



80 PLATFORMS

ENABLING PRACTICAL LEARNING
OF CYBERSECURITY



Publisher:

SecurityBezTabu.pl

E-mail: kontakt@securitybeztabu.pl

ContaCt: <https://securitybeztabu.pl/kontakt/>

Copyright © by Security Bez Tabu®, 2024

Place and date of publication: Warsaw, July 2024

Content and graphic design: Wojciech Ciemski

Text proofreading: Dorota Księżopolska

All rights reserved. Unauthorized distribution of this publication, in whole or in part, in any form and without the publication's name, is prohibited.

Unauthorized dissemination of this publication, in whole or in part, constitutes a violation of copyright law.

Use this knowledge responsibly: the author is not liable for any potential damages resulting from the application of the information contained in this publication.

Please note that creating this publication required a significant amount of time and effort. We kindly ask you tag the author. If you use it in trainings or consultations, please ensure to credit the source and author in accordance with citation guidelines.

Dear Reader,

If you would like to share your thoughts about this publication, feel free to write to me at:

kontakt@securitybeztabu.pl

I would love to hear your feedback, suggestions, or review.



About author



WOJCIECH CIEMSKI

- A practitioner supporting digital transformation
- One of the global "40 under 40 in Cybersecurity 2024" ranking
- Top IT speaker in Poland since 2021
- Author of the bestseller "Cybersecurity in Questions and Answers"

With over a decade of experience in the IT and cybersecurity industry, Wojciech is the founder of the iconic blog Security Bez Tabu®, which has become one of the most influential sources of cybersecurity knowledge in Poland. He plays a pivotal role as a vCISO and also thrives as a lecturer, auditor, and pentester. Over the past three years, he has trained more than 2,000 people and conducted over 500 hours of live training sessions.

Wojciech is unafraid to voice his thoughts—even when they are controversial. He speaks his mind openly, firmly believing that honesty and courage are the cornerstones of meaningful change. As a visionary with a clear mission, he steadfastly follows his path, regardless of the obstacles he encounters. His determination and consistency inspire others, demonstrating that unconventional approaches and passion can reshape reality. Where others see barriers, he sees opportunities, and his vision influences not only the evolution of cybersecurity but also the people who have the privilege of working with him.

His mission is to educate and inspire current and future IT professionals, contributing to a safer digital future. His presentations captivate, inspire, and earn admiration from audiences.



introduction

"It does not matter how slowly you go, as long as you do not stop."

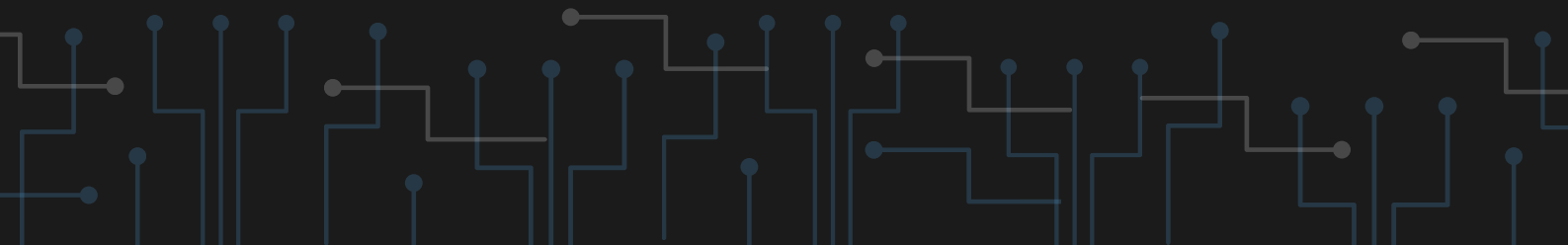
Confucius

We all know that practice is the most crucial aspect of learning cybersecurity. However, we often face a challenge I call the "student's paradox"—an abundance of enthusiasm and willingness but a lack of clear direction and resources, which can easily discourage further learning. Fortunately, there are numerous platforms offering practical challenges that help develop skills in real-world scenarios.

In this ebook, we present 80 such resources to help you kickstart and continue your journey in cybersecurity. Importantly, not all of these platforms rely on the popular CTF (Capture The Flag) model. Many of them are GitHub-hosted projects, making them widely accessible and easy to dive into.

Whether you're a beginner or already have some experience in the field, you'll definitely find something for yourself. So don't wait any longer—immerse yourself in the world of cybersecurity and start your journey with one of the recommended platforms! Now, you have no excuse not to improve your skills and knowledge in this incredibly important domain.

Since many platforms cover vastly different topics, I decided that the only logical way to organize them was alphabetically. This order does not reflect any ranking or assessment.

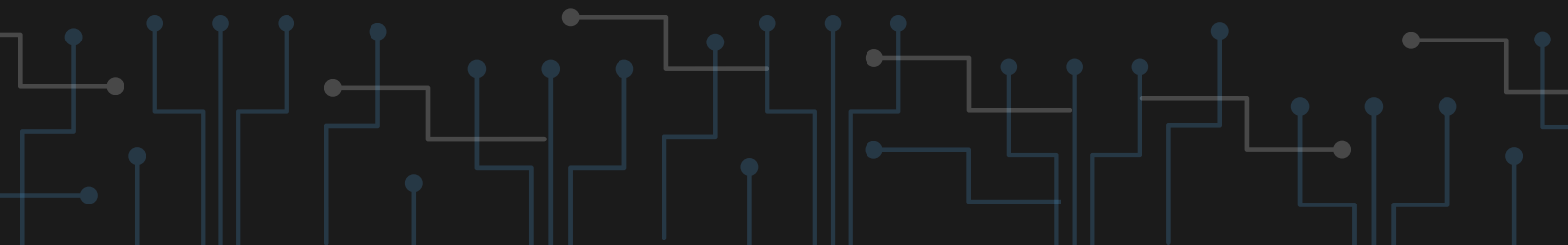




AD Lab

[HTTPS://GITHUB.COM/ALEBOV/AD-LAB](https://github.com/Alebov/AD-Lab)

AD Lab is a GitHub repository that offers a fully functional Active Directory (AD) penetration testing lab environment. Created by Alebov, it includes various AD configurations and vulnerabilities, allowing users to simulate real-world attack scenarios in a controlled setup. This lab is ideal for security professionals and enthusiasts who want to understand AD security, exploit common AD vulnerabilities, and practice mitigation techniques.





API Security University

[HTTPS://WWW.APISECUNIVERSITY.COM/](https://www.apisecuniversity.com/)

API Security University provides a wealth of educational resources focused on API security. It offers courses, tutorials, and best practices for securing APIs against various threats. The platform is intended for developers, security professionals, and anyone interested in learning about API vulnerabilities, protection mechanisms, and the latest trends in API security.

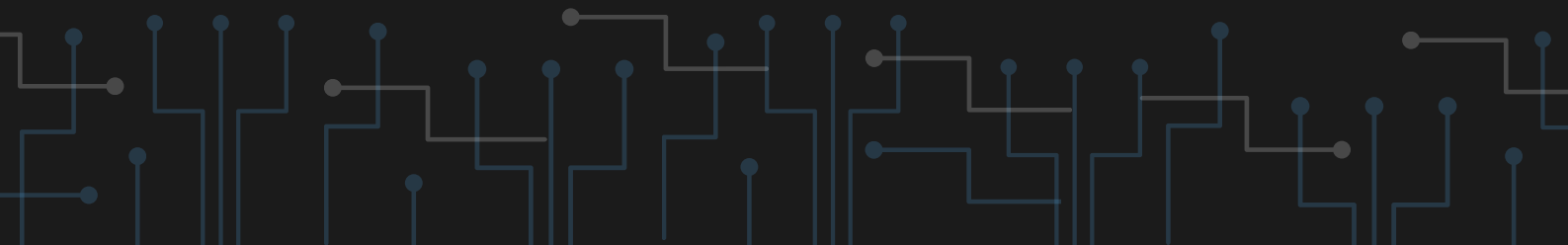




AWSGoat

[HTTPS://GITHUB.COM/INE-LABS/AWSGOAT](https://github.com/ine-labs/awsgoat)

AWSGoat is a deliberately vulnerable AWS infrastructure designed for educational purposes. It allows users to practice and refine their skills in identifying and exploiting vulnerabilities within a controlled AWS environment. This platform provides hands-on experience through various scenarios, each simulating real-world cloud security challenges. AWSGoat is an excellent tool for both beginners and experienced practitioners alike.

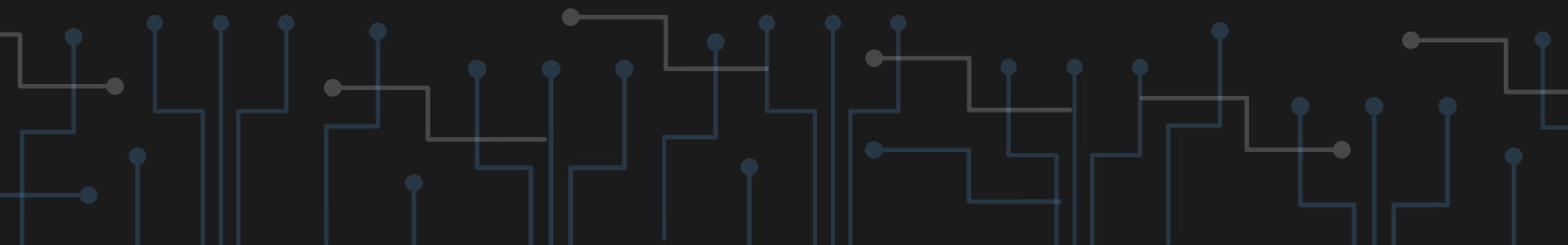




AzureGoat

[HTTPS://GITHUB.COM/INE-LABS/AZUREGOAT](https://github.com/INE-Labs/AzureGoat)

AzureGoat offers a deliberately unsecured Azure environment designed to facilitate learning and practicing cloud security techniques specific to Microsoft Azure. It provides numerous scenarios that mimic real-world security issues. This platform is ideal for cybersecurity enthusiasts to hone their skills in identifying and mitigating vulnerabilities specific to the Azure platform.





CI/CD Goat

***[HTTPS://GITHUB.COM/CIDER-SECURITY-RESEARCH/CICD-
GOAT](https://github.com/cider-security-research/cicd-goat)***

CI/CD Goat is a project by Cider Security that provides a deliberately vulnerable continuous integration and continuous delivery (CI/CD) environment. It is ideal for security practitioners to test and learn about CI/CD security. The platform offers 11 unique challenges, each focusing on specific CI/CD security threats, including dependency chain abuse and pipeline-based access control. The environment is containerized using Docker, making it easy to set up and run locally.





CloudGoat

[HTTPS://GITHUB.COM/RHINOSECURITYLABS/CLOUDGOAT](https://github.com/rhinosecuritylabs/cloudgoat)

CloudGoat is an AWS "Vulnerable by Design" tool developed by Rhino Security Labs. It offers various capture-the-flag-style scenarios, each focusing on different aspects of AWS security. CloudGoat enables users to deploy intentionally vulnerable AWS environments to practice exploitation techniques and gain a deeper understanding of common security pitfalls.

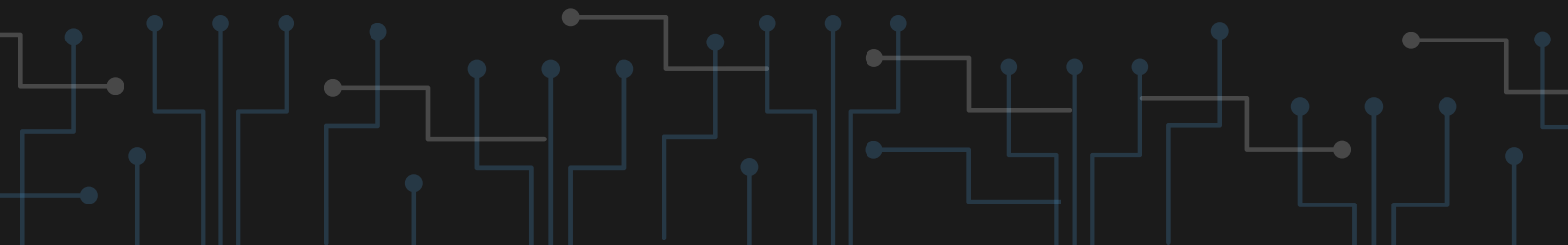




CloudLabsAD

[HTTPS://GITHUB.COM/CHVANCOOTEN/CLOUDLABSAD](https://github.com/chvancooten/cloudlabsad)

CloudLabsAD is an open-source platform designed for simulating Active Directory environments in the cloud. It enables cybersecurity professionals to configure and test AD setups and vulnerabilities within a cloud framework. CloudLabsAD is an excellent resource for those looking to understand and secure Active Directory configurations, offering realistic scenarios for both training and research purposes.

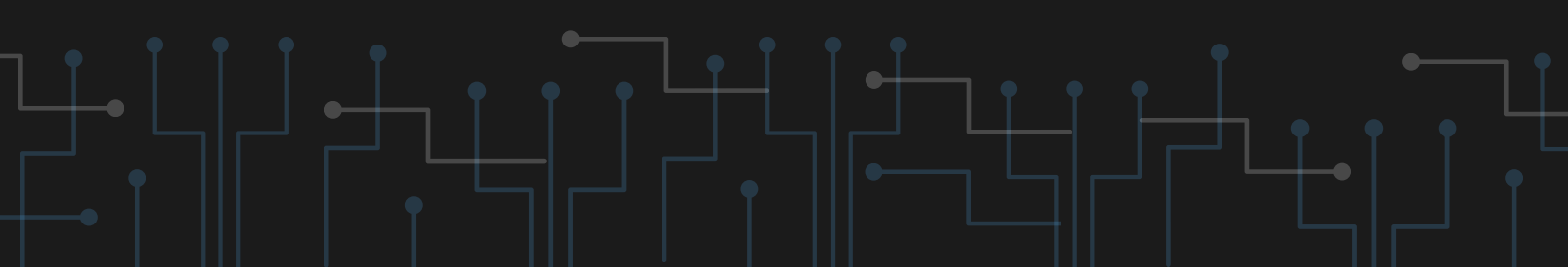




CodeWars

[HTTPS://WWW.CODEWARS.COM/](https://www.codewars.com/)

CodeWars is a dynamic programming platform where developers improve their skills through a series of coding challenges known as kata. With its community-driven approach, users can create, solve, and discuss a wide range of problems in various programming languages. The platform provides an engaging way to practice coding, enhance problem-solving abilities, and learn new techniques.

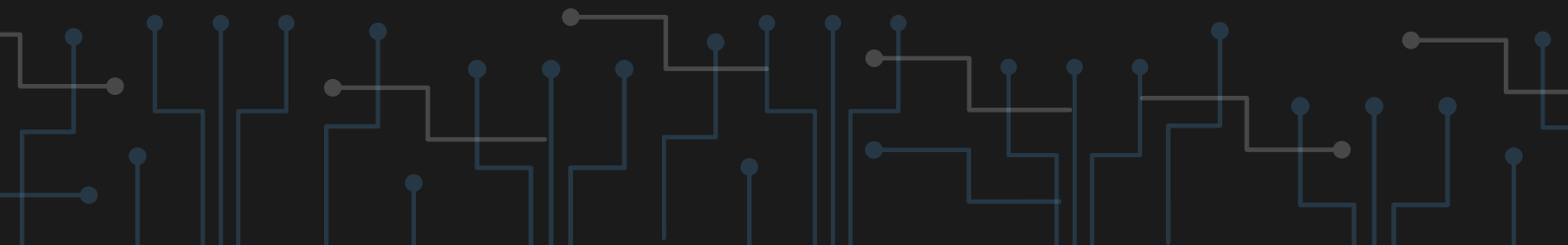




Crackmes

[HTTPS://CRACKMES.ONE/](https://crackmes.one/)

Crackmes is a specialized platform designed for reverse engineering enthusiasts. It features a collection of crackmes—small programs created to challenge users in the fields of reverse engineering and software cracking. These exercises vary in difficulty and offer a hands-on approach to learning how to analyze, understand, and manipulate software. By solving these challenges, users can refine their skills in debugging, disassembly, and binary analysis.

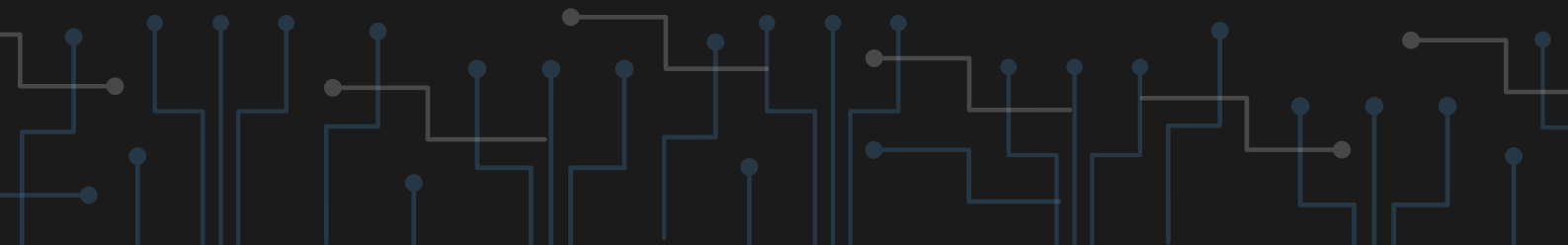




CryptoHack

[HTTPS://CRYPTOHACK.ORG/](https://cryptoHack.org/)

CryptoHack is an engaging platform that turns learning cryptography into a series of interactive puzzles and challenges. Designed for both beginners and advanced users, it covers fundamental topics such as symmetric and public-key cryptography, elliptic curves, and hashing functions. By solving these puzzles, users gain a deep understanding of cryptographic principles and practices.

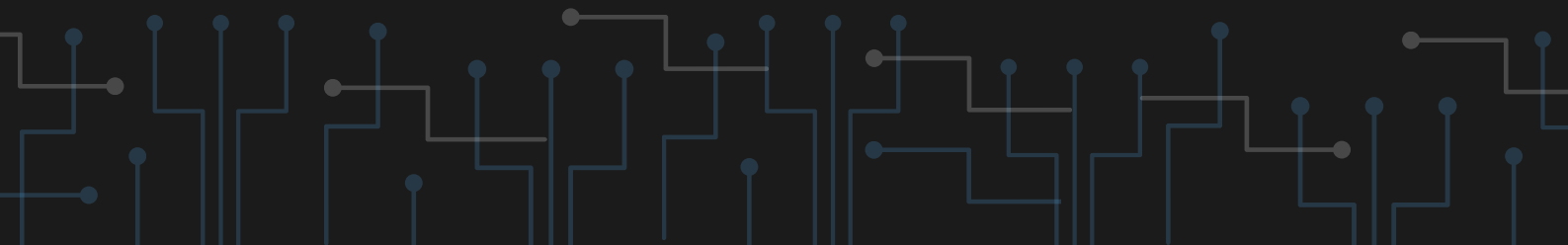




Cryptopals

[HTTPS://CRYPTOPALS.COM/](https://cryptopals.com/)

Cryptopals is a popular set of cryptographic challenges designed to educate and test individuals' skills in cryptography. It offers hands-on exercises ranging from beginner to advanced levels, covering foundational concepts such as block cipher modes, public-key cryptography, and padding oracle attacks. Each challenge is crafted to enhance problem-solving abilities and deepen the understanding of cryptographic principles.





CTFTime

[HTTPS://CTFTIME.ORG/](https://ctftime.org/)

CTFTime is the leading platform for Capture The Flag (CTF) competitions, aggregating information about CTF events worldwide. It is not a learning platform itself but serves as a central hub for cybersecurity enthusiasts to participate in, organize, and track CTF contests. Users can join teams, compete in various challenges, and improve their rankings on the global leaderboard. CTFTime supports a vibrant community, fostering collaboration and competition among cybersecurity professionals and hobbyists.





CyberDefenders

[HTTPS://CYBERDEFENDERS.ORG/](https://cyberdefenders.org/)

CyberDefenders is a training platform for "blue teams," focused on equipping SOC analysts and DFIR professionals with practical skills. It offers immersive labs, real-world scenarios, and certification programs such as Certified CyberDefender (CCD). The platform emphasizes defensive cybersecurity techniques, ranging from threat hunting to incident response, providing users with comprehensive preparation for mitigating and defending against cyber threats.

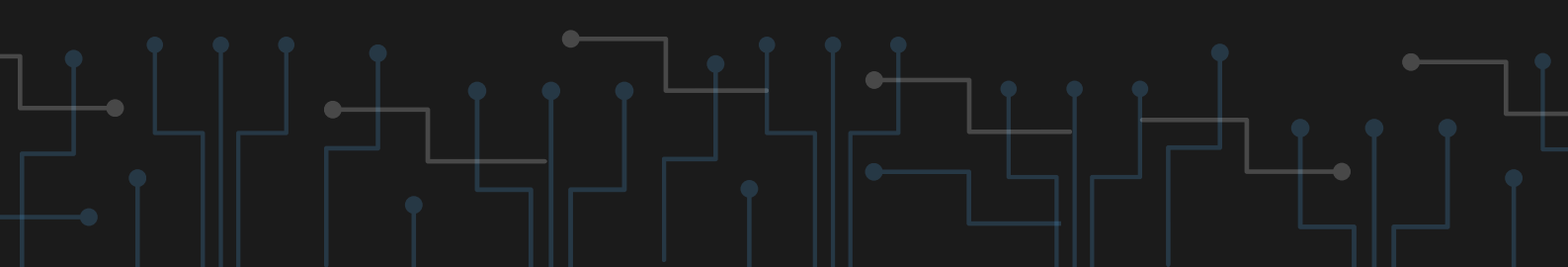




Damn Vulnerable Bank

[HTTPS://GITHUB.COM/REWANTHTAMMANA/DAMN-VULNERABLE-BANK/](https://github.com/rewanthtamma/Damn-Vulnerable-Bank/)

Damn Vulnerable Bank is a deliberately insecure Android application developed for educational purposes. It allows cybersecurity enthusiasts to practice and enhance their skills in identifying and exploiting vulnerabilities. Designed as a realistic banking app, it provides a hands-on approach to understanding various security flaws, such as insecure data storage, broken authentication, and cross-site scripting.

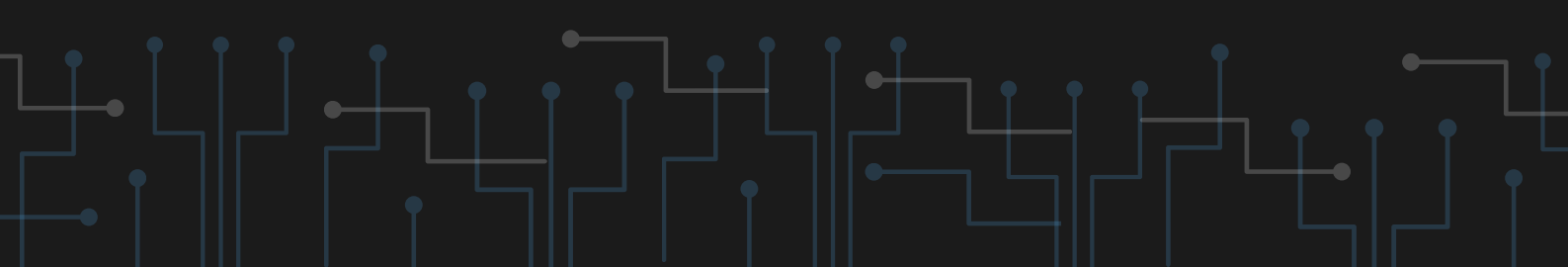




Damn Vulnerable C# Application (API)

[HTTPS://GITHUB.COM/APPSECGO/DVCSHARP-API](https://github.com/appsecgo/dvcsharp-api)

Damn Vulnerable C# Application (API) is a deliberately vulnerable ASP.NET Core web API designed to help security professionals and developers practice and improve their skills in identifying and mitigating common API vulnerabilities. The platform simulates a real-world environment, allowing users to explore issues such as SQL injection, insecure deserialization, and improper authentication mechanisms.

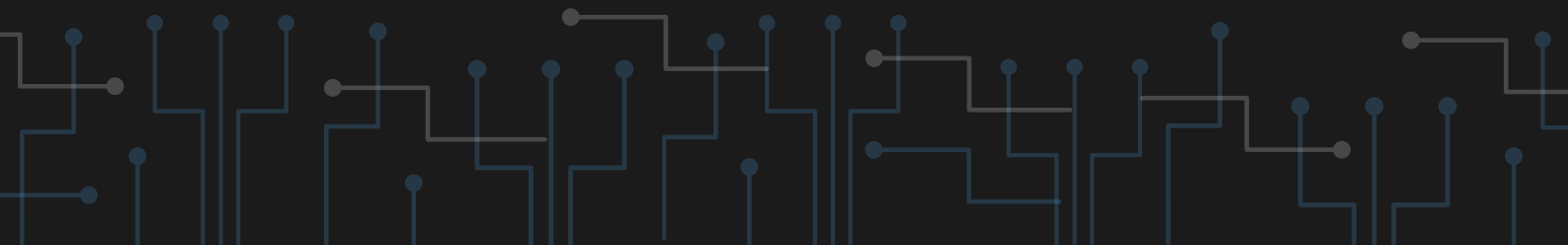




Damn Vulnerable Cloud Application

[HTTPS://GITHUB.COM/M6A-UDS/DVCA](https://github.com/m6a-uds/dvca)

Damn Vulnerable Cloud Application is a deliberately insecure cloud application designed to demonstrate and teach how to identify and exploit cloud-specific security issues, particularly in AWS environments. This project showcases common cloud vulnerabilities, such as privilege escalation and misconfigured services. It provides a realistic environment for security enthusiasts and professionals to enhance their cloud security skills.

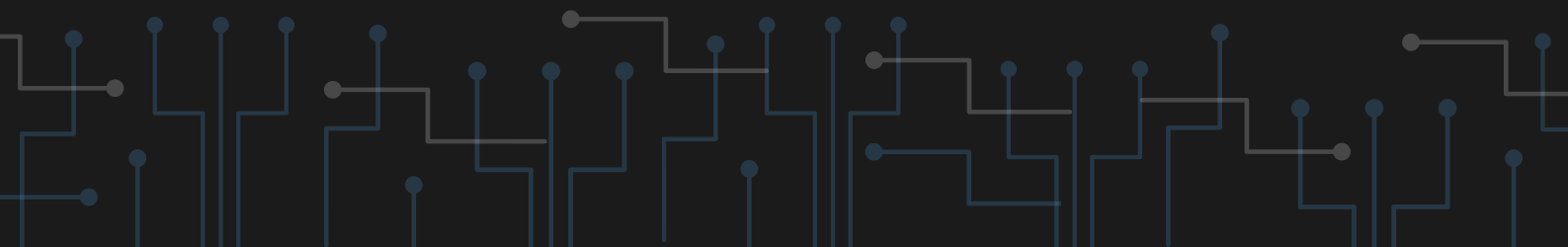




Damn Vulnerable DeFi

[HTTPS://WWW.DAMNVULNERABLEDEFI.XYZ/](https://www.damnulnerabledefi.xyz/)

Damn Vulnerable DeFi is a platform designed to teach the complexities of decentralized finance (DeFi) security through practical challenges. It offers a series of exercises that simulate real-world DeFi vulnerabilities, helping users understand and mitigate issues such as smart contract exploits, flash loan attacks, and reentrancy problems. The platform is aimed at developers, security researchers, and blockchain enthusiasts.

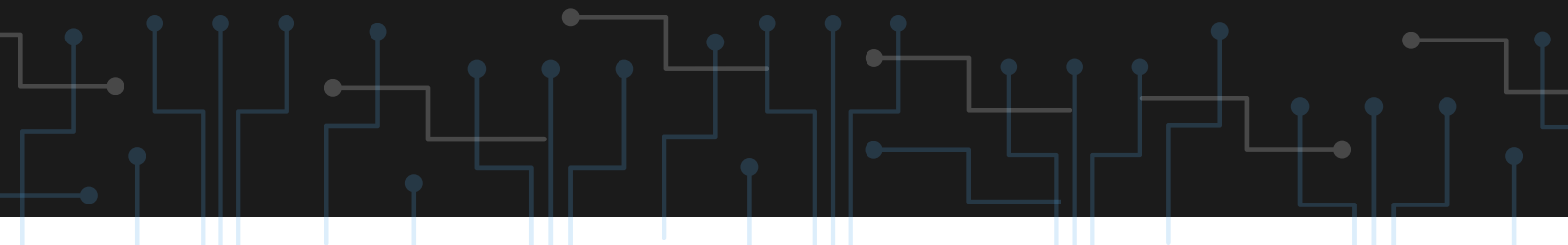




Damn Vulnerable Functions as a Service

[HTTPS://GITHUB.COM/WE45/DVFAAS-DAMN-VULNERABLE-FUNCTIONS-AS-A-SERVICE](https://github.com/we45/dvfaas-damn-vulnerable-functions-as-a-service)

Damn Vulnerable Functions as a Service (DVFAaaS) is an educational platform designed to help developers, DevOps engineers, and security professionals understand serverless vulnerabilities. Hosted on AWS Lambda, DVFAaaS features deliberately insecure serverless functions. The project aligns with the OWASP Serverless Top 10, making it ideal for those looking to deploy and learn through hands-on practice. The platform is primarily built in Python using the Chalice framework and utilizes Terraform for deployment.

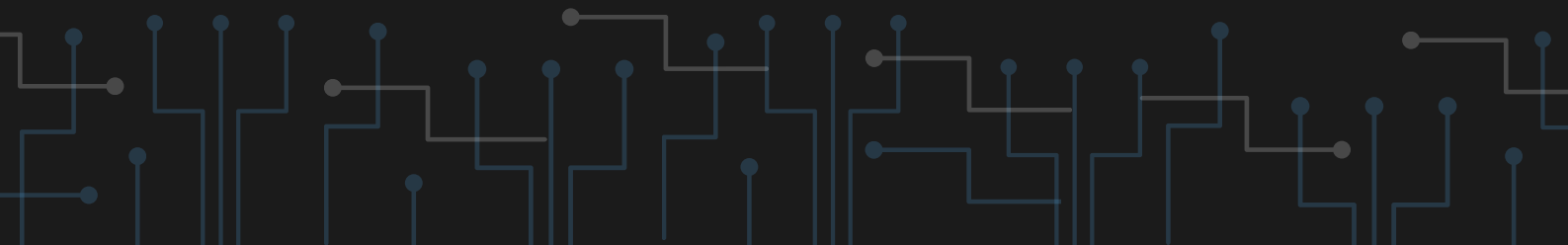




Damn Vulnerable Grade Management System

[HTTPS://GIT.LOGICALHACKING.COM/BROWSERSECURITY/DVGM](https://git.logicalhacking.com/browsersecurity/dvgm)

Damn Vulnerable Grade Management System (DVGM) is an open-source project designed to demonstrate common web security vulnerabilities in a simulated academic environment. It allows users to explore and exploit various vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

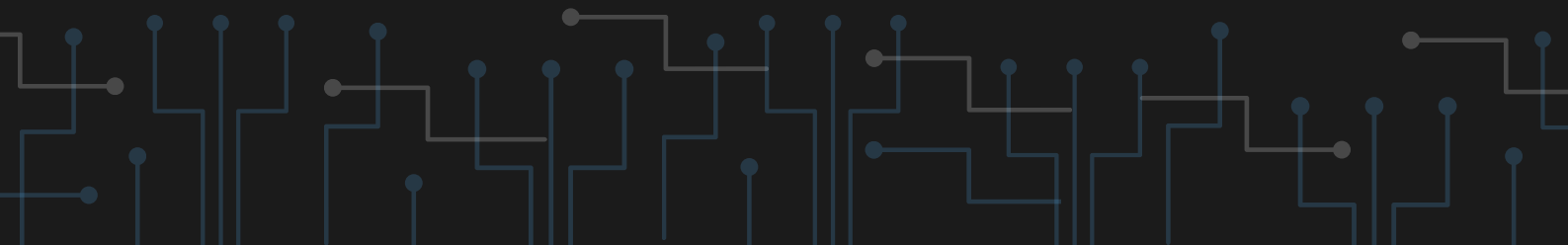




Damn Vulnerable GraphQL Application (DVGA)

[HTTPS://GITHUB.COM/DOLEVF/DAMN-VULNERABLE-GRAPHQL-APPLICATION](https://github.com/dolevf/damn-vulnerable-graphql-application)

Damn Vulnerable GraphQL Application (DVGA) provides a controlled environment for exploring and understanding security threats associated with GraphQL. It offers a series of intentionally flawed GraphQL configurations, allowing users to learn through hands-on practice by identifying and mitigating vulnerabilities such as query batching, information disclosure, and more.

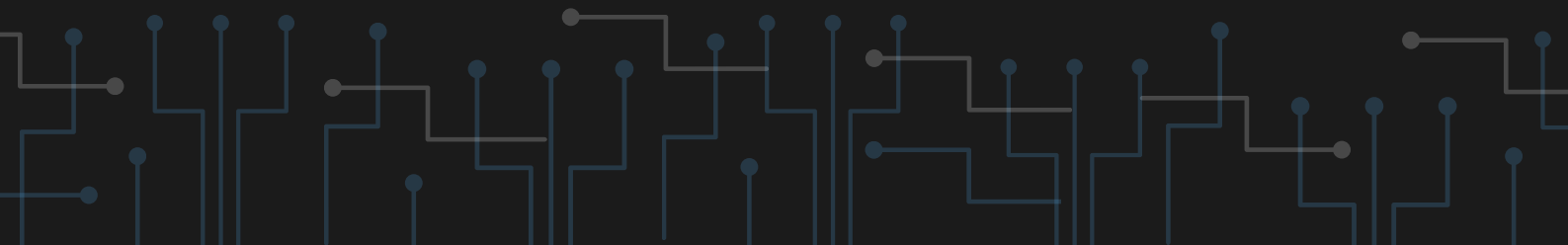




Damn Vulnerable Hybrid Mobile App (DVHMA)

[HTTPS://GITHUB.COM/LOGICALHACKING/DVHMA](https://github.com/logicalhacking/dvhma)

Damn Vulnerable Hybrid Mobile App (DVHMA) is a deliberately insecure Android application designed to help security professionals and developers understand common vulnerabilities in hybrid mobile applications. Built using Apache Cordova, DVHMA exposes issues such as injection flaws in the JavaScript-to-Java bridge, enabling hands-on practice in identifying and mitigating these security vulnerabilities.

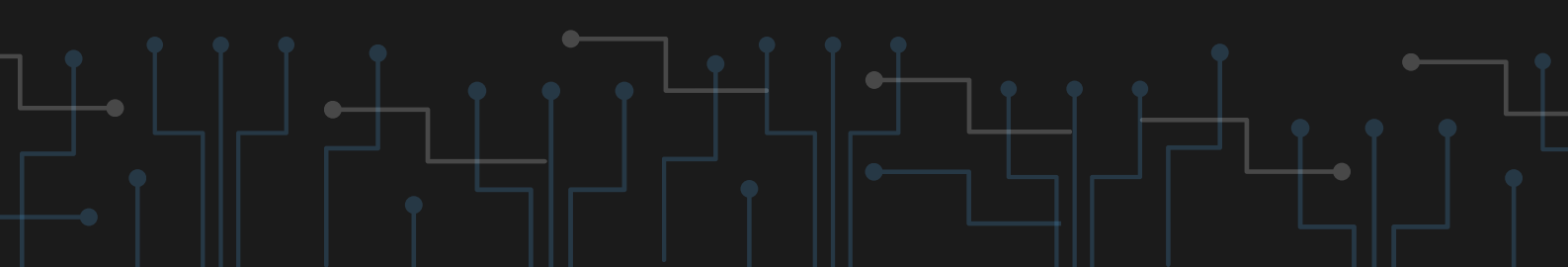





Damn Vulnerable iOS App (DVIA)

[HTTPS://GITHUB.COM/PRATEEK147/DVIA](https://github.com/prateek147/dvia)

Damn Vulnerable iOS App (DVIA) is an iOS application intentionally filled with security vulnerabilities. It is designed to help security enthusiasts and developers learn about iOS security by exploiting various vulnerabilities, including improper data storage, insufficient transport layer protection, and insecure communication.

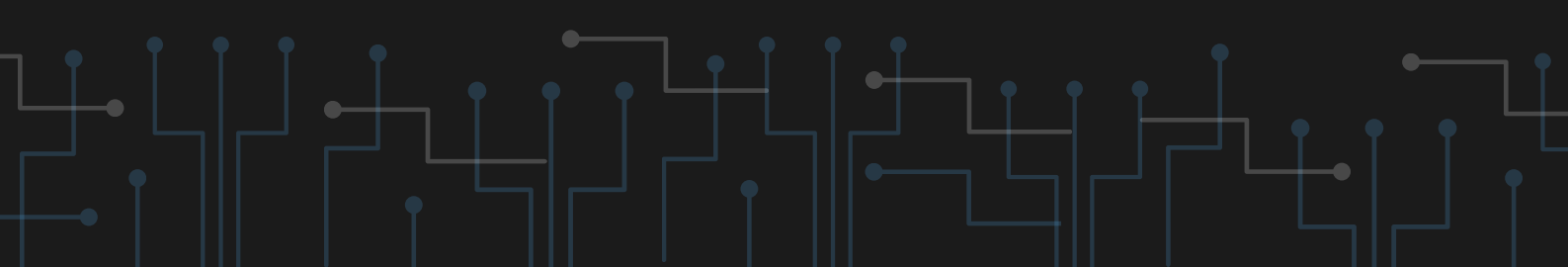




Damn Vulnerable iOS App v2 (DVIA-v2)

[HTTPS://GITHUB.COM/PRATEEK147/DVIA-V2](https://github.com/prateek147/dvia-v2)

Damn Vulnerable iOS App v2 (DVIA-v2) is an updated version of the original Damn Vulnerable iOS App. It introduces new challenges and security issues to explore, serving as an educational tool for advanced iOS security learning. DVIA-v2 provides real-world scenarios to test various security skills, covering topics such as insecure local storage, network vulnerabilities, and authentication flaws.





Damn Vulnerable IoT Device (DVID)

[HTTPS://GITHUB.COM/VULCAINREO/DVID](https://github.com/Vulcainreo/DVID)

Damn Vulnerable IoT Device (DVID) is a deliberately insecure IoT device platform designed to help researchers, developers, and security professionals understand common vulnerabilities in IoT devices. This platform provides hands-on exposure to typical IoT security issues, such as insecure communication, weak authentication mechanisms, and inadequate firmware validation.

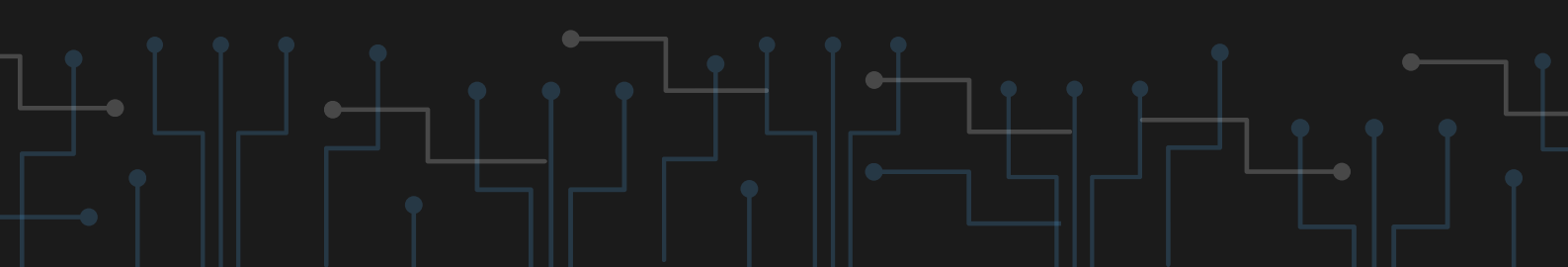




Damn Vulnerable Java (EE) Application (DVJA)

[HTTPS://GITHUB.COM/APPSECCO/DVJA](https://github.com/appsecco/dvja)

Damn Vulnerable Java (EE) Application (DVJA) is a deliberately insecure Java Enterprise Edition web application designed for training and testing in security. Hosted on GitHub, DVJA is an excellent resource for developers and security professionals looking to practice identifying and mitigating vulnerabilities in a real-world Java environment. The application includes common security flaws, providing hands-on experience in exploiting and securing Java applications.

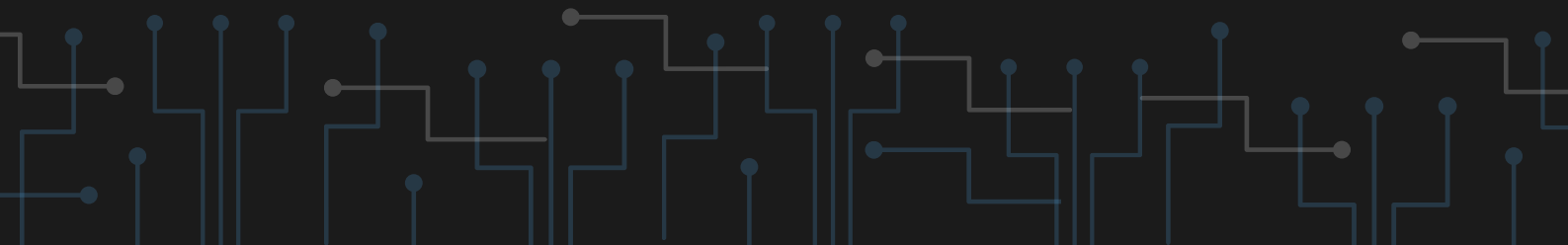




Damn Vulnerable NodeJS Application (DVNA)

[HTTPS://GITHUB.COM/APPSECCO/DVNA](https://github.com/appsecco/dvna)

Damn Vulnerable NodeJS Application (DVNA) provides a platform for learning and testing security vulnerabilities specific to Node.js applications. Available on GitHub, DVNA is designed to help developers and security enthusiasts practice their skills in identifying and fixing security flaws in a Node.js environment. The application includes various deliberately introduced vulnerabilities, offering a hands-on approach to Node.js security.

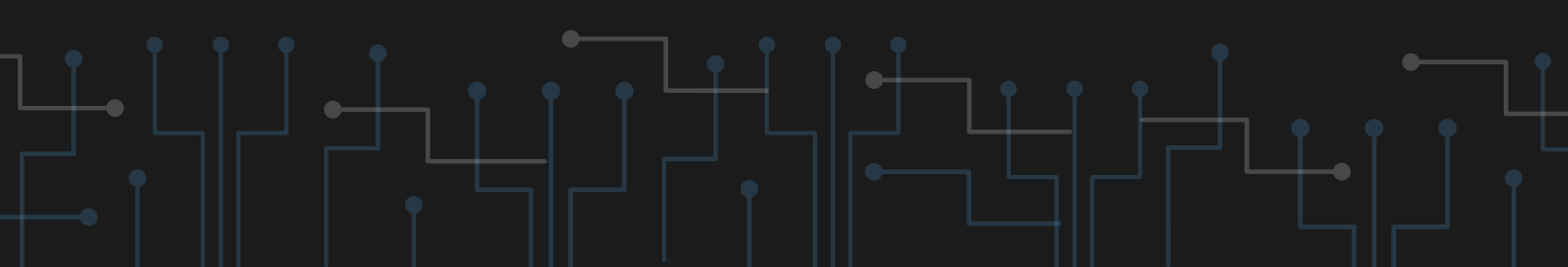




Damn Vulnerable Python Web App (DVPWA)

[HTTPS://GITHUB.COM/ANXOLERD/DVPWA](https://github.com/ANXOLERD/DVPWA)

Damn Vulnerable Python Web App (DVPWA)
is a deliberately vulnerable Python web
application designed for teaching and
testing web application security.

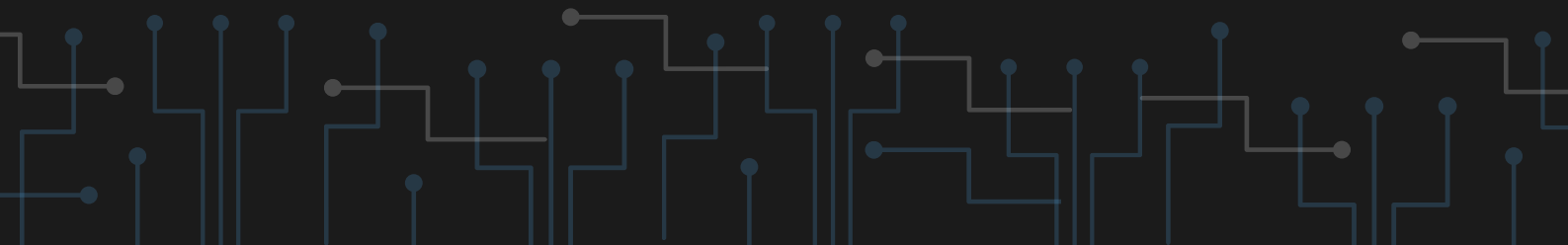




Damn Vulnerable Rails Application (DVRA)

[HTTPS://GITHUB.COM/GUILLEIGUARAN/DVRA](https://github.com/GuilleGuaran/DVRA)

Damn Vulnerable Rails Application (DVRA) is a deliberately insecure Ruby on Rails web application designed for educational purposes. Hosted on GitHub, DVRA serves as a practical tool for developers and security experts to practice identifying and mitigating vulnerabilities in a Rails environment. The application includes several common security flaws, providing hands-on experience in exploiting and securing Rails applications.





Damn Vulnerable Restaurant

[HTTPS://GITHUB.COM/THEOWNI/DAMN-VULNERABLE-RESTAURANT-API-GAME](https://github.com/TheOWNI/damn-vulnerable-restaurant-api-game)

Damn Vulnerable Restaurant is a deliberately insecure Web API game designed for developers, ethical hackers, and security engineers to practice identifying and exploiting vulnerabilities. Built using the Python FastAPI framework, it offers a training environment that can be easily extended with new endpoints and security flaws. It is an ideal platform for learning and improving API security skills.

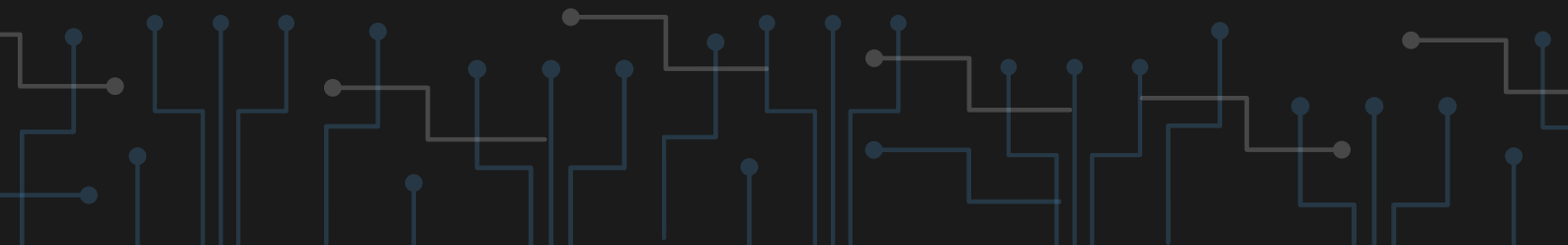




Damn Vulnerable Router Firmware (DVRF)

[HTTPS://GITHUB.COM/PRAETORIAN-INC/DVRF](https://github.com/praetorian-inc/dvrf)

The Damn Vulnerable Router Firmware (DVRF) project is a hands-on educational tool designed to teach users about hardware security and processor architectures beyond the x86_64 space. Tailored for the Linksys E1550 device and compatible with QEMU for emulation, DVRF provides real-world scenarios for practicing vulnerability detection and exploitation in a controlled environment. It includes access to source code and detailed guides, making it an invaluable resource for learning.

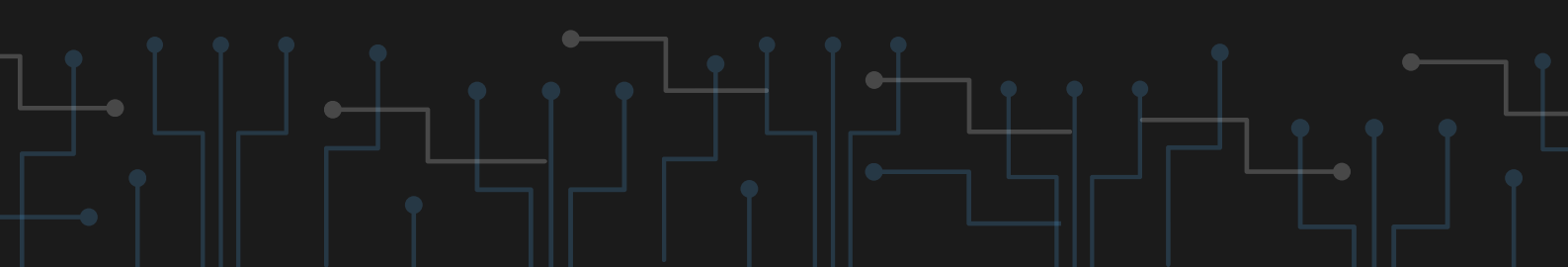




Damn Vulnerable Serverless Application (DVSA)

[HTTPS://GITHUB.COM/OWASP/DVSA](https://github.com/OWASP/DVSA)

Damn Vulnerable Serverless Application (DVSA) is an OWASP project designed to help security professionals and developers understand common security issues in serverless applications. The platform simulates a serverless environment with intentionally insecure configurations and vulnerabilities. It allows users to practice and learn how to identify, exploit, and mitigate these issues effectively.

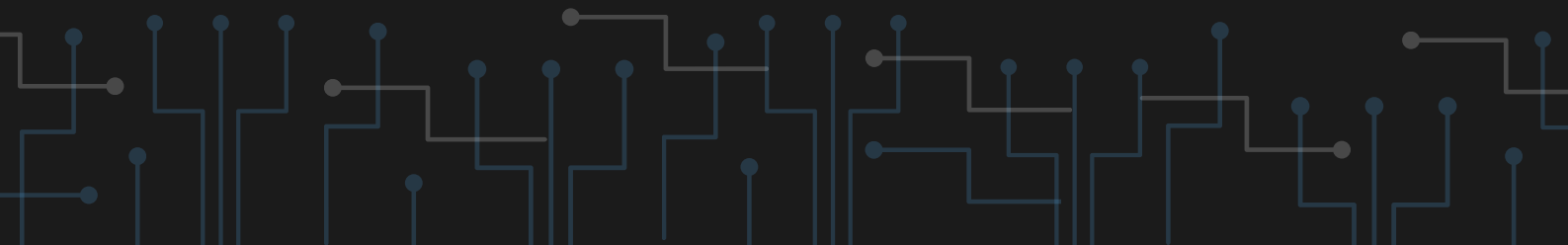




Damn Vulnerable Thick Client App

[HTTPS://GITHUB.COM/SRINIOX00/DVTA](https://github.com/srinioX00/DVTA)


Damn Vulnerable Thick Client App is a C# .NET-based application designed to help security enthusiasts and professionals practice and understand vulnerabilities specific to thick client applications. The project includes various intentionally introduced security flaws, allowing users to explore common issues such as insecure storage, improper data handling, and weak authentication mechanisms.



Damn Vulnerable Web Application (DVWA)

[HTTPS://GITHUB.COM/DIGININJA/DVWA](https://github.com/digininja/dvwa)

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application designed to help security professionals and developers learn about web application security. DVWA includes a range of vulnerabilities, from SQL Injection to Cross-Site Scripting, allowing users to practice exploiting these issues in a safe environment. With multiple security levels, DVWA helps users understand how different security mechanisms impact an application's susceptibility to attacks.



Damn Vulnerable Web Services

[HTTPS://GITHUB.COM/SNOOPYSECURITY/DVWS-NODE](https://github.com/snoopyscurity/dvws-node)

Damn Vulnerable Web Services is a deliberately insecure web application and API designed for training and educational purposes in web services security. The platform allows users to explore a wide range of vulnerabilities, such as SQL Injection, Cross-Site Scripting (XSS), and Server-Side Request Forgery (SSRF). It serves as a valuable resource for developers and security enthusiasts to practice identifying and mitigating web service vulnerabilities.

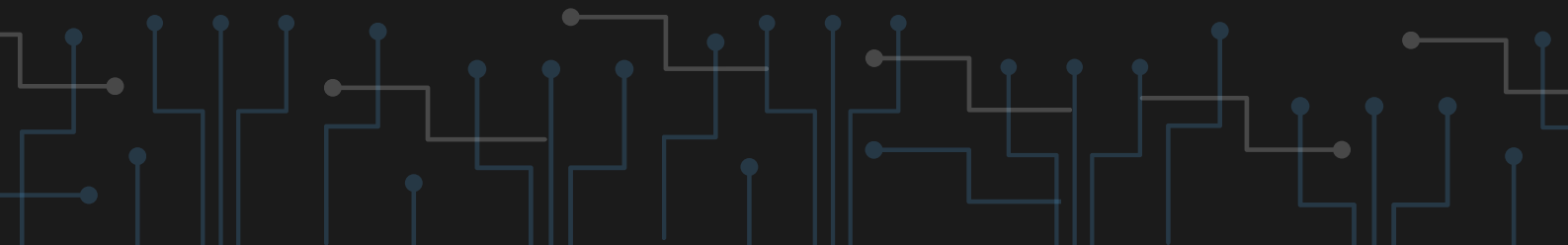




Damn Vulnerable WordPress Site (DVWPS)

[HTTPS://GITHUB.COM/VIANASW/DVWPS](https://github.com/vianasw/dvwps)

Damn Vulnerable WordPress Site (DVWPS) is a deliberately vulnerable WordPress setup created for security training purposes. It includes multiple exploitable vulnerabilities, allowing users to practice and enhance their skills in identifying and mitigating common WordPress security issues.

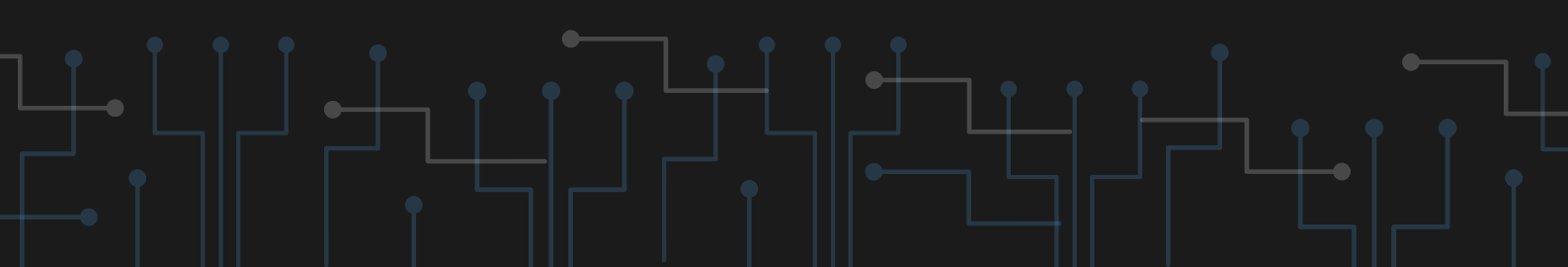




Ethernaut

[HTTPS://ETHERNAUT.OPENZEPPELIN.COM/](https://ethernaut.openzeppelin.com/)

Ethernaut is an interactive wargame developed by OpenZeppelin, specifically designed to teach Ethereum smart contract security. Players progress through various levels, each representing a different vulnerability in smart contracts. By solving these challenges, users gain hands-on experience in identifying, exploiting, and fixing vulnerabilities in smart contracts.

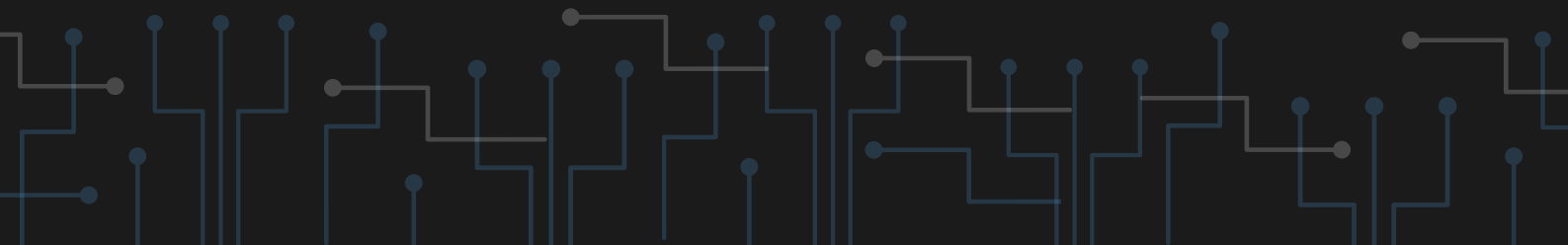




Expose Lab

[HTTPS://GITHUB.COM/ASHIFCODER/EXPOSELAB](https://github.com/ashifcoder/exposelab)

Expose Lab is an educational platform offering a collection of web application and Active Directory vulnerabilities for learning purposes. It includes various scenarios that simulate real-world security threats, allowing users to practice and enhance their skills in vulnerability assessment and penetration testing. The platform also features a mini CTF, providing an engaging environment for hands-on learning and skill development.



Game Of AD (GOAD)

[HTTPS://GITHUB.COM/ORANGE-CYBERDEFENSE/GOAD](https://github.com/Orange-Cyberdefense/GOAD)

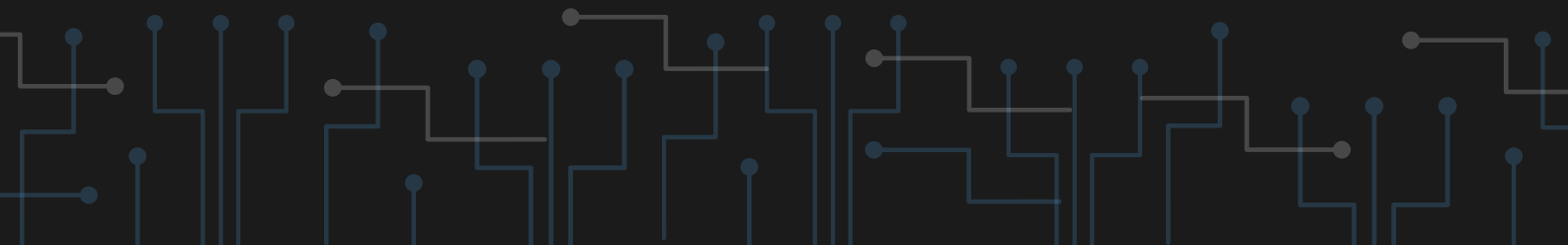
Game Of Active Directory (GOAD) is a comprehensive, hands-on lab designed for cybersecurity enthusiasts and professionals to master Active Directory (AD) security. Developed by Orange Cyberdefense, the platform simulates a real-world AD environment, enabling users to learn various attack and defense techniques through practical exercises. The lab setup includes common AD components and vulnerabilities, providing an immersive environment for skill development.



Google CTF

[HTTPS://CAPTURETHEFLAG.WITHGOOGLE.COM/](https://capturetheflag.withgoogle.com/)

Google CTF is an annual Capture The Flag competition organized by Google, aimed at security researchers, students, and enthusiasts. The event features a variety of challenges, ranging from beginner to expert levels, covering topics such as cryptography, binary exploitation, network security, and reverse engineering. Participants can compete in both online qualifying rounds and an on-site final event.

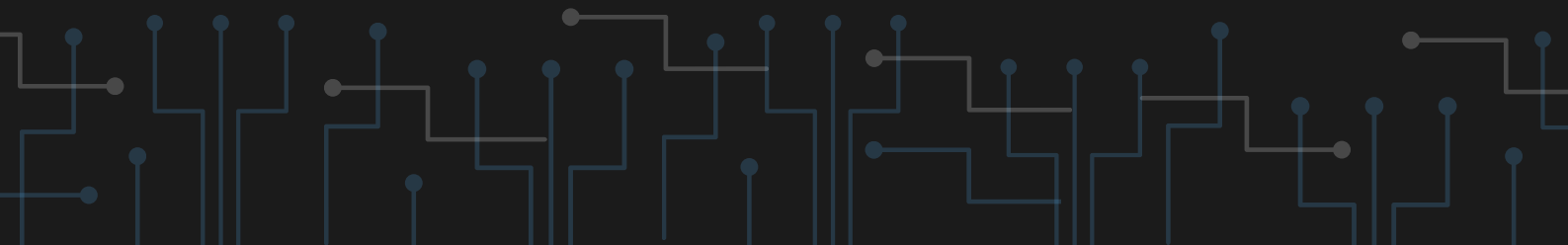




HackMyVM

[HTTPS://HACKMYVM.EU/](https://hackmyvm.eu/)

HackMyVM is a community-driven platform offering a diverse collection of virtual machines (VMs) tailored for cybersecurity practice. Each virtual machine presents unique challenges and vulnerabilities, allowing users to practice penetration testing, vulnerability assessment, and ethical hacking in a controlled environment. It provides a rich repository of scenarios that help sharpen practical skills and stay up-to-date with the latest security threats.

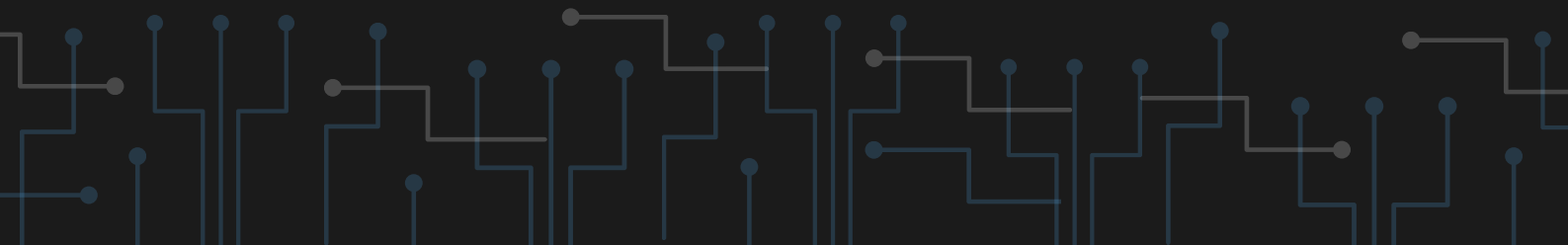




HackTheBox

[HTTPS://ACADEMY.HACKTHEBOX.COM/](https://academy.hackthebox.com/)

HackTheBox Academy is an advanced online educational platform offering structured cybersecurity training through interactive courses and hands-on labs. Designed for all skill levels, from beginners to experienced professionals, it covers topics such as penetration testing, defensive security, and specialized attack techniques. The academy provides real-world scenarios, browser-based pentesting labs, and certifications to help users develop and validate their cybersecurity skills.

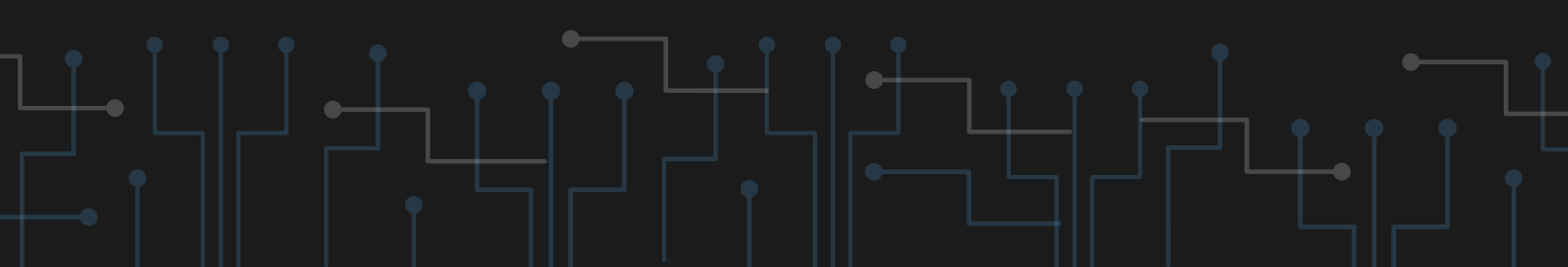




Hands-on Azure Security Labs

[HTTPS://GITHUB.COM/DAVISANC/AZURESECURITYLABS](https://github.com/davisanc/azuresecuritylabs)

Hands-on Azure Security Labs, available on GitHub, offer a comprehensive series of practical labs designed to enhance understanding of Azure IaaS security. These labs cover essential security topics, such as Network Security Groups (NSG), Azure Networking logs, firewall management, application security with WAF, storage security through encryption, and secure VPN access. The labs are ideal for both beginners and advanced users, providing hands-on experience with real-world Azure security scenarios.





IAM Vulnerable

[HTTPS://GITHUB.COM/BISHOPFOX/IAM-VULNERABLE](https://github.com/BishopFox/IAM-Vulnerable)

IAM Vulnerable is a deliberately insecure AWS Identity and Access Management (IAM) environment designed by BishopFox. This project is ideal for security professionals looking to test their skills in identifying and exploiting common IAM misconfigurations. It includes various scenarios that reflect real-world vulnerabilities, helping users understand the importance of secure IAM policies and best practices.

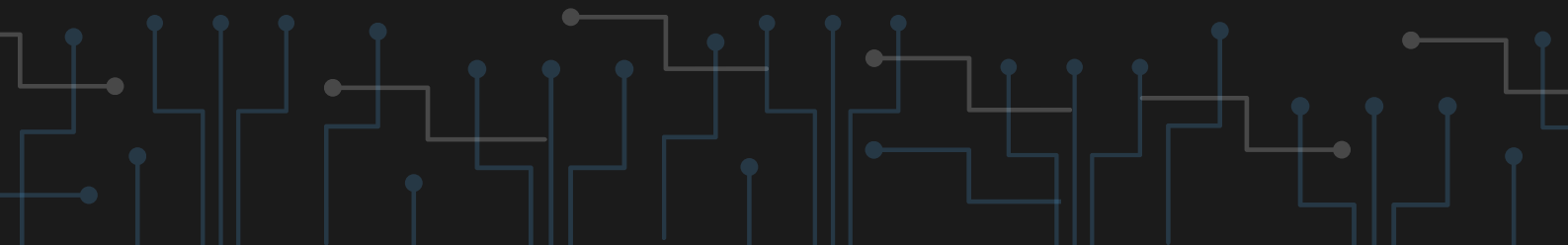




ICS Security Labs

[HTTPS://GITHUB.COM/ICSSECURITYLABS/ICSSECURITYLABS](https://github.com/ICSSECURITYLABS/ICSSECURITYLABS)

ICS Security Labs is a repository dedicated to the security of Industrial Control Systems (ICS). This project includes various lab exercises aimed at teaching the fundamentals of ICS security. It covers topics such as threat modeling, vulnerability assessment, and incident response. The labs feature different ICS protocols and provide hands-on insights into securing critical infrastructure.





LetsDefend

[HTTPS://WWW.LETSDEFEND.IO/](https://www.letsdefend.io/)

LetsDefend offers a comprehensive training environment designed for blue team professionals. The platform simulates real-world cyber defense scenarios, enabling users to enhance their skills in incident response, threat hunting, and security operations. Through an interactive dashboard, users can investigate security incidents, analyze threat data, and work on realistic cases that closely mimic real-world cybersecurity challenges.

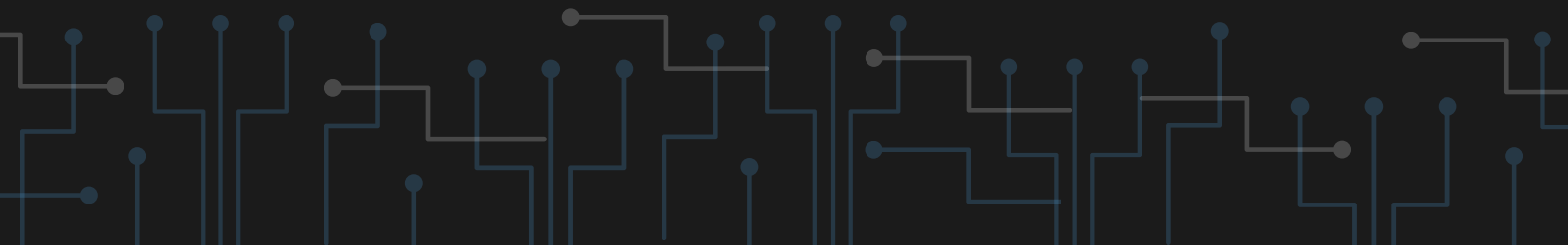




MemLabs

[HTTPS://GITHUB.COM/STUXNET999/MEMLABS](https://github.com/stuxnet999/memlabs)

MemLabs is an educational resource offering Capture-The-Flag (CTF)-style labs focused on memory forensics. MemLabs provides various challenges that simulate real-world memory analysis scenarios. These labs help users develop skills in detecting and analyzing malicious activities within memory dumps, making it an essential tool for anyone looking to specialize in digital forensics and incident response.

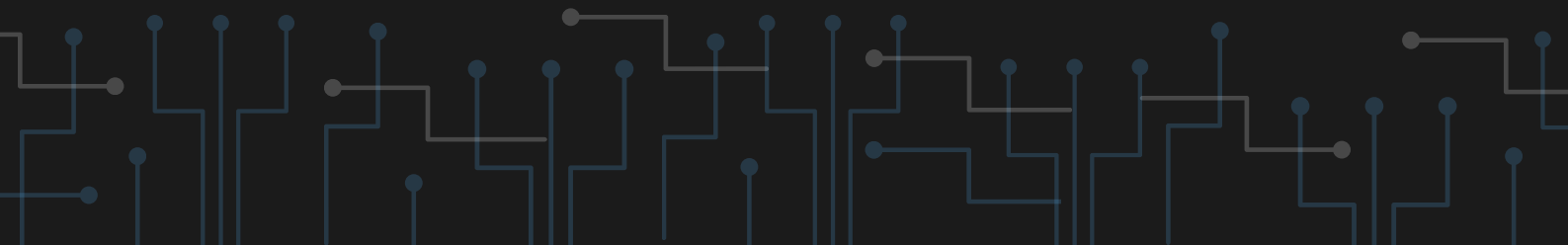




Offensive Security Labs

[HTTPS://WWW.OFFSEC.COM/LABS/](https://www.offsec.com/labs/)

Offensive Security Labs provide a cutting-edge training ground for cybersecurity professionals, focusing on offensive techniques. These labs offer access to diverse environments that simulate real-world networks and applications, allowing users to practice and refine their penetration testing and red teaming skills. With varying levels of difficulty and continuously updated lab environments, they provide an immersive and dynamic learning experience.

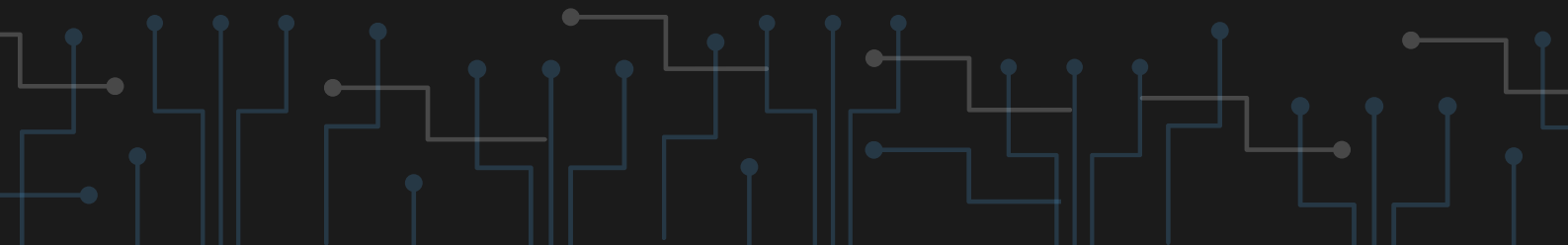




OverTheWire

[HTTPS://OVERTHEWIRE.ORG/WARGAMES/](https://overthewire.org/wargames/)

OverTheWire offers a series of interactive cybersecurity wargames aimed at helping users develop and improve their security skills. Each game, such as Bandit, Natas, and Leviathan, presents unique challenges focusing on different aspects of security. Players can test their proficiency in Linux command-line usage, network vulnerabilities, and cryptography concepts. The games are accessed via SSH, allowing participants to practice in a realistic, hands-on environment. OverTheWire is ideal for both beginners and advanced users, providing a progressive and engaging learning experience.

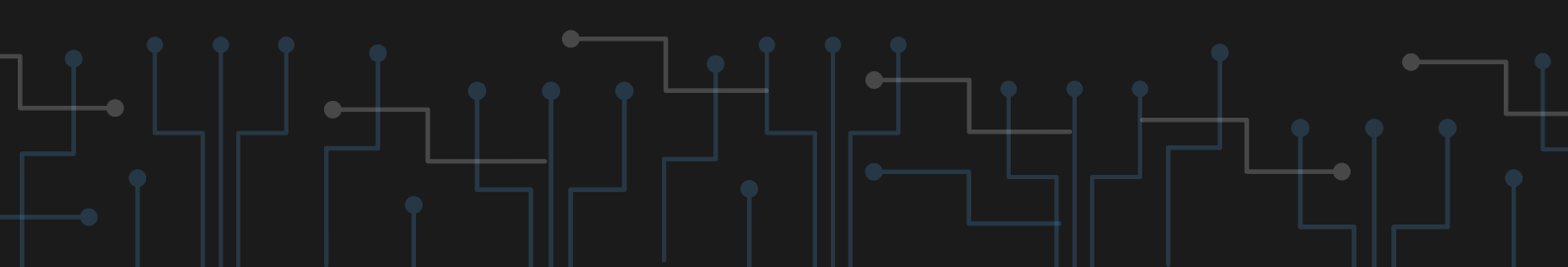




OWASP crAPI

[HTTPS://GITHUB.COM/OWASP/CRAPI](https://github.com/OWASP/crAPI)

OWASP crAPI (Completely Ridiculous API) is a deliberately vulnerable API designed for training purposes in API security. It provides a realistic environment where developers and security professionals can learn about API security issues and test their skills. crAPI includes various intentionally introduced vulnerabilities, offering hands-on experience in identifying and mitigating API-related threats.

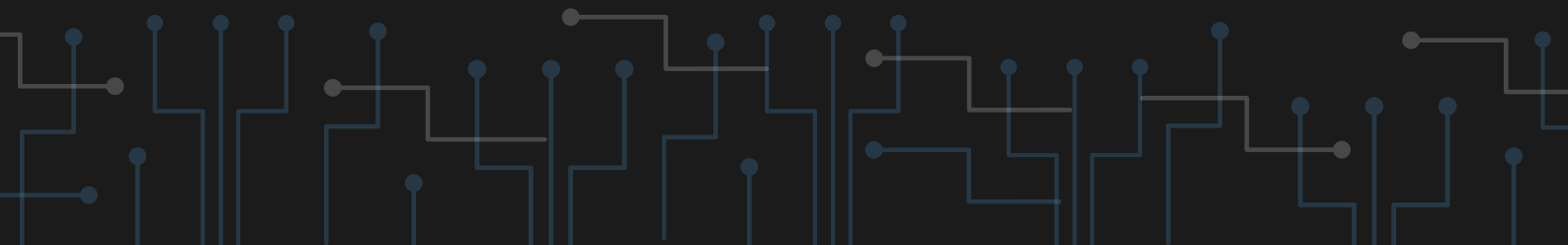




OWASP Juice Shop

[HTTPS://GITHUB.COM/JUICE-SHOP/JUICE-SHOP](https://github.com/juice-shop/juice-shop)

OWASP Juice Shop is a deliberately insecure web application developed for educational purposes in web security. It simulates a modern e-commerce platform with numerous vulnerabilities, providing a hands-on learning environment for web security enthusiasts. Users can practice exploiting common web application weaknesses such as XSS, SQL Injection, and CSRF. Juice Shop is ideal for those seeking practical experience in web security and also includes a mini CTF platform to enhance engagement and learning.

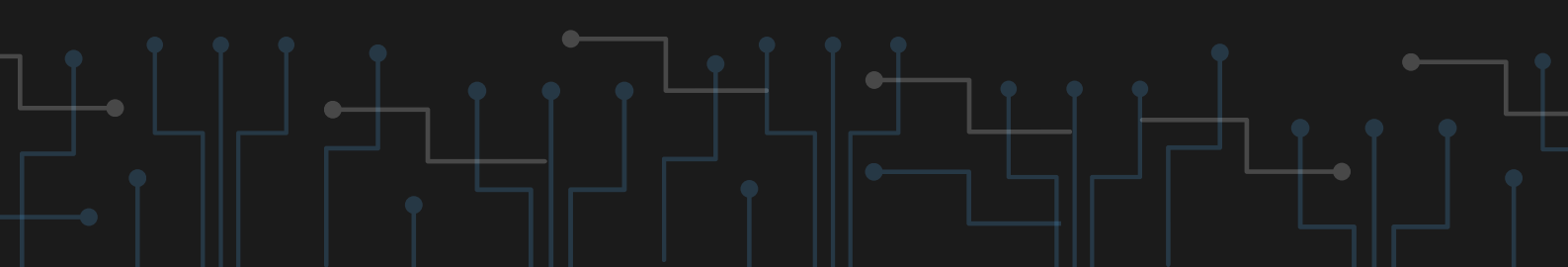




OWASP Mutillidae II

[HTTPS://GITHUB.COM/WEBPWNIZED/MUTILLIDAE](https://github.com/webpwnized/mutillidae)

OWASP Mutillidae II is an open-source, deliberately vulnerable web application designed for educational purposes. It covers a wide range of security issues, including the OWASP Top Ten vulnerabilities. Mutillidae II provides a robust platform for learning and testing web security skills, allowing users to practice exploiting and mitigating vulnerabilities in a controlled environment.

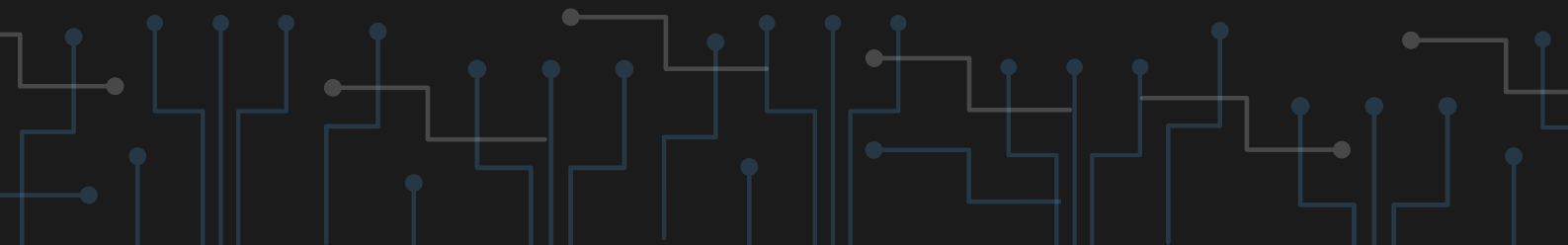




OWASP NodeGoat

[HTTPS://GITHUB.COM/OWASP/NODEGOAT](https://github.com/OWASP/NodeGoat)

OWASP NodeGoat is an educational tool designed to help developers understand and mitigate the OWASP Top 10 security risks in Node.js applications. It offers a hands-on environment where users can explore real-world vulnerabilities and learn best practices for securing web applications. By engaging with NodeGoat, developers gain valuable insights into common security flaws and effective methods for addressing them.

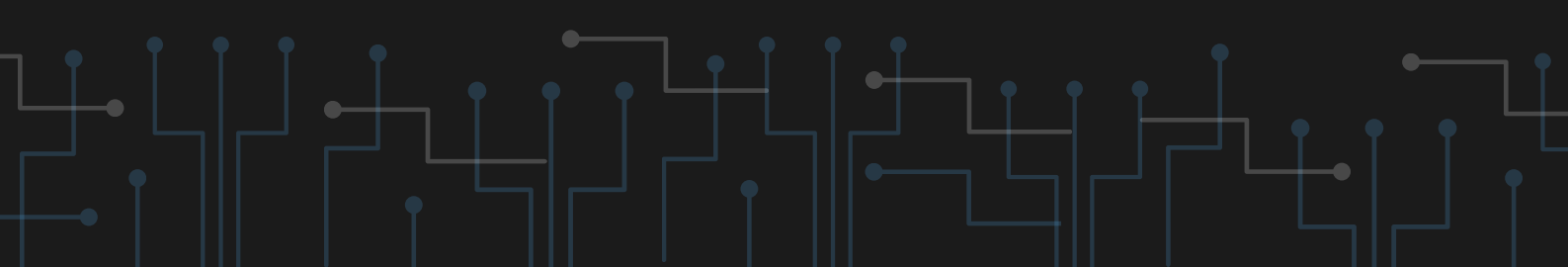




PicoCTF

[HTTPS://PICOCTF.ORG/](https://picoctf.org/)

PicoCTF is a renowned cybersecurity platform developed by Carnegie Mellon University, primarily targeted at high school students. It provides an engaging, gamified environment where participants solve challenges to learn fundamental cybersecurity concepts and skills.





PortSwigger Web Security Academy

[HTTPS://PORTSWIGGER.NET/WEB-SECURITY](https://portswigger.net/web-security)

PortSwigger Web Security Academy offers free, high-quality online labs for anyone interested in web application security. The academy features interactive labs and detailed tutorials covering various aspects of web security, from basic vulnerabilities to advanced exploitation techniques. This resource is ideal for security professionals and developers looking to deepen their understanding of web security. The labs primarily focus on using Burp Suite and prepare users for the Burp Suite Certified Practitioner (BSCP) exam.

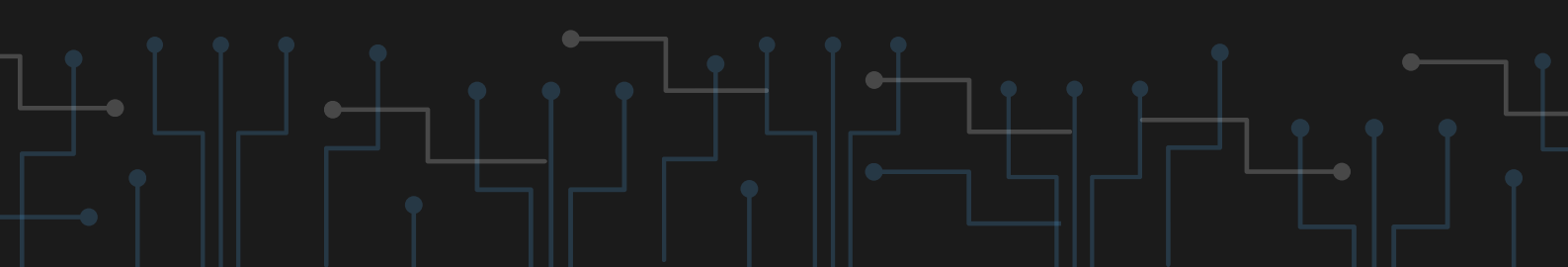




PWNable.kr

[HTTPS://PWNABLE.KR/](https://pwnable.kr/)

PWNable.kr is an engaging platform dedicated to binary exploitation challenges. Designed for cybersecurity enthusiasts, it offers a range of levels from beginner to advanced, allowing users to sharpen their skills in reverse engineering, binary exploitation, and debugging. Each challenge simulates real-world security vulnerabilities, providing a practical environment to apply theoretical knowledge. PWNable.kr fosters a deeper understanding of system security and the complexities of binary code manipulation.

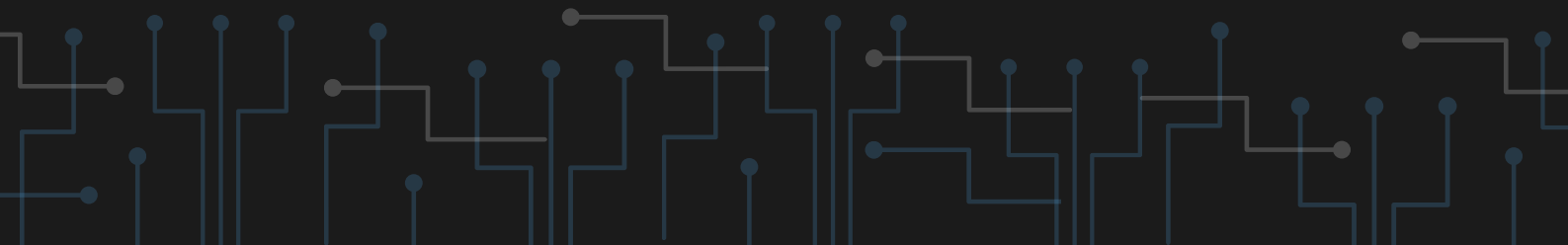




PurpleCloud

[HTTPS://GITHUB.COM/IKNOWJASON/PURPLECLOUD](https://github.com/iknowjason/purplecloud)

PurpleCloud is a versatile tool that creates small Active Directory domains on the Azure platform, configured for hybrid cyber range and identity simulations. It is invaluable for security professionals and educators who require a hands-on environment to explore Azure Active Directory configurations, implement security measures, and simulate attacks. The automated lab deployment provided by PurpleCloud facilitates practical learning and experimentation, making it an essential resource for developing real-world security skills.

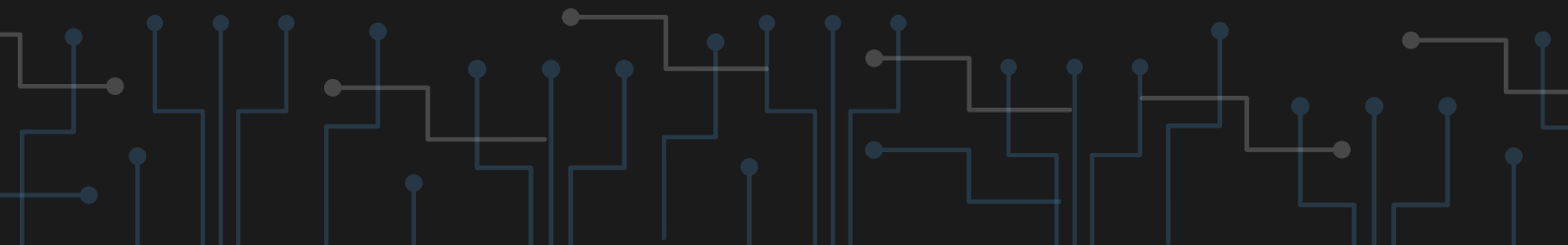




PWNED Labs

[HTTPS://PWNEDLABS.IO/](https://pwnedlabs.io/)

PWNED Labs is a comprehensive cybersecurity training platform offering a wide range of hands-on labs and challenges. It is designed for all skill levels, from beginners to seasoned professionals, covering various aspects of cybersecurity, including penetration testing, reverse engineering, and exploit development. With real-world scenarios and up-to-date content, PWNED Labs equips users with the skills and knowledge needed to stay ahead in the rapidly evolving field of cybersecurity.

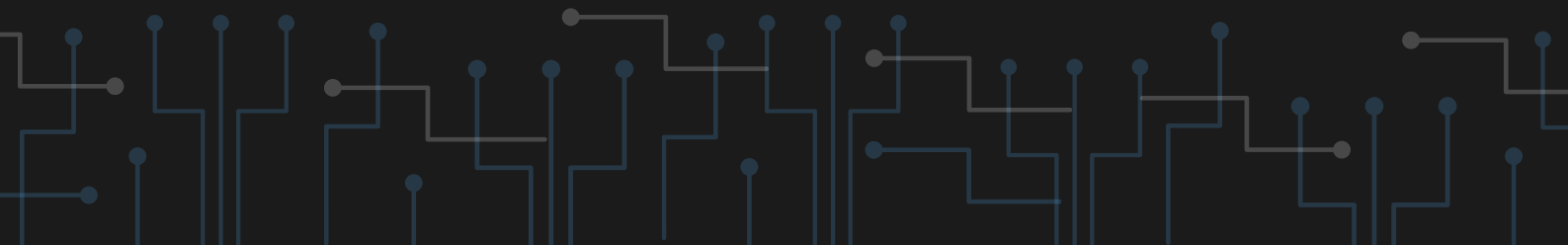




RE Challenges

[HTTPS://CHALLENGES.RE/](https://challenges.re/)

RE Challenges is a professionally curated website focused on reverse engineering exercises. Created by Dennis Yurichev, it draws inspiration from Project Euler and other renowned platforms. The site offers numerous tasks categorized by difficulty, encouraging users to analyze and understand complex code structures. With a wide range of challenges, from simple to advanced, RE Challenges provides an excellent resource for honing reverse engineering skills.

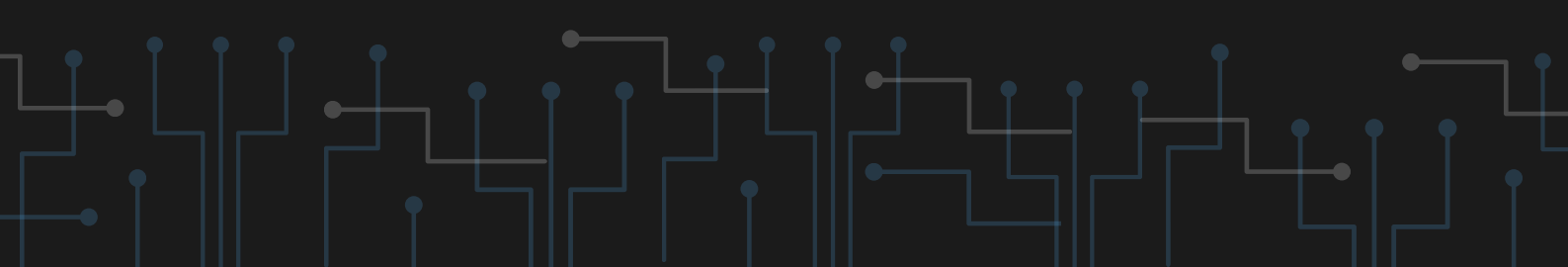




RHme Challenges 2015

[HTTPS://GITHUB.COM/RISCURE/RHME-2015](https://github.com/riscure/rhme-2015)

RHme Challenges 2015 presents a sophisticated hacking challenge based on an Arduino system. Launched during BlackHat Amsterdam 2015, this moderately difficult challenge requires participants to apply both hardware and software attack techniques to extract flags and ultimately recover the administrator key. This challenge is ideal for security enthusiasts looking to deepen their understanding of low-level hardware security and explore various exploit techniques, including side-channel attacks and fault injection.

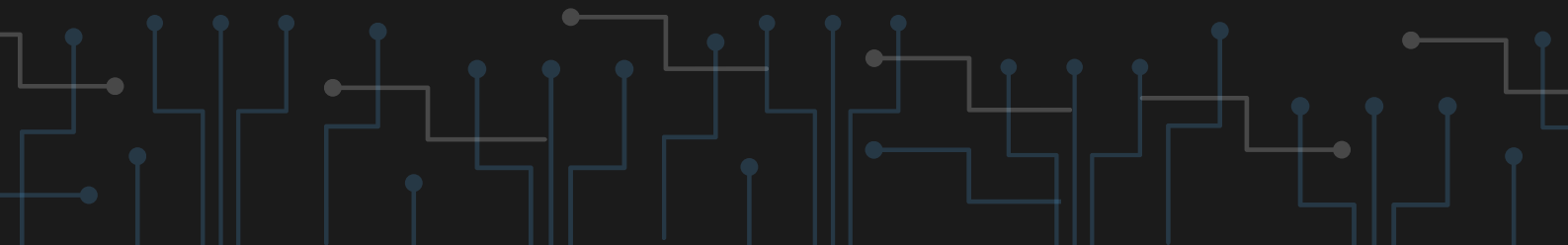




RHme Challenges 2016

[HTTPS://GITHUB.COM/RISCURE/RHME-2016](https://github.com/riscure/rhme-2016)

RHme Challenges 2016 continues the tradition of complex hardware-based hacking challenges. Participants are tasked with exploiting vulnerabilities in an Arduino-based system, focusing on both hardware and software attack vectors. This challenge emphasizes creative problem-solving and deep technical knowledge, offering an opportunity to master advanced low-level security techniques.

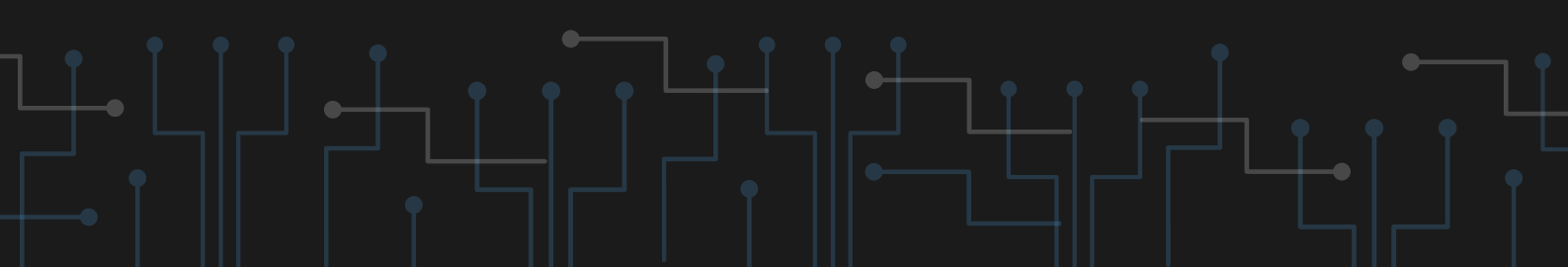




RHme Challenges 2017

[HTTPS://GITHUB.COM/RISCURE/RHME-2017](https://github.com/riscure/rhme-2017)

RHme Challenges 2017 delivers another year of advanced hacking challenges designed to push participants' skills to the limit. It focuses on the combination of hardware manipulation and software exploitation, requiring a detailed understanding of embedded systems security. This challenge is ideal for both experienced security professionals and hobbyists looking to test and expand their expertise in low-level and embedded system vulnerabilities.

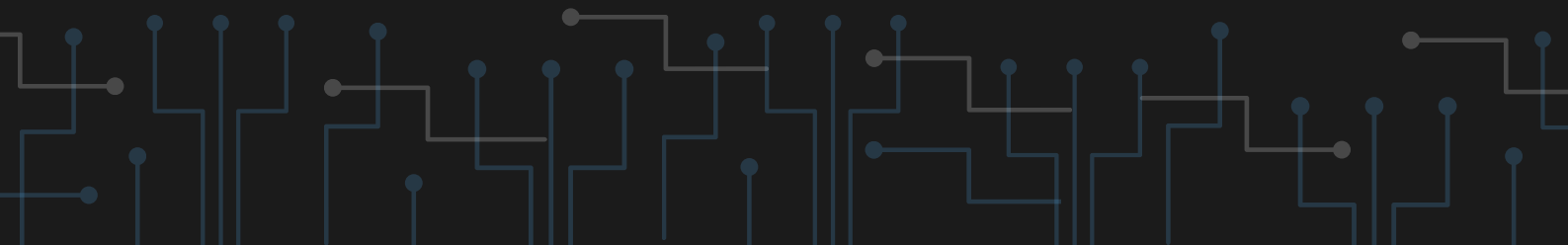




Root Me

[HTTPS://WWW.ROOT-ME.ORG/](https://www.root-me.org/)

Root Me is a comprehensive platform offering a wide range of cybersecurity challenges and CTF exercises. Covering categories such as network security, cryptography, forensics, and more, Root Me provides users with an interactive environment for hands-on practice. Suitable for both beginners and experts, the platform combines educational resources with a community-driven approach to learning cybersecurity through practical experience.

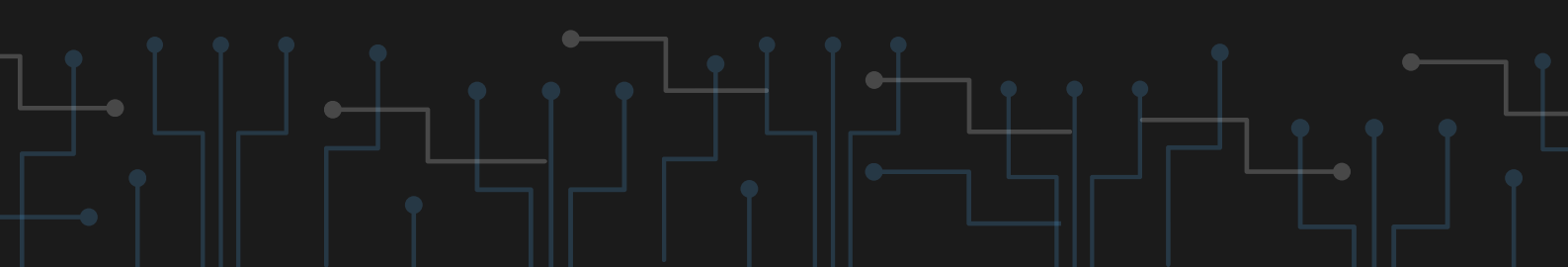




ROP Emporium

[HTTPS://ROPEMPORIUM.COM/](https://ropemporium.com/)

ROP Emporium offers a collection of challenges focused on Return-Oriented Programming (ROP). Designed to teach and test skills in binary exploitation, the platform emphasizes hands-on learning through a series of scenarios that gradually increase in difficulty. It is an ideal resource for both beginners and advanced users. Each challenge simulates real-world vulnerabilities, allowing participants to practice exploit development techniques in a controlled environment.

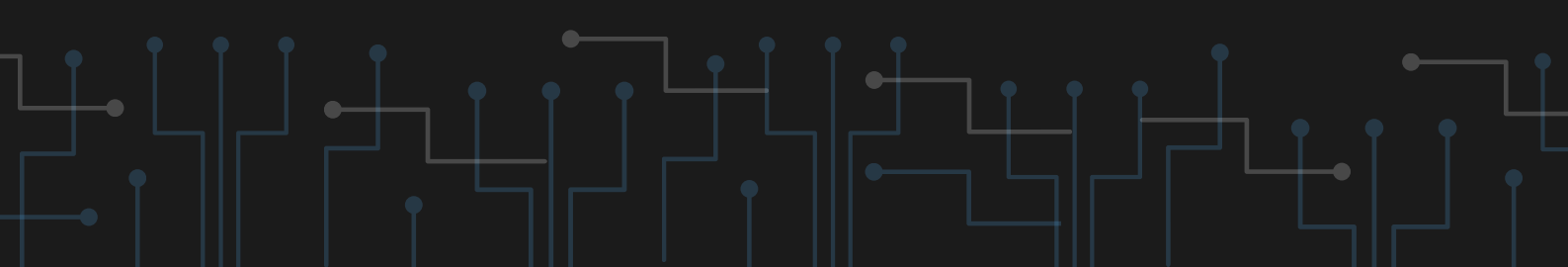




Sad Servers

[HTTPS://SADSERVERS.COM/](https://sadservers.com/)

Sad Servers is a training platform designed for DevOps professionals and Site Reliability Engineers (SREs). It offers a variety of challenges focused on troubleshooting Linux servers. These scenarios mimic real-world server issues, helping users develop skills in debugging and incident management. From fixing Kubernetes deployments to resolving web server configuration errors, each task provides a comprehensive, hands-on educational experience.

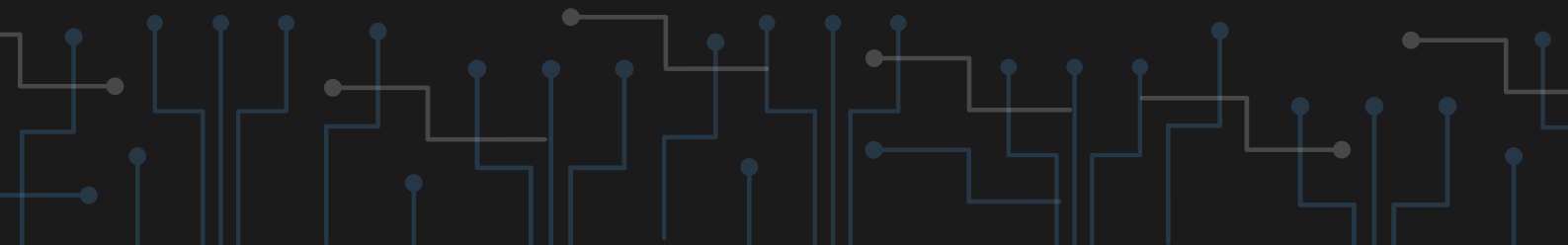




SadCloud

[HTTPS://GITHUB.COM/NCCGROUP/SADCLOUD](https://github.com/NCCGROUP/SADCLOUD)

SadCloud is an open-source project developed by NCC Group, focusing on cloud security misconfigurations. Hosted on GitHub, the repository provides a collection of common cloud security issues and their exploit scripts. SadCloud serves as an educational resource, helping users identify and mitigate potential threats in cloud infrastructures while promoting better security practices and awareness in managing cloud services.

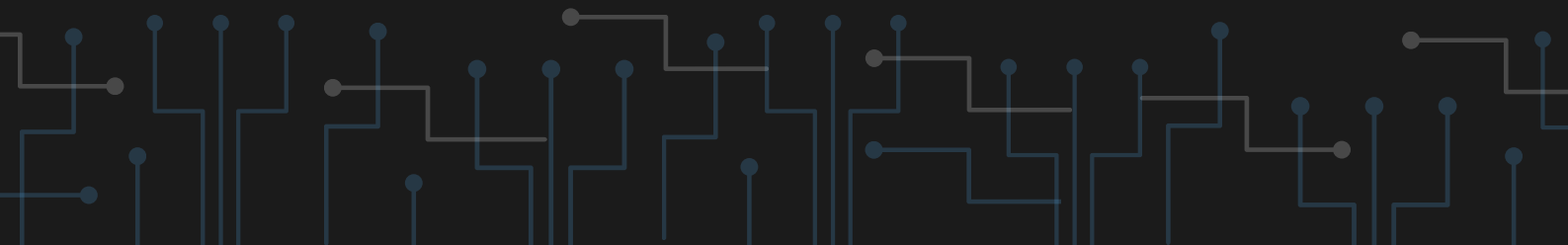




SANS Holiday Hack Challenge

[HTTPS://HOLIDAYHACKCHALLENGE.COM/2023/](https://holidayhackchallenge.com/2023/)

The SANS Holiday Hack Challenge is an annual cybersecurity competition that blends festive themes with serious security challenges. Organized by the SANS Institute, the event features a variety of puzzles and scenarios covering a broad range of cybersecurity topics, from digital forensics to penetration testing. Each year, participants engage in a fun, narrative-driven adventure while solving complex security problems, making it both an educational and entertaining experience.

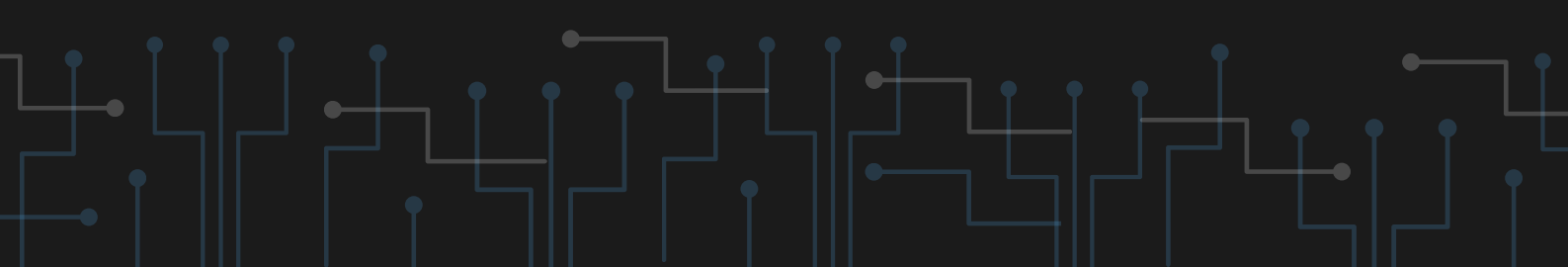




TryHackMe

[HTTPS://TRYHACKME.COM/](https://tryhackme.com/)

TryHackMe is an interactive cybersecurity training platform offering a wide range of hands-on labs and challenges designed to enhance the skills of both beginners and experts. It uses a Capture The Flag (CTF) format, allowing users to explore various cybersecurity topics through guided exercises and real-world scenarios. The platform covers areas such as penetration testing, network security, and digital forensics, providing an engaging and practical learning experience.

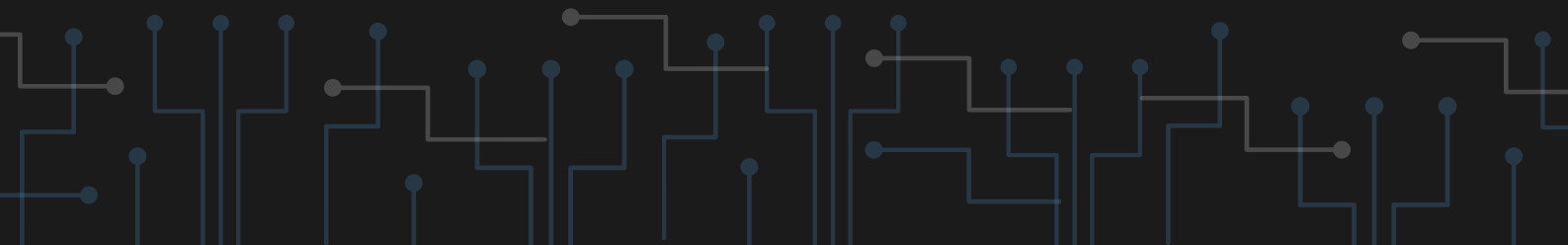




UnderTheWire

[HTTPS://UNDERTHEWIRE.TECH/WARGAMES](https://underthewire.tech/wargames)

UnderTheWire offers a series of PowerShell-based wargames designed to teach and enhance Windows PowerShell scripting skills through hands-on challenges. Each game provides a set of tasks simulating real-world scenarios, requiring participants to apply their knowledge and problem-solving abilities to progress. It is an ideal platform for developing practical PowerShell proficiency in a structured, engaging way.





vAPI

[HTTPS://GITHUB.COM/ROOTTUSK/VAPI](https://github.com/roottusk/vapi)

vAPI (Vulnerable Adversely Programmed Interface) offers a self-service API designed to mimic OWASP API Security Top 10 vulnerabilities. Ideal for security testing and learning, vAPI provides a realistic environment for developers and security professionals to understand and mitigate common API flaws. It is easy to deploy via Docker or manual setup, offering a comprehensive and accessible platform for expanding knowledge of API security.

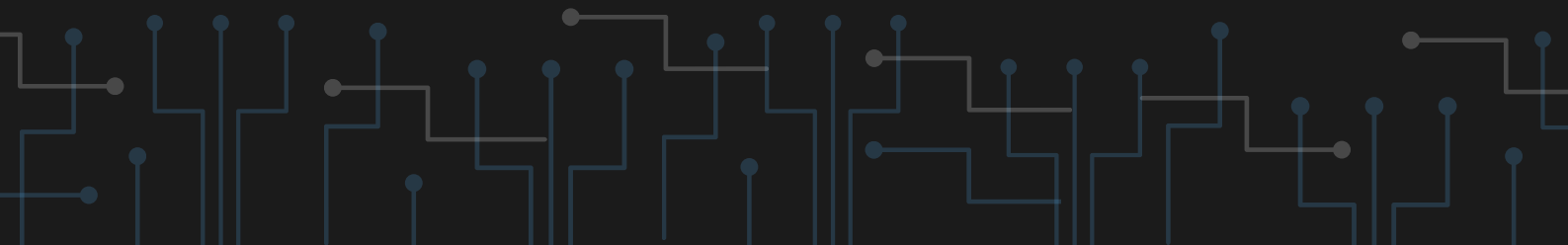




Vulnerable Active Directory

[HTTPS://GITHUB.COM/SAFEBUFFER/VULNERABLE-AD](https://github.com/safebuffer/vulnerable-ad)

Vulnerable Active Directory provides a deliberately insecure Active Directory (AD) environment designed for penetration testing and security assessments. This platform is ideal for cybersecurity enthusiasts and professionals to explore AD weaknesses and improve their defensive and offensive security skills.

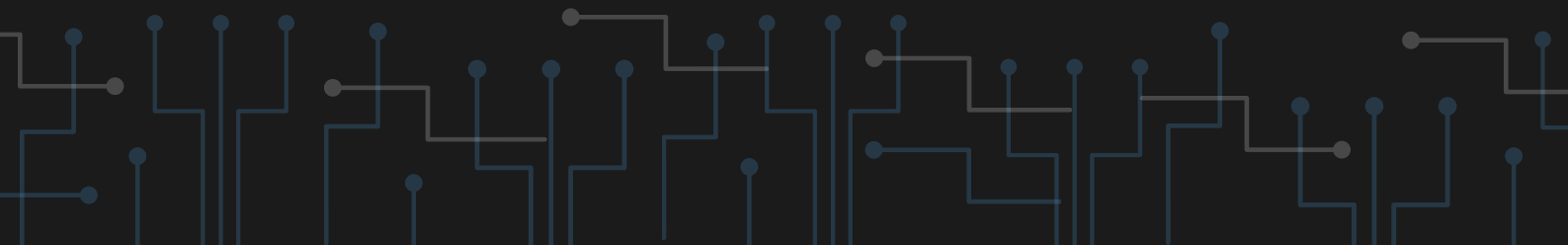




Vulnerable Active Directory Plus

***[HTTPS://GITHUB.COM/WATEREXECUTION/VULNERABLE
-AD-PLUS](https://github.com/WATEREXECUTION/VULNERABLE-AD-PLUS)***

Vulnerable Active Directory Plus enhances the capabilities of a standard insecure AD environment by adding advanced scenarios and complexity. Tailored for experienced security professionals, the platform offers comprehensive exercises that replicate sophisticated attack vectors, making it a robust tool for refining penetration testing and Active Directory exploitation skills.

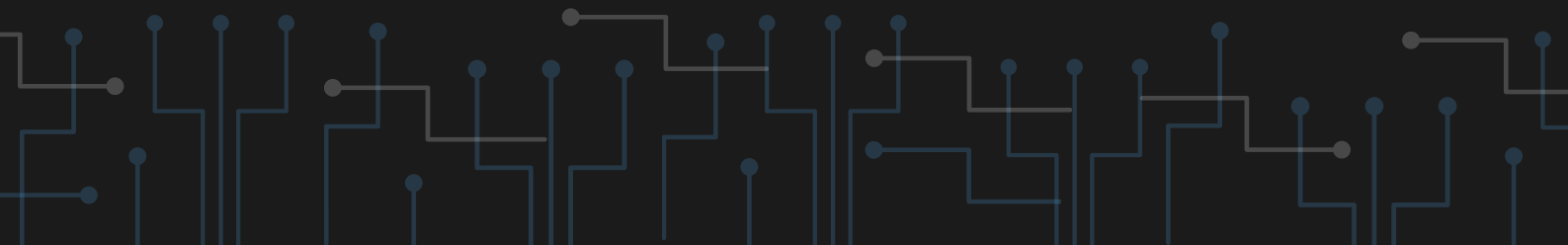




Vulnerable AD

[HTTPS://GITHUB.COM/SAFEBUFFER/VULNERABLE-AD](https://github.com/safebuffer/vulnerable-ad)

The Vulnerable Active Directory project on GitHub provides a comprehensive guide for setting up a local Active Directory environment intentionally configured to be vulnerable to common attacks. This resource is invaluable for cybersecurity students and professionals seeking a safe space to practice penetration testing techniques within Active Directory infrastructure. It replicates real-world attack scenarios in a controlled lab environment, making it an ideal hands-on learning tool.

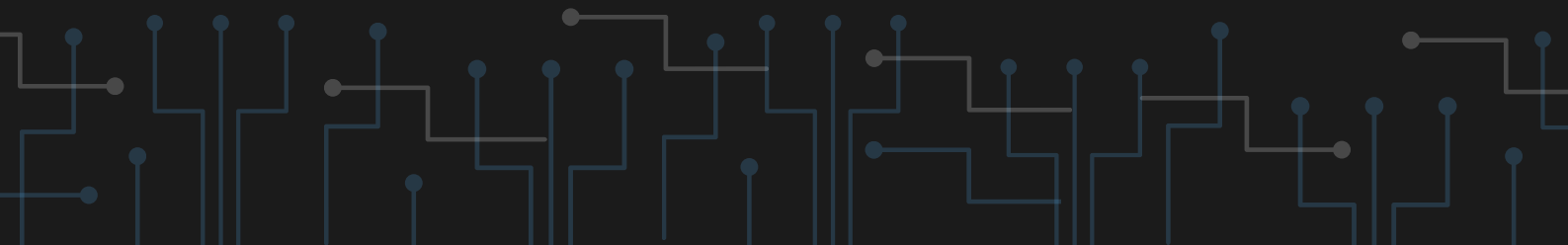




Vulnerable App with Examples from OWASP

[HTTPS://GITHUB.COM/EREVOS/VAMPI](https://github.com/erevos/vampi)

Vulnerable App with Examples by OWASP demonstrates the risks of improper secret management through practical examples. This educational platform highlights common mistakes in handling secrets. By showcasing what not to do, it equips developers with the knowledge needed to effectively secure sensitive information.





Vulnerable REST API (VAmPI)

[HTTPS://GITHUB.COM/EREVOS/VAMPI](https://github.com/erevos/vampi)

VAmPI (Vulnerable REST API) provides a hands-on platform for security testing against OWASP API Security Top 10 vulnerabilities. Designed for practicing the identification and mitigation of API security issues, VAmPI offers a realistic environment to improve understanding and response to common API security threats.

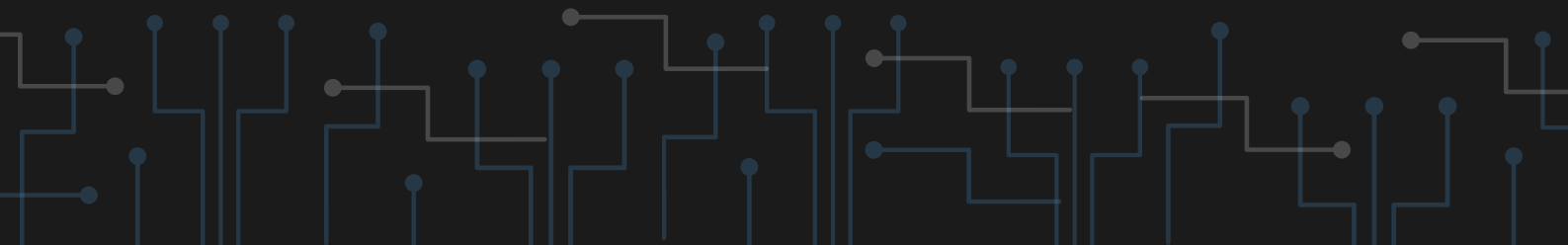




VulnHub

[HTTPS://WWW.VULNHUB.COM/](https://www.vulnhub.com/)

VulnHub provides an extensive collection of deliberately vulnerable virtual machines designed to simulate real-world security vulnerabilities. The platform offers a range of difficulty levels suitable for both beginners and experienced individuals. It promotes a hands-on learning approach, allowing users to download and exploit these virtual machines in a controlled environment, making it an excellent resource for developing and honing cybersecurity skills.





VulnLab

[HTTPS://WWW.VULNLAB.COM/](https://www.vulnlab.com/)

VulnLab is a dynamic platform for cybersecurity enthusiasts and professionals, enabling skill testing through simulated hacking challenges. In addition to web application vulnerabilities, the platform offers penetration testing and red teaming exercises with over 100 vulnerable machines, ranging from simple devices to complex Active Directory environments. The challenges come with varying difficulty levels, accompanied by notes, hints, and guides. Regularly updated content ensures the platform stays current and engaging for users.

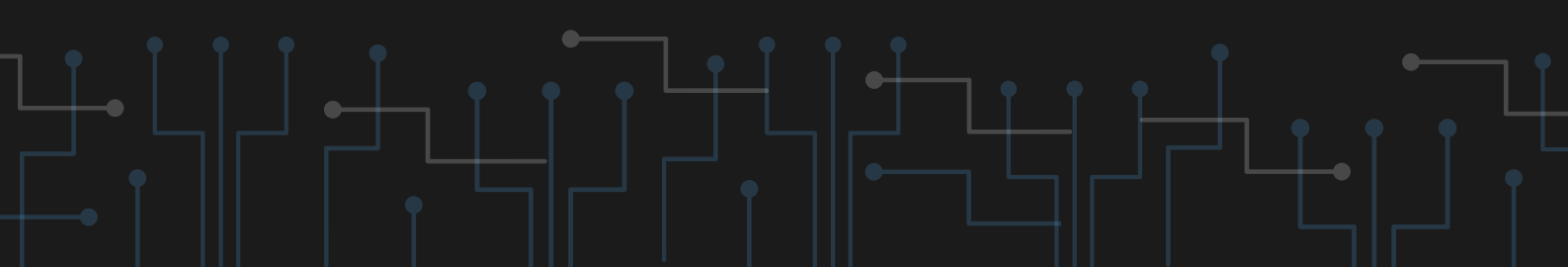




Webhacking.kr

[HTTPS://WEBHACKING.KR/](https://webhacking.kr/)

Webhacking.kr is a platform for individuals looking to master web application security through hands-on challenges. It offers a variety of tasks, ranging from beginner to expert levels, focusing on real-world web vulnerabilities. Users can hone their skills in areas such as SQL injection, cross-site scripting (XSS), and other web-based attacks.

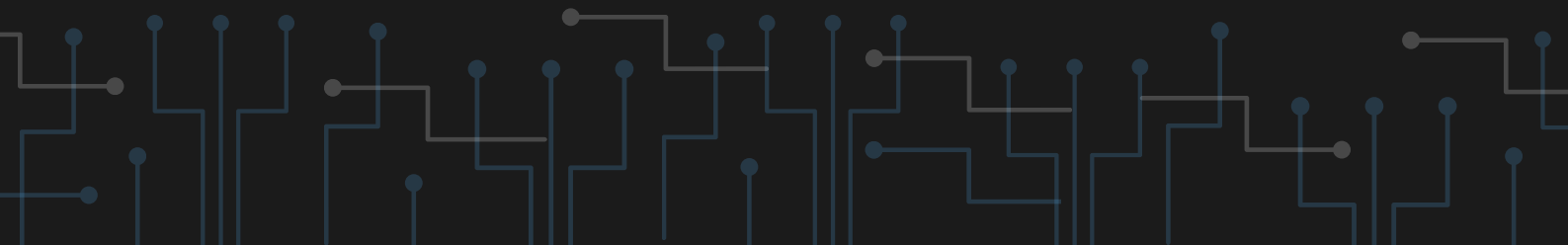




XSS Game

[HTTPS://XSS.PWNFUNCTION.COM/](https://xss.pwnfunction.com/)

XSS Game, developed by PwnFunction, is an interactive platform dedicated to teaching and testing skills related to Cross-Site Scripting (XSS) vulnerabilities. It offers a series of progressive challenges that simulate real-world scenarios, allowing users to practice identifying and exploiting XSS flaws. The game-like format makes learning engaging and effective, providing an immersive experience for mastering XSS techniques.





***If you find this resource
valuable, share it with
others!***

:)

***And for more valuable publications
available EXCLUSIVELY to readers, sign
up at:***

<https://securitybeztabu.pl/newsletter/>