https://doi.org/10.2352/ISSN.2470-1173.2018.06.MOBMU-100

Cybersecurity and Forensic Challenges - A Bibliographic Review

Reiner Creutzburg

Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab,, P.O.Box 2132, D-14737 Brandenburg, Germany

Email: creutzburg@th-brandenburg.de

Abstract

The aim of this paper is to give a bibliographic review of the growing number of different Cybersecurity and Forensic Challenges for educational and vocational training purposes.
Special attention is given to the hacking lab, which enables effective training in cybersecurity and computer forensics in the university environment and in vocational education and training.

Introduction

Nowadays, small- and medium-sized enterprises (SME) have to deal more and more with the issue of IT security. Due to the ever-growing popularity of mobile devices, but also by the general acceptance of IT technology in everyday life, new security threats to corporate data occur every day [1-13].

Due to different terms and conditions within a company, there is no single security solution to counter all different threats.

In addition, dependent on the experience of the administrators, devices and services may be misconfigured and thus open security vulnerabilities.

Companies can protect themselves against such risks by assessing using penetration testing to get an accurate analysis of the threats and develop individual security concepts. However, there are two major challenges. How can companies be aware of the importance of security inspections? How can a check be offered so inexpensive that even in the face of SMEs regular checks are made possible?

One solution is to completely automate the vulnerability and penetration tests and to reduce the necessary oral audits to an essential minimum. With this approach, security audits could be carried out efficiently and with reduced effort and businesses are encouraged to perform these important checks regularly.

Introduction - Virtual University and Blended Learning

Nowadays, traditional educational institutions, such as public schools, colleges and universities and business organizations, use more and more the possibilities of electronic on-line training, the so-called ”e-Learning” [4]. Due to the growing worldwide development of information, communication and computer technologies one can observe more and more acceptance of this kind of training opportunities in our society [1],[3],[7-21]. Not only is the global network of computers over the Internet and the versatility of digital media and products involved in the rise, but also the changing social conditions. Multimedia learning environments are independent of space and time (see figures 1-5). Thus, learners can decide flexibly despite their private, social and professional obligations on their learning processes. One can increasingly observe that colleges and universities more and more have to adjust to this present generation of students and respond by increasing the flexibility of the courses. For this reason, online degree programs, or suitable combinations of classroom and online studies (blended learning) are increasingly offered. It is well-known that man learns about 80% of its knowledge and skills by informal learning compared to learning from formal learning. Unfortunately, often this fact is not taken into account by planners and decision-makers from school, university and companies. A well-known example is the now already for 10 years successfully operating ”Virtuelle Fachhochschule (Virtual University)”, an association of 10 established Universities of Applied Sciences in Germany and Switzerland [2]. A special feature applies to new students, who often have to start and face various ”entry level” difficulties in a higher education experience. This can have various causes (e.g. of a longer working period after high school, army and civilian activities, family situation, social status, career changers, migration background, additional employment to earn money while studying, lack of student loan assistance, etc.).

In order to help these students and to ease the entry to facilitate study and the associated intensive teaching and learning process, the following two projects were carried out [1].

Virtual Tutorials

In this project not already well-known facts about online teaching should be explored, but rather are demonstrated, as additional virtual online tutorials are successfully introduced into the undergraduate course Algorithms and Data Structures of the Department of Informatics and Media of Applied Sciences Brandenburg in order to give the opportunity to all students to better understand the educational content of this course through a variety of complementary tools to deepen their knowledge and practice with exercises. Nowadays there is a variety of virtual learning spaces, such as Adobe Connect, TeamViewer or iLinc [5]. The University of Applied Sciences Brandenburg uses mainly the iLinc software offered by the company netucate systems GmbH [3]. This tool offers a number of opportunities to use learning materials and to interact with the students. The network performance and stability clearly showed that the use of virtual learning spaces of Netucate with the iLinc software for online virtual tutorials is well suited and the performance is very good. The netucate system allows the effective use of whiteboards, application sharing, integrated browser and other features. We have introduced in the undergraduate course on Algorithms and Data Structures a combination of classroom study and e-learning as a typical blended learning scenario. It is important to mention here that the online tutorial will not replace your presence time in the university, but an additional structural support to individual learning processes. It allows students great flexibility, regardless of time and place they can deepen their thematic knowledge and their priorities. Additionally, several Wikipedia books on specific topics on Algorithms and Data Structures were created and corresponding annotated link lists for multimedia animations were added in the course site of the Moodle server (see Chapter 3).

Additionally, for the digital recording of handwriting in the virtual learning space, a novel Bluetooth pen of the company Papershow [6] was available. This pen enables a vibrant design of presentations, as handwritten notes, sketches or drawings are transmitted in real time and significantly "softer, smoother and more fluid handwriting" on the monitor screen in the virtual learning space and works much better than conventional graphics tablets (digitizers, pen tablets) for writing. In addition, all tutorials are recorded and made available free to all students at any time. Despite progressive developments in the electronic communications students always should feel that the teacher is present during the entire virtual lecture and are accessible through interaction.

Creation of a Multimedia Repository

As part of this project, several multimedia repositories were made on the individual topics of Algorithms and Data Structures and made available to students online. These multimedia repositories consist of both new and custom-made Wikipedia books, Wikipedia links and on the other hand, of annotated list of links to selected interesting multimedia elements on the web. Wikipedia books have the advantage that they allow a skillful selection of available Wikipedia article in the Internet in a clever saved form in a book structure, without copyright restrictions. These Wikipedia books are available at any time, are easily accessible, and can be updated on the web easily by recompiling (since the basic structure is stored by the teacher at the Wikipedia website).

Mobile Apps

Evaluation

It is well-known that everyone learns differently. One can make a division into the following four types of learning by Vester [17], who addressed that the learning effectiveness can be increased by proper perception of each channel (optical / visual, auditory, tactile, cognitive). The project described here supports especially the case, the perception of visual / visual and auditory learning styles and supplemented by the Wikipedia books and annotated Internet link lists the collection of material for the classical theory in didactic teaching. In particular, this collection of animations on various topics (as for example searching, sorting, pattern recognition, tree and graph algorithms) found the students' interest and increased significantly the motivation for further study of the course material. The project of virtual tutorial was evaluated for the time of December 2012 until August 2013. The success was clearly measurable. A detailed review of the study results based on the rating lists on the subject Algorithms and Data Structures for the last 2 years in the tests and repeated tests yielded the following results: The failure rate in the tests was in the academic year 2012/2013 has reduced to 10,2The overall average of the examination mark in all three undergraduate programs in Computer Science, Medical Informatics, and Applied Computer Science (ACS) has been slightly improved from 2.9 to 2.6. The average grade of foreign students and students with an immigrant background significantly improved from 3.3 to 2.8. Particularly noteworthy is the improvement of the examination results of female students in this group by more than one grade from 3.4 to 2.2, which was apparently caused by the use of a female student as a tutor that had an extremely positive impact on the working atmosphere within the tutorials and virtual tutorials. Conducted evaluation of the course based on the evaluation forms of this form of learning revealed an overall rating of 1.7. Through the creation of lists of links, and appropriate integration of multimedia repository into Moodle pages FH Brandenburg and the Virtual High School, the sustainability of the project is saved. Therefore the project can "live" forever and must be kept up to date only with minimal effort from the teachers themselves. It is important to mention that it does not create any further costs. Since the developed learning content is based on Wikipedia or free Internet content, now and in the future basically no copyright issues will arise [1].

Summary

In this paper we have described our experiences by using virtual tutorials, Wikipedia books and multimedia-based teaching in a course on Algorithms and Data Structures. We describe our work, the benefits and success we gained from using virtual tutorials held in Netucate iLinc sessions and the use of various multimedia and animation elements for the support of deeper understanding of the ordinary lectures held in the standard classroom on Algorithms and Data Structures for undergraduate computer sciences students. The advantage of the use of Wikipedia books to support the blended learning process using modern mobile devices is clearly documented. Finally, some first statistical measures of improved student's scores after introducing this new form of teaching support are documented.

References

[1] Knackmuß, J.; R. Creutzburg: The Benefit and Support of Virtual Tutorials, Wikipedia Books and Multimedia-Based Teaching in a Course on Algorithms and Data Structures, Proceedings NWK-14, 2013, pp. 427-428

[2] Wikipedia: E-Learning `http://de.wikipedia.org/wiki/ELearning`

[3] Knackmuß, J.; R. Creutzburg: The Benefit and Support of Virtual Tutorials, Wikipedia Books and Multimedia-Based Teaching in a Course of SPIE2014

[4] Creutzburg, R.; A. Lugmayr: Multimedia-Based Teaching in Signal and Image Processing. In: H. Ruokamo; O. Nykänen, S. Pohjolainen; P. Hietala (Eds.) Proceed. 10th Internat. PEG Conference on "Intelligent Computer and Communications Technology - Learning in Online Communities", PEG 2001, June 2001, Tampere, Finland, pp. 149-153

[5] Astleitner, H.; Wiesner, C.: An integrated model of multimedia learning and motivation. Journal of Educational Multimedia and Hypermedia, 13 (2004), pp. 3-21

[6] Bagui, S.: Reasons for increased learning using multimedia. Journal of Educational Multimedia and Hypermedia, 7, (1998), pp. 3-18

[7] Bourne, J.; Harris, D.A.; Mayadas, F.: Anytime, Online En-

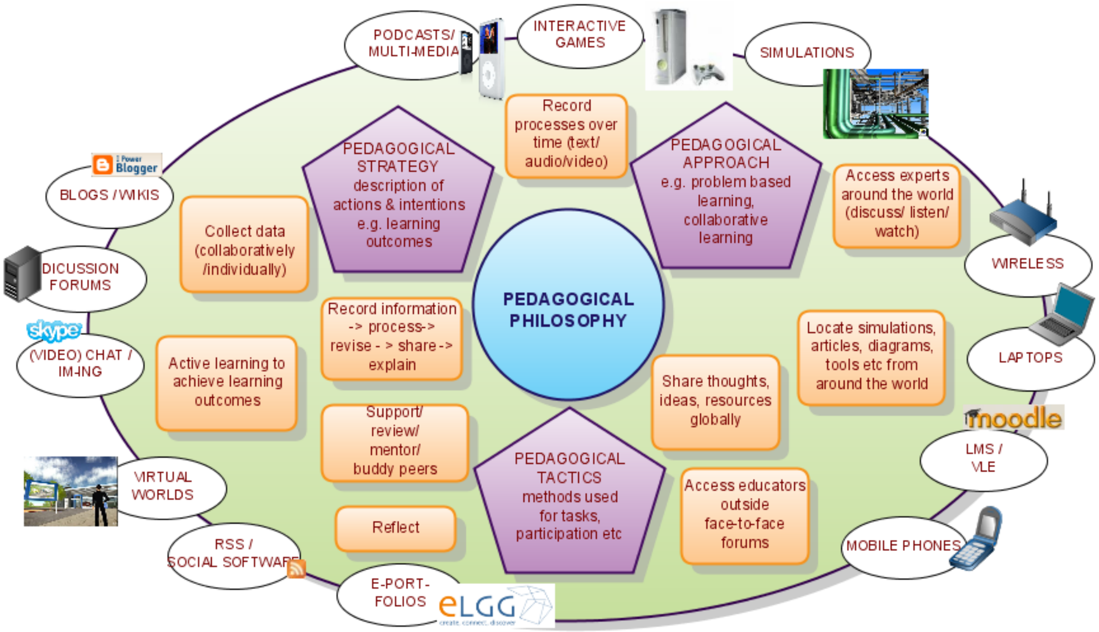
PODCASTS/ MULTI-MEDIA
INTERACTIVE GAMES
SIMULATIONS
BLOGS / WIKIS
Power Blogger
DICUSSION FORUMS
skype
(VIDEO) CHAT / IM-ING
VIRTUAL WORLDS
RSS / SOCIAL SOFTWARE
E-PORT-FOLIOS
eLGG
create, connect, discover
MOBILE PHONES
LMS / VLE
moodle
LAPTOPS
WIRELESS
PEDAGOGICAL STRATEGY description of actions & intentions e.g. learning outcomes
Record processes over time (text/ audio/video)
PEDAGOGICAL APPROACH e.g. problem based learning, collaborative learning
Access experts around the world (discuss/ listen/ watch)
Collect data (collaboratively /individually)
PEDAGOGICAL PHILOSOPHY
Record information -> process-> revise - > share -> explain
Locate simulations, articles, diagrams, tools etc from around the world
Active learning to achieve learning outcomes
Share thoughts, ideas, resources globally
Support/ review/ mentor/ buddy peers
PEDAGOGICAL TACTICS methods used for tasks, participation etc
Access educators outside face-to-face forums
Reflect

Figure 1. *Illustration of pedagogical philosophy concepts [??]*

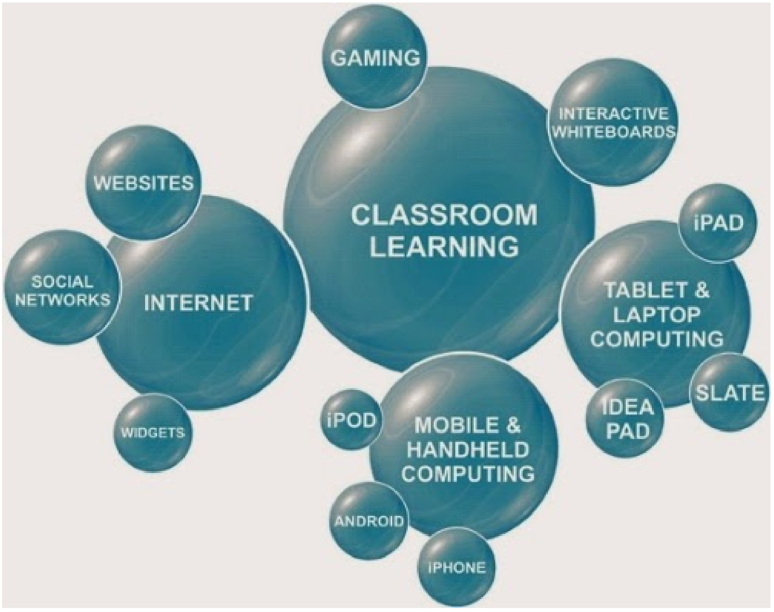

Figure 2. *Platforms of blended learning and 21st Century Learning [??]*

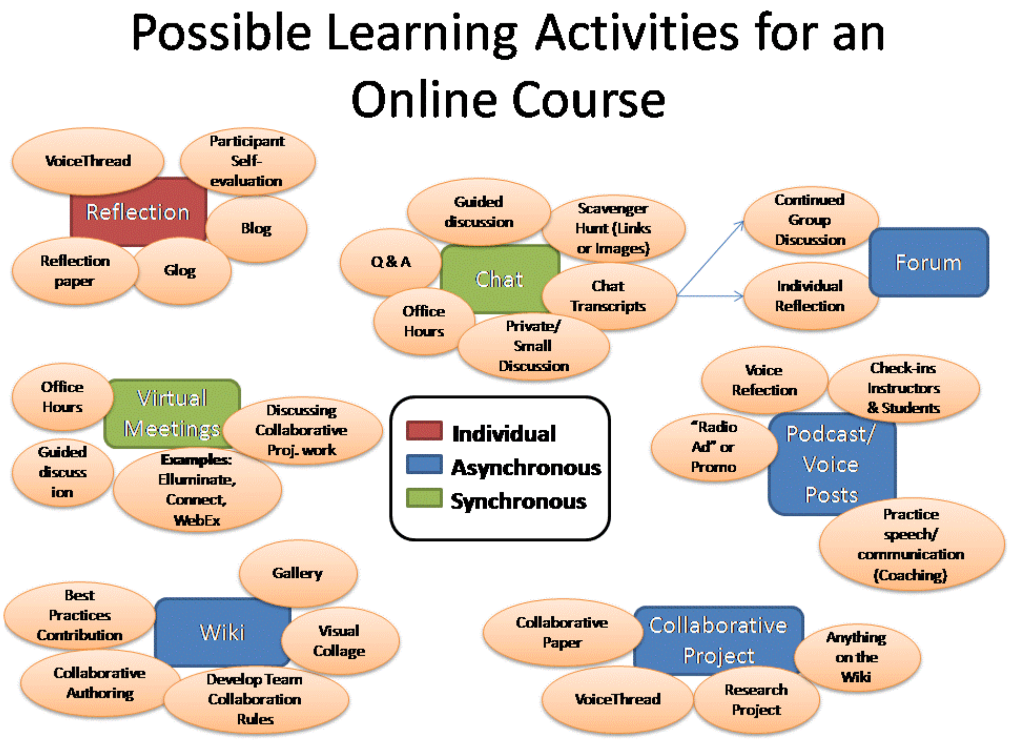

Figure 3. *Illustration of possible learning activities for an online course [??]*

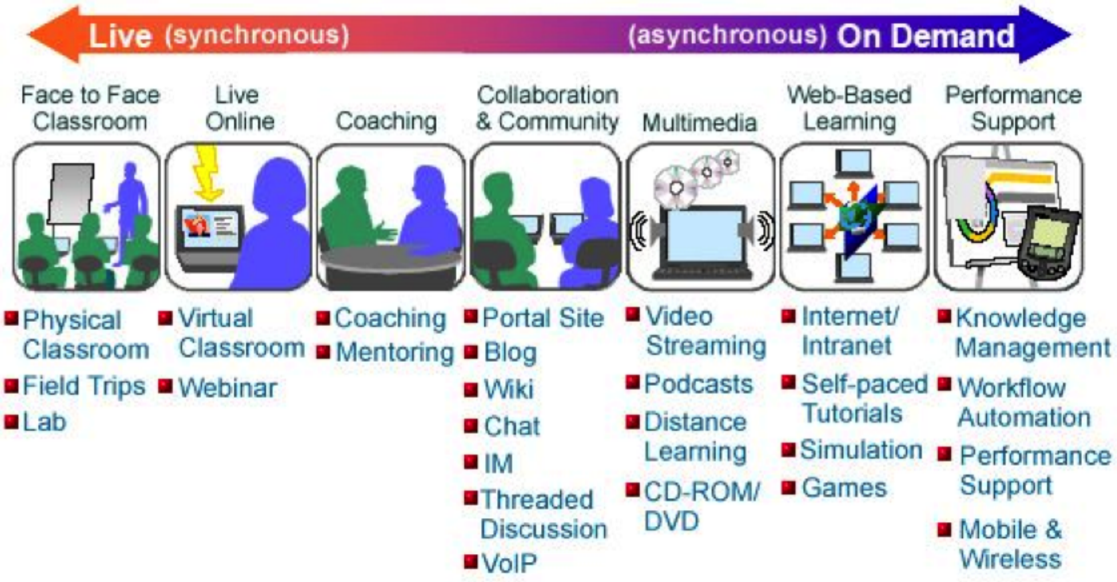

Figure 4. *Variety of E-Learning instructional methods and activities [??]*

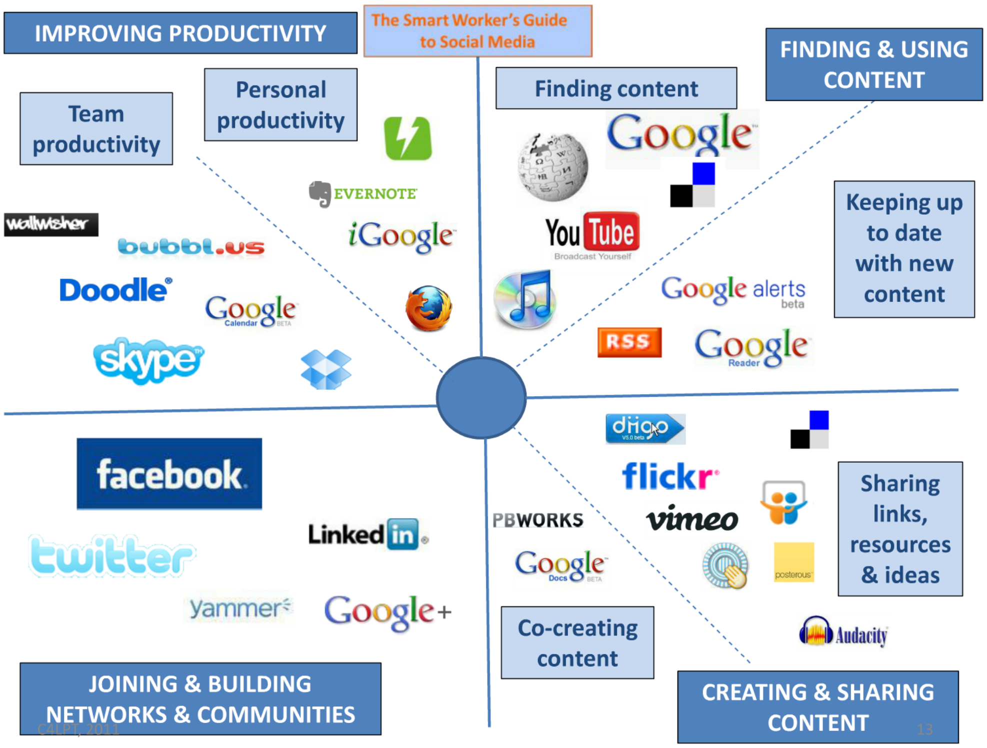

Figure 5. *Components in modern social learning [??]*

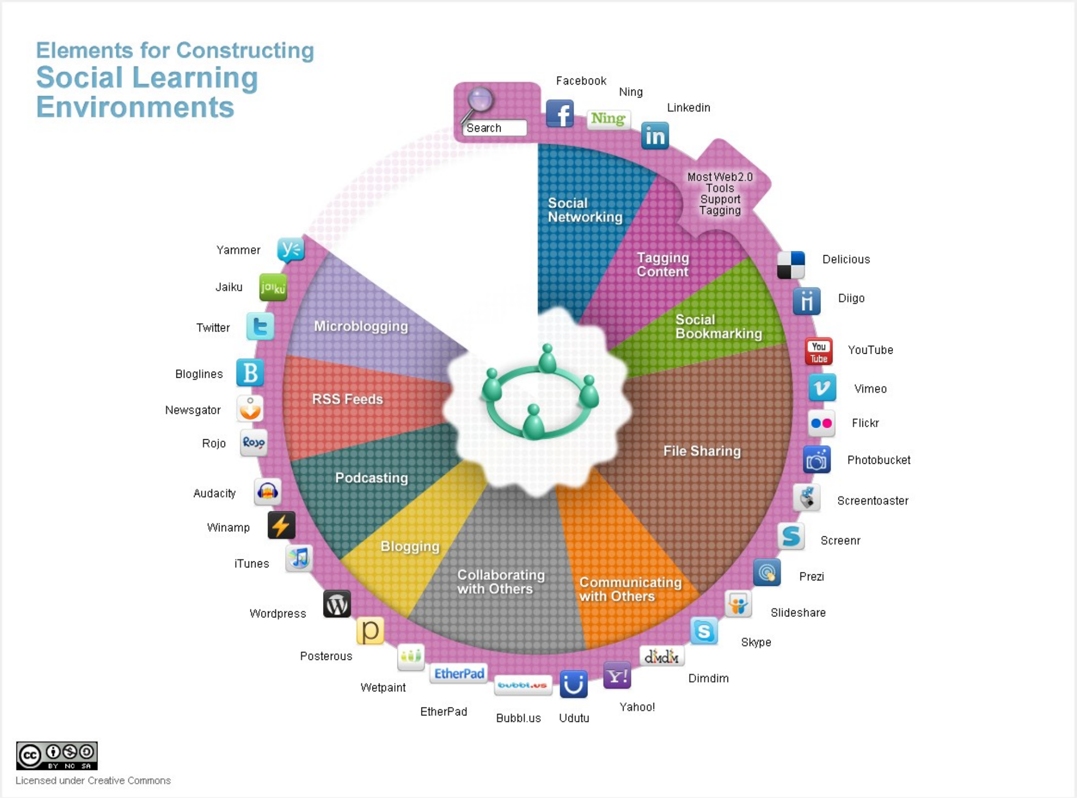

Figure 6. *Elements-for-constructing-social-learning-environments.*

gineering Education: Learning Anywhere, Journal of Engineering Education Vol. 94, (2005), No. 1

[8] Ellis, T. (2004). Animating to Build Higher Cognitive Understanding: A Model for Studying Multimedia Effectiveness in Education, Journal of Engineering Education, Vol 93, (2004), No. 1, pp. 59-64

[9] Mayer, R. E.; Moreno, R. (2002). Animation as an aid to multimedia learning. Educational Psychology Review, 14, 87-9911

[10] Hart, J. The future of learning is social. http://de.slideshare.net/janehart/the-future-of-learning-is-social-9304670

[11] Tremp, H. Förderung der Kompetenzentwicklung mittels “New Blended Learning” – Kombination von E-Learning und Social Software anhand des Hochschulunterrichts im Thema Software-Engineering. VDM Verlag Dr. Müller 2010)

[12] Wikipedia: Blended learning https://en.wikipedia.org/wiki/Blended_learning

[13] Wikipedia books on Algorithms and Data Structures (Ed. by Wikipedians, Reiner Creutzburg, Jenny Knackmuß). https://www.researchgate.net/profile/Reiner_Creutzburg/publications/?pubType=book&ev=prf_pubs_book

[14] Vester, F.: Denken, Lernen, Vergessen. dtv: München 1998

[15] Moodle server of TH Brandenburg http://moodle.th-brandenburg.de

Site name	URL	Description
natch competition	URL	bbbbbbbbbbbbbbbbbbbbbbbbbbbbb bbbbbbbbb bbbbbbbbbbb.
Arizona Cyber Warfare Range	URL	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	URL	More than 350 hands-on challenges (free and paid) to master IT security and it's growing day by day.
BodgeIt Store	URL	The BodgeIt Store is a vulnerable web application which is currently aimed at people who are new to pen testing.
Bright Shadows	URL	Training in Programming, JavaScript, PHP, Java, Steganography, and Cryptography (among others).
bWAPP	URL	bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
Cyber Degrees	URL	Free online cyber security Massive Open Online Courses (MOOCS).
Commix testbed	URL	A collection of web pages, vulnerable to command injection flaws.
CryptOMG	URL	CryptOMG is a configurable CTF style test bed that highlights common flaws in cryptographic implementations.
Cyber Security Base	URL	Cyber Security Base is a page with free courses by the University of Helsinki in collaboration with F-Secure.
Cybersecuritychallenge UK	URL	Cyber Security Challenge UK runs a series of competitions designed to test your cyber security skills.
CyberTraining 365	URL	Cybertraining365 has paid material but also offers free classes. The link is directed at the free classes.
Cybrary.it	URL	Free and Open Source Cyber Security Learning.
Damn Small Vulnerable Web	URL	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	URL	Damn Vulnerable Android App (DVAA) is an Android application which contains intentional vulnerabilities.
Damn Vulnerable Hybrid Mobile App	URL	Damn Vulnerable Hybrid Mobile App (DVHMA) is a hybrid mobile app (for Android) that intentionally contains vulnerabilities.
Damn Vulnerable iOS App	URL	Damn Vulnerable iOS App (DVIA) is an iOS application that is damn vulnerable.
Damn Vulnerable Linux	URL	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	URL	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	URL	Short and simple vulnerable PHP web application that naive scanners found to be perfectly safe.
Damn Vulnerable Thick Client App	URL	DVTA is a Vulnerable Thick Client Application developed in C sharp .NET with many vulnerabilities.
Damn Vulnerable Web App	URL	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	URL	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.

List of Cybersecurity Challenges, Part I

Site name	URL	Description
Damn Vulnerable Web Sockets	URL	Damn Vulnerable Web Sockets (DVWS) is a vulnerable web application which works on web sockets for client-server communication.
Damnvulnerable.me	URL	A deliberately vulnerable modern-day app with lots of DOM-related bugs.
Dareyourmind	URL	Online game, hacker challenge.
DIVA Android	URL	Damn Insecure and vulnerable App for Android.
EnigmaGroup	URL	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	URL	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	URL	Vulnerable Web app designed as a learning platform to test various SQL injection Techniques.
Exploit-exercises.com	URL	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	URL	Set of labs and an exploitable framework for you to hack mobile an application on Android.
Game of Hacks	URL	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	URL	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	URL	A security research network where like-minded individuals could work together towards the common goal of knowledge.
GoatseLinux	URL	GSL is a Vmware image you can run for penetration testing purposes.
Google Gruyere	URL	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	URL	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	URL	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	URL	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	URL	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.

List of Cybersecurity Challenges, Part II

Site name	URL	Description
Hack.me	URL	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.
Hackademic	URL	Offers realistic scenarios full of known vulnerabilities (especially, of course, the OWASP Top Ten) for those trying to practice their attack skills.
Hackazon	URL	A modern vulnerable web app.
Hackertest.net	URL	HackerTest.net is your own online hacker simulation with 20 levels.
Hacking-Lab	URL	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	URL	HackSys Extreme Vulnerable Driver is intentionally vulnerable Windows driver developed for security enthusiasts to learn and polish their exploitation skills at Kernel level.
HackThis!!	URL	Test your skills with more than 50 hacking levels, covering all aspects of security.
Hackxor	URL	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 and difficulty. Contains XSS, CSRF, SQLi, ReDoS, DOR, command injection, etc.
Halls of Valhalla	URL	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	URL	Provides numerous interesting “hacking” challenges to the user.
Hellbound Hackers	URL	Learn a hands-on approach to computer security. Learn how hackers break in, and how to keep them out.
Holynix	URL	Holynix is a Linux VMware image that was deliberately built to have security holes for the purposes of penetration testing.
HSCTF3	URL	is an international online hacking competition designed to educate high schoolers in computer science.
Information Assurance Support Environment (IASE)	URL	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	URL	Free CISSP Training course.
ISC2 Center for Cyber Safety and Education	URL	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	URL	Vulnerable Java based Web Application.
Juice Shop	URL	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	URL	This vulnerable machine is a good starting point for beginners.
LAMPSecurity Training	URL	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.
Magical Code Injection Rainbow	URL	The Magical Code Injection Rainbow! MCIR is a framework for building configurable vulnerability testbeds. MCIR is also a collection of configurable vulnerability testbeds.

List of Cybersecurity Challenges, Part III

Site name	URL	Description
McAfee HacMe Sites Metasploit Unleashed	URL URL	Search the page for HacMe and you'll find a suite of learning tools. Free Ethical Hacking Course.
Metasploitable 3	URL	Metasploitable3 is a VM that is built from the ground up with a large number of security vulnerabilities.
Microcorruption CTF	URL	Challenge: given a debugger and a device, find an input that unlocks it. Solve the level with that input.
Morning Catch	URL	Morning Catch is a VMware virtual machine, similar to Metasploitable, to demonstrate and teach about targeted client-side attacks and post-exploitation.
Moth	URL	Moth is a VMware image with a set of vulnerable Web Applications and scripts.
Mutillidae	URL	OWASP Mutillidae II is a free, open source, deliberately vulnerable web application providing a target for web-security enthusiast.
MysteryTwister C3	URL	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)	URL	Short courses on Information Security and Privacy Awareness. They have a section for executives, managers and IT Administrators as well.
OpenSecurityTraining.info	URL	OpenSecurityTraining.info is dedicated to sharing training material for computer security classes, on any topic, that are at least one day long.
Overthewire	URL	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	URL	OWASP Broken Web Applications Project is a collection of vulnerable web applications that is distributed on a Virtual Machine.
OWASP GoatDroid	URL	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	URL	iGoat is a learning tool for iOS developers (iPhone, iPad, etc.).
OWASP Mutillidae II	URL	OWASP Mutillidae II is a free, open source, deliberately vulnerable web-application providing a target for web-security enthusiast.
OWASP Security Shepherd	URL	The OWASP Security Shepherd project is a web and mobile application security training platform.
OWASP SiteGenerator	URL	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	URL	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	URL	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.
Pentestit.ru	URL	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	URL	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	URL	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.

List of Cybersecurity Challenges, Part IV

Site name	**URL**	**Description**
Professor Messer	URL	Good free training video's, not only on Security but on CompTIA A, Network and Microsoft related as well.
Puzzlemall	URL	PuzzleMall - A vulnerable web application for practicing session puzzling.
Pwnable.kr	URL	'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	URL	PwnOS is a vulnerable by design OS .. and there are many ways you can hack it.
Reversing.kr	URL	This site tests your ability to Cracking and Reverse Code Engineering.
Ringzero	URL	Challenges you can solve and gain points.
Risk3Sixty	URL	Free Information Security training video, an information security examination and the exam answer key.
Root Me	URL	Hundreds of challenges and virtual environments. Each challenge can be associated with a multitude of solutions so you can learn.
RPISEC/MBE	URL	Modern Binary Exploitation Course materials.
RPISEC/Malware	URL	Malware Analysis Course materials.
SANS Cyber Aces	URL	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	URL	Scene One is a pen testing scenario liveCD made for a bit of fun and learning.
SEED Labs	URL	The SEED project has labs on Software, Network, Web, Mobile and System security and Cryptography labs.
SentinelTestbed	URL	Vulnerable website. Used to test sentinel features.
SG6 SecGame	URL	Spanish language, vulnerable GNU/Linux systems.
SlaveHack	URL	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	URL	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	URL	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	URL	SocketToMe SocketToMe is little application for testing web sockets.
SQLI labs	URL	SQLI labs to test error based, Blind boolean based, Time based.
Sqlilabs	URL	Lab set-up for learning SQL Injection Techniques.
SQLzoo	URL	Try your Hacking skills against this test system. It takes you through the exploit step-by-step.
Stanford SecuriBench	URL	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	URL	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	URL	A hacker wargames site but also with much more.
Try2Hack	URL	Try2hack provides several security-oriented challenges for your entertainment. The challenges are diverse and get progressively harder.
UltimateLAMP	URL	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	URL	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.

List of Cybersecurity Challenges, Part V

Site name	URL	Description
Vulnhub	URL	An extensive collection of vulnerable VMs with user-created solutions.
Vulnix	URL	A vulnerable Linux host with configuration weaknesses rather than purposely vulnerable software versions.
Vulnserver	URL	Windows-based threaded TCP server application that is designed to be exploited.
W3Challs	URL	W3Challs is a penetration testing training platform, which offers various computer challenges, in categories related to security.
WackoPicko	URL	WackoPicko is a vulnerable web application used to test web application vulnerability scanners.
Web Attack and Exploitation Distro	URL	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	URL	Web Security Dojo is a preconfigured, stand-alone training environment for Web Application Security.
WebGoat	URL	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	URL	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	URL	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	URL	XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security.

List of Cybersecurity Challenges, Part VI

Site name	URL
BadStore	http://www.badstore.net/
BodgeIt Store	http://code.google.com/p/bodgeit/
Butterfly Security Project	http://thebutterflytmp.sourceforge.net/
bWAPP	http://www.mmeit.be/bwapp/ http://sourceforge.net/projects/bwapp/files/bee-box/
Commix	https://github.com/stasinopoulos/commix-testbed
CryptOMG	https://github.com/SpiderLabs/CryptOMG
Damn Vulnerable Node Application (DVNA)	https://github.com/quantumfoam/DVNA/
Damn Vulnerable Web App (DVWA)	http://www.dvwa.co.uk/
Damn Vulnerable Web Services (DVWS)	http://dvws.professionallyevil.com/
Drunk Admin Web Hacking Challenge	https://bechtsoudis.com/work-stuff/challenges/drunk-admin-web-hacking-challenge/
Exploit KB Vulnerable Web App	http://exploit.co.il/projects/vuln-web-app/
Foundstone Hackme Bank	http://www.mcafee.com/us/downloads/free-tools/hacme-bank.aspx
Foundstone Hackme Books	http://www.mcafee.com/us/downloads/free-tools/hacmebooks.aspx
Foundstone Hackme Casino	http://www.mcafee.com/us/downloads/free-tools/hacme-casino.aspx
Foundstone Hackme Shipping	http://www.mcafee.com/us/downloads/free-tools/hacmeshipping.aspx
Foundstone Hackme Travel	http://www.mcafee.com/us/downloads/free-tools/hacmetravel.aspx
GameOver	http://sourceforge.net/projects/null-gameover/
hackxor	http://hackxor.sourceforge.net/cgi-bin/index.pl
Hackazon	https://github.com/rapid7/hackazon
LAMPSecurity	http://sourceforge.net/projects/lampsecurity/
Moth	http://www.bonsai-sec.com/en/research/moth.php
NOWASP / Mutillidae 2	http://sourceforge.net/projects/mutillidae/
OWASP BWA	http://code.google.com/p/owaspbwa/
OWASP Hackademic	http://hackademic1.teilar.gr/
OWASP SiteGenerator	https://www.owasp.org/index.php/Owasp_SiteGenerator
OWASP Bricks	http://sourceforge.net/projects/owaspbricks/
OWASP Security Shepherd	https://www.owasp.org/index.php/OWASP_Security_Shepherd
PentesterLab	https://pentesterlab.com/
PHDays iBank CTF	http://blog.phdays.com/2012/05/once-again-about-remote-banking.html
SecuriBench	http://suif.stanford.edu/~livshits/securibench/
SentinelTestbed	https://github.com/dobin/SentinelTestbed
SocketToMe	http://digi.ninja/projects/sockettome.php
sqli-labs	https://github.com/Audi-1/sqli-labs
MCIR (Magical Code Injection Rainbow)	https://github.com/SpiderLabs/MCIR
sqlilabs	https://github.com/himadriganguly/sqlilabs
VulnApp	http://www.nth-dimension.org.uk/blog.php?id=88
PuzzleMall	http://code.google.com/p/puzzlemall/
WAED	http://www.waed.info
WebGoat.NET	https://github.com/jerryhoff/WebGoat.NET/
WebSecurity Dojo	http://www.mavensecurity.com/web_security_dojo/
XVWA	https://github.com/s4n7h0/xvwa
Zap WAVE	http://code.google.com/p/zaproxy/downloads/detail?name=zap-wave-0.1.zip

Vulnerable Web Applications

Site name	URL
21LTR	http://21ltr.com/scenes/
Damn Vulnerable Linux	http://sourceforge.net/projects/virtualhacking/files/os/dvl/
exploit-exercises - nebula, protostar, fusion	http://exploit-exercises.com/download
heorot: DE-ICE, hackerdemia	http://hackingdojo.com/downloads/iso/De-ICE_S1.100.iso http://hackingdojo.com/downloads/iso/De-ICE_S1.110.iso http://hackingdojo.com/downloads/iso/De-ICE_S1.120.iso http://hackingdojo.com/downloads/iso/De-ICE_S2.100.iso hackerdemia-http://hackingdojo.com/downloads/iso/De-ICE_S1.123.iso
Holynix	http://sourceforge.net/projects/holynix/files/
Kioptrix	http://www.kioptrix.com/blog/
LAMPSecurity	http://sourceforge.net/projects/lampsecurity/
Metasploitable	http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/
neutronstar	http://neutronstar.org/goatselinux.html
PenTest Laboratory	http://pentestlab.org/lab-in-a-box/
Pentester Lab	https://www.pentesterlab.com/exercises
pWnOS	http://www.pwnos.com/
RebootUser Vulnix	http://www.rebootuser.com/?page_id=1041
SecGame No. 1:	Sauron http://sg6-labs.blogspot.co.uk/2007/12/secgame-1-sauron.html
scriptjunkie.us	http://www.scriptjunkie.us/2012/04/the-hacker-games/
UltimateLAMP	http://www.amanhardikar.com/mindmaps/practice-links.html
TurnKey Linux	http://www.turnkeylinux.org/
Bitnami	https://bitnami.com/stacks
Elastic Server	http://elasticserver.com
OS Boxes	http://www.osboxes.org
VirtualBoxes	http://virtualboxes.org/images/
VirtualBox Virtual Appliances	https://virtualboximages.com/
CentOS	http://www.centos.org/
Default Windows Clients	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise https://dev.windows.com/en-us/microsoft-edge/tools/vms/
Default Windows Server	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview
Default VMWare vSphere	http://www.vmware.com/products/vsphere/

Vulnerable Operation System Installations

Site name	URL
Exploit-DB	http://www.exploit-db.com/
Old Apps	http://www.oldapps.com/
Old Version	http://www.oldversion.com/
VirtualHacking Repo	sourceforge.net/projects/virtualhacking/files/apps%40realworld/

Sites for Downloading Older Versions of Various Software

Site name	URL
Acunetix acuforum	http://testasp.vulnweb.com/
Acunetix acublog	http://testaspnet.vulnweb.com/
Acunetix acuart	http://testphp.vulnweb.com/
Cenzic crackmebank	http://crackme.cenzic.com
HP freebank	http://zero.webappsecurity.com
IBM altoromutual	http://demo.testfire.net/
Mavituna testsparker	http://aspnet.testsparker.com
Mavituna testsparker	http://php.testsparker.com
NTOSpider Test Site	http://www.webscantest.com/

Vulnerable Operation System Installations

Site name	URL
Embedded Security CTF	https://microcorruption.com
EnigmaGroup	http://www.enigmagroup.org/
Escape	http://escape.alf.nu/
Google Gruyere	http://google-gruyere.appspot.com/
Gh0st Lab	http://www.gh0st.net/
Hack This Site	http://www.hackthissite.org/
HackThis	http://www.hackthis.co.uk/
HackQuest	http://www.hackquest.com/
Hack.me	https://hack.me
Hacking-Lab	https://www.hacking-lab.com
Hacker Challenge	http://www.dareyourmind.net/
Hacker Test	http://www.hackertest.net/
hACME Game	http://www.hacmegame.org/
Halls Of Valhalla	http://halls-of-valhalla.org/beta/challenges
Hax.Tor	http://hax.tor.hu/
OverTheWire	http://www.overthewire.org/wargames/
PentestIT	http://www.pentestit.ru/en/
CSC Play on Demand	https://pod.cybersecuritychallenge.org.uk/
pwn0	https://pwn0.com/home.php
RootContest	http://rootcontest.com/
Root Me	http://www.root-me.org/?lang=en
Security Treasure Hunt	http://www.securitytreasurehunt.com/
Smash The Stack	http://www.smashthestack.org/
SQLZoo	http://sqlzoo.net/hack/
TheBlackSheep and Erik	http://www.bright-shadows.net/
ThisIsLegal	http://thisislegal.com/
Try2Hack	http://www.try2hack.nl/
WabLab	http://www.wablab.com/hackme
XSS: Can You XSS This?	http://canyouxssthis.com/HTMLSanitizer/
XSS Game	https://xss-game.appspot.com/
XSS: ProgPHP	http://xss.progphp.com/

Sites for Improving Your Hacking Skills

Site name	URL
CAPTF Repo	http://captf.com/
CTFtime (Details of CTF Challenges)	http://ctftime.org/ctfs/
CTF write-ups repository	https://github.com/ctfs
Reddit CTF Announcements	http://www.reddit.com/r/securityctf
shell-storm Repo	http://shell-storm.org/repo/CTF/
VulnHub	https://www.vulnhub.com

Sites for Improving Your Hacking Skills

Site name	URL
Damn Vulnerable Android App (DVAA)	https://code.google.com/p/dvaa/
Damn Vulnerable FirefoxOS Application (DVFA)	https://github.com/pwnetrationguru/dvfa/
Damn Vulnerable iOS App (DVIA)	http://damnvulnerableiosapp.com/
ExploitMe Mobile Android Labs	http://securitycompass.github.io/AndroidLabs/
ExploitMe Mobile iPhone Labs	http://securitycompass.github.io/iPhoneLabs/
Hacme Bank Android	http://www.mcafee.com/us/downloads/free-tools/hacme-bank-android.aspx
InsecureBank	http://www.paladion.net/downloadapp.html
NcN Wargame	http://noconname.org/evento/wargame/
OWASP iGoat	http://code.google.com/p/owasp-igoat/
OWASP Goatdroid	https://github.com/jackMannino/OWASP-GoatDroid-Project

Mobile Apps

Site name	URL
binjitsu	https://github.com/binjitsu/binjitsu
CTFd	https://github.com/isislab/CTFd
Mellivora	https://github.com/Nakiami/mellivora
NightShade	https://github.com/UnrealAkama/NightShade
MCIR	https://github.com/SpiderLabs/MCIR
Docker	https://www.docker.com/
Vagrant	https://www.vagrantup.com/
NETinVM	http://informatica.uv.es/ carlos/docencia/netinvm/
SmartOS	https://smartos.org/
SmartDataCenter	https://github.com/joyent/sdc
vSphere Hypervisor	https://www.vmware.com/products/vsphere-hypervisor/
GNS3	http://sourceforge.net/projects/gns-3/
OCCP	https://opencyberchallenge.net/
XAMPP	https://www.apachefriends.org/index.html

Lab

Site name	URL
VulnVPN	`http://www.rebootuser.com/?page_id=1041`
VulnVoIP	`http://www.rebootuser.com/?page_id=1041`
Vulnserver	`http://www.thegreycorner.com/2010/12/introducing-vulnserver.html`
NETinVM	`http://informatica.uv.es/~carlos/docencia/netinvm/`
DVRF	`https://github.com/praetorian-inc/DVRF`
HackSys	Extreme Vulnerable Driver `http://www.payatu.com/hacksys-extreme-vulnerable-driver/`
VirtuaPlant	`https://github.com/jseidl/virtuaplant`
Fosscomm	`https://github.com/nikosdano/fosscomm`
Morning Catch	`http://blog.cobaltstrike.com/2014/08/06/introducing-morning-catch-a-phishing-paradise/`
AWBO	`https://labs.snort.org/awbo/awbo.html`

Miscellaneous