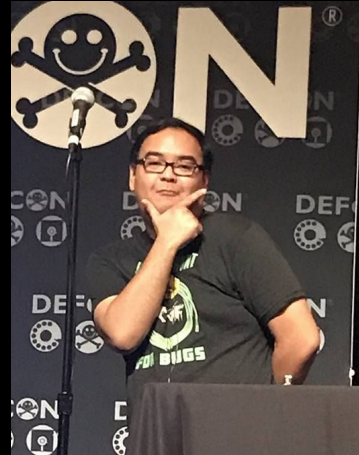
JP Villanueva
@swagnetow

Bugcrowd University Introduction

1. What is BCU?
2. Module structure?
3. Bounty basics
4. How do Labs work?
5. Prerequisites
6. Tools
7. Resources

bugcrowd.com

Goals

Level-up our crowd:

1. Analyze critical bug classes

2. Analyze common newcomer questions

3. **Bring training to the crowd**

Public Crowd

Submitted Crowd

ACS Qual Crowd

ACS + BG Checked
&
ID Verify

ACADEMY

ACADEMY

Modules

Phase 1

Newcomer modules

- Introduction to BCU
- What makes a good submission
- Introduction to Burp Suite
- Reconnaissance and Discovery

Intermediate modules

- Insecure Direct Object References
- Security Misconfiguration
- Server Side Request Forgery

Next phases

- Threat Modeling a Web Application

- XML External Entity Injection
- Web Services Testing
- Cross Site Scripting
- ++

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

```
                 Sublist3r

        # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```
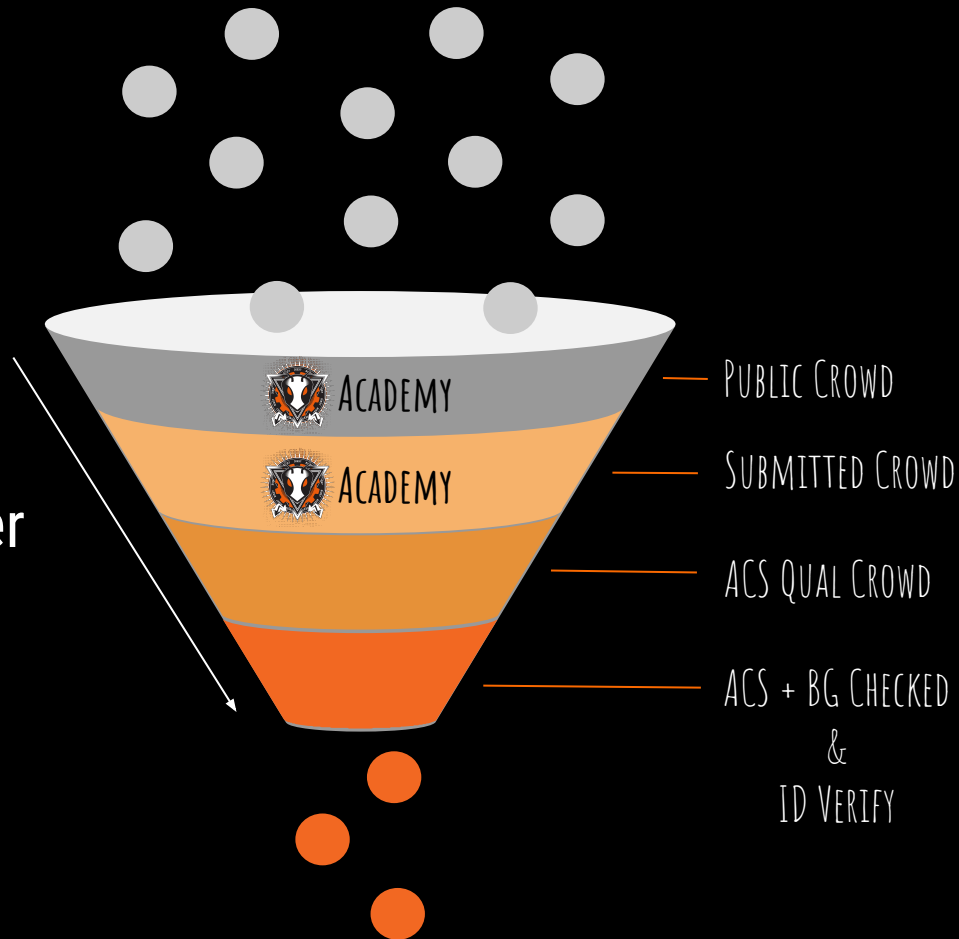
Modules

Each module has a few sections

| Brief Introduction to the Topic | Where to find the bug | Variants, examples, and more | Tooling | Labs | Resources |

A Program Brief

bugcrowd

How it Works   Solutions   Customers   Resources   Programs   About

Request a Demo

Tesla
Accelerating the world's transition to sustainable energy

🏳 **$100 – $10,000** per vulnerability
ⓑ Managed by Bugcrowd

SUBMIT REPORT   ☆

Program details   Hall of Fame

Tweet   Share 148

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting process.

For vehicle or product related services
While we use Bugcrowd as a platform for rewarding all issues, please report vehicle and product related issues directly to vulnerability@teslamotors.com, using our GPG key to encrypt reports containing sensitive information.

Third-party bugs
If issues reported to our bug bounty program affect a third-party library, external project, or another vendor, Tesla reserves the right to forward details of the issue to that party without further discussion with the researcher. We will do our best to coordinate and communicate with researchers through this process.

Responsible Disclosure Guidelines
We will investigate legitimate reports and make every effort to quickly correct any vulnerability. To encourage responsible reporting, we will not take legal action against you nor ask law enforcement to investigate you providing you comply with the following Responsible Disclosure Guidelines:

- Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC).
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our services.
- Do not modify or access data that does not belong to you.
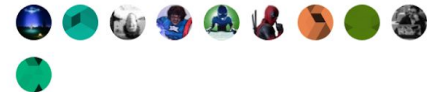- Give Tesla a reasonable time to correct the issue before making any information public.

298 vulnerabilities rewarded

Validation within **3 days**
75% of submissions are accepted or rejected within 3 days

$957.97 average payout (last 3 months)

Latest hall of famers

View all 387

Targets

*.something.com means any subdomains found are also in scope. Like:

admin.something.com

Also out of scope targets are listed.

Reward tables and focus areas

Sometimes these tables can show you where to focus as well:

Rewards

We pay rewards ranging from $100 to $10,000. Rewards are administered according to the following guidelines:

- RCE: Up to $10,000
- SQLi: $500–$10,000
- XSS: $100–$1,000
- CSRF: $100–$500
- Authentication bypass: Up to $10,000
- Horizontal privilege escalation: $500-$3,000
- Vertical privilege escalation: $500–$10,000
- Vehicle or product related vulnerabilities: case-by-case (report directly, see above)

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

                 Sublist3r

        # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```
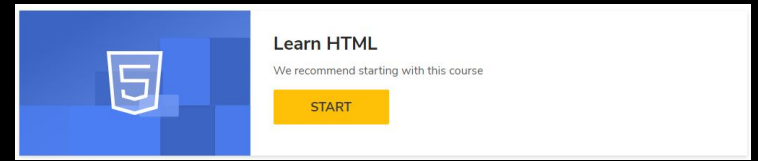
Labs

Labs

There are hundreds of open source labs and CTF challenges for module topics.

We will **curate** the best ones to help you learn the topic in as much depth as possible.

Students will set up their own lab environments.

bugcrowd.com

Insecure Direct Object Reference

Bugcrowd Open Source Software Lab Guide

Prerequisites

There is no "right" path to becoming a hacker. There are, however, some areas in which you will need to be familiar in to understand the module topics if you are starting from scratch.

We recommend the following Codecademy courses (or familiarity) before starting BCU:
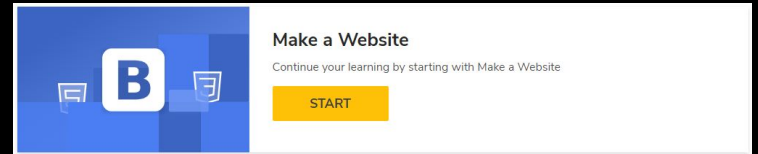
Learn HTML

We recommend starting with this course

START
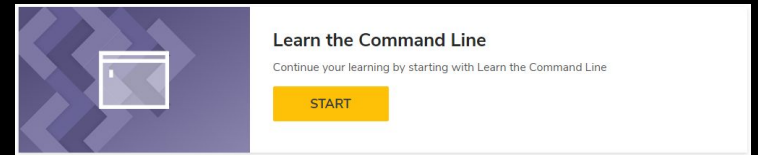
Learn JavaScript

Continue your learning by starting with Learn JavaScript

START
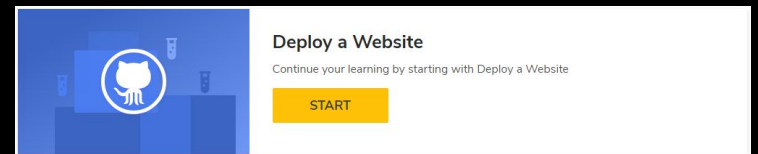
Make a Website

Continue your learning by starting with Make a Website

START

Learn the Command Line

Continue your learning by starting with Learn the Command Line

START
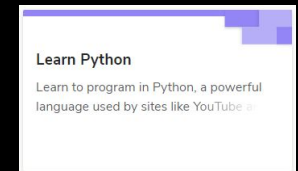
Deploy a Website

Continue your learning by starting with Deploy a Website

START

Learn SQL

Learn to communicate with databases using SQL, the standard data

Learn Python

Learn to program in Python, a powerful language used by sites like YouTube a

Core Toolset

Portswigger's Burp Suite:

OWASP ZAP
Proxy

Firefox (or Chrome)

Useful extensions:

- **FoxyProxy**
- BuiltWith or Wapplyzer
- Open Multiple URLs
- Copy Tab URLs
- Snap Links Plus
- Link Gopher
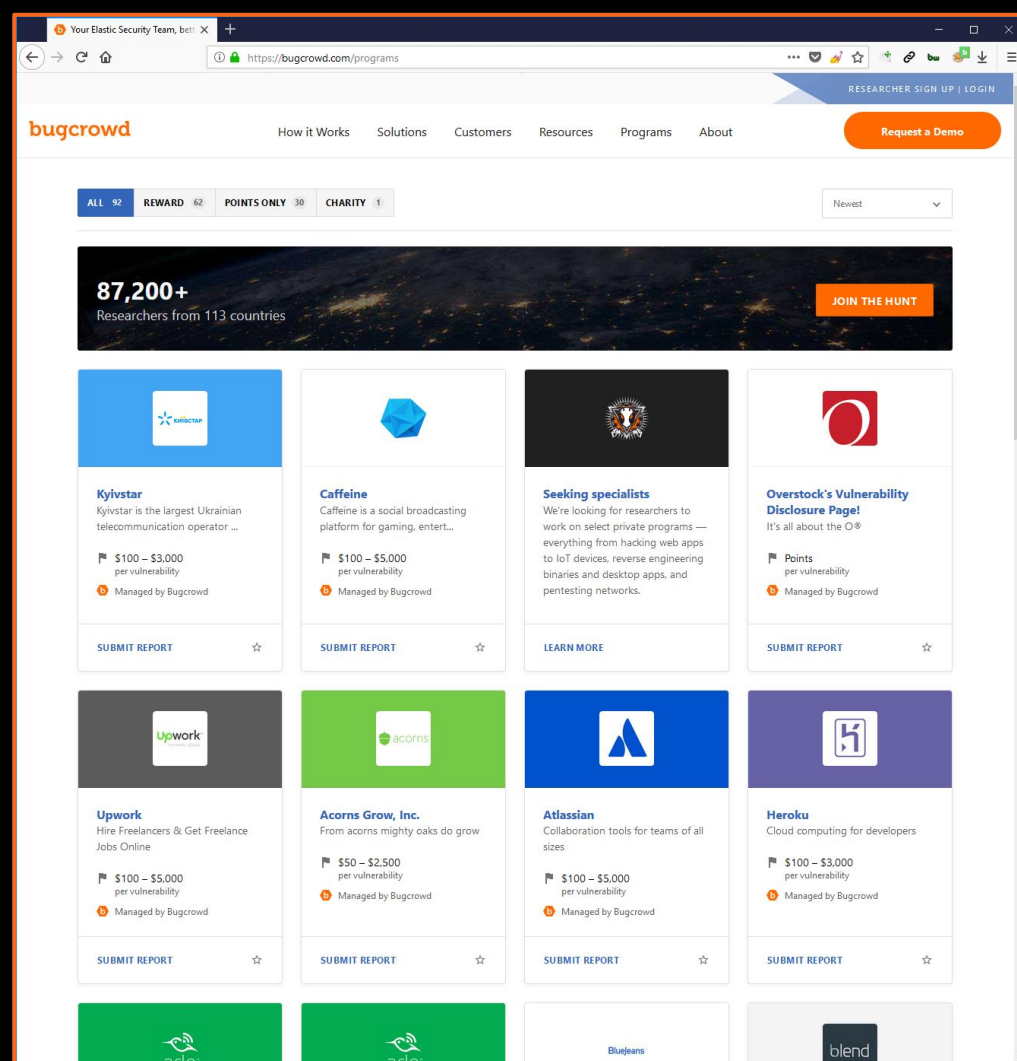
Virtual machines

Several of the labs we will utilize will be virtual machines, ISOs, or require you to host a web server. To this end Virtualbox or VMware are required.

VM's you might find useful for training are a personal sandboxed Ubuntu install and possibly Kali Linux.

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

                  Sublist3r

         # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our request
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```
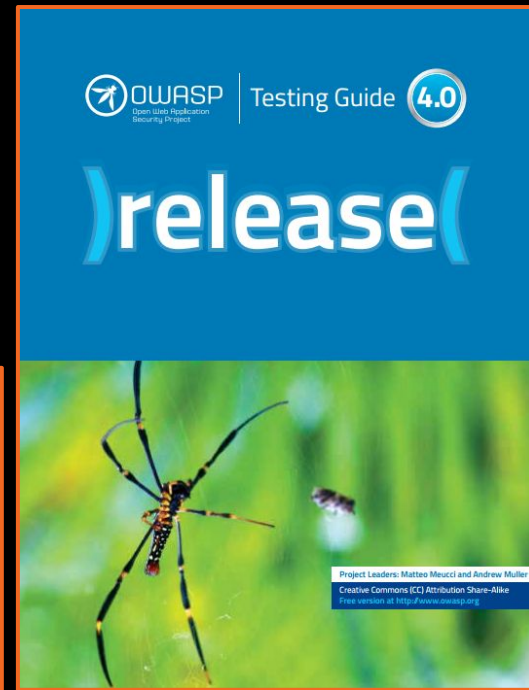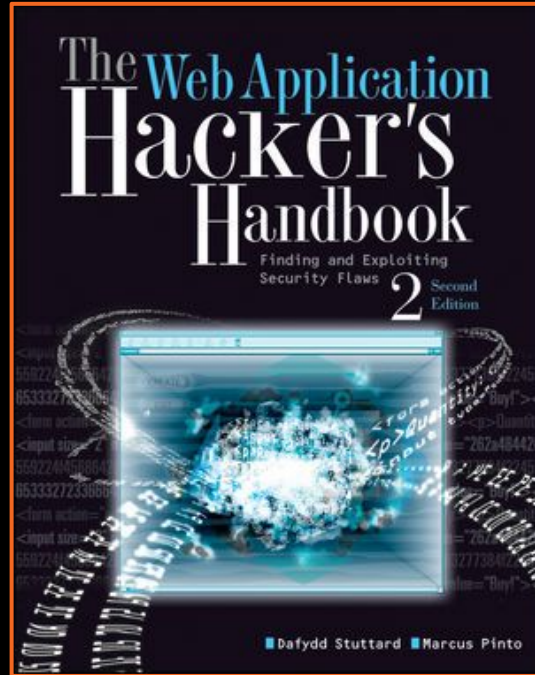
Resources

Related written course material

These two resources will be referenced in each module so you can read along and supplement BCU.

Many consider them to be the de facto web application hacking resources.

OWASP Vulnerable Web Applications Directory Project

The OWASP VWADP keeps track of many of the industries vulnerable apps created for learning.

People to Follow

In order to stay cutting edge each module will contain a Twitter list of researchers or accounts who we consider to offer value or broadcast advents related to the module topic.

Mobile
A public list by Jason Haddix
Mobile Hackery

Members **Subscribers**
33 15

Edit Delete

Tweets >
List members >
List subscribers >

List members

Prateek Gianchandani @prateekg147
iOS Hacker. Nature Lover.
Following

Moloch @LittleJoeTables
I like computers
Follow

Aditya Agrawal @exploitprotocol
Author of PentestBox(@pentestbox). Occasional Bug Bounty Participant. Railfan. Defence Enthusiast. Message me if i can be of any help.
Following

David Weinstein @insitusec
Security Research & CTO @NowSecureMobile Science'ing the sh!t out of mobile security 😱
Follow

Sira @siratool
Follow

Zach Lanier @quine
Principal Research Consultant at @atredis | Opinions == mine.
Following

Technologeeks @Technologeeks
#iOS/#OSX, #Android/#Linux #Internals & #Security.Consulting. Training. Unique #debugging tools for #MacOS/#iOS.
Follow

Kendo Alex @KendoXan
A confusing mix Kendo, climbing, photography, music and digital forensics. There is no one group I fit in 😜
Following

Kernel Quest @crakun
RCE, Danglin Ptr, UAF, Dbl Free, Buff Over/ Underflow, Off-By-1, Int Overflow/ Castin, Type Confuson, OOB, Race Cond, Inject, Logic Bug, Sym Link, Side Chanel
Follow

Justin Engler @justinengler
Security Professional
Follow

Garrett Held @GxHELD
Security Engineering @ Twilio
Follow

thuxnder @thuxnder
mov r0, pc; bx lr;
Follow

Felix M. @pleed_
IT-Sec, memgrinding
Follow

Sebas Guerrero ⚡ @0xroot
-
Follow