joe-shenouda / **awesome-cyber-skills**

Watch 69 | Star 731 | Fork 152

A curated list of hacking environments where you can train your cyber skills legally and safely http://www.shenouda.nl

92 commits | **1** branch | **0** releases | **5** contributors | Apache-2.0

Branch: **master** | New pull request | Find file | Clone or download

joe-shenouda Update README.md — Latest commit 13725a3 on Nov 23, 2017

CONTRIBUTING	Contribution Guidelines	a year ago
LICENSE	Update LICENSE	a year ago

README.md	Update README.md	6 months ago
_config.yml	Set theme jekyll-theme-architect	a year ago

README.md

awesome-cyber-skills

A curated list of hacking environments where you can train your cyber skills legally and safely

For everyone in the Information Security business, it's important to understand the enemy, the hacker. Understanding the enemy makes you the best defender you can be to secure the digital world.

> By knowing your enemy, you can defeat your enemy.

In the USA, the most senior police officers, even long after their pension, are advising residents how to secure their homes better. They come to your house and tell you where your weak points are around the house. They can advise this because they KNOW their enemy, the criminal that wants to break into the house and his techniques.

Training your cyber skills means also keeping your hacking skills up to date. To do this, you need an environment to practice in, legally and safely.

For this purpose, I have made a list of websites you can visit and practice your cyber skills. Every site has a different angle on the whole thing, so I'll summarize in a couple of words its specifics.

Some sites will offer you tutorials to help you, others will require you to find things on your own.

I will update this post below regularly and add sites to this post so bookmark it and/or follow me to see the latest overview.

If you are missing a site not mentioned in the list, feel free to contribute.

CONTRIBUTORS

- foleranser
- filinpavel
- BenDrysdale
- HrushikeshK

About the author

Joe Shenouda has extensive experience in IT, ICS & Information Security as an international hands-on technical engineer, trainer, consultant & research fellow with a successful record in developing & leading technical corporate Cybersecurity programs for military & global organizations.

Joe uses risk management in the planning phase while implementing the correct defense measures at the right place & has lead teams doing that. He has done 100-s of security assessments & audits for numerous customers.

Apart from vulnerability assessments, Joe gives LIVE hack shows where, with your permission, he will take over a server/computer, a phone or hack everyone in the room in one hit, without hurting anyone.

Using the latest hacking techniques, he will also educate the audience to explain what just happened. Joe uses Man-in-the-Middle attacks, ARP Poisoning, Sniffing, Script injections, DNS spoofing & hijacks sessions that are happening on devices & explains how to prevent them in a LIVE setting.

He can also simulate a DOS attack that brings the strongest networks down.

Well known in The Netherlands as "The Netdetective", Joe presented a MTV show on hacking for young adults.

He started his Information Security career at Tilburg University in 1999 where he did research on Cybersecurity, Cybercrime, cyber forensics, privacy & data protection.

He has a strong expertise in concept & cyber security architecture development with a lot of hands-on technical experience in cybersecurity systems. Joe was responsible for significant research work through OSINT & Darknet intel & he was the lead responsible for numerous Information Assurance projects that involved cybersecurity approaches & systems for detection, prevention, & mitigation of malicious activity.

Joe also spoke frequently on cyber security & hacking at professional conferences & published articles & blogs on issues relating to cybersecurity.

🌿 Visit me on LinkedIn or Twitter

Please share this list if you find it useful. Let me know if you like it

A□wes□□ø□□me□Cyber□~□Skil□ls

Site name	Description
$natch competition	Remote banking system containing common vulnerabilities.
Arizona Cyber Warfare Range	The ranges offer an excellent platform for you to learn computer network attack (CNA), computer network defense (CND), and digital forensics (DF). You can play any of these roles.
Avatao	More than 350 hands-on challenges (free and paid) to master IT security and it's growing day by day.
BodgeIt Store	The BodgeIt Store is a vulnerable web application which is currently aimed at people who are new to pen testing.
Bright Shadows	Training in Programming, JavaScript, PHP, Java, Steganography, and Cryptography (among others).
bWAPP	bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.

Site name	Description
Cyber Degrees	Free online cyber security Massive Open Online Courses (MOOCS).
Commix testbed	A collection of web pages, vulnerable to command injection flaws.
CryptOMG	CryptOMG is a configurable CTF style test bed that highlights common flaws in cryptographic implementations.
Cyber Security Base	Cyber Security Base is a page with free courses by the University of Helsinki in collaboration with F-Secure.
Cybersecuritychallenge UK	Cyber Security Challenge UK runs a series of competitions designed to test your cyber security skills.
CyberTraining 365	Cybertraining365 has paid material but also offers free classes. The link is directed at the free classes.
Cybrary.it	Free and Open Source Cyber Security Learning.
Damn Small Vulnerable Web	Damn Small Vulnerable Web (DSVW) is a deliberately vulnerable web application written in under 100 lines of code, created for educational purposes. It supports the majority of (most popular) web application vulnerabilities together with appropriate attacks.
Damn Vulnerable Android App	Damn Vulnerable Android App (DVAA) is an Android application which contains intentional vulnerabilities.
Damn Vulnerable Hybrid Mobile App	Damn Vulnerable Hybrid Mobile App (DVHMA) is a hybrid mobile app (for Android) that intentionally contains vulnerabilities.
Damn Vulnerable iOS App	Damn Vulnerable iOS App (DVIA) is an iOS application that is damn vulnerable.

Site name	Description
Damn Vulnerable Linux	Damn Vulnerable Linux (DVL) is everything a good Linux distribution isn't. Its developers have spent hours stuffing it with broken, ill-configured, outdated, and exploitable software that makes it vulnerable to attacks.
Damn Vulnerable Router Firmware	The goal of this project is to simulate a real-world environment to help people learn about other CPU architectures outside of the x86_64 space. This project will also help people get into discovering new things about hardware.
Damn Vulnerable Stateful Web App	Short and simple vulnerable PHP web application that naïve scanners found to be perfectly safe.
Damn Vulnerable Thick Client App	DVTA is a Vulnerable Thick Client Application developed in C# .NET with many vulnerabilities.
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 classroom environment.
Damn Vulnerable Web Services	Damn Vulnerable Web Services is an insecure web application with multiple vulnerable web service components that can be used to learn real-world web service vulnerabilities.
Damn Vulnerable Web Sockets	Damn Vulnerable Web Sockets (DVWS) is a vulnerable web application which works on web sockets for client-server communication.
Damnvulnerable.me	A deliberately vulnerable modern-day app with lots of DOM-related bugs.
Dareyourmind	Online game, hacker challenge.

Site name	Description
DIVA Android	Damn Insecure and vulnerable App for Android.
EnigmaGroup	Safe security resource, trains in exploits listed in the OWASP Top 10 Project and teach members the many other types of exploits that are found in today's applications.
ENISA Training Material	The European Union Agency for Network and Information Security (ENISA) Cyber Security Training. You will find training materials, handbooks for teachers, toolsets for students and Virtual Images to support hands-on training sessions.
exploit.co.il Vulnerable Web App	exploit.co.il Vulnerable Web app designed as a learning platform to test various SQL injection Techniques.
Exploit-exercises.com	exploit-exercises.com provides a variety of virtual machines, documentation and challenges that can be used to learn about a variety of computer security issues such as privilege escalation, vulnerability analysis, exploit development, debugging, reverse engineering, and general cyber security issues.
ExploitMe Mobile	Set of labs and an exploitable framework for you to hack mobile an application on Android.
Game of Hacks	This game was designed to test your application hacking skills. You will be presented with vulnerable pieces of code and your mission if you choose to accept it is to find which vulnerability exists in that code as quickly as possible.
GameOver	Project GameOver was started with the objective of training and educating newbies about the basics of web security and educate them about the common web attacks and help them understand how they work.
Gh0stlab	A security research network where like-minded individuals could work together towards the common goal of knowledge.

Site name	Description
GoatseLinux	GSL is a Vmware image you can run for penetration testing purposes.
Google Gruyere	Labs that cover how an application can be attacked using common web security vulnerabilities, like cross-site scripting vulnerabilities (XSS) and cross-site request forgery (XSRF). Also, you can find labs how to find, fix, and avoid these common vulnerabilities and other bugs that have a security impact, such as denial-of-service, information disclosure, or remote code execution.
Gracefully Vulnerable Virtual Machine	Graceful’s VulnVM is VM web app designed to simulate a simple eCommerce style website which is purposely vulnerable to a number of well know security issues commonly seen in web applications.
Hack The Box	Hack The Box is an online platform allowing you to test your penetration testing skills and exchange ideas and methodologies with other members of similar interests. In order to join you should solve an entry-level challenge.
Hack This Site	More than just another hacker wargames site, Hack This Site is a living, breathing community with many active projects in development, with a vast selection of hacking articles and a huge forum where users can discuss hacking, network security, and just about everything.
Hack Yourself First	This course is designed to help web developers on all frameworks identify risks in their own websites before attackers do and it uses this site extensively to demonstrate risks.
Hack.me	Hack.me aims to be the largest collection of "runnable" vulnerable web applications, code samples and CMS's online. The platform is available without any restriction to any party interested in Web Application Security.

Site name	Description
Hackademic	Offers realistic scenarios full of known vulnerabilities (especially, of course, the OWASP Top Ten) for those trying to practice their attack skills.
Hackazon	A modern vulnerable web app.
Hackertest.net	HackerTest.net is your own online hacker simulation with 20 levels.
Hacking-Lab	Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents. Furthermore, Hacking-Lab is providing the CTF and mission style challenges for the European Cyber Security Challenge with Austria, Germany, Switzerland, UK, Spain, Romania and provides free OWASP TOP 10 online security labs.
HackSys Extreme Vulnerable Driver	HackSys Extreme Vulnerable Driver is intentionally vulnerable Windows driver developed for security enthusiasts to learn and polish their exploitation skills at Kernel level.
HackThis!!	Test your skills with 50+ hacking levels, covering all aspects of security.
Hackxor	Hackxor is a web app hacking game where players must locate and exploit vulnerabilities to progress through the story. Think WebGoat but with a plot and a focus on realism&difficulty. Contains XSS, CSRF, SQLi, ReDoS, DOR, command injection, etc.
Halls of Valhalla	Challenges you can solve. Valhalla is a place for sharing knowledge and ideas. Users can submit code, as well as science, technology, and engineering-oriented news and articles.
Hax.Tor	Provides numerous interesting “hacking” challenges to the user.
Hellbound Hackers	Learn a hands-on approach to computer security. Learn how hackers break in, and how to keep them out.

Site name	Description
Holynix	Holynix is a Linux VMware image that was deliberately built to have security holes for the purposes of penetration testing.
HSCTF3	HSCTF is an international online hacking competition designed to educate high schoolers in computer science.
Information Assurance Support Environment (IASE)	Great site with Cybersecurity Awareness Training, Cybersecurity Training for IT Managers, Cybersecurity Training for Cybersecurity Professionals, Cybersecurity Technical Training, NetOps Training, Cyber Law Awareness, and FSO Tools Training available online.
InfoSec Institute	Free CISSP Training course.
ISC2 Center for Cyber Safety and Education	Site to empower students, teachers, and whole communities to secure their online life through cyber security education and awareness with the Safe and Secure Online educational program; information security scholarships; and industry and consumer research.
Java Vulnerable Lab	Vulnerable Java based Web Application.
Juice Shop	OWASP Juice Shop is an intentionally insecure web app for security training written entirely in Javascript which encompasses the entire OWASP Top Ten and other severe security flaws.
Kioptrix VM	This vulnerable machine is a good starting point for beginners.
LAMPSecurity Training	LAMPSecurity training is designed to be a series of vulnerable virtual machine images along with complementary documentation designed to teach Linux,apache,PHP,MySQL security.

Site name	Description
Magical Code Injection Rainbow	The Magical Code Injection Rainbow! MCIR is a framework for building configurable vulnerability testbeds. MCIR is also a collection of configurable vulnerability testbeds.
McAfee HacMe Sites	Search the page for HacMe and you'll find a suite of learning tools.
Metasploit Unleashed	Free Ethical Hacking Course.
Metasploitable 3	Metasploitable3 is a VM that is built from the ground up with a large number of security vulnerabilities.
Microcorruption CTF	Challenge: given a debugger and a device, find an input that unlocks it. Solve the level with that input.
Morning Catch	Morning Catch is a VMware virtual machine, similar to Metasploitable, to demonstrate and teach about targeted client-side attacks and post-exploitation.
Moth	Moth is a VMware image with a set of vulnerable Web Applications and scripts.
Mutillidae	OWASP Mutillidae II is a free, open source, deliberately vulnerable web application providing a target for web-security enthusiast.
MysteryTwister C3	MysteryTwister C3 lets you solve crypto challenges, starting from the simple Caesar cipher all the way to modern AES, they have challenges for everyone.
National Institutes of Health (NIH)	Short courses on Information Security and Privacy Awareness. They have a section for executives, managers and IT Administrators as well.
OpenSecurityTraining.info	OpenSecurityTraining.info is dedicated to sharing training material for computer security classes, on any topic, that are at least one day long.

Site name	Description
Overthewire	The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.
OWASP Broken Web Applications Project	OWASP Broken Web Applications Project is a collection of vulnerable web applications that is distributed on a Virtual Machine.
OWASP GoatDroid	OWASP GoatDroid is a fully functional and self-contained training environment for educating developers and testers on Android security. GoatDroid requires minimal dependencies and is ideal for both Android beginners as well as more advanced users.
OWASP iGoat	iGoat is a learning tool for iOS developers (iPhone, iPad, etc.).
OWASP Mutillidae II	OWASP Mutillidae II is a free, open source, deliberately vulnerable web-application providing a target for web-security enthusiast.
OWASP Security Shepherd	The OWASP Security Shepherd project is a web and mobile application security training platform.
OWASP SiteGenerator	OWASP SiteGenerator allows the creating of dynamic websites based on XML files and predefined vulnerabilities (some simple, some complex) covering .Net languages and web development architectures (for example, navigation: Html, Javascript, Flash, Java, etc...).
Pentest.Training	Pentest.Training offers a fully functioning penetration testing lab which is ever increasing in size, complexity and diversity. The lab has a fully functioning Windows domain with various Windows OS's. There is also a selection of Boot2Root Linux machines to practice your CTF and escalation techniques and finally, pre-built web application training machines.
Pentesterlab	This exercise explains how you can, from a SQL injection, gain access to the administration console, then in the administration console, how you can run commands on the system.

Site name	Description
Pentestit.ru	Pentestit.ru has free labs that emulate real IT infrastructures. It is created for practicing legal pen testing and improving penetration testing skills. OpenVPN is required to connect to the labs.
Peruggia	Peruggia is designed as a safe, legal environment to learn about and try common attacks on web applications. Peruggia looks similar to an image gallery but contains several controlled vulnerabilities to practice on.
PicoCTF	picoCTF is a 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.
Professor Messer	Good free training video's, not only on Security but on CompTIA A+, Network and Microsoft related as well.
Puzzlemall	PuzzleMall - A vulnerable web application for practicing session puzzling.
Pwnable.kr	'pwnable.kr' is a non-commercial wargame site which provides various pwn challenges regarding system exploitation. while playing pwnable.kr, you could learn/improve system hacking skills but that shouldn't be your only purpose.
Pwnos	PwnOS is a vulnerable by design OS .. and there are many ways you can hack it.
Reversing.kr	This site tests your ability to Cracking & Reverse Code Engineering.
Ringzero	Challenges you can solve and gain points.
Risk3Sixty	Free Information Security training video, an information security examination and the exam answer key.

Site name	Description
Root Me	Hundreds of challenges and virtual environments. Each challenge can be associated with a multitude of solutions so you can learn.
RPISEC/MBE	Modern Binary Exploitation Course materials.
RPISEC/Malware	Malware Analysis Course materials.
SANS Cyber Aces	SANS Cyber Aces Online makes available, free and online, selected courses from the professional development curriculum offered by The SANS Institute, the global leader in cyber security training.
Scene One	Scene One is a pen testing scenario liveCD made for a bit of fun and learning.
SEED Labs	The SEED project has labs on Software, Network, Web, Mobile and System security and Cryptography labs.
SentinelTestbed	Vulnerable website. Used to test sentinel features.
SG6 SecGame	Spanish language, vulnerable GNU/Linux systems.
SlaveHack	My personal favorite: Slavehack is a virtual hack simulation game. Great for starters, I've seen kids in elementary school playing this!
SlaveHack 2 *BETA*	Slavehack 2 is a sequel to the original Slavehack. It's also a virtual hack simulation game but you will find features much closer to today's Cyber reality.
Smashthestack	This network hosts several different wargames, ranging in difficulty. A wargame, in this context, is an environment that simulates software vulnerabilities and allows for the legal execution of exploitation techniques.
SocketToMe	SocketToMe SocketToMe is little application for testing web sockets.

Site name	Description
SQLI labs	SQLI labs to test error based, Blind boolean based, Time based.
Sqlilabs	Lab set-up for learning SQL Injection Techniques.
SQLzoo	Try your Hacking skills against this test system. It takes you through the exploit step-by-step.
Stanford SecuriBench	Stanford SecuriBench is a set of open source real-life programs to be used as a testing ground for static and dynamic security tools. Release .91a focuses on Web-based applications written in Java.
The ButterFly - Security Project	The ButterFly project is an educational environment intended to give an insight into common web application and PHP vulnerabilities. The environment also includes examples demonstrating how such vulnerabilities are mitigated.
ThisIsLegal	A hacker wargames site but also with much more.
Try2Hack	Try2hack provides several security-oriented challenges for your entertainment. The challenges are diverse and get progressively harder.
UltimateLAMP	UltimateLAMP is a fully functional environment allowing you to easily try and evaluate a number of LAMP stack software products without requiring any specific setup or configuration of these products.
Vicnum	Vicnum is an OWASP project consisting of vulnerable web applications based on games commonly used to kill time. These applications demonstrate common web security problems such as cross-site scripting, SQL injections, and session management issues.
Vulnhub	An extensive collection of vulnerable VMs with user-created solutions.

Site name	Description
Vulnix	A vulnerable Linux host with configuration weaknesses rather than purposely vulnerable software versions.
Vulnserver	Windows-based threaded TCP server application that is designed to be exploited.
W3Challs	W3Challs is a penetration testing training platform, which offers various computer challenges, in categories related to security
WackoPicko	WackoPicko is a vulnerable web application used to test web application vulnerability scanners.
Web Attack and Exploitation Distro	WAED is pre-configured with various real-world vulnerable web applications in a sandboxed environment. It includes pen testing tools as well.
Web Security Dojo	Web Security Dojo is a preconfigured, stand-alone training environment for Web Application Security.
WebGoat	WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. You can install and practice with WebGoat.
Wechall	Focussed on offering computer-related problems. You will find Cryptographic, Crackit, Steganography, Programming, Logic and Math/Science. The difficulty of these challenges varies as well.
XSS-game	In this training program, you will learn to find and exploit XSS bugs. You'll use this knowledge to confuse and infuriate your adversaries by preventing such bugs from happening in your applications.
XVWA	XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security.

A□wes□□ø□□me□Cyber□~□Skil□ls