

[Freshdesk](#) – The easy-to-use customer support software that helps you deliver delightful customer experiences.

8 Vulnerable Web Applications to Practice Hacking Legally

By [Ashlin Jenifa](#)



There's no better way to improve confidence in ethical hacking skills than to put them to the test.

It can be challenging for [ethical hackers](#) and [penetration testers](#) to test their capabilities legally, so having websites designed to be insecure and provide a safe environment to test hacking skills is a fantastic way to keep oneself challenged.

Websites and web apps designed to be insecure and provide a secure hacking environment are ideal grounds for learning. New hackers can learn how to find [vulnerabilities](#) with them, and security professionals and [bug bounty](#) hunters can increase their expertise and find some other new vulnerabilities.

Use of Vulnerable Web Apps

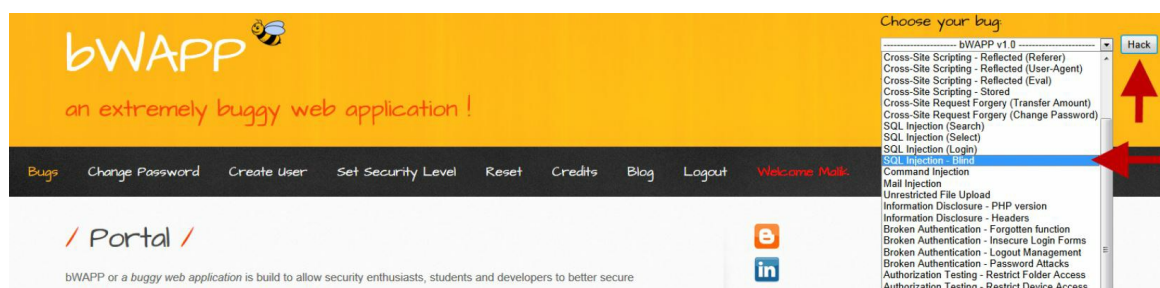
Leveraging these intentionally created vulnerable websites and web apps for testing gives you a safe environment to practice your testing legally while being on the right side of the law. In this manner, you can hack without entering dangerous territory that could lead to your arrest.

These applications are designed to assist security enthusiasts in learning and sharpening their information security and penetration testing abilities.

In this article, I have listed several types of apps that have been purposefully designed insecure, often known as "Damn Vulnerable."

1 Buggy Web Application

The Buggy Web Application, often known as [BWAPP](#), is a free and open-source tool. It's a [PHP](#) application that uses a [MySQL](#) database as its back-end. This Bwapp has over 100 bugs for you to work on, whether you're preparing for a task or just want to keep your ethical hacking abilities up to standard. This covers all of the major (and most prevalent) security flaws.





More than 100 online application vulnerabilities and defects are included in this tool, which was derived from the OWASP Top 10 Project. The following are some of the flaws:

Cross-site scripting (XSS) and cross-site request forgery (CSRF)

DoS (denial-of-service) attacks

Man-in-the-middle attacks

Server-side request forgery (SSRF)

SQL, OS Command, HTML, PHP, and **SMTP** injections, etc.

This web application will assist you in conducting lawful ethical hacking and pen testing.

You can easily download this bwapp by [clicking here](#).

2 Damn Vulnerable Web Application

Damn Vulnerable Web Application, often known as **DVWA**, is developed in PHP and MySQL. It is intentionally left vulnerable so security professionals and ethical **hackers** can test their skills without legally compromising anyone's system. To run, DVWA requires the installation of a web server, PHP, and MySQL. If you don't already have a web server set up, the quickest approach to install DVWA is to download and install 'XAMPP.' **XAMPP is available for download here.**

Damn Vulnerable Web Application (DVWA)

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

DOWNLOAD

SOURCE CONTROL

BUG REPORTING

WIKI

This damn vulnerable web app provides some vulnerabilities to test on.

Brute-force

Command Execution

CSRF and File Inclusion

XSS and SQL injection

Insecure file upload

The main advantage of DVWA is that we can set the security levels to practice testing on each vulnerability. Each level of security needs a unique set of talent. Security researchers can examine what is going on at the back-end thanks to the developers' decision to publish the source code. This is excellent for researchers to learn about these problems and to assist others in learning

about them.

3 Google Gruyere

We don't often see the words "cheese" and "hacking" used together, but this website is full of holes, just like delicious cheese.

Gruyere is an excellent choice for beginners who want to learn how to locate and exploit **vulnerabilities** and how to fight against them. It also uses "cheesy" coding, and the entire design is based on cheese.

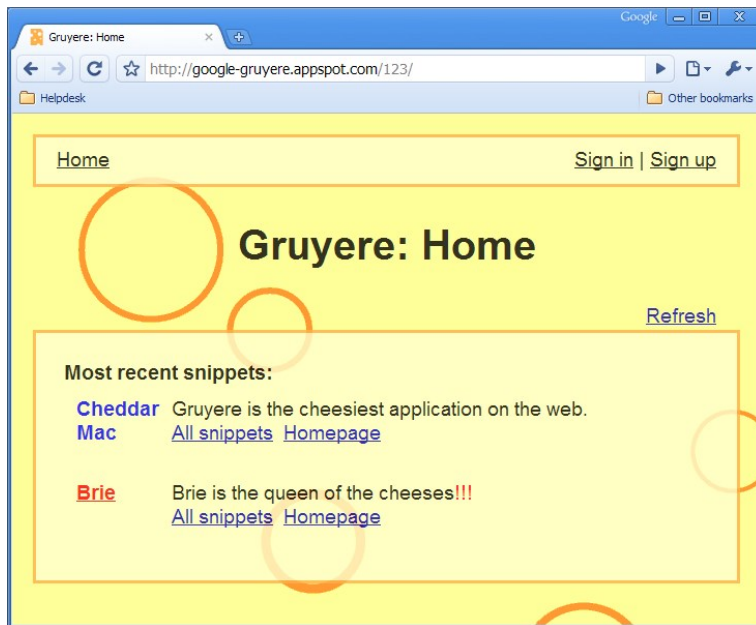


image source: [Google gruyere](#)

To make things easier, it's written in **Python** and categorized by vulnerability kinds. They'll provide you with a brief description of the vulnerability you'll locate, exploit, and identify using black-box or white-box hacking (or a combination of both techniques) for each task. Some of them are :

Information disclosure

SQL injection

Cross-site request forgery

Denial-of-service attacks

Although some prior knowledge is required, this is the best option for beginners.

4 WebGoat

This list includes another OWASP item and one of the most popular. **WebGoat** is an unsafe program that can be used to learn about common server-side application issues. It's intended to assist people in learning about application security and practicing pentesting techniques.

Each lesson allows you to learn about a specific security flaw and then attack it in the app.

Choose another language: **English**

Logout ?

Http Basics

OWASP WebGoat v5.4

< Hints Show Params Show Cookies Lesson Plan Show Java Solution

Restart this Lesson

Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code. You may also try using WebScarab for the first time.

Enter your Name: **Go!**

OWASP Foundation | Project WebGoat | Report Bug

Some of the vulnerabilities featured in Webgoat are :

Buffer overflows

Improper error handling

Injection flaws

Insecure communication and configuration

Session management flaws

Parameter tampering

5 Metasploitable 2

Among security researchers, **Metasploitable 2** is the most commonly exploited online application. High-end tools like Metasploit and **Nmap** can be used to test this application by security enthusiasts.

The main purpose of this vulnerable application is **network testing**. It was modeled after the prominent Metasploit program, which security researchers use to discover security flaws. You might even be able to find a shell for this program. **WebDAV**, **phpMyAdmin**, and DVWA are all built-in features in this application.

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```

You may not be able to find the application's GUI, but you can still use numerous tools via the terminal or command line to exploit it. You can look at its ports, services, and version, among other things. This will assist you in assessing your ability to learn the Metasploit tool.

6 Damn Vulnerable iOS App

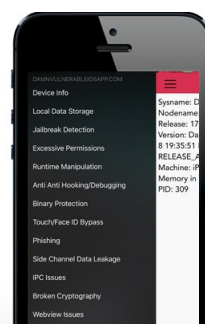
DVIA is an iOS program that allows mobile security enthusiasts, experts, and developers to practice penetration testing. It has recently been re-released and is now freely available on GitHub.

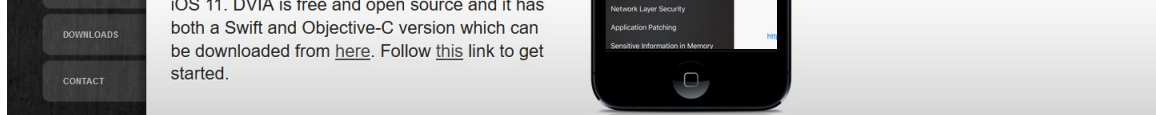


Damn Vulnerable iOS Application (DVIA)

A vulnerable app to test your iOS Penetration Testing Skills

Damn Vulnerable iOS App (DVIA) is an iOS application that is damn vulnerable. Its main goal is to provide a platform to mobile security enthusiasts/professionals or students to test their iOS penetration testing skills in a legal environment. This project is developed and maintained by [@prateekg147](#). The vulnerabilities and solutions covered in this app are tested up to iOS 14.4. DVIA is available on GitHub.





Following the OWASP Top 10 mobile risks, DVIA contains typical iOS app vulnerabilities. It's developed in Swift, and all vulnerabilities have been tested up to iOS 11. You'll need Xcode to use it.

Some of the features available in DVIA are:

Jail-break detection

Phishing

Broken cryptography

Runtime manipulation

Application patching

Binary patching

7 OWASP Mutillidae II

Mutillidae II is an open-source and free program developed by OWASP. Many security enthusiasts have utilized it since it provides an easy-to-use online hacking environment. It features a variety of vulnerabilities as well as recommendations to help the user to exploit them. This web application is for you to brush up on your abilities if penetration testing or hacking is your pastime.

It contains a variety of vulnerabilities to test, including click-jacking, authentication bypass, and more. Its vulnerabilities section, also includes subcategories that provide further alternatives.



You'll need to install **XAMPP** on your system. However, Mutillidae includes XAMPP. Even switching between secure and insecure modes is possible. **Mutillidae** is a complete lab environment that includes everything you need.

8 Web Security Dojo

WSD is a virtual machine with various tools such as Burp Suite and **ratproxy** and target machines (such as WebGoat). It's an open-source training environment based on the **Ubuntu** 12.04 operating system. For some objectives, it also contains training materials and user guides.

You don't need to run any other tools to use it; all you need is this VM. You'll need to install and run VirtualBox 5 (or later) initially, or you can use **VMware** instead. Then, import the ova file into VirtualBox/VMware, and you're done. It will have the same feel as any other Ubuntu OS.





This VM is ideal for self-study and learning by beginners, professionals, and teachers who want to teach about vulnerabilities.

Conclusion 🧐

You must have hands-on experience with insecure applications before entering the professional realm of information security. It aids in the development of your abilities.

It also assists you in identifying and practicing your weak areas. By practicing ethical hacking on purpose-built applications, you will better understand your hacking abilities and where you stand in the security realm. It is beneficial to share information. You can use these web applications to show others how to spot typical web application flaws.



Ashlin Jenifa
Author

Hey there, my name is Ashlin, and I'm a senior technical writer. I've been in the game for a while now, and I specialize in writing about all sorts of cool technology topics like Linux, Networking, Security, Dev Tools, Data Analytics, and Cloud... [read more](#)

Vulnerable Web Apps

1. Buggy Web Application
2. Damn Vulnerable Web Application
3. Google Gruyere
4. WebGoat
5. Metasploitable 2
6. Damn Vulnerable iOS App
7. OWASP Mutillidae II
8. Web Security Dojo

More great readings

1. 7 High Paying Job Roles in IT
2. How to Learn Digital Marketing Online?
3. Where to Find Free Online Courses to Learn Something New?
4. 10 Free Online Courses by Google to Upskill Yourself
5. 8 Platforms to Host Virtual Career Fairs in 2023

Thanks to our Sponsors



More great readings on Career



Kickstart Your Software Testing Career With These Courses and Resources

By [Satish Shethi](#) on October 10, 2023

At some point in your working life, you've probably thought about a career in software testing. Software testing is the process of executing tests on a software application to determine if it meets predetermined requirements.



Google Task Mate

How to Earn Money Through Google Task Mate

By [Tamal Das](#) on October 9, 2023

Want to earn some easy money at your leisure? Are you interested in traveling and reckoning exciting places? Do you enjoy answering survey questions that make technologies better? If yes, you will love Google Task Mate.



8 Premium Resume Builder to Build a Powerful Professional Resume

By [Ruby Goyal](#) on October 8, 2023

Resumes and CVs are one of the most crucial and elemental parts of your interview process that may make or break your candidature.



How to Become a Certified Salesforce Admin in 2023

By [Durga Prasad Acharya](#) on October 8, 2023

Becoming a certified Salesforce admin is rewarding for your career.



How to Become an AWS Cloud Practitioner in 2023: Courses and Resources

By [Naman Yash](#) on October 6, 2023

The AWS Cloud Practitioner Certification requires a basic understanding of AWS services and usage cases, invoice and cost methods, security principles, and how the cloud affects your organization.



AWS Certification – What are the Options and How to become Certified?

By [Abhishek Kothari](#) on October 6, 2023

Become an AWS certified expert for better career growth!

Power Your Business

Some of the tools and services to help your business grow.

The text-to-speech tool that uses AI to generate realistic human-like voices.

[Try Murf AI](#) →

Web scraping, residential proxy, proxy manager, web unlocker, search engine crawler, and all you need to collect web data.

[Try Brightdata →](#)

Monday.com is an all-in-one work OS to help you manage projects, tasks, work, sales, CRM, operations, workflows, and more.

[Try Monday →](#)

Intruder is an online vulnerability scanner that finds cyber security weaknesses in your infrastructure, to avoid costly data breaches.

[Try Intruder →](#)

Your trusted source for Technology Resources

© Geekflare, 71-75 Shelton Street, London, WC2H 9JQ

COMPANY

[About](#)

[Advertise](#)

[Sitemap](#)

[Careers](#)

[Contact](#)

LEGAL

[Terms](#)

[Privacy](#)

[Disclosure](#)

[Cookie Policy](#)

[Scam Awareness](#)

FAMILY

[Siterelic](#)

[ByteBrief](#)

[Domsignal](#)