Penetration testing on a vulnerable environment

The following sections list online web application challenges and virtual machine and ISO images that contain vulnerable applications. These resources can be used to learn penetration testing in your own system environment.

Online web application challenges

The following table lists several websites that provide several challenges, which you can use to learn penetration testing:

URL	Description
https://pentesteracademylab.appspot.com/	It contains four free challenges in the web application area such as form bruteforcing and HTTP basic authentication attack.
https://hack.me/	Hack.me is a free, community-based project powered by eLearnSecurity. The community can build, host, and share vulnerable web application code for educational and research purposes.
https://www.hacking-lab.com/caselist/	Hacking-Lab provides a security lab with various security challenges that you can try. They even provide a Live CD that will enable access into the 'Hacking-Lab's remote security lab.
https://google-gruyere.appspot.com/	This codelab shows how web application vulnerabilities can be exploited and how to defend against these attacks.
http://www.enigmagroup.org/	Enigma Group provides its members with a legal and safe security resource where they can develop their pen-testing skills on the various challenges provided by this site. These challenges cover the exploits listed in the **OWASP** (**The Open Web Application Security Project**) top 10 projects and teach members many other types of exploits that are found in today's applications, thus helping them to become better programmers in the meantime.
https://www.owasp.org/index.php /OWASP_Hackademic_Challenges_Project	The OWASP Hackademic Challenges Project is an open source project that helps you to test your knowledge on web application security. You can use it to actually attack web applications in a realistic but controllable and safe environment.
https://www.hackthissite.org/	Hack This Site is a free, safe, and legal training ground for hackers to test and expand their hacking skills. It also has a vast selection of hacking articles and a huge forum where users can discuss hacking, network security, and just about everything.

Virtual machines and ISO images

The following table lists several virtual machines and ISO images that can be installed on your machine as targets to learn penetration testing:

URL	Description
http://vulnhub.com/	It contains various VMs to allow anyone to gain a practical hands-on experience in digital security, computer application, and network administration.
http://exploit-exercises.com/	This 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.
https://www.pentesterlab.com/exercises/	This provides various web application security exercise materials, such as SQL injection, Axis2 and Tomcat manager, and MoinMoin code execution. In each exercise, you will have an explanation tutorial and also the vulnerable application in the ISO image.

URL	Description
http://hackxor.sourceforge.net	Hackxor is a webapp hacking game where players must locate and exploit vulnerabilities to progress through the story. It contains XSS, CSRF, SQLi, ReDoS, DOR, command injection, and so on.
https://www.mavensecurity.com/web_security_dojo/	A free open-source, self-contained training environment for web application security and penetration testing.
http://www.bonsai-sec.com/en/research/moth.php	Moth is a VMware image with a set of vulnerable web applications and scripts, which you may use for: • Testing web application security scanners • Testing **Static Code Analysis** (**SCA**) tools • Giving an introductory course on web application security
http://exploit.co.il/projects/vuln-web-app/	The exploit.co.il vulnerable web app is designed as a learning platform to test various SQL injection techniques, and it is a fully functional website with a content management system based on fckeditor.
http://sourceforge.net/projects/lampsecurity/	LAMPSecurity training is designed to be a series of vulnerable virtual machine images along with complementary documentation designed to teach Linux, Apache, PHP, and MySQL security.
https://bechtsoudis.com/work-stuff/challenges/drunk-admin-web-hacking-challenge/	The challenge includes an image hosting web service that has various design vulnerabilities. You must enumerate the various web service features and find an exploitable vulnerability in order to read system-hidden files.
https://code-google-com.db19.linccweb.org/p/owaspbwa/	OWASP Broken Web Applications Project, a collection of vulnerable web applications, is distributed on a virtual machine in VMware compatible format.
http://sourceforge.net/projects/bwapp/files/bee-box/	bee-box is a custom Linux VMware virtual machine preinstalled with bWAPP. bee-box gives you several ways to hack and deface the bWAPP website. It's even possible to hack bee-box to get root access. With bee-box, you have the opportunity to explore all bWAPP vulnerabilities!
http://information.rapid7.com/download-metasploitable.html?LS=1631875&CS=web	The Metasploitable 2 virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities.