Where To Learn Ethical Hacking & Penetration Testing

infosecmatter.com/where-to-learn-ethical-hacking-and-penetration-testing

August 12, 2020

Many people keep asking how to get into the information security field and how to become ethical hacker or a penetration tester.

Whether you are a seasoned IT professional looking to get into the infosec industry or you are just starting your journey, here is something that can definitely kick-start your career in the right direction.

In this blog post we are going to be talking about resources where we can legally learn and practice ethical hacking, penetration testing, CTF (Capture the flag) and wargaming.

Why practice hacking?

Websites where we can legally practice ethical hacking skills are probably one of the best ways how to get into the field of offensive security.

But even experienced penetration testers and red teamers can benefit from it a lot, because as we all know in the infosec world – there is never an end to anything in this field.

We must always keep learning new tricks and keep sharpening our skills, because the industry never stops evolving.

Online learning resources

Here's a list of some of the best online resources for practicing ethical hacking skills covering variety of technological areas.

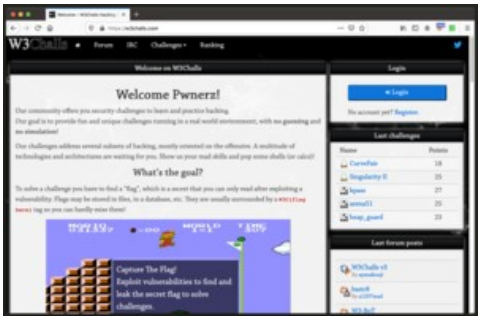
1. WeChall.net

WeChall.net is one of the long standing hacking challenge and problem solving sites. It contains challenges from many different areas including:

- Web application exploitation (PHP, MySQL, Javascript ..)
- Linux command line and shell
- Crypto and steganography
- Programming challenges
- Source code analysis …

The site contains more than 145 high quality challenges, with detailed scoreboard system and integration with other similar training websites.

2. W3challs.com



W3challs.com offers unique challenges running in a real world environment, with no guessing and no simulation. The challenges cover areas including:

- Reverse engineering and cracking (Windows, Linux)
- Binary exploitation (Linux, ARM)
- Web application exploitation
- Cryptography
- Forensics …

The site contains almost 100 high quality challenges.

3. OverTheWire.org

OverTheWire.org is a training site with more than 16 high quality wargames, with multiple levels of difficulty in each wargame, altogether containing more than 180 challenges.

The flavor of these wargames cover areas such as:

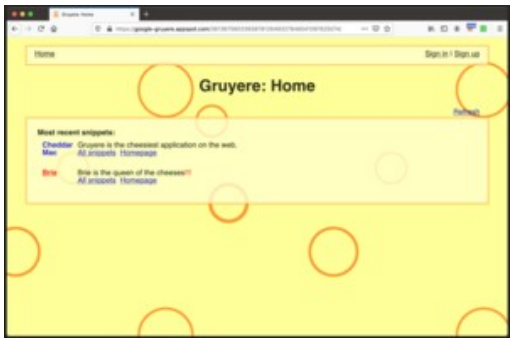
- Linux command line and shell
- Web application exploitation
- Linux binary exploitation (assembler)

- Coding / hacking techniques
- Reverse engineering …

Most challenges are in a form of SSH shell access with a vulnerable program and its source code available.

4. Google Gruyere

Google Gruyere is a vulnerable web application written in Python, which also teaches defenses. It covers typical web application security problems such as:



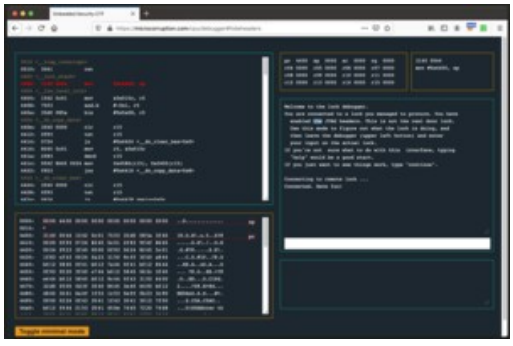
- Cross-Site Scripting (XSS)
- Cross-Site Forgery (XSRF)
- Path traversal
- Code execution
- AJAX vulnerabilities
- Information disclosure …

Every challenge contains **hints**, a **solution** (exploit) and a **fix** section discussing best coding practices on how to fix those vulnerabilities.

It is a really well made application which teaches both sides of the fence (offense and defense). And it can also be downloaded for offline use!

5. Microcorruption.com

Microcorruption.com is a CTF project for practicing embedded electronic device security.



The goal is to reverse engineer an electronic lock and bypass its security features.

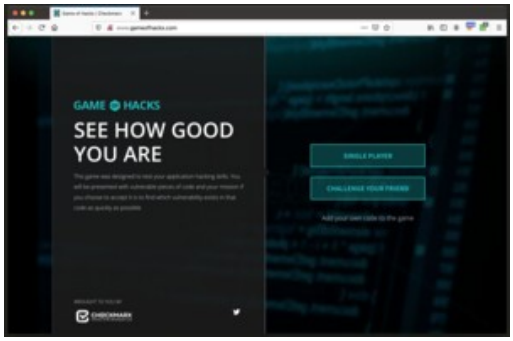
This CTF is definitely not for beginners, but it does contain a very nice tutorial explaining various areas of the debugger such as:

- Code disassembly
- Live memory dump
- CPU registry states
- I/O console …

A manual with assembly instructions for the device is also included.

6. Game of Hacks

Game of Hacks is a website where you have to read a programming code and find vulnerability in the code.



It is super fun and quick challenge, ideal for people who want to get proficient in source code review, application security and vulnerability analysis.

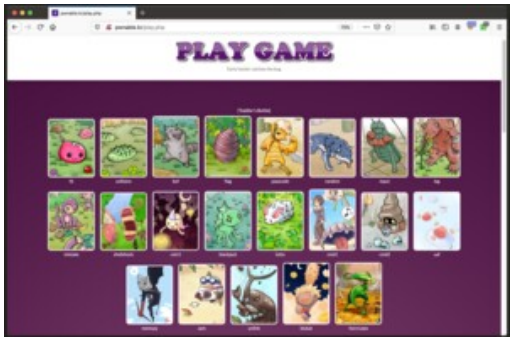
The challenges include snippets of code from the following programming languages and possibly more:

- Javascript
- C++, C
- Python
- Java
- PHP …

Each challenge consist of 5 random code snippets where you have to select the correct answer as fast as possible.

7. Pwnable.kr

Pwnable.kr is a CTF site containing more than 65 high quality wargames aimed to practice skills of UNIX system exploitation and binary exploitation.



This website will challenge you in the following areas:

- UNIX system knowledge
- Reverse-engineering
- Linux kernel internals
- Bug exploitation
- Programming
- Cryptography …

Most of the challenges consist of a network server which you have to exploit remotely or an SSH shell access with instructions in the home directory.

In most cases the source code of the vulnerable program (typically in C or C++) is available.

8. Hack The Box

Hack The Box is a popular online platform with a large number of vulnerable machines, free for you to exploit and test your skills.

This allows you to learn and master your pentesting skills holistically. It is a playground where almost nothing is forbidden and where you get to practice all these areas:

- Network reconnaissance
- Vulnerability discovery
- Real world exploitation
- Privilege escalation
- Network scanning
- Pivoting and lateral movement
- Web application vulnerabilities …

It is probably the closest thing to OSCP that you can possibly get.

9. Hacking-Lab

Hacking-Lab is an online ethical hacking platform that aims to teach offensive security and penetration testing holistically.

It contains hundreds of challenges practicing many different aspects of penetration testing, forensics, web application security, mobile security, cryptography, networking, reverse engineering, vulnerability scanning and many other related topics.

Have a look on the list of challenges available on the platform to get the picture of just how comprehensive this platform is.

The only downside might be that it is not free and requires a membership fee.

10. SmashTheStack

SmashTheStack is a wargaming network hosting several wargames with more than 48 challenges in total.

The flavor of challenges include:

- Networking
- Binary exploitation
- Reverse engineering

- Assembly challenges
- Cryptography and encryption
- Web application vulnerabilities

This is definitely very interesting and unique collection of challenges to play!

11. IO wargame

IO wargame is a collection of 4 wargames focused on binary exploitation, reverse engineering and cracking of programs on UNIX platform with focus on different processor architectures.

The following architectures are currently covered by the site:

- x86
- x86_64
- ARMv7

The site contains around 60 challenges in total. All of them are in a form of SSH shell access with a vulnerable program and sometimes its source code available.

If you ever wanted to get proficient with GDB and Radare2, this is definitely for you.

12. Defend the Web

Defend the Web is an interactive cyber security platform for practicing web application security topics.

It contains more than 60 challenges in the playground section covering topics such as:

- Web application security
- CAPTCHA bypass
- Cryptography
- SQL injection
- Javascript …

It also comes with a collection of coding and hacking articles discussing the vulnerabilities in detail and with code examples.

13. Hellbound Hackers

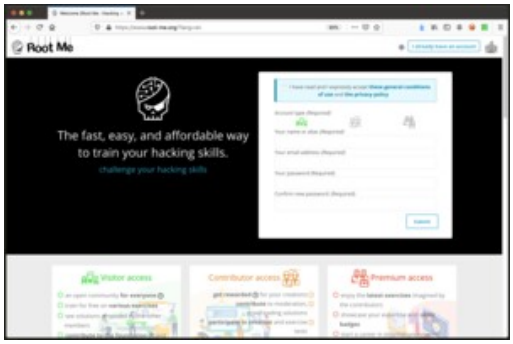
Hellbound Hackers is a site containing many different simulated security challenges from the following categories:

- Web application exploitation
- Application cracking (Windows)
- Cryptography and steganography
- Programming and code patching
- Social engineering and tracking
- Privilege escalation
- Realistic challenges …

The challenges are very well made, diverse and captivating. With around 170 challenges in total, this site can really teach you a lot of tricks!

14. Root Me

Root Me is a cyber security learning platform covering whole range of topics such as:



- Binary exploitation (Linux, Windows, x86, x64, ARM, MIPS, kernel)
- Web application security (client and server)
- Forensics, log file analysis, dump file analysis
- Network services, packet capture and analysis
- Cracking, cryptoanalysis, steganography
- Programming ans scripting
- Realistic challenges …

There is more than 370 challenges in total and 170 virtual environments to practice ethical hacking skills. This is truly a remarkable learning platform with many real world applicable challenges.

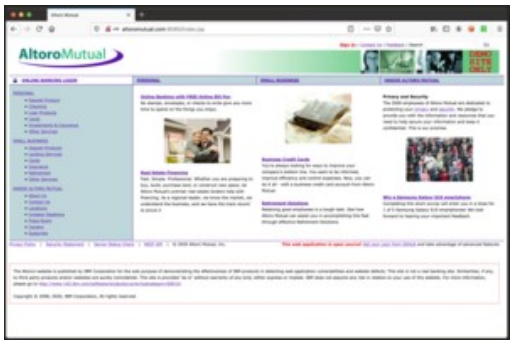
15. Altoro Mutual

Altoro Mutual is a sample banking J2EE web application for practicing ethical hacking against a bank.

It's a web application, so you can practice all sorts of attacks such as:

- Cross-Site Scripting (XSS)
- Indirect Object Reference (IDOR)
- Sensitive data disclosure

- Authorization issues
- SQL injections …



You can either deploy your own instance or use the demo site available at http://altoromutual.com:8080/

Log in with jsmith/demo1234 or admin/admin and start playing.

16. CloudGoat

CloudGoat is AWS (Amazon Web Services) deployment tool which will help you deploy a vulnerable AWS cloud environment for you to practice hands-on real world cloud penetration testing.

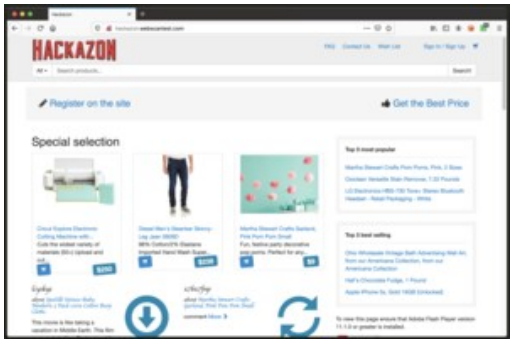
After you deploy your infrastructure with CloudGoat, you can then practice several “capture-the-flag” style scenarios in your cloud.

Currently there are 7 scenarios available which entail all sorts of tasks and challenges. The goal is, as an attacker, to compromise the cloud. This will give you real hands-on and practical experience with the cloud security topics.

In order to play with this, you will have to be spending around $1-3 per day for your AWS cloud, depending on your usage.

17. Hackazon

Hackazon is free, vulnerable testing website that is an online storefront using typical modern technologies.



It has an AJAX interface, strict workflows and RESTful API’s for a mobile application. This provides uniquely-effective training and testing experience resembling a real world penetration testing target.

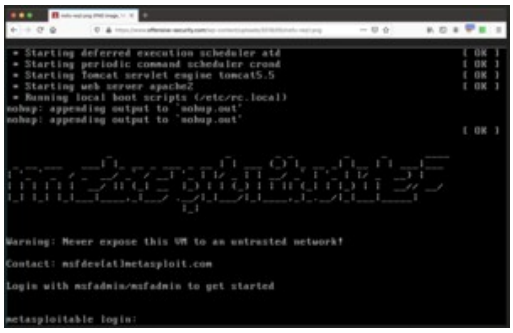
You can either deploy your own instance or use the demo site available at http://hackazon.webscantest.com/

Offline learning resources

Here's a list of some of the best resource available for practicing ethical hacking techniques and mastering penetration testing skills offline without Internet access.

18. Metasploitable2

Metasploitable2 is an intentionally vulnerable Linux virtual machine, specifically designed for learning UNIX environment and Metasploit framework skills.



But that's not all! It also contains:

- OWASP Mutillidae – A deliberately vulnerable web-application
- DVWA – Damn Vulnerable Web Application

So it's really a comprehensive VM where we can also practice discovery and exploitation of web applications.

Download VM here, see guide here.

19. Metasploitable3

Metasploitable3 is a next iteration of Metasploitable, but this time it comes with 2 vulnerable virtual machines:

- Windows Server 2008
- Ubuntu Linux 14.04

Both VMs are pre-installed with tons of modern software (see the list) and contain large amount of security vulnerabilities. It is therefore very rich playground, ideal targets for testing exploits with Metasploit.

Note that there are no VMs to be downloaded – you have to build the VMs yourself using a build script (github).

20. Damn Vulnerable iOS Application (DVIA)

Damn Vulnerable iOS Application (DVIA) is a set of two vulnerable iOS applications for practicing iOS penetration testing skills.

The challenges include vulnerabilities that can be found during real world pentests of mobile applications:

- Jailbreak detection
- Local Data Storage issues

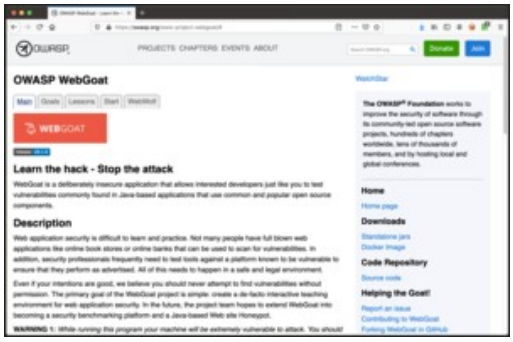
- Face/Touch ID Bypass
- Broken cryptography
- Certificate pinning
- Data Leakage …

It comes with tutorial on how to start and a detailed blog post series on iOS application security (link).

Highly recommended for anyone looking into mobile application penetration testing!

21. OWASP WebGoat

OWASP WebGoat is a deliberately insecure J2EE web application for practicing exploitation of vulnerabilities commonly found in Java-based applications and applications that use popular open source components.

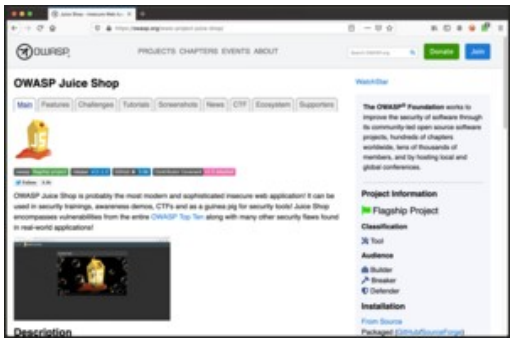


It is a realistic teaching environment full of real world scenarios with hints, code snippets and detailed explanations of the vulnerabilities.

This is one of the best resources for learning web application security with tons of related material where you really get to practice the OWASP Top 10 vulnerabilities.

22. OWASP Juice Shop

OWASP Juice Shop is probably the most modern web application full of bugs. It is an e-shop application written in Node.js, Express and Angular, so it is very very modern.



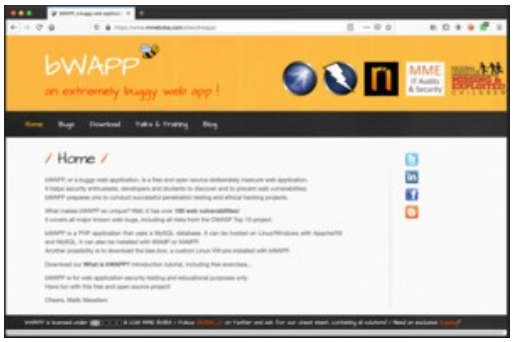
The application contains over 95 hacking challenges (list) of varying difficulty, from the following categories:

- Broken access control and authentication
- Improper input validation with many different injections
- Cryptography issues and security misconfiguration
- Cross-Site Scripting (XSS)
- XML External Entity (XXE)
- Sensitive data exposure
- Insecure deserialization …

This project will most definitely help to get you up to speed for pentesting of e-commerce sites, e-shops and alike.

23. bWAPP

bWAPP is an extremely buggy web application with over 100 bugs. It covers all OWASP Top 10 vulnerabilities and much more. For instance:



- Injections (SQL, iFrame, SSI, PHP, XML, XPath, LDAP…)
- Cross-Site Scripting (XSS), Cross-Site Tracing (XST)
- AJAX and Web Services issues (jQuery/JSON/XML/SOAP/WSDL)
- XML External Entity (XXE) and Server Side Request Forgery (SSRF)
- Authentication, authorization and session issues
- Arbitrary file access, directory traversals
- Local and remote file inclusions (LFI/RFI)
- Heartbleed and Shellshock vulnerability (OpenSSL)
- HTTP protocol tampering …

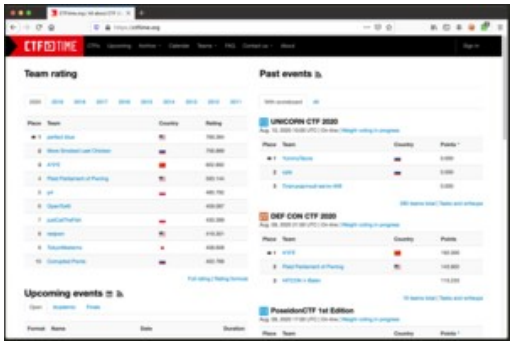
See the full list of bugs for more details.

More learning resources

If you would like even more challenges, check out the following massive resources.

24. CTFTime

CTFTime is a portal archiving CTF events and CTF competitions that took place somewhere around the world.



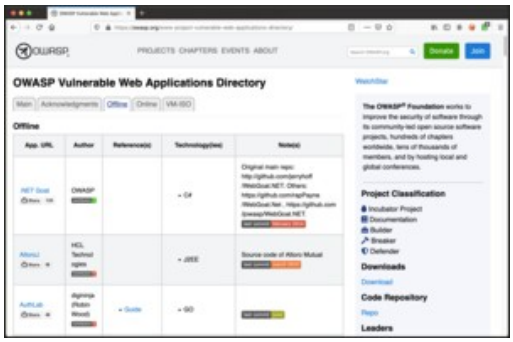
There are literally hundreds of these events happening each year and some of them have really excellent challenges.

The main mission of CTFtime is to track these events and archive the challenges (and the writeups). It is therefore an excellent source of information.

In fact, it contains thousands and thousands of challenges in the archive, so this offers virtually unlimited potential for learning.

25. OWASP VWAD

OWASP VWAD stands for Vulnerable Web Applications Directory and it is a comprehensive and well maintained registry of all known vulnerable web applications currently available.



It is a repository of more than 130 currently active projects for practicing ethical hacking. They are categorized in the following 3 lists:

- Offline resources (link)
- Online resources (link)
- Downloadable VM ISO (link)

Most of the resources listed on this page are included in the OWASP VWAD directory, so go check it out if you want more. There might be some interesting projects specific to your area of focus.

Conclusion

As we all know, practice makes perfect, and with penetration testing this is twice as true. Good CTF players typically make good penetration testers.

If you just don't know where to start, simply open the first site and start exploring. Start solving the challenges from the easiest one and continue progressing to the harder ones. Clear as many of them as you can and reach as far as you can.

If you found this useful and you would like more content like this, please subscribe to our mailing list and follow us on Twitter and Facebook and get notified about new additions!

TAGS | AWS | Binary | Bindshell | Challenge | Cloud security | Competition | Cracking | CTF | Ethical hacking | Exploitation | Forensics | Hacking | Learning | Metasploit | Penetration testing | Practice | Reverse engineering | SQL injection | Training | Wargame | Web applications | Webshell | XSS

MOST VIEWED TOOLS