

Hacking 101

Filip Holec

\$ whoami

- CTO of ENGETO, Ethical Hacking course creator & lecturer
- CTF player [tuna]
- security enthusiast
- former Red Hat Quality Engineer, RHCE

\$ whatis

- introduction to ethical hacking
- motivation, required skillset
- **resources to get you started**
- Q&A

\$ ethical hacking

- hacker - originally, someone who makes furniture with an axe
- otherwise, hacking is quite a positive word
 - although not in media and specific countries
- red teaming and blue teaming
- pentesting

\$ motivation

- challenge one's abilities
- learn new area in IT - it_skill++
- potential main source of income
 - bug bounty, pentesting, internal security expert
- emerging market for cyber security
 - increase from \$3.5B in 2004 to \$115B in 2018



\$ motivation [H1 report 2018]

- learn tips and techniques
- be challenged
- have fun
- make money
- advance one's career
- do good in the world & help others
- protect and defend
- show off

\$ skillset

- learn how to program.
- get one of the open-source Unixes and learn to use and run it.
- learn how to use the World Wide Web and write HTML.
- if you don't have functional English, learn it.
- **try harder / never give up** mindset.

\$ attitude

- the world is full of fascinating problems waiting to be solved.
- no problem should ever have to be solved twice.
- boredom and drudgery are evil.
- freedom is good.
- attitude is no substitute for competence.

\$ resources to learn from

- vulnerable web apps
- online platforms for security education
- ctfs
- written content online - articles, blogs, ...
- books
- podcasts
- conferences
- + bug bounty
- + tools

\$ vulnerable web apps

- OWASP - curated list of web applications available
 - https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project
- both online & offline + ISOs

[...] list of vulnerable web applications available to security professionals for hacking and offensive activities, so that they can attack realistic web environments... without going to jail :)

\$ web apps - online platforms

- Hack The Box - machines & challenges
 - <https://www.hackthebox.eu/invite> - test to get invite code to HTB
- Avatao - e.g. CrySys 2019
 - <https://platform.avatao.com/discover/paths>
- Over The Wire - online wargames (Bandit, Natanz, ...)
 - <https://overthewire.org/wargames/>

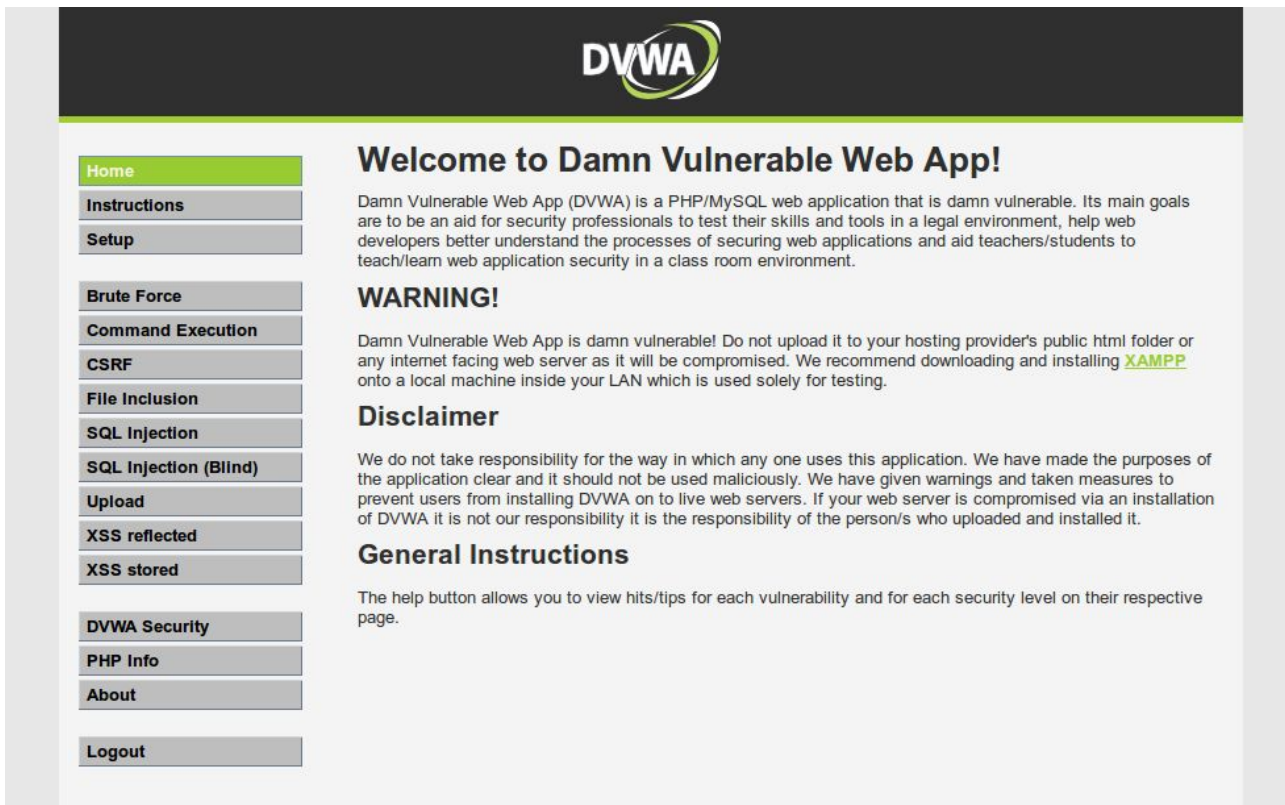
- OWASP Juice Box / DVWA / bWAPP
 - available via link on previous slide

\$ owasp juice shop



Name	Description	Status
Basket Access	Access someone else's basket.	solved
Christmas Special	Order the Christmas special offer of 2014.	solved
Deprecated Interface	Use a deprecated B2B interface that was not properly shut down.	solved
Five-Star Feedback	Get rid of all 5-star customer feedback.	solved
Login Admin	Log in with the administrator's user account.	solved
Login MC SafeSearch	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	solved
Password Strength	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	solved
Security Policy	Behave like any "white-hat" should.	solved
Weird Crypto	Inform the shop about an algorithm or library it should definitely not use the way it does.	solved

\$ dvwa



DVWA

Home

- Instructions
- Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

\$ bwapp

bwAPP
an extremely buggy web app!

Choose your bug:
----- bWAPP Xmas Hacking Challenge ----- Hack

Set your security level:
low Set Current: low

[Bugs](#) [Set Security Level](#) [Credits](#) [Blog](#) [Logout](#) [Welcome Bee](#)



/ Portal /





bwAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bwAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for educational purposes only.

Which bug do you want to hack today? :)

----- bWAPP Xmas Hacking Challenge -----
SQL Injection (Search)

Hack

bwAPP is for educational purposes only / Follow @MME_IT on Twitter and receive our cheat sheet, updated on a regular basis / © 2014 MME BVBA

\$ other online materials

- Hacker news - <https://news.ycombinator.com/>
 - news curated by community - top posts are most relevant
- Hacksplaining - <https://www.hacksplaining.com/>
 - security training for developers
- VulnHub - <https://www.vulnhub.com/>
 - provide materials that allows anyone to gain practical 'hands-on' experience in security
- Live overflow - <https://liveoverflow.com/>
 - place to learn about topics such as buffer/heap overflows, reverse engineering, vulnerability analysis, debugging, fuzzing and generally hacking
- Smash the stack - <http://smashthestack.org/>
 - wargaming network

\$ ctfs

- Capture The Flag
 - competition for security professionals and students / enthusiasts
 - <https://ctftime.org/> - aggregator for CTFs
 - goal: test one's skills in a series of challenges
 - typically have time constraint (weekend)
 - a lot of them have a reward - either reputation or money

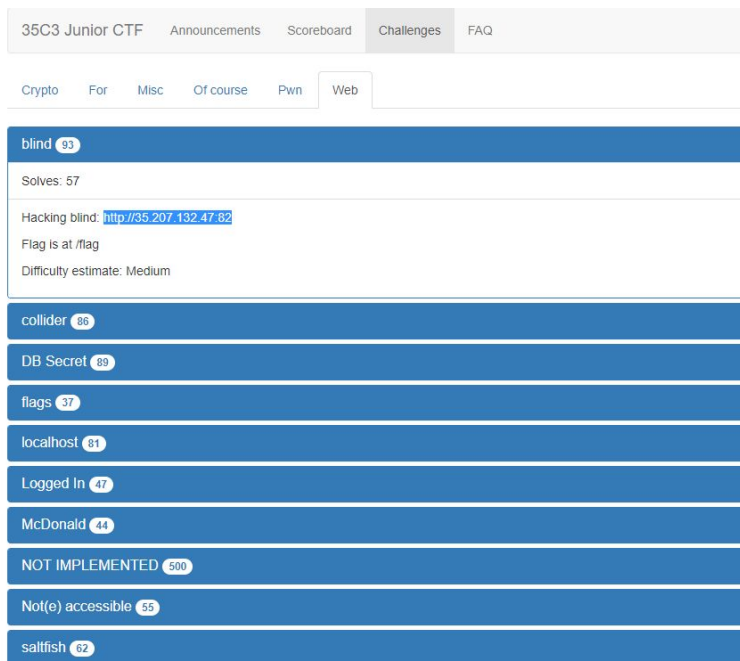
\$ use case - PicoCTF

- PicoCTF - <https://2018game.picoctf.com/>
 - *PICOCTF IS A FREE COMPUTER SECURITY GAME TARGETED AT MIDDLE AND HIGH SCHOOL STUDENTS. THE GAME CONSISTS OF A SERIES OF CHALLENGES CENTERED AROUND A UNIQUE STORYLINE WHERE PARTICIPANTS MUST REVERSE ENGINEER, BREAK, HACK, DECRYPT, OR DO WHATEVER IT TAKES TO SOLVE THE CHALLENGE*

The screenshot shows the PicoCTF website interface. At the top, there is a blue navigation bar with links for "Game", "Engblems", "Shell", "Scoreboard", and "News". Below the navigation bar, the page is divided into two main sections: "Problems" on the left and "Score: 0" on the right. A light blue notification box is centered on the page, stating: "We have exhausted server capacity to support new accounts. This will be fixed in the near future. For status updates, please see [this Piazza post](#). For status on problems, read the [Problem Statuses](#) pinned post on Piazza. This will include any problems that have been disabled or revised." Below the notification, there is a list of problems. The first problem is "Forensics Warmup 1 - Points: 50 - (Solves: 18601)" with the category "Forensics - Unsolved". The problem description is "Can you unzip this file for me and retrieve the flag?". There is a "Submit!" button and a text input field. The second problem is "Forensics Warmup 2 - Points: 50 - (Solves: 17598)" with the category "Forensics - Unsolved". The problem description is "Hmm for some reason I can't open this PNG? Any ideas?". There is a "Submit!" button and a text input field. The third problem is "General Warmup 1 - Points: 50 - (Solves: 23273)" with the category "General Skills - Unsolved".

\$ use case - 35C3 Junior

- 35c3 Junior CTF - <https://junior.35c3ctf.ccc.ac/>
 - *Some of them are working - mainly to see the concept of CTF*



The screenshot shows the 35C3 Junior CTF website interface. At the top, there are navigation tabs: "35C3 Junior CTF", "Announcements", "Scoreboard", "Challenges", and "FAQ". Below these are sub-tabs for "Crypto", "For", "Misc", "Of course", "Pwn", and "Web". The "Challenges" tab is active, displaying a list of challenges. The "blind" challenge is highlighted, showing its details: "Solves: 57", "Hacking blind: <http://35.207.132.47:82>", "Flag is at /flag", and "Difficulty estimate: Medium". Other challenges listed include "collider", "DB Secret", "flags", "localhost", "Logged in", "McDonald", "NOT IMPLEMENTED", "Not(e) accessible", and "saltfish".

Challenge Name	Solves
blind	93
collider	86
DB Secret	89
flags	37
localhost	81
Logged in	47
McDonald	44
NOT IMPLEMENTED	500
Not(e) accessible	55
saltfish	62

\$ use case - Czech CTF example

- The Catch - <https://www.thecatch.cz/>
 - 1-4 members
 - Czech round in Prague, finals in Japan
- CTFs at/for conferences
 - <https://konferencesecurity.cz/>
 - <https://2019.prague.wordcamp.org/ctf/>
 - Catch The Qubit for <https://qubitconference.com/>

\$ use case - Slovak CTF example

- Guardians 2019 - <https://wargame.sk/>
- only for individuals - no teams
- storyline - elections: compromised security
 - prevent data leak that could harm candidates

\$ online written resources

- OWASP Top Ten Project
 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- write-ups from disclosed bug bounties
- awesome-bug-bounty, awesome-security and awesome-pentest lists
 - e.g. <https://github.com/djadmin/awesome-bug-bounty>
- write-ups of past CTFs
- + written/video write-ups on retired Hack The Box machines
 - Valentine - <https://www.youtube.com/watch?v=XYXNvemgJUo>

\$ books

- the web application hacker's handbook: finding and exploiting security flaws
 - 2nd edition [Dafydd Stuttard, Marcus Pinto]
- OWASP testing guide v4
 - free, https://www.owasp.org/index.php/OWASP_Testing_Project
- the hacker playbook 3: practical guide to penetration testing [Peter Kim]
- hacking: the art of exploitation [Jon Erickson]
- web hacking 101 [Peter Yaworski] - bug bounties

\$ podcasts

- hackable - <https://hackablepodcast.com/>
 - view on security from consumer point of view, recommended for beginners

- unsupervised learning - <https://danielmiessler.com/podcast/>
 - content curation as a service
 - ~30 minute overview of news in security, technology and humans
 - senior IT Security researcher
 - Creator and leader of the OWASP IOT security project & SecLists project

\$ others

- Pentester Land - <https://pentester.land/>
 - really nice resource with news, cheatsheets, conference news etc.
- Zero Daily - <https://www.hackerone.com/zerodaily>
 - Hacking, AppSec, and Bug Bounty newsletter
- The Secure Developer
 - <https://www.heavybit.com/library/podcasts/the-secure-developer/>
 - podcast about security for developers, covering tools and best practices

\$ certifications

- OSCP, OSCE by offensive security
- CEH - certified ethical hacker
- CISSP, Security+
- ... + a lot more
- **not needed if starting with security/bug bounty**
- mainly a **formal** requirement in job descriptions

\$ conferences

- OWASP Local Chapters
- DEFCON & BlackHat - largest ones, LV, US (+ onsite/online CTF)
- Chaos Communication Congress - every year, DE (+ onsite/online CTF)
- **Security Session** - Brno, CZ (+ onsite CTF)
- Def Camp - important sec conference in CEE, RO (+ onsite CTF)
- Hacktivity - Budapest, HU
- nearly all of them publish talks & materials online
 - e.g. <https://media.ccc.de/> and others

\$ bug bounty

- break software & get paid in the process
- earn \$ and reputation
- everyone can start, just register at a bug bounty platform
 - <https://www.hackerone.com/start-hacking>
- start with public programs, then get invites into private ones
 - or use <https://ctf.hacker101.com/>

\$ bug bounty platforms

- hackerone
 - <https://hackerone.com/bug-bounty-programs>
- bugcrowd
 - <https://bugcrowd.com/programs>
- hactrophy [SK]
- bountysource
- ... plus private programs
 - facebook
 - google

\$ tools used by security experts

- OWASP ZAP - active scanner + proxy
- burp suite - proxy
- firefox - web browser
- nmap - network scanner
- wireshark - network traffic analyzer
- hydra - bruteforce password cracker
- sqlmap - SQL Injection checker
- gobuster/dirb - enumerate endpoints
- nikto - web application scanner
- SPARTA - GUI application to simplify network penetration testing
- binwalk - analysis of a resource (img/zip) to see resources within

\$ tips and hints

- find a team you can work with
- challenge yourself
- try harder attitude
- ... add your own in

\$ q&a

**NOT SURE IF THEY'RE CLAPPING FOR MY
PRESENTATION**



OR BECAUSE ITS FINISHED