

sedian

Seguridad Digital
de Andalucía



Recurso de aprendizaje

Sitios de CTF y pentesting
para practicar tus habilidades
de hacking y ciberseguridad



Junta de Andalucía

ÍNDICE

1.INTRODUCCIÓN.....	3
2.ATENEA.....	3
3.HACK THE BOX.....	4
4.WEB-SECURITY ACADEMY.....	5
5.OWASP JUICE SHOP.....	5
6.PENTESTERLAB.....	6
7.VULNHUB.....	7
8.TRYHACKME.....	8
9.HACKER 101.....	8
10.ATTACK & DEFENSE.....	9
11.CTF ANTICHAT.....	10
12.CAPTURE THE FLAG AT UCF.....	11
13.EXPLOIT EDUCATION.....	11
14.CSAW 365.....	12
15.HACK.ME.....	13
16.XSS GAME.....	14
17.HACKING-LAB.....	15
18.ENIGMA GROUP.....	15
19.CTFLEARN.....	16
20.RINGZERO TEAM ONLINE.....	17

21.HACK THIS SITE.....	17
22.W3CHALLS.....	18
23.GAME OF HACKS.....	19
24.WEBGOAT PROJECT.....	19
25.SQLI LABS.....	20
26.PICOCTF.....	21
27.DEFEND THE WEB.....	21
28.OVERTHEWIRE.....	22
29.GOOGLE GRUYERE.....	23
30.MUTILLIDAE.....	24
31.DAMN VULNERABLE WEB APPLICATION.....	25
32.BWAPP.....	26
33.METASPLOITABLE 2.....	26
34.METASPLOITABLE 3.....	27

1 . INTRODUCCIÓN

Por su utilidad práctica recogemos en este documento un listado de sitios web¹ de CTF y pentesting para practicar tus habilidades de hacking y ciberseguridad.

“La práctica es un maestro excepcional.”

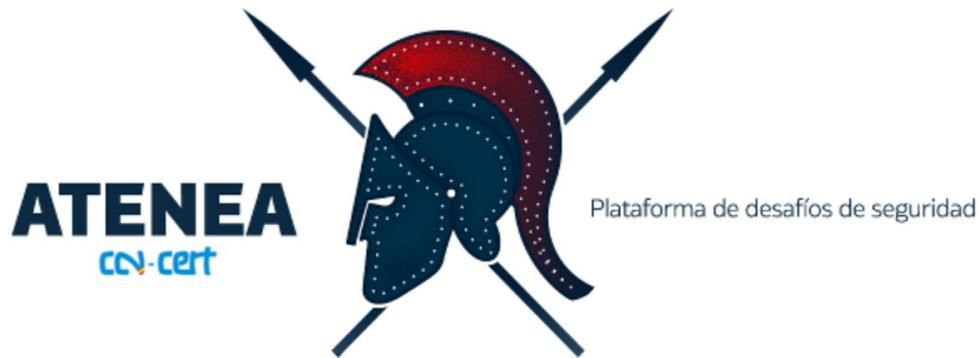
Plinio el Joven (62-113) Escritor romano.

La información incluida en este documento tiene como finalidad facilitar únicamente recursos de aprendizaje que pueden ser utilizados de manera autodidacta. **SEDIAN no se hace responsable del funcionamiento o mantenimiento de dichas webs y herramientas.** Por tanto, antes de acceder a cualquiera de estos servicios y de facilitar cualquier dato, le recomendamos encarecidamente revise los términos y condiciones de uso de los mismos para preservar la seguridad y privacidad de sus datos.

2 . ATENEA

ATENEA es una plataforma de desafíos de seguridad informática **desarrollada por el CCNCERT.** Los retos presentados abarcan diferentes campos, como criptografía y esteganografía, exploiting, forense, networking y reversing, entre otros.

¹ Algunos de los sitios que aparecen referenciados en este documento han sido extraídos del artículo titulado [50 sitios de CTF y pentesting para practicar sus habilidades de hacking y ciberseguridad en 2021.](#)



[Sitio web ATENEA](#)

3.HACK THE BOX



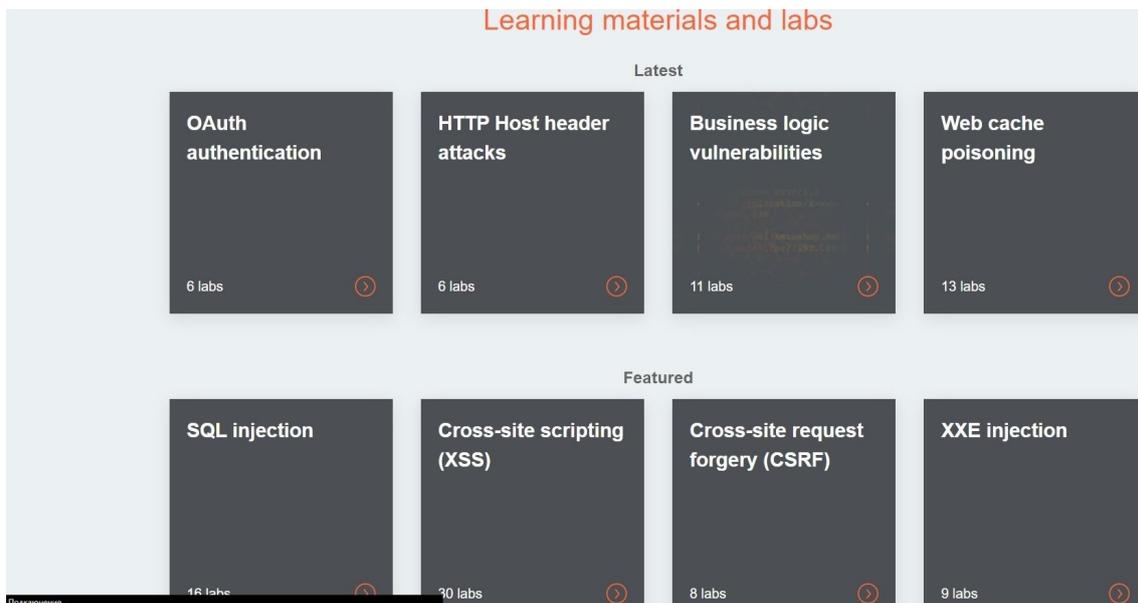
Es una de las plataformas de pentesting más importantes del mundo, disponiendo de 127 sistemas vulnerables, 65 tareas CTF y múltiples implementaciones virtuales de AD hardcore.

Durante los más recientes años Hack The Box se ha convertido en una herramienta popular entre los expertos en pentesting, ya que presenta una interfaz web conveniente para la administración de instancias activas de

máquinas virtuales, amplio soporte técnico y una lista de hosts vulnerables constantemente actualizada.

[Sitio web Hack the Box](#)

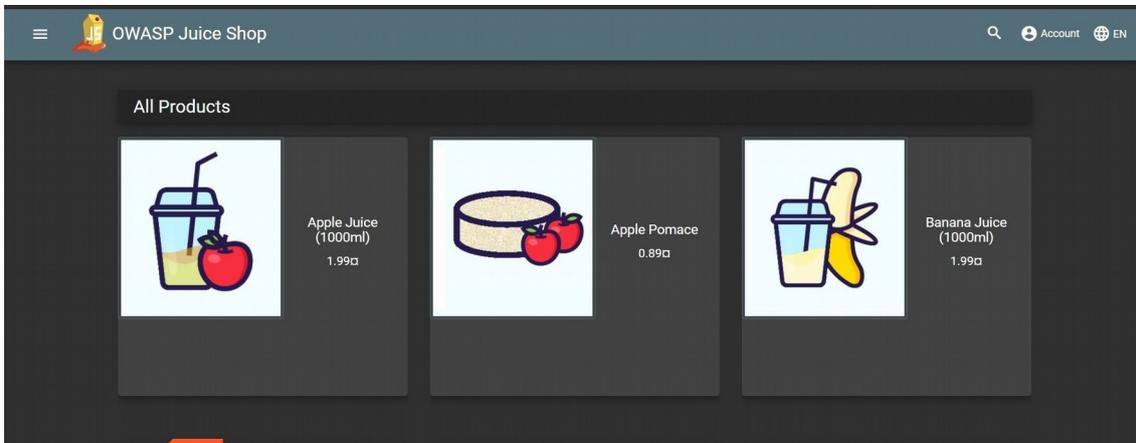
4 . WEB-SECURITY ACADEMY



Plataforma desarrollada por los creadores de Burp Suite muy popular entre los cazadores de recompensas por vulnerabilidades.

[Sitio web Security Academy](#)

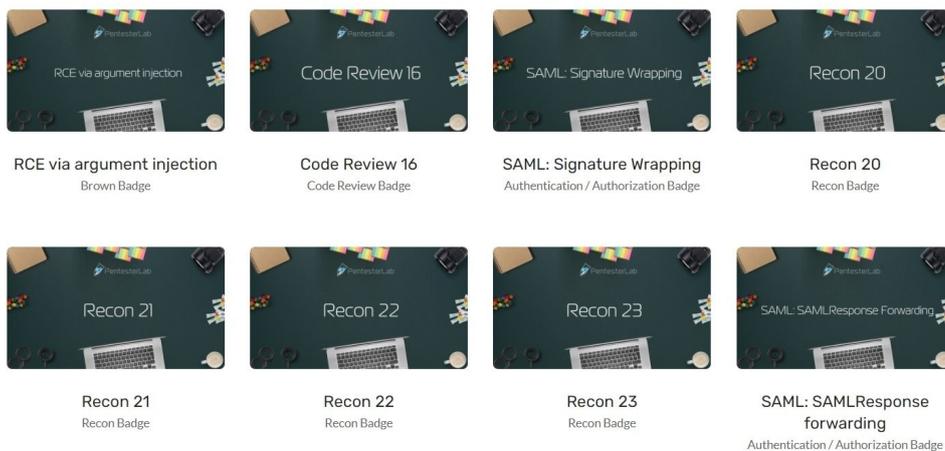
5.OWASP JUICE SHOP



Aplicación web escrita en JavaScript con fines de entrenamiento en pentesting. Esta plataforma está llena de fallas de seguridad diseñadas para que los usuarios puedan explotarlas, como un método fantástico para la capacitación en ciberseguridad.

[Sitio web Owasp Juice Shop](#)

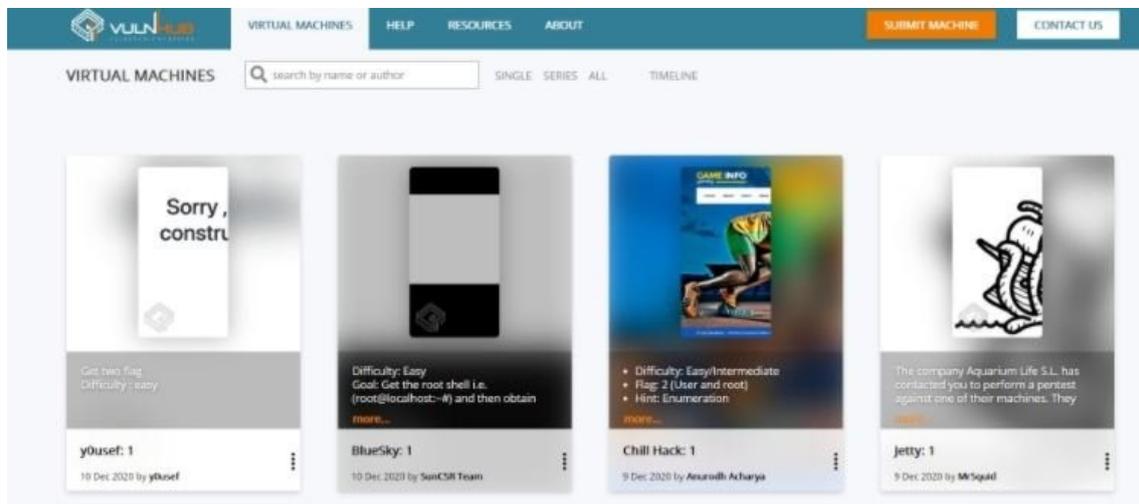
6 .PENTESTERLAB



Plataforma que proporciona laboratorios en línea dedicados al despliegue de pruebas de penetración. Este sitio web ofrece una gran variedad de actividades gratuitas para todos los interesados en perfeccionar sus habilidades en pentesting.

[Sitio web Pentesterlab](#)

7. VULNHUB



Gran biblioteca de máquinas virtuales que presenta un entorno con ejercicios de pentesting para todos los gustos y niveles de conocimiento.

[Sitio web Vulnhub](#)

8 . TRYHACKME



Plataforma de reciente creación que permite a los entusiastas de la ciberseguridad familiarizarse con temas muy interesantes. A diferencia de otras plataformas de carácter autodidacta, TryHackMe emplea toda clase de técnicas para facilitar el aprendizaje, acompañado a los usuarios a lo largo de todo el proceso.

[Sitio web TryHackMe](#)

9.HACKER 101

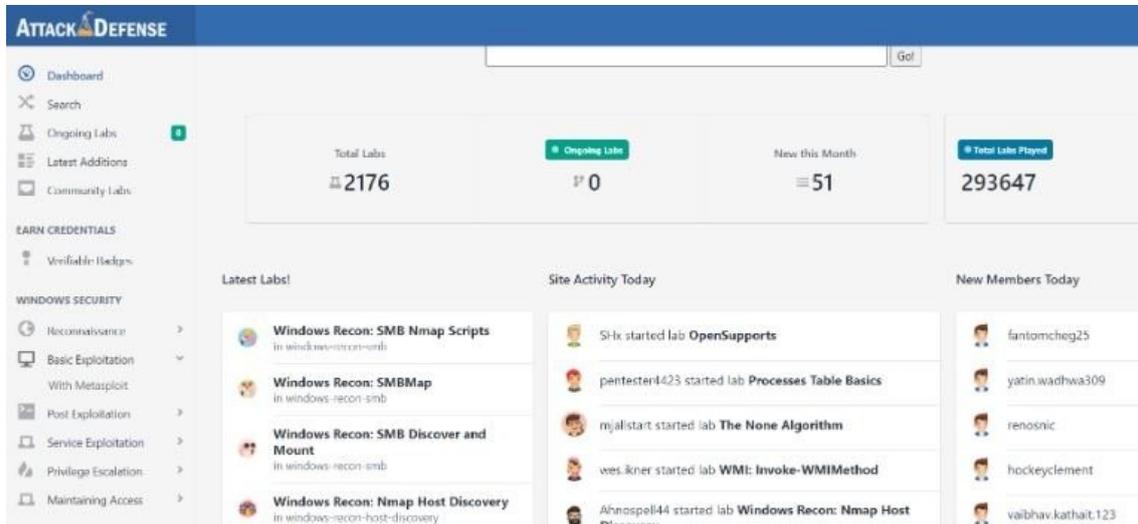
You've earned 0 invitations, 0 / 26 points to your next private invitation. [Learn more about invitations.](#)

Difficulty (Points)	Name	Skills	Completion	
Trivial (1 / flag)	A little something to get you started	Web	0 / 1	Go Hints Restart
Easy (2 / flag)	Micro-CMS v1	Web	0 / 4	Go Hints Restart
Moderate (3 / flag)	Micro-CMS v2	Web	0 / 3	Go Hints Restart
Hard (9 / flag)	Encrypted Pastebin	Web, Crypto	0 / 4	Go Hints Restart
Moderate (6 / flag)	Photo Gallery	Web	0 / 3	Go Hints Restart
Moderate (5 / flag)	Cody's First Blog	Web	0 / 3	Go Hints Restart
Easy (4 / flag)	Postbook	Web	0 / 7	Go Hints Restart
Moderate (0 / flag)	Ticketastic: Demo Instance	Web	0 / 0	Go Hints Restart

Sitio didáctico gratuito para cualquier entusiasta del hacking respaldada por la reconocida plataforma recompensas por vulnerabilidades HackerOne.

[Sitio web Hacker101](#)

10. ATTACK & DEFENSE



Con más de 2100 actividades de hacking los usuarios de Attack & Defense podrán desarrollar al 100% sus capacidades para el pentesting.

[Sitio web Attack & Defense](#)

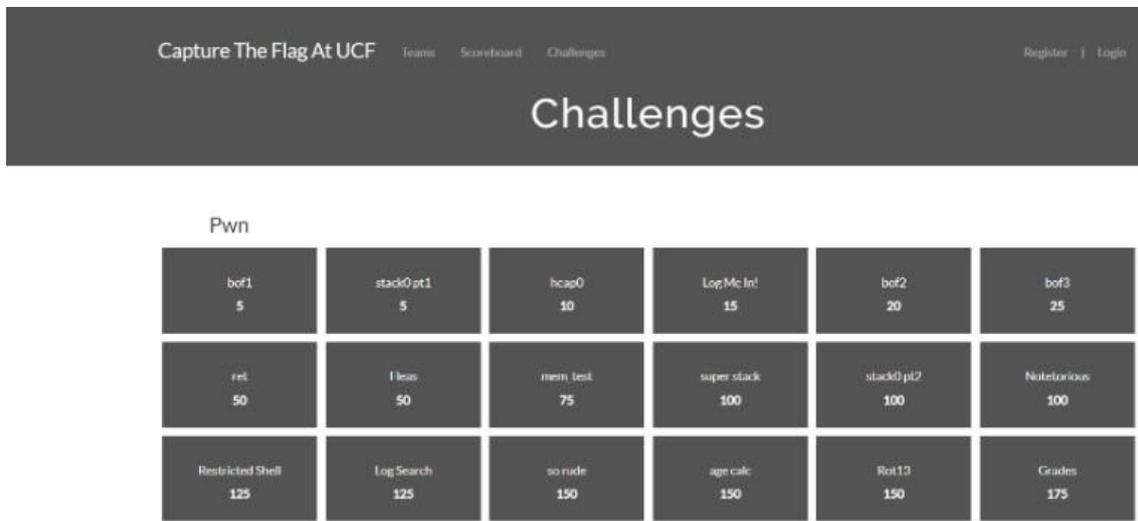
11.CTF ANTICHAT



Plataforma para completar tareas enfocadas en la explotación de vulnerabilidades e identificar indicadores de compromiso en los sistemas analizados.

[Sitio web CTF Antichat](#)

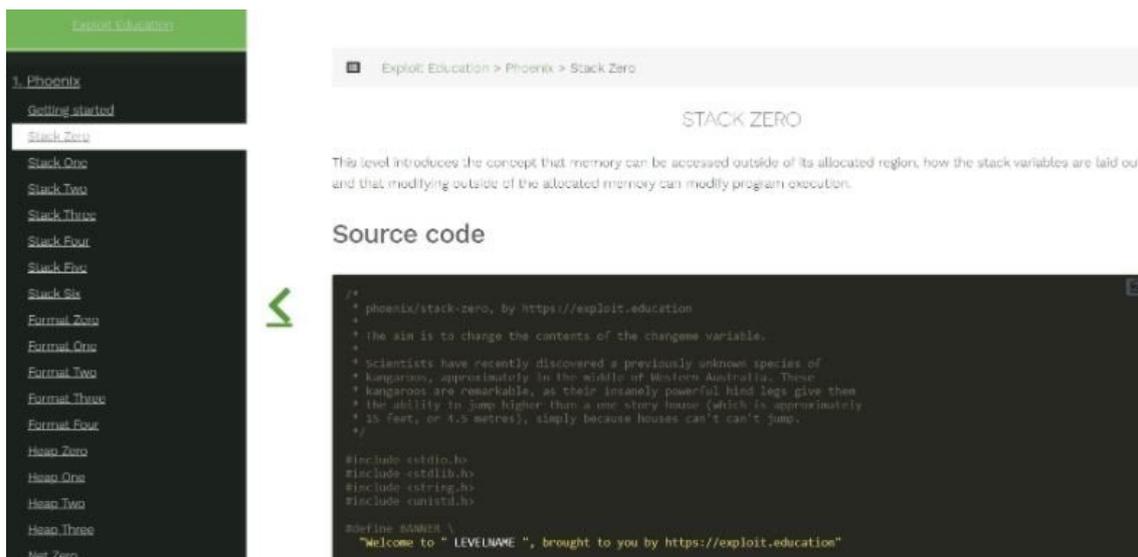
12. CAPTURE THE FLAG AT UCF



Recurso con gran cantidad de tareas en varias áreas del pentesting.

[Sitio web Capture The Flag at UCF](#)

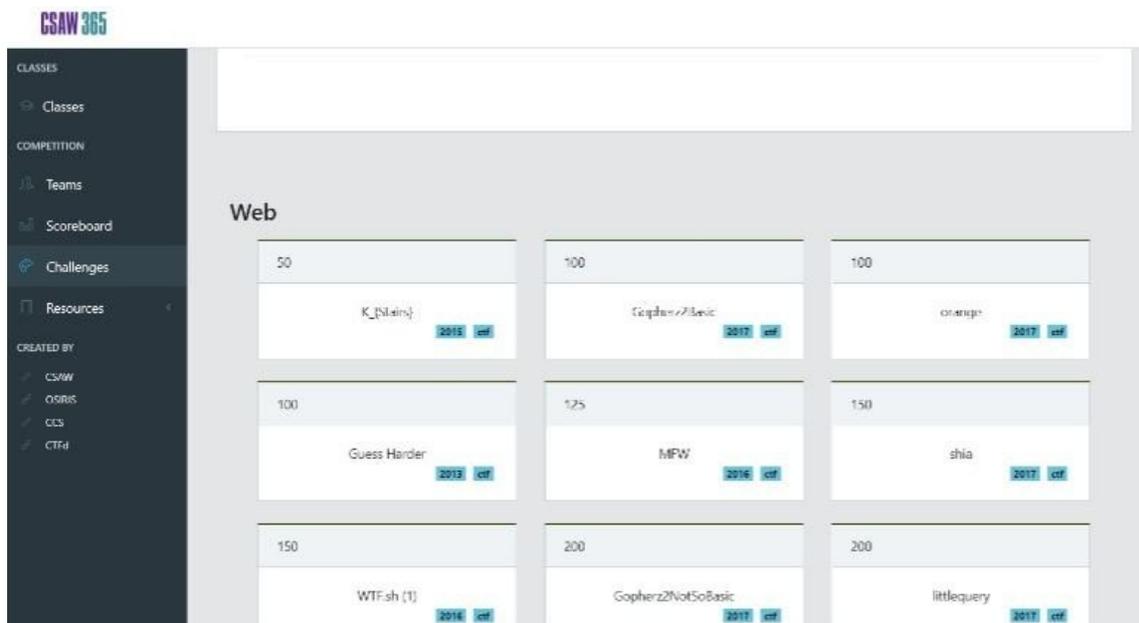
13. EXPLOIT EDUCATION



Exploit Education proporciona muchos recursos que cualquiera puede utilizar para aprender sobre análisis de vulnerabilidades, desarrollo de exploits, pentesting, análisis binario y muchos otros problemas de ciberseguridad.

[Sitio web Exploit Education](#)

14.CSAW 365



Comunidad de expertos en ciberseguridad que permite compartir una gran cantidad de información útil para el hacking.

[Sitio web CSAW 365](#)

15.HACK.ME



Hack.me es una gran colección de aplicaciones web vulnerables para poner en práctica sus habilidades de hacking. Todas las aplicaciones son proporcionadas por los miembros de la plataforma y cada una de ellas se puede iniciar en un entorno sandbox.

[Sitio web Hack.Me](#)

16.XSS GAME



Programa de Google diseñado para practicar la búsqueda de vulnerabilidades XSS.

[Sitio web XSS GAME](#)

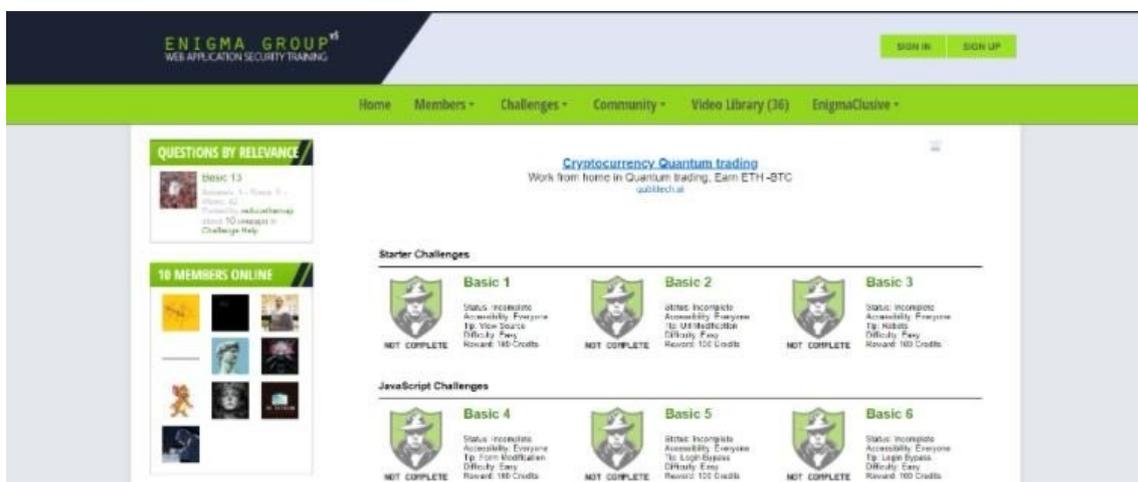
17. HACKING-LAB



Plataforma en línea para aprender sobre seguridad de redes y hacking ético. Los hackers podrán desarrollar sus habilidades forenses, de criptografía e ingeniería inversa.

[Sitio web Hacking-Lab](#)

18. ENIGMA GROUP

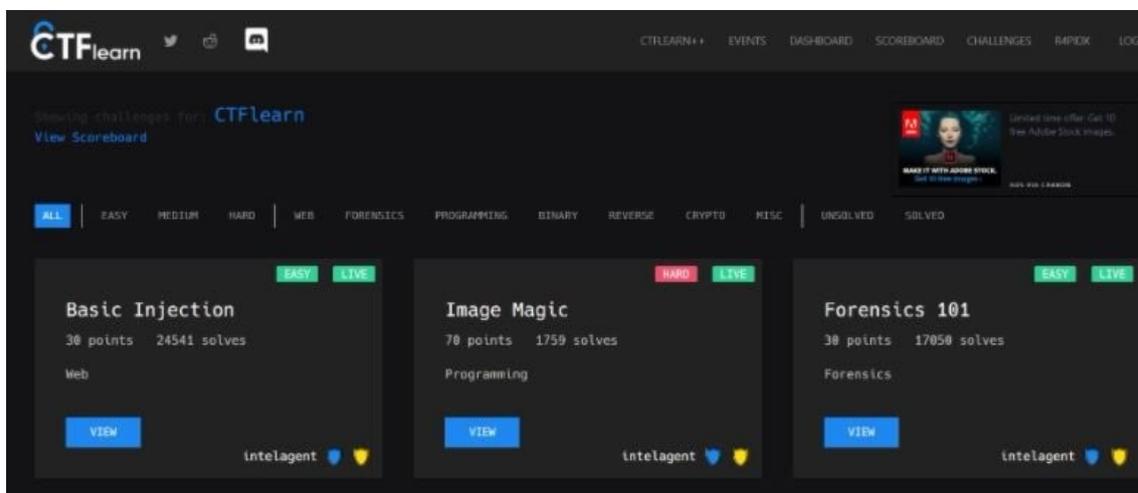


Sitios de CTF y pentesting

Enigma Group contiene más de 300 tareas de hacking con un enfoque en los 10 principales exploits de OWASP. El sitio tiene casi 48 mil miembros activos y organiza concursos Capture The Flag de forma semanal.

[Sitio web Enigma Group](#)

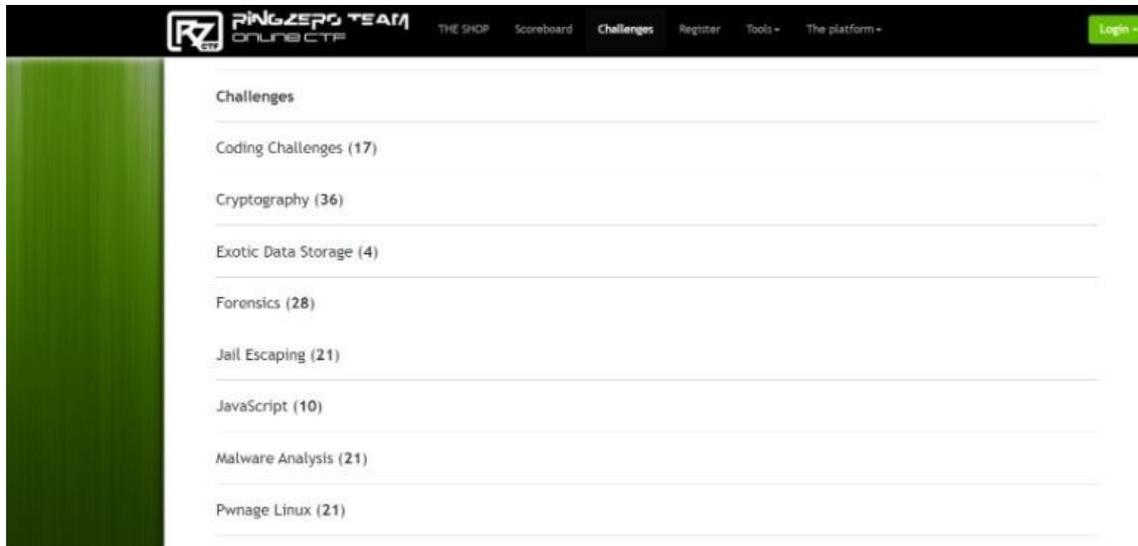
19 .CTFLEARN



CTFlearn es una plataforma que permite a los entusiastas del hacking poner en práctica sus habilidades y competir con otros investigadores. Esta plataforma almacena un amplio conjunto de actividades gratuitas en toda clase de áreas.

[Sitio web CTFlearn](#)

20.RINGZER0 TEAM ONLINE



RingZero Team Online CTF ofrece más de 200 desafíos que pondrán a prueba sus habilidades de hacking en múltiples áreas, desde criptografía, análisis de malware hasta inyección SQL y pentesting.

[Sitio web RingZero Team Online](#)

21.HACK THIS SITE



Sitio gratuito de juegos de guerra para que cualquier usuario pueda probar y mejorar sus habilidades de hacking, desde tareas básicas hasta complejos análisis. Este sitio web también incluye un foro para que los usuarios puedan compartir sus experiencias con la comunidad del hacking ético y pentesting.

[Sitio web Hack This Site](https://www.hackthissite.org/)

22 .W3CHALLS

Points	Challenge	Solvers	Tags	Forums	Votes	Status
1	Change your browser	9032				up
5	Mobile-Downloads	1295				up
7	.htaccess	2088				up
8	Databasic	1584				up
9	Authentication	1359				up
10	An image gallery	909				up
12	Temporal attack	902				up
15	WebCompany	561				up
16	Vip Web Army	265				up
16	Temporary attack	261				up
17	W3News	178				up

W3Challs es una plataforma de aprendizaje multitarea organizada en una variedad de categorías, incluyendo hacking, juegos de guerra, análisis forense, criptografía, esteganografía y programación en múltiples lenguajes.

[Sitio web W3Challs](#)

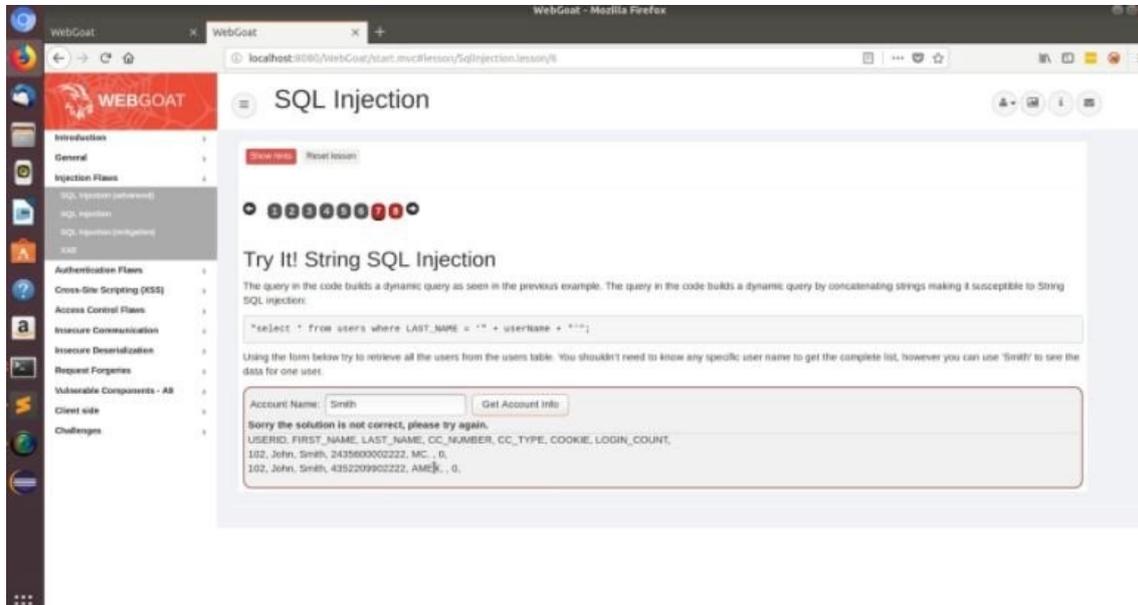
23 .GAME OF HACKS



Game of Hacks muestra un conjunto de fragmentos de código en un cuestionario con múltiples opciones, entre las cuales los usuarios deberán identificar la vulnerabilidad correspondiente.

[Sitio web Game of Hacks](#)

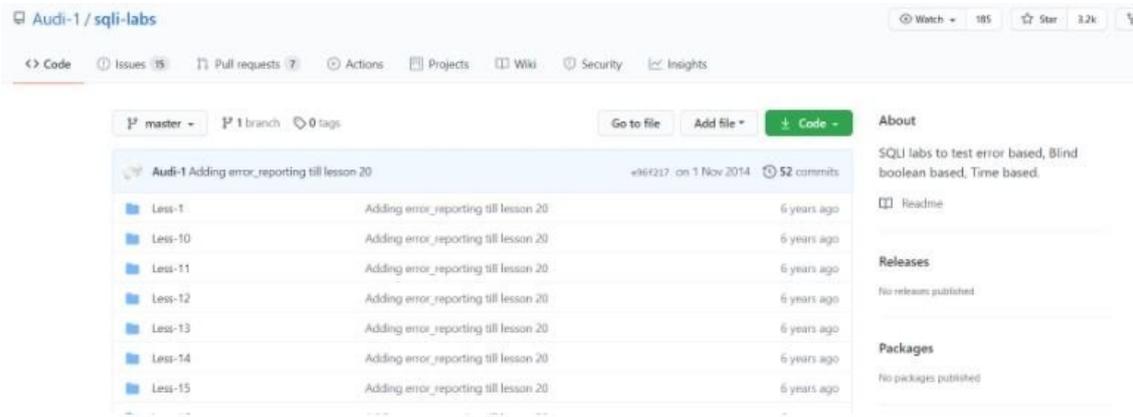
24.WEBGOAT PROJECT



Sitio especialmente enfocado en la formación de hackers éticos y expertos en pentesting. WebGoat es una herramienta multiplataforma que puede ser ejecutada en cualquier sistema operativo con Apache Tomcat y Java SDK.

[Sitio web WebGoat Project](#)

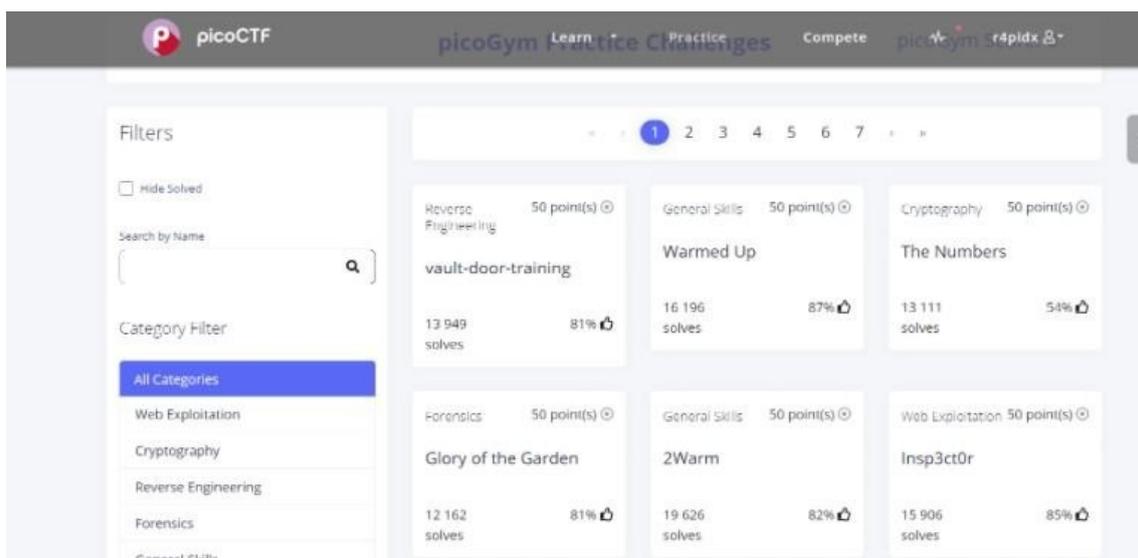
25. SQLI LABS



Plataforma que permite a los usuarios probar habilidades para trabajar con inyecciones SQL y cuenta con 65 tareas ordenadas según su nivel de dificultad.

[Sitio web SQLI Labs](#)

26. PICOCTF



Recurso muy interesante con una gran cantidad de tareas e instrucciones para los entusiastas del pentesting.

[Sitio web PicoCTF](#)

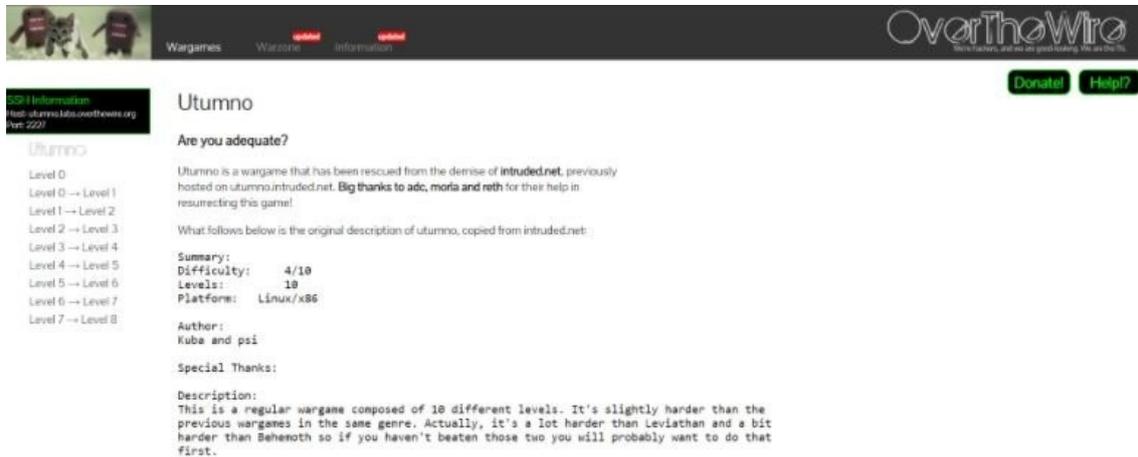
27.DEFEND THE WEB



Plataforma de seguridad interactiva donde los investigadores pueden mejorar sus habilidades de hacking. Defend the Web cuenta con más de 60 niveles de dificultad para desarrollar las más sofisticadas habilidades.

[Sitio web Defend the Web](#)

28. OVERTHEWIRE



Plataforma ideal para todos los interesados en el estudio teórico de la seguridad informática sin importar su nivel de experiencia.

Incluso los hackers principiantes pueden encontrar gran orientación para la resolución de cuestiones prácticas en OverTheWire.

[Sitio web OverTheWire](#)

29. GOOGLE GRUYERE



Web Application Exploits and Defenses

A Codelab by Bruce Leban, Magthe Sendre, and Paitso Tabriz

Want to beat the hackers at their own game?

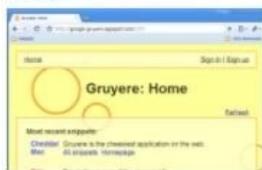
- Learn how hackers find security vulnerabilities!
- Learn how hackers exploit web applications!
- Learn how to stop them!

This codelab shows how web application vulnerabilities can be exploited and how to defend against these attacks. The best way to learn things is by doing, so you'll get a chance to do some real penetration testing, actually exploiting a real application. Specifically, you'll learn the following:

- How an application can be attacked using common web security vulnerabilities, like cross-site scripting (XSS) and cross-site request forgery (CSRF).
- 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.

To get the most out of this lab, you should have some familiarity with how a web application works (e.g., general knowledge of HTML, templates, cookies, Ajax, etc.).

Gruyere



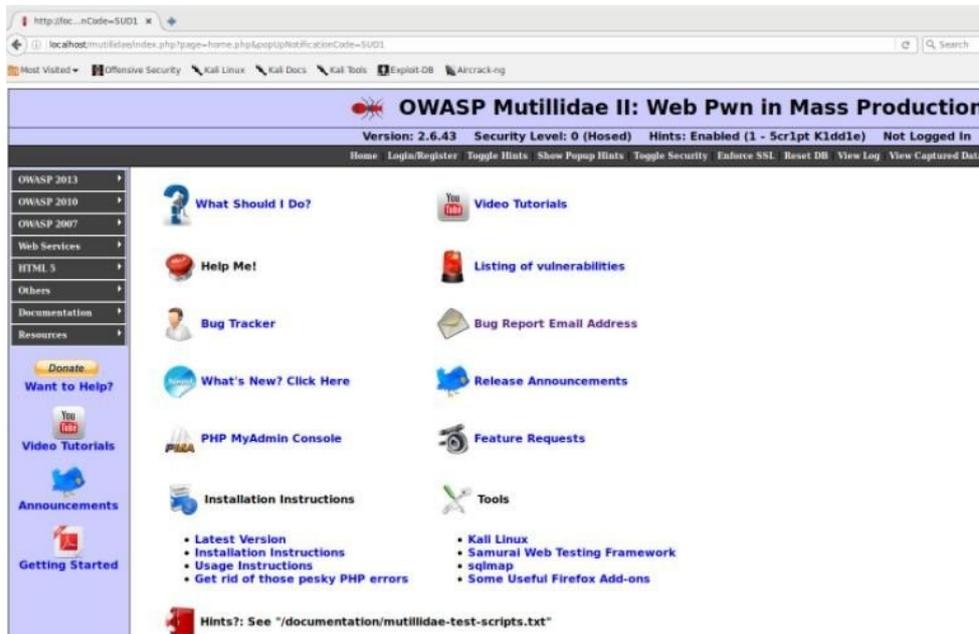
This codelab is built around **Gruyere** (gru.grab0r.com) - a small, cheesy web application that allows its users to publish snippets of text and store assorted files. "Unfortunately," Gruyere has multiple security bugs ranging from cross-site scripting and cross-site request forgery, to information disclosure, denial of service, and remote code execution. The goal of this codelab is to guide you through discovering some of these bugs and learning ways to fix them both in Gruyere and in general.

The codelab is organized by types of vulnerabilities. In each section, you'll find a brief description of a vulnerability and a **task** to find an instance of that vulnerability in Gruyere. Your job is to play the role of a malicious hacker and find and exploit the security bugs. In this codelab, you'll use both black-box hacking and white-box hacking. In **black-box hacking**, you try to find security bugs by experimenting with the application and manipulating input fields and URLs, parameters, trying to cause application errors, and looking at the HTTP requests and responses to guess server behavior. You do not have access to the source code, although understanding how to view source and being able to view http headers (as you can in Chrome or LiveHTTPHeaders for Firefox) is valuable. Using a web proxy like Burp or ZAP may be helpful in creating or modifying requests. In **white-box hacking**, you have access to the source code and can use automated or manual analysis to identify bugs. You can keep Gruyere as it's open source; you can read through the source code to try to find bugs. Gruyere is written in Python, so some familiarity with Python can be helpful. However, the security vulnerabilities covered are not Python-specific and you can do most of the lab without even looking at the code. You can run a local instance of Gruyere to assist in your hacking. For example, you can create an administrator account on your local instance to learn how administrative features work and then apply that knowledge to the instance you want to hack. Security researchers use both hacking techniques, often in combination, in real life.

Plataforma escrita en Python que ofrece capacidades de pentesting y hacking de sombrero negro y sombrero blanco para que los expertos aprendan a pensar como investigadores y cibercriminales.

[Sitio web Google Gruyere](http://gru.grab0r.com)

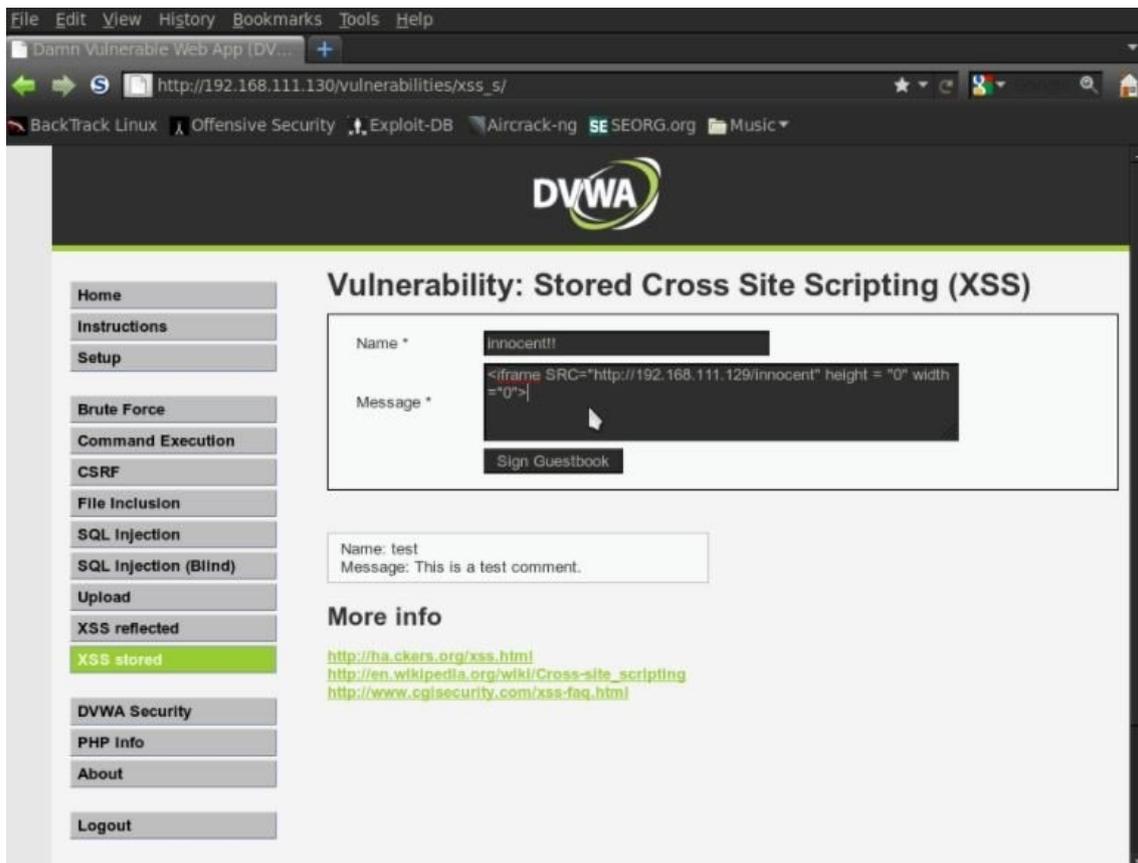
30.MUTILLIDAE



Plataforma gratuita de código abierto para el pentesting de aplicaciones web. La aplicación se proporciona como una instancia de PHP / MySQL para auto-implementación.

[Sitio web Multillidae](#)

31.DAMN VULNERABLE WEB APPLICATION



Plataforma de gran ayuda para los profesionales de la seguridad que deseen probar sus habilidades en un entorno legal. Al igual que el ejemplo anterior, esta aplicación se proporciona como una instancia de PHP / MySQL para auto-implementación.

[Sitio web Damn Vulnerable Web Application](http://www.damn-vulnerable-web-application.com/)

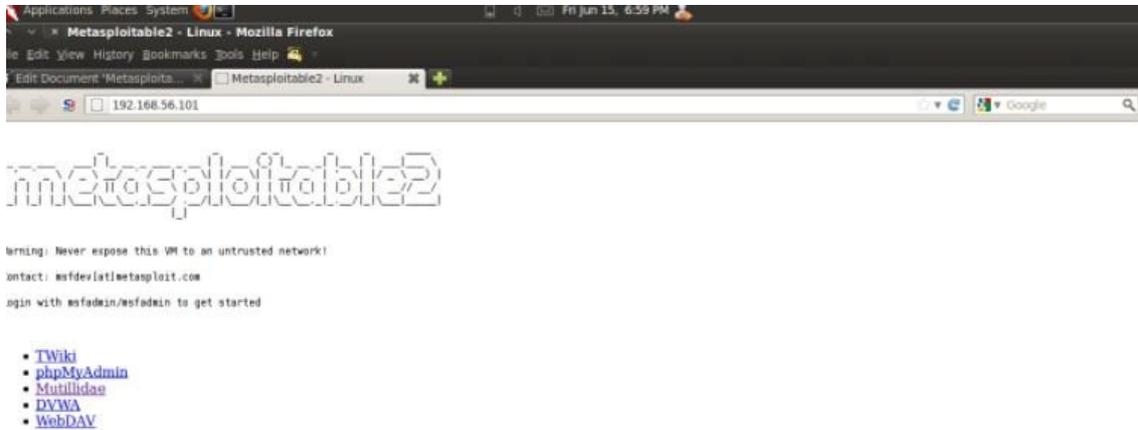
32 . BWAPP



Aplicación web especializada de código abierto que contiene alrededor de 100 vulnerabilidades clasificadas según la metodología OWASP.

[Sitio web BWAPP](#)

33 .METASPLOITABLE 2



Metasploitable 2 es como un saco de boxeo para pentesters y programas como Metasploit y Nmap. Todos los puertos están abiertos y todas las vulnerabilidades conocidas están presentes en esta plataforma.

[Sitio web Metasploitable 2](#)

34 .METASPLOITABLE 3



Máquina virtual gratuita que permite a los usuarios simular ataques usando Metasploit. Esta es una de las herramientas favoritas de los especialistas en ciberseguridad.

[Sitio web Metasploitable 3](#)