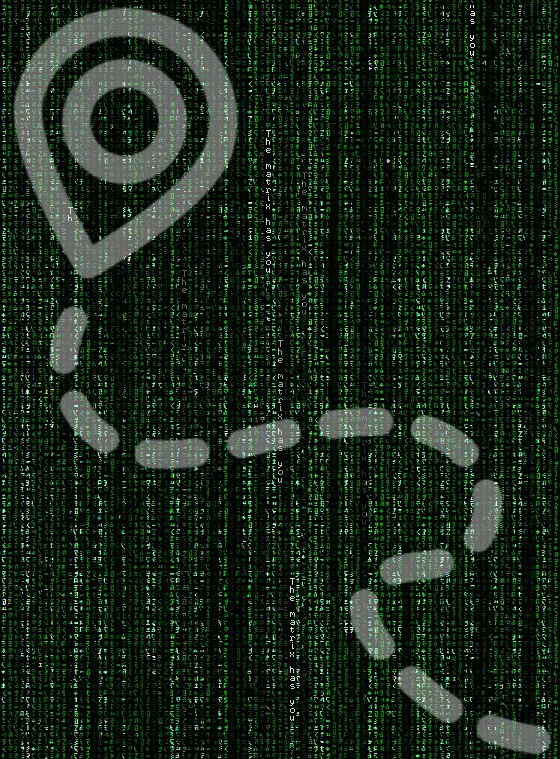
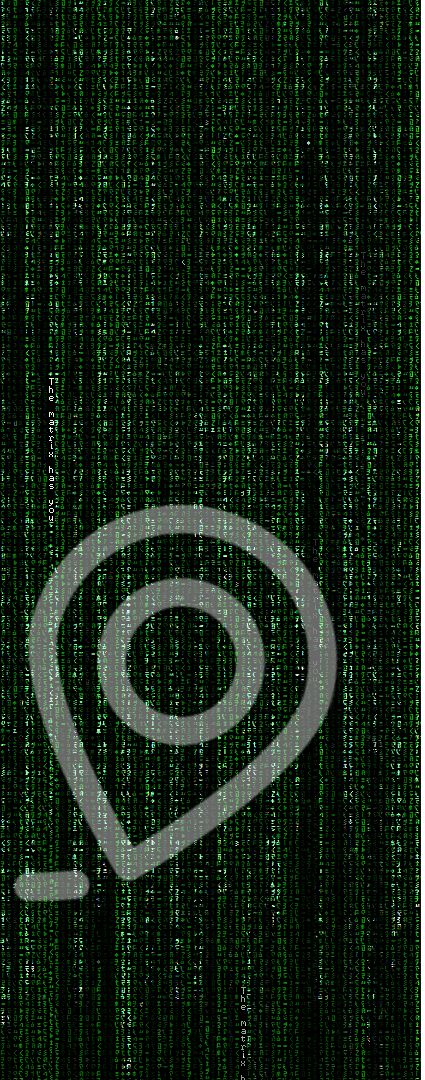
ROADMAP RED TEAM



mx61tt

Ementa



Web

Mobile

Infra

Red Team

App Sec

Web

Portswigger Academy

Server-side topics

For complete beginners, we recommend starting with our server-side topics. These vulnerabilities are typically easier to learn because you only need to understand what's happening on the server. Our materials and labs will help you develop some of the core knowledge and skills that you will rely on time after time.

SQL injection

SQL injection is an old-but-gold vulnerability responsible for many high-profile data breaches. Although relatively simple to learn, it can potentially be used for some high-severity exploits. This makes it an ideal first topic for beginners, and essential knowledge even for more experienced users.

Go to topic → 18 Labs

Authentication

Go to topic → 14 Labs

Path traversal

Go to topic → 6 Labs

Command injection

Go to topic → 5 Labs

Business logic vulnerabilities

New lab added

Go to topic → 11 Labs

Portswigger Academy

Client-side topics

Client-side vulnerabilities introduce an additional layer of complexity, which can make them slightly more challenging. These materials and labs will help you build on the server-side skills you've already learned and teach you how to identify and exploit some gnarly client-side vectors as well.

Cross-site scripting (XSS)

Simply put, XSS is one of the most important vulnerabilities out there. It's both incredibly common and extremely powerful, especially when used as part of a wider exploit chain. This is a huge topic, with plenty of labs for complete beginners and seasoned pros alike.

Go to topic → 30 Labs

Cross-site request forgery (CSRF)

Go to topic → 12 Labs

Cross-origin resource sharing (CORS)

Go to topic → 3 Labs

Clickjacking

Go to topic → 5 Labs

DOM-based vulnerabilities

Go to topic → 7 Labs

Portswigger Academy

Advanced topics

These topics aren't necessarily more difficult to master but they generally require deeper understanding and a wider breadth of knowledge. We recommend getting to grips with the basics before tackling these labs, some of which are based on pioneering techniques discovered by our world-class research team.

Insecure deserialization

Deserialization has a reputation for being difficult to get your head around but it can be much easier to exploit than you might think. We'll guide you through the process step-by-step so you can pick off some high-severity bugs that even experienced testers may have missed altogether.

Go to topic → 10 Labs

Web LLM attacks

Go to topic → 4 Labs

GraphQL API vulnerabilities

Go to topic → 5 Labs

Server-side template injection

Go to topic → 7 Labs

Web cache poisoning

Go to topic → 13 Labs

Burp Suite Certified Practitioner

Why become a Burp Suite Certified Practitioner?

Successfully passing the Burp Suite Certified Practitioner exam indicates a high-level proficiency in web security testing. It is aimed at penetration testers, and the organizations that employ them.

Prove your proficiency

- Demonstrate a deep knowledge of the latest vulnerability classes and how to exploit them.
- Showcase your skills with Burp Suite Professional.
- Prove your hacking ability to employers and the community.

LEARN MORE

Upskill your team

- Prove the proficiency of your testing team to potential clients.
- Easily identify the best new talent to join your team.
- Develop your team's expertise with knowledge of the latest vulnerability classes and how to exploit them.

LEARN MORE

New to web security? Start your journey here →

Burp Suite Certified Practitioner

$99

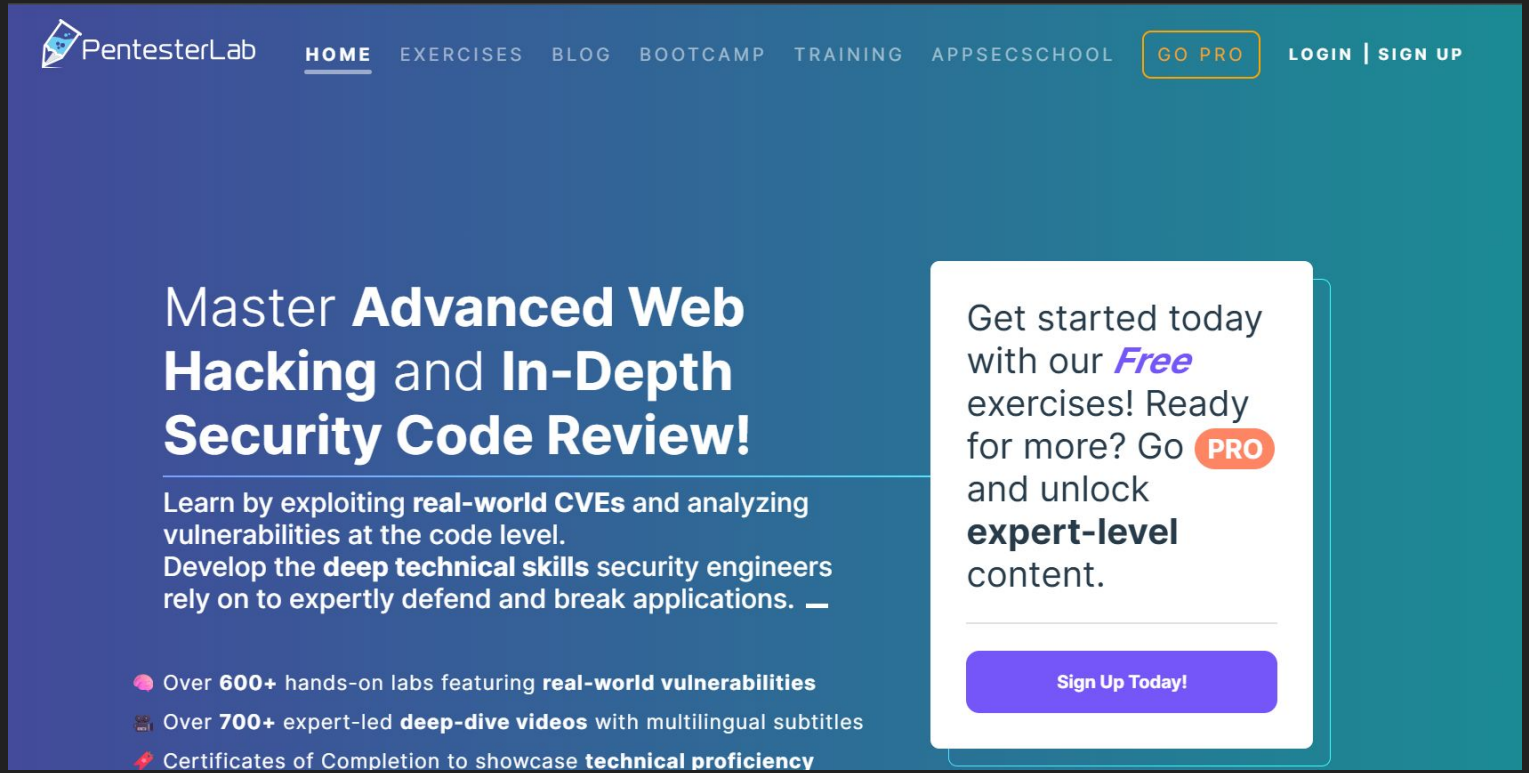
Buying your exam

When you're ready, and have completed all of the required preparation, you can purchase your exam credit. Remember, you'll also need access to an active subscription of Burp Suite Professional to be able to take the exam.

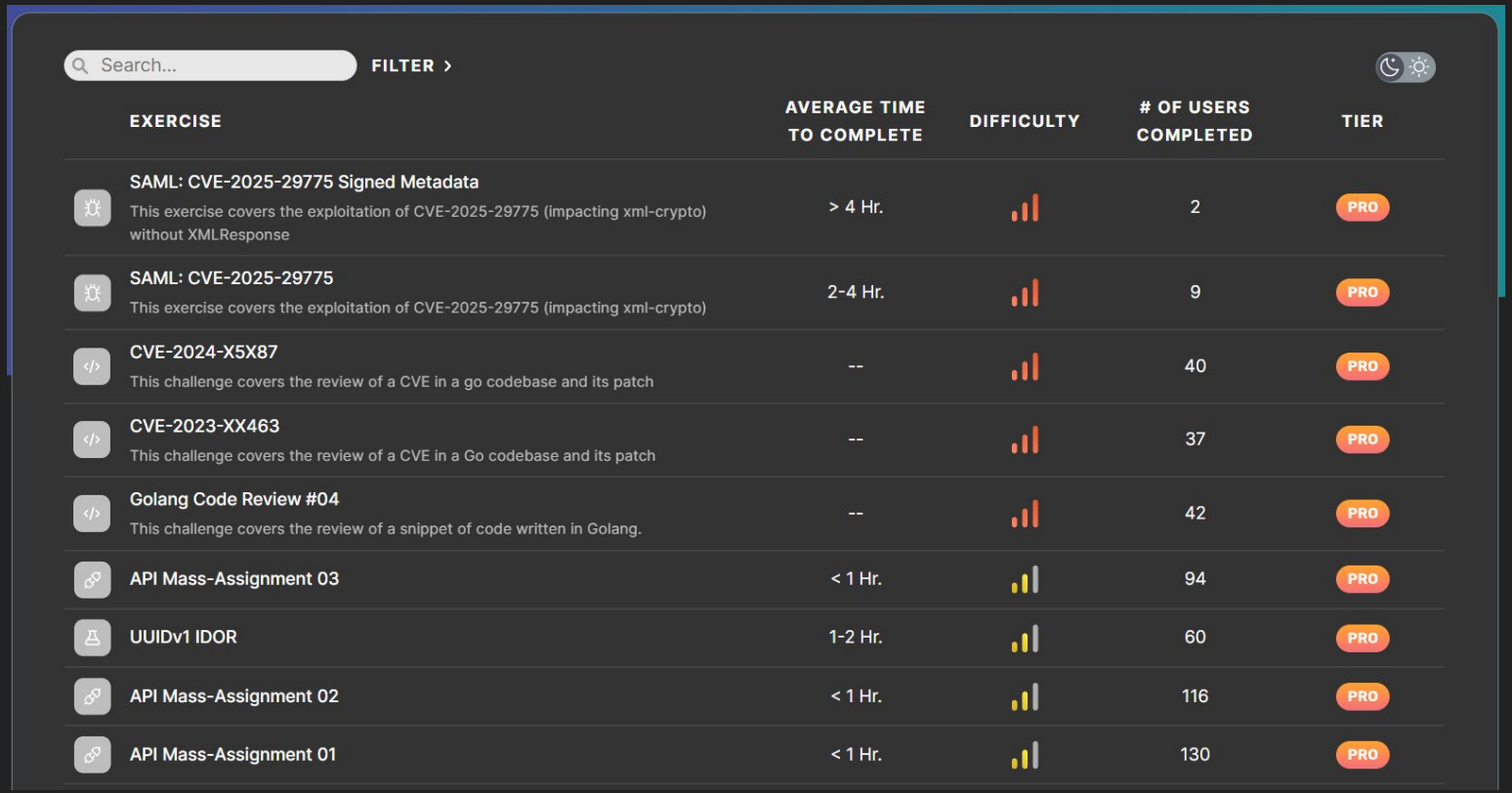
Get Burp Suite Certified for $99 →

Buy Burp Suite Professional for $475 →

PentesterLab



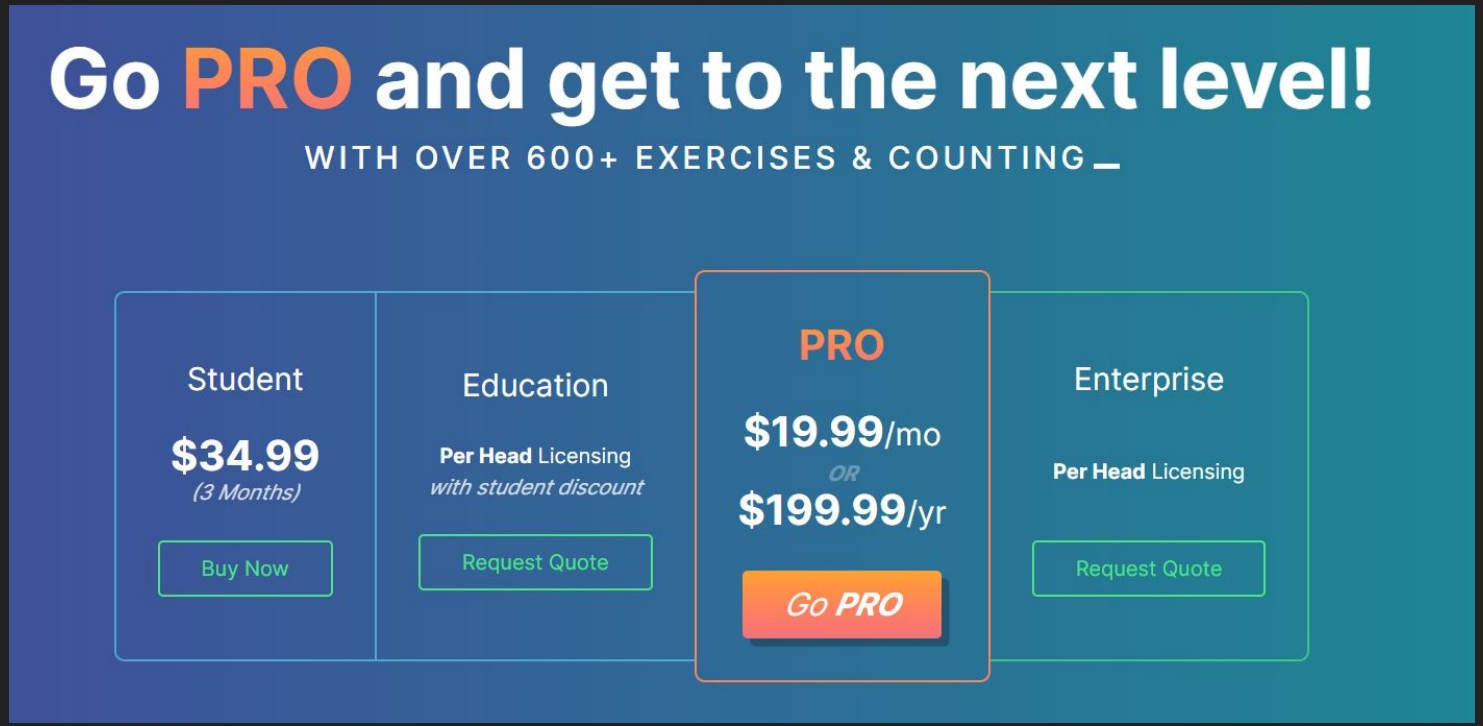
Pentester Lab



EXERCISE	AVERAGE TIME TO COMPLETE	DIFFICULTY	# OF USERS COMPLETED	TIER
SAML: CVE-2025-29775 Signed Metadata This exercise covers the exploitation of CVE-2025-29775 (impacting xml-crypto) without XMLResponse	> 4 Hr.		2	PRO
SAML: CVE-2025-29775 This exercise covers the exploitation of CVE-2025-29775 (impacting xml-crypto)	2-4 Hr.		9	PRO
CVE-2024-X5X87 This challenge covers the review of a CVE in a go codebase and its patch	--		40	PRO
CVE-2023-XX463 This challenge covers the review of a CVE in a Go codebase and its patch	--		37	PRO
Golang Code Review #04 This challenge covers the review of a snippet of code written in Golang.	--		42	PRO
API Mass-Assignment 03	< 1 Hr.		94	PRO
UUIDv1 IDOR	1-2 Hr.		60	PRO
API Mass-Assignment 02	< 1 Hr.		116	PRO
API Mass-Assignment 01	< 1 Hr.		130	PRO

Pentester Lab

$20/mo



Web Hacking na Prática

Web Hacking na Prática

Aulas práticas e objetivas

Um curso completo para transformarvocê em um profissional altamente capacitado no mercado de Segurança Ofensiva

Ministrado por:

Carlos Vieira
Fundador da Crowsec Edtech

01 Bases

- [x] **Redes de computadores**
  - Modelo OSI
  - TCP/IP
  - ARP
  - BGP
  - DNS
  - NAT
  - Protocolos (HTTP, FTP, SSH, RDP, SMB)
- [x] **Infraestrutura (Apache, Nginx, Tomcat)**
- [x] **Cloud Native (Api Gateway, LB, Micro-services, Service Mesh)**
- [x] **WAF / CDN**
- [x] **Programação para Hacking**
- [x] **Desenvolvimento Seguro (DevSecOps)**
- [x] **API Security**

02 Essential Web Hacking

Web Hacking na Prática

Aulas práticas e objetivas

Um curso completo para transformarvocê em um profissional altamente capacitado no mercado de Segurança Ofensiva

Ministrado por:

Carlos Vieira
Fundador da Crowsec Edtech

01 Bases

02 Essential Web Hacking

03 Advanced Web Hacking

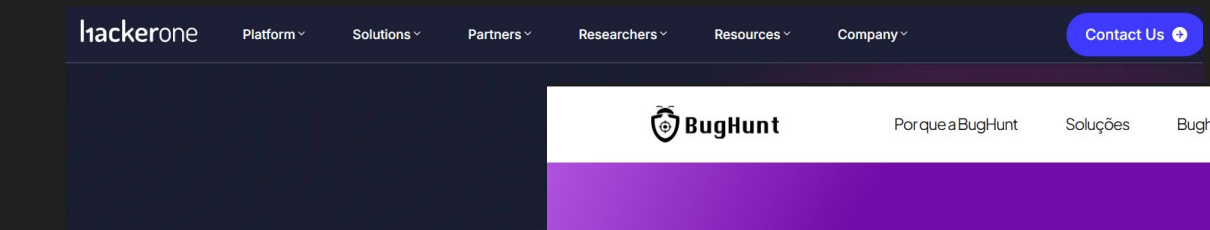
✅ SQL Injection (E, B, T)

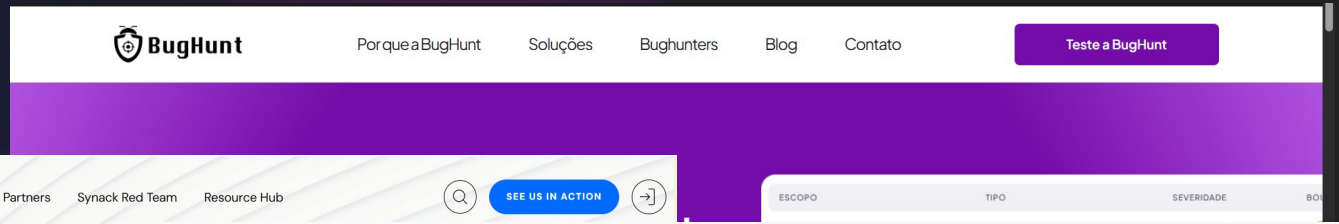
- PHP Wrapper
- Log Poisoning / Log Injection
- Type Juggling
- Server Side Request Forgery (SSRF)
- Protocol Smuggling (Mysql)
- Protocol Smuggling (Redis)
- Protocol Smuggling (FastCGI)
- Protocol Smuggling (Zabbix)
- Protocol Smuggling (Memcache)
- SSRF – AWS Metadata
- Server Side Template Injection
- SSTI (Twig)
- SSTI (Jinja)
- SSTI (ERB)
- OGNL/EL Injection (Spring)

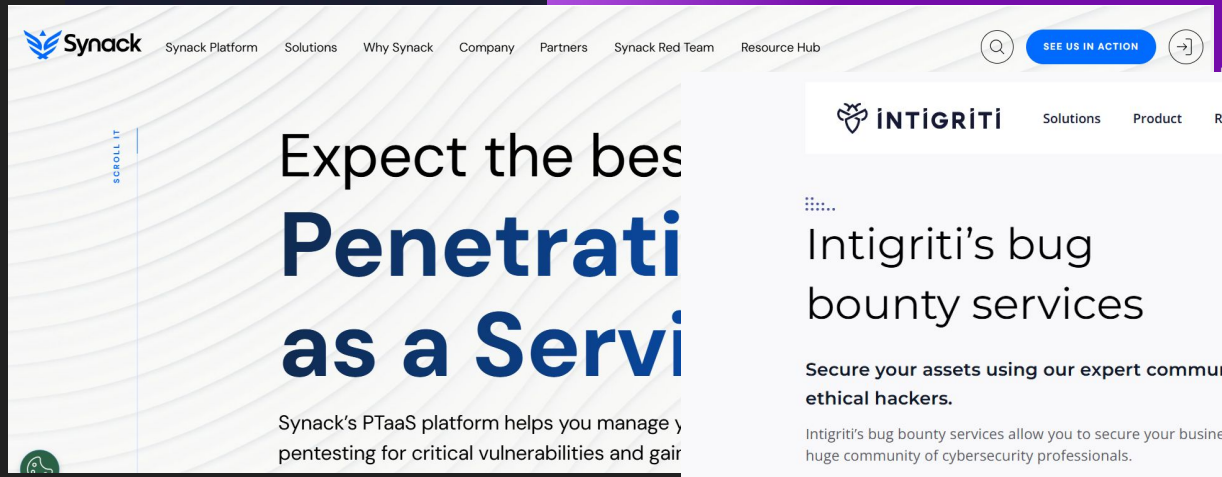
Web Hacking na Prática

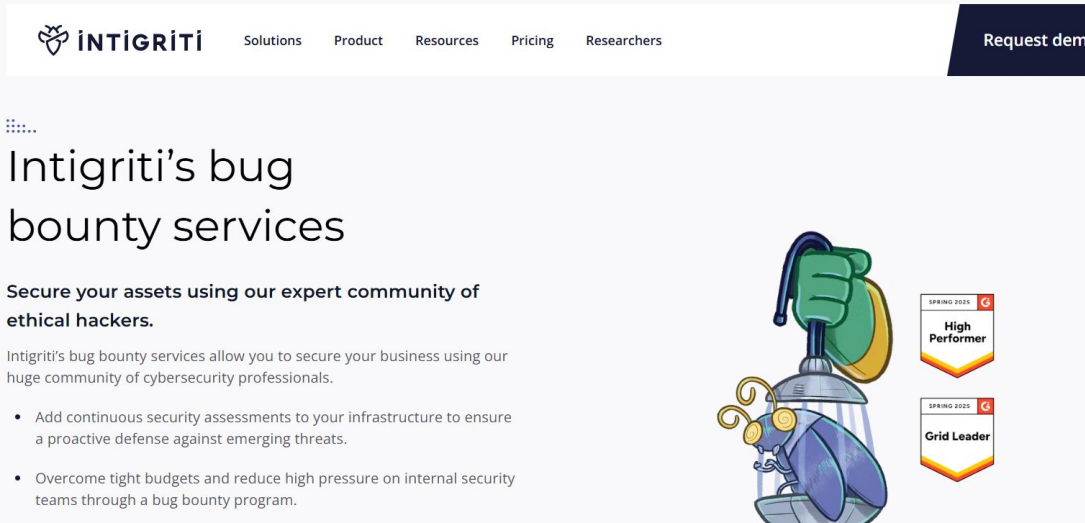
R$ 2997,00

Bug Bounty


hackerone
Platform
Solutions
Partners
Researchers
Resources
Company
Contact Us


BugHunt
Por que a BugHunt
Soluções
Bughunters
Blog
Contato
Teste a BugHunt
ESCOPO
TIPO
SEVERIDADE


Synack
Synack Platform
Solutions
Why Synack
Company
Partners
Synack Red Team
Resource Hub
SEE US IN ACTION
SCROLL LT
Expect the bes
Penetrati
as a Servi
Synack's PTaaS platform helps you manage y
pentesting for critical vulnerabilities and gair


İNTİGRİTİ
Solutions
Product
Resources
Pricing
Researchers
Request dem
Intigriti's bug
bounty services
Secure your assets using our expert community of ethical hackers.
Intigriti's bug bounty services allow you to secure your business using our huge community of cybersecurity professionals.
Add continuous security assessments to your infrastructure to ensure a proactive defense against emerging threats.
Overcome tight budgets and reduce high pressure on internal security teams through a bug bounty program.
SPRING 2025
High Performer
SPRING 2025
Grid Leader

Mobile

Udemy

R$ 24,90

TI e software › Rede e segurança › Hacking ético

Hacking and Pentesting Android Applications

Learn how to pentest Android Applications using the modern day pentesting tools and techniques

4,5 ★★★★½ (812 classificações) 5.125 alunos

Criado por Srinivas .

Última atualização em 07/2021 Inglês Português [Automático], Inglês [Automático], Mais 2

TI e software › Rede e segurança › Teste de intrusão

Hacking and Pentesting iOS Applications

Learn how to pentest iOS Applications using the modern day pentesting tools and techniques

4,2 ★★★★☆ (654 classificações) 15.645 alunos

Criado por Srinivas .

Última atualização em 07/2021 Inglês Inglês [Automático], Espanhol [Automático]

R$ 24,90 ~~R$ 113,90~~
78% de desconto

Pessoal Equipes

R$ 24,90 ~~R$ 113,90~~
78% de desconto

Udemy

Conteúdo do curso

7 seções • 48 aulas • Duração total: 4h 36m — Expandir todas as seções

Course Introduction	1 aulas • 3m
Introduction	3 aulas • 18m
Setting up Android Pentesting Lab	6 aulas • 27m
Android Application Penetration Testing - Basics	14 aulas • 1h 31m
Android Application Penetration Testing - Advanced	22 aulas • 2h 17m
Conclusion	1 aulas • 1m
Bonus Section	1 aulas • 1m

Conteúdo do curso

7 seções • 48 aulas • Duração total: 3h 41m — Expandir todas as seções

Course Introduction		1 aulas • 3m
Course Introduction	Visualizar	02:35
Basics of iOS Apps		3 aulas • 9m
Setting up iOS Pentesting lab		10 aulas • 48m
iOS Application Penetration Testing - Basics		13 aulas • 54m
iOS Application Penetration Testing - Advanced		19 aulas • 1h 48m
Conclusion		1 aulas • 1m
Bonus Section		1 aulas • 1m

Udemy

Conteúdo do curso

7 seções • 48 aulas • Duração total: 4h 36m — Expandir todas as seções

Course Introduction	1 aulas • 3m
Introduction	3 aulas • 18m
Setting up Android Pentesting Lab	6 aulas • 27m
Android Application Penetration Testing - Basics	14 aulas • 1h 31m
Android Application Penetration Testing - Advanced	22 aulas • 2h 17m
Conclusion	1 aulas • 1m
Bonus Section	1 aulas • 1m

Conteúdo do curso

7 seções • 48 aulas • Duração total: 3h 41m — Expandir todas as seções

Course Introduction		1 aulas • 3m
Course Introduction	Visualizar	02:35
Basics of iOS Apps		3 aulas • 9m
Setting up iOS Pentesting lab		10 aulas • 48m
iOS Application Penetration Testing - Basics		13 aulas • 54m
iOS Application Penetration Testing - Advanced		19 aulas • 1h 48m
Conclusion		1 aulas • 1m
Bonus Section		1 aulas • 1m

Sec4US

SEC4US Home Consultoria Treinamentos Certificações Ca

Hacking Mobile Application - Android

Aprenda as principais técnicas para a realização de testes de invasão (Pentest) em dispositivos móveis Android seguindo as melhores práticas do mercado como Owasp Mobile Security Top 10, bem como a experiência prática no dia a dia de realização de Pentest em dispositivos Móveis.

Sobre o treinamento | Habilidades | Requisitos

em dispositivos móveis. Durante o treinamento são explorados os conceitos da Owasp Mobile Top 10 para a realização de um pentest, indo desde a preparação inicial do ambiente de testes até testes avançados como quebra de proteções (SSL pinning, root, debug e screenshot), SQL Injection, quebra de criptografia adicional de meio e muito mais.

Este treinamento é dividido em 2 fases, onde a primeira fase ocorre em metodologia EAD compondo 20 horas, sendo disponibilizada em formato de vídeo aula gravada, a segunda fase é realizada ao vivo tendo duração de 40 horas. Caso tenha alguma dúvida verifique os detalhes de cada módulo no PDF da ementa completa.

Instrutor

Thiago Martins

(Kirito)

Programa de estudos

1. Preparação do ambiente de testes
2. Criação de dispositivos Android virtuais
3. Utilização de dispositivo físico Android
4. Entendendo Arquitetura do Android
5. Engenharia reversa de aplicação Android
6. Modificando e recompilando aplicação Android
7. Hooking de classes e métodos
8. Bypass de detecção de root
9. Bypass de detecção de emulador
10. Bypass de detecção do frida
11. Bypass de proteção de screenshot
12. Bypass de múltiplas pinagens SSL
13. Reconhecendo e entendendo código ofuscado
14. Criando plugin para o Burp com Python
15. Interceptando e alterando tráfego criptografado
16. Armazenamento de dados inseguros
17. Explorando Content Providers
18. Explorando SQL Injection
19. Vazamento de dados confidenciais
20. OWASP Mobile Security Top 10

SecSUS

R$ 3000,00

Hacking Mobile Application - Android

Aprenda as principais técnicas para a realização de testes de invasão (Pentest) em dispositivos móveis Android seguindo as melhores práticas do mercado como Owasp Mobile Security Top 10, bem como a experiência prática no dia a dia de realização de Pentest em dispositivos Móveis.

Dificuldade
● ● ● ● ○

Carga horária
60 horas

Disponibilidade
Ao vivo via internet

Idioma
Português

Próximas turmas

Datas:	09/06/2025 - 20/06/2025
Horários:	19:00 - 23:00
Metodologia:	Online
Investimento:	R$ 3.000,00

Inscreva-se aqui

Sobre o treinamento | **Habilidades** | **Requisitos**

O Hacking Mobile Application é um treinamento 100% prático destinado aos profissionais de TI que desejam se aperfeiçoar na área de Pentest e de Segurança Ofensiva, pois aborda técnicas de invasão em dispositivos móveis Android. O Treinamento foi inteiramente modelado conforme as

8kSec

8kSec Academy

COURSES | LIVE TRAINING | AFFILIATE PROGRAM | TESTIMONIALS | CONTACT US | FAQ | JOIN FOR FREE

Self-paced Course

Practical Mobile Application Exploitation (On-demand)

Designed for both beginners and advanced enthusiasts, you'll learn how to reverse engineer and conduct thorough security audits of iOS and Android applications. You'll get a deeper insight into common bug categories, and detailed walkthroughs on how to exploit them. Learn how tools like Ghidra, Frida, LLDB, and more can be used to assist you during Mobile application assessments, or research.

LEVEL

Beginner / Intermediate

VIDEO

23 hours - 140 videos

8kSec

← Back to course page

Practical Mobile Application Exploitation

69 %

Course Preview

Welcome to the Course

Setting up the iOS Testing Environ...

Intro to iOS Apps

Debugging iOS Apps

Introduction to iOS Reverse Engine...

iOS App Containers and Data Anal...

Exploiting Android Flutter

In this module, we explore the security internals of Flutter applications running on Android devices. You will learn how to intercept and analyze network traffic from Flutter-based apps, addressing the challenges posed by Flutter's handling of device proxies. The module will discuss the techniques for bypassing TLS verification both manually and using advanced tools like Frida, ensuring effective traffic interception and manipulation. Through hands-on demonstrations, you will understand Flutter's implementation of TLS verification and certificate pinning, and how to exploit these mechanisms to gain deeper insights into app communications.

By the end of this module, you will be equipped with the knowledge and skills to assess, exploit, and secure Flutter application traffic, enhancing your mobile security expertise.

8kSec

CERTIFICATION DETAILS | EXAM OBJECTIVES | PREREQUISITES | FORMAT | PASSING CRITERIA | CERTIFICATE

The CMSE certification exam, spanning 48 hours, rigorously evaluates your expertise across a range of domains:

1. iOS Application Security: Secure iOS apps through dynamic and static analysis, vulnerability identification, and effective mitigation strategies.
2. Android Application Security: Safeguard Android apps by employing advanced analysis techniques, identifying vulnerabilities, and implementing security measures.
3. Cross Platform Threat Detection: Detect common mobile threats across both iOS and Android platforms, including malware, rootkits, and backdoors.
4. Dynamic Analysis: Execute and analyze mobile apps to uncover behavior patterns and potential malicious activities.
5. Static Analysis: Dissect mobile app binaries to expose their internal structure and reveal vulnerabilities.
6. Reverse Engineering: Employ advanced tools to reverse engineer mobile app code and identify exploitable weaknesses.
7. Behavior Profiling: Profile the actions and intents of mobile apps to identify potential security risks.
8. Advanced Threat Mitigation: Devise effective strategies for mitigating and countering complex mobile threats.
9. Vulnerability Exploitation: Demonstrate the ability to identify and exploit vulnerabilities in real world scenarios.

8kSec

$ 1199

Designed for both beginners and advanced enthusiasts, you'll learn how to reverse engineer and conduct thorough security audits of iOS and Android applications. You'll get a deeper insight into common bug categories, and detailed walkthroughs on how to exploit them. Learn how tools like Ghidra, Frida, LLDB, and more can be used to assist you during Mobile application assessments, or research.

LEVEL

Beginner / Intermediate

VIDEO

23 hours - 140 videos

CERTIFICATION EXAM

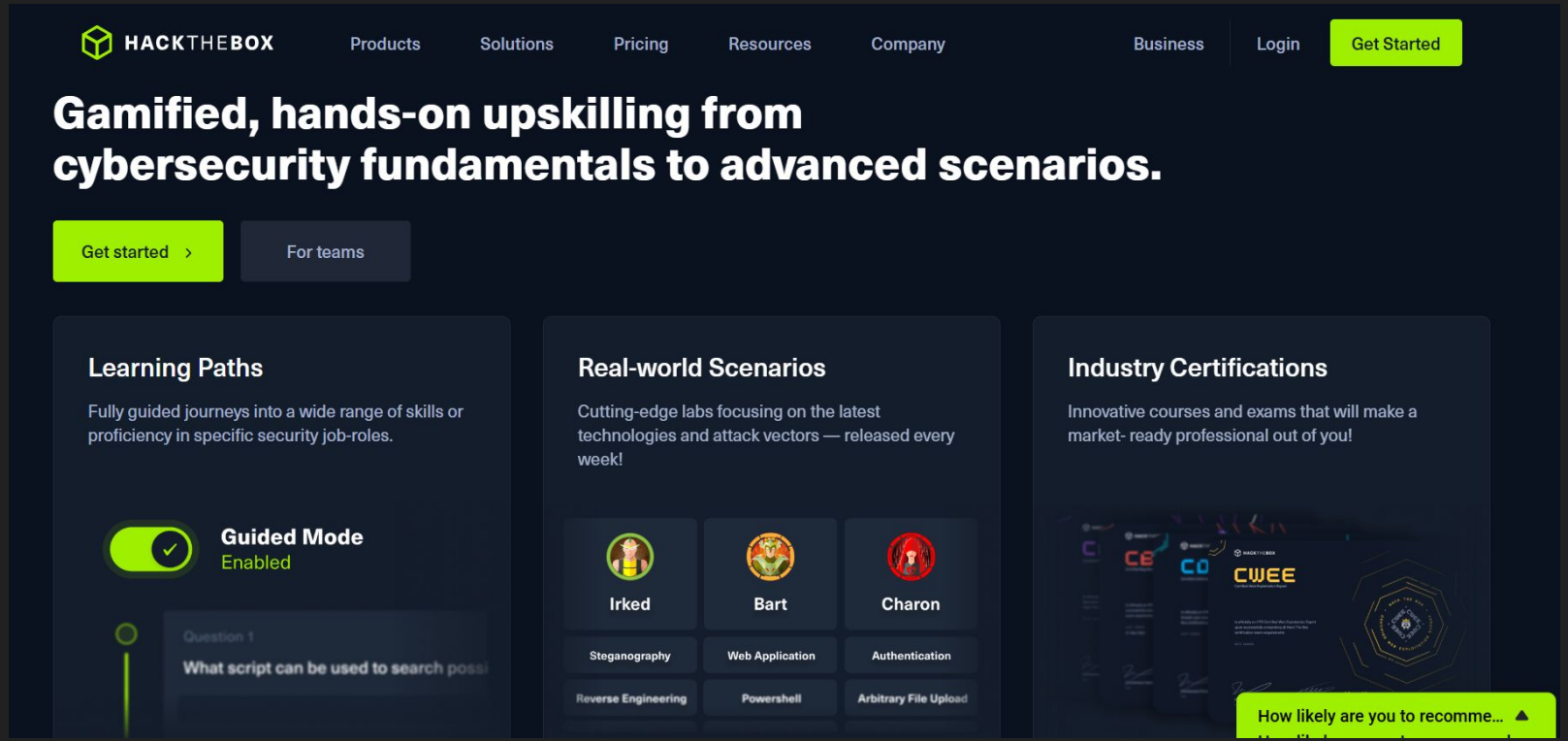
Included

A path to
CMSE certification

Enroll ~~$1,499~~ **$1,199**

See syllabus

Infra


HACKTHEBOX
Products
Solutions
Pricing
Resources
Company
Business
Login
Get Started
Gamified, hands-on upskilling from cybersecurity fundamentals to advanced scenarios.
Get started
For teams
Learning Paths
Fully guided journeys into a wide range of skills or proficiency in specific security job-roles.
Guided Mode
Enabled
Question 1
What script can be used to search possi
Real-world Scenarios
Cutting-edge labs focusing on the latest technologies and attack vectors — released every week!
Irked
Bart
Charon
Steganography
Web Application
Authentication
Reverse Engineering
Powershell
Arbitrary File Upload
Industry Certifications
Innovative courses and exams that will make a market- ready professional out of you!
CWEE
How likely are you to recomme...

HackTheBox

HTB ACCOUNT

Product Settings | User Settings | Security Settings

Welcome mx61tt,

Access the Hack The Box multiverse and develop yourself as a cybersecurity professional.

HTB Academy

Learn and get certified

Begin or advance your journey in cybersecurity with our online learning paths and earn industry certifications to prove your expertise.

Start learning

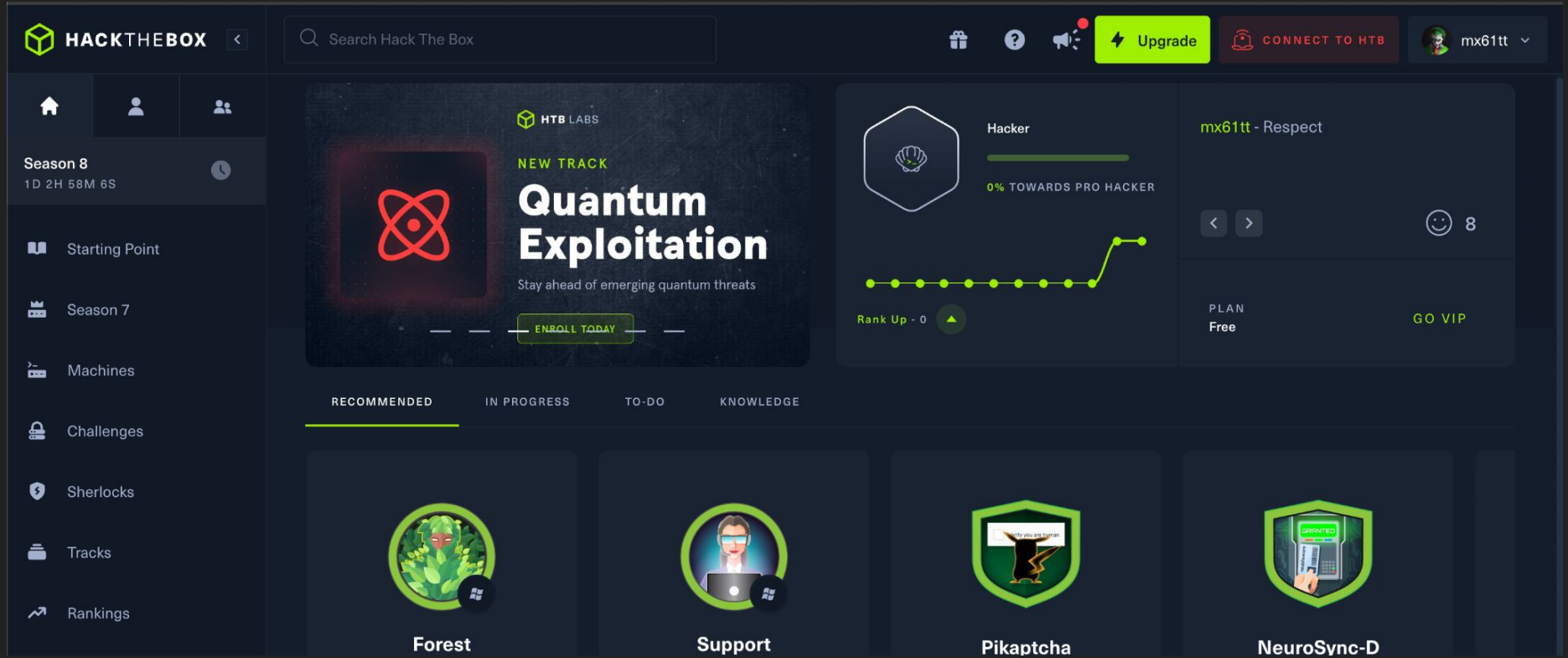
HTB Labs

Practice with hands-on Labs

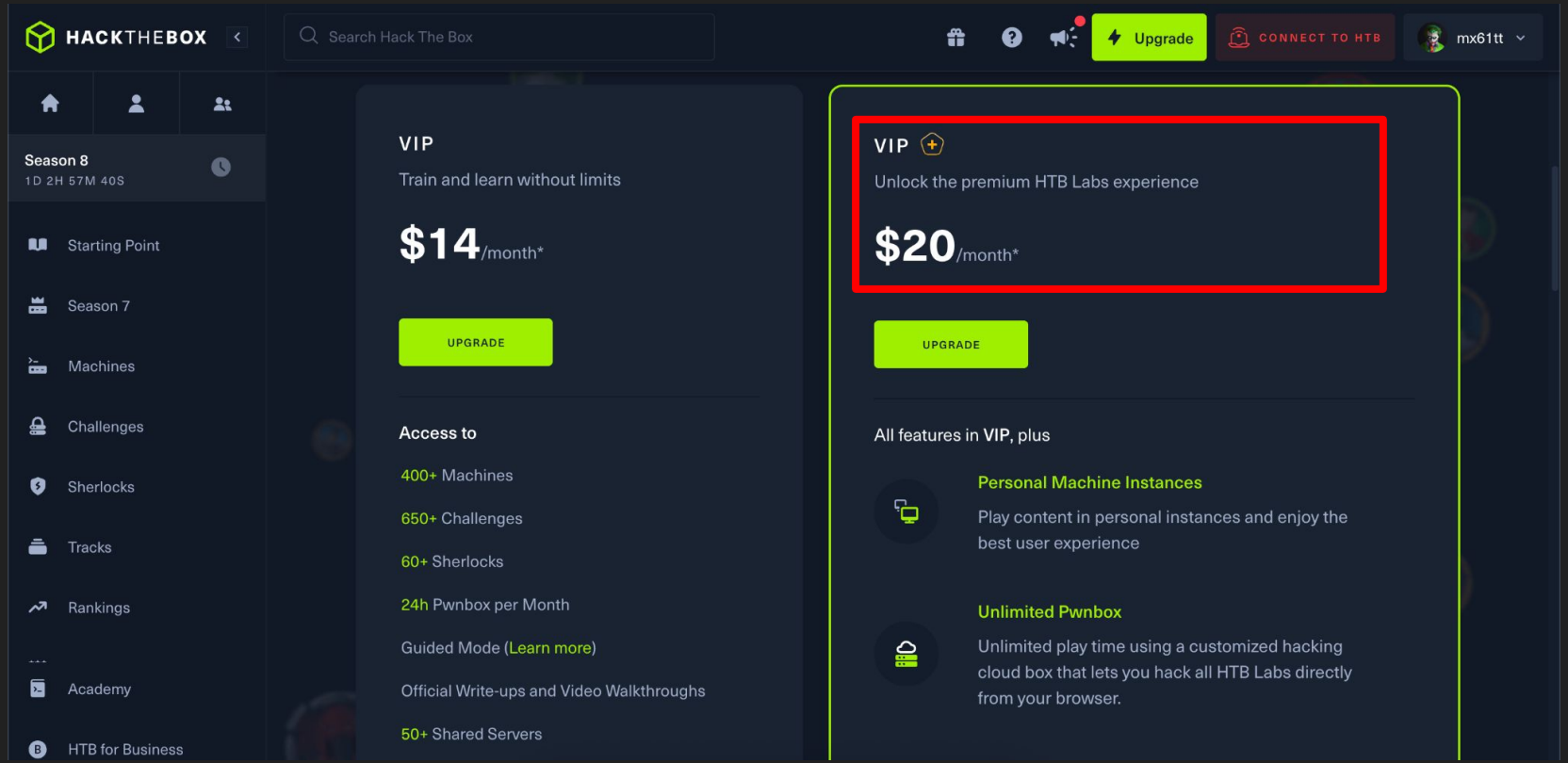
Access cybersecurity labs simulating real-world vulnerabilities, misconfigurations, and incidents. With releases every week!

Start playing

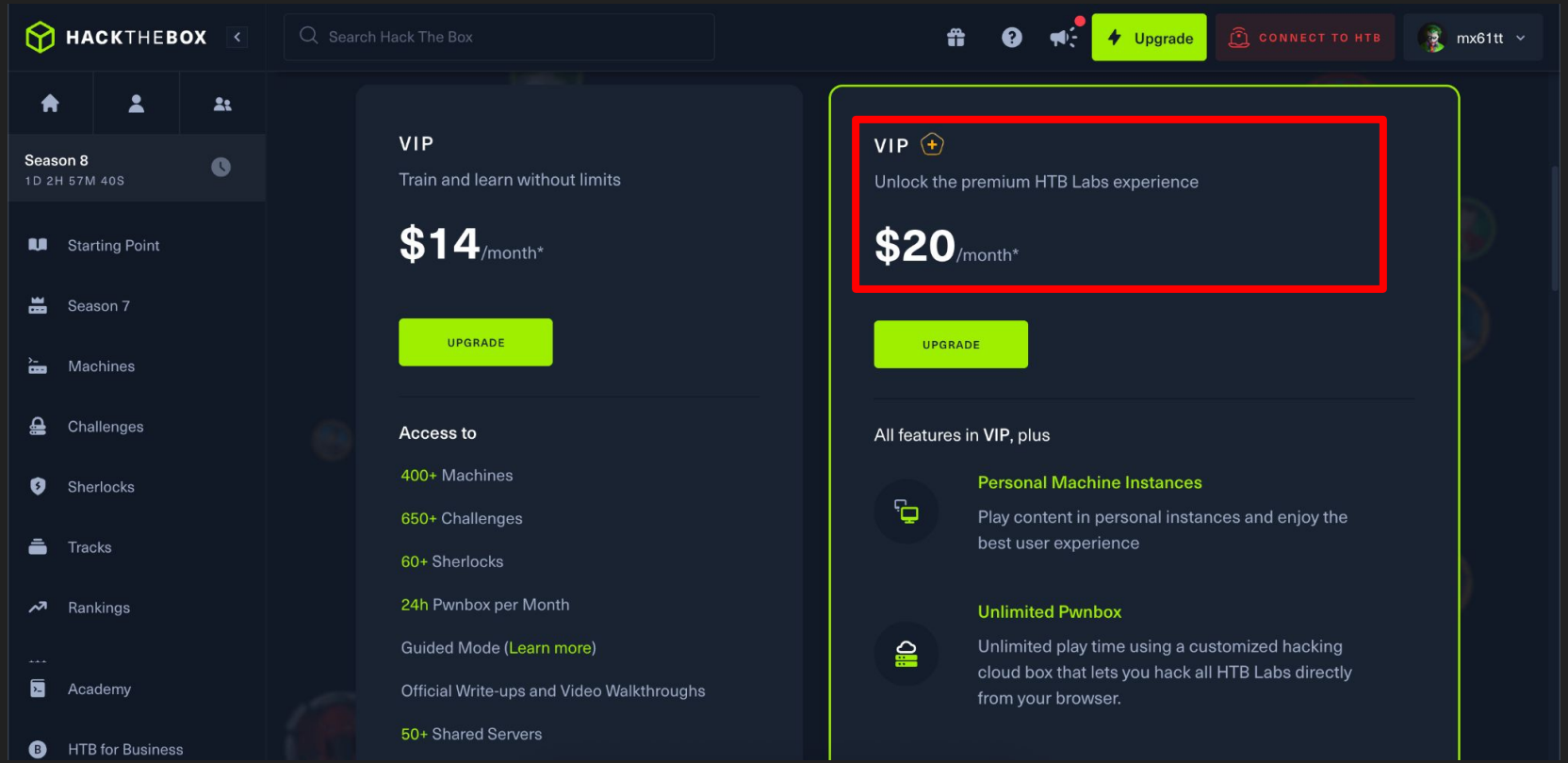
HackTheBox


HACKTHEBOX
Search Hack The Box
Upgrade
CONNECT TO HTB
mx61tt
Season 8
1D 2H 58M 6S
Starting Point
Season 7
Machines
Challenges
Sherlocks
Tracks
Rankings
HTB LABS
NEW TRACK
Quantum Exploitation
Stay ahead of emerging quantum threats
ENROLL TODAY
Hacker
0% TOWARDS PRO HACKER
mx61tt - Respect
8
Rank Up - 0
PLAN
Free
GO VIP
RECOMMENDED
IN PROGRESS
TO-DO
KNOWLEDGE
Forest
Support
Pikaptcha
NeuroSync-D

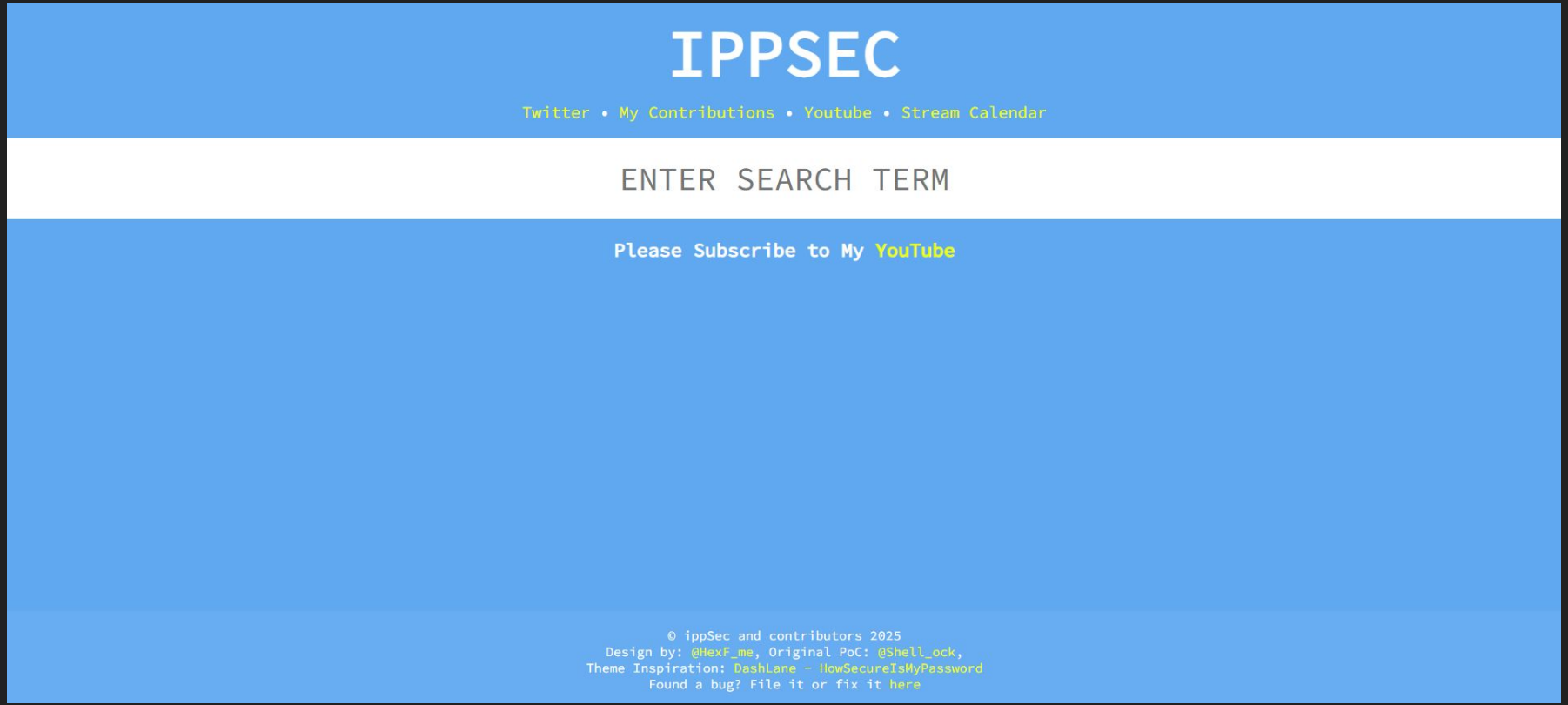
HackTheBox


HACKTHEBOX
Search Hack The Box
Upgrade
CONNECT TO HTB
mx61tt
Season 8
1D 2H 57M 40S
Starting Point
Season 7
Machines
Challenges
Sherlocks
Tracks
Rankings
Academy
HTB for Business
VIP
Train and learn without limits
$14/month*
UPGRADE
Access to
400+ Machines
650+ Challenges
60+ Sherlocks
24h Pwnbox per Month
Guided Mode (Learn more)
Official Write-ups and Video Walkthroughs
50+ Shared Servers
VIP
Unlock the premium HTB Labs experience
$20/month*
UPGRADE
All features in VIP, plus
Personal Machine Instances
Play content in personal instances and enjoy the best user experience
Unlimited Pwnbox
Unlimited play time using a customized hacking cloud box that lets you hack all HTB Labs directly from your browser.

HackTheBox


HACKTHEBOX
Search Hack The Box
Upgrade
CONNECT TO HTB
mx61tt
Season 8
1D 2H 57M 40S
Starting Point
Season 7
Machines
Challenges
Sherlocks
Tracks
Rankings
Academy
HTB for Business
VIP
Train and learn without limits
$14/month*
UPGRADE
Access to
400+ Machines
650+ Challenges
60+ Sherlocks
24h Pwnbox per Month
Guided Mode (Learn more)
Official Write-ups and Video Walkthroughs
50+ Shared Servers
VIP
Unlock the premium HTB Labs experience
$20/month*
UPGRADE
All features in VIP, plus
Personal Machine Instances
Play content in personal instances and enjoy the best user experience
Unlimited Pwnbox
Unlimited play time using a customized hacking cloud box that lets you hack all HTB Labs directly from your browser.

HackTheBox + IPPSEC



HackTheBox + IPPSEC

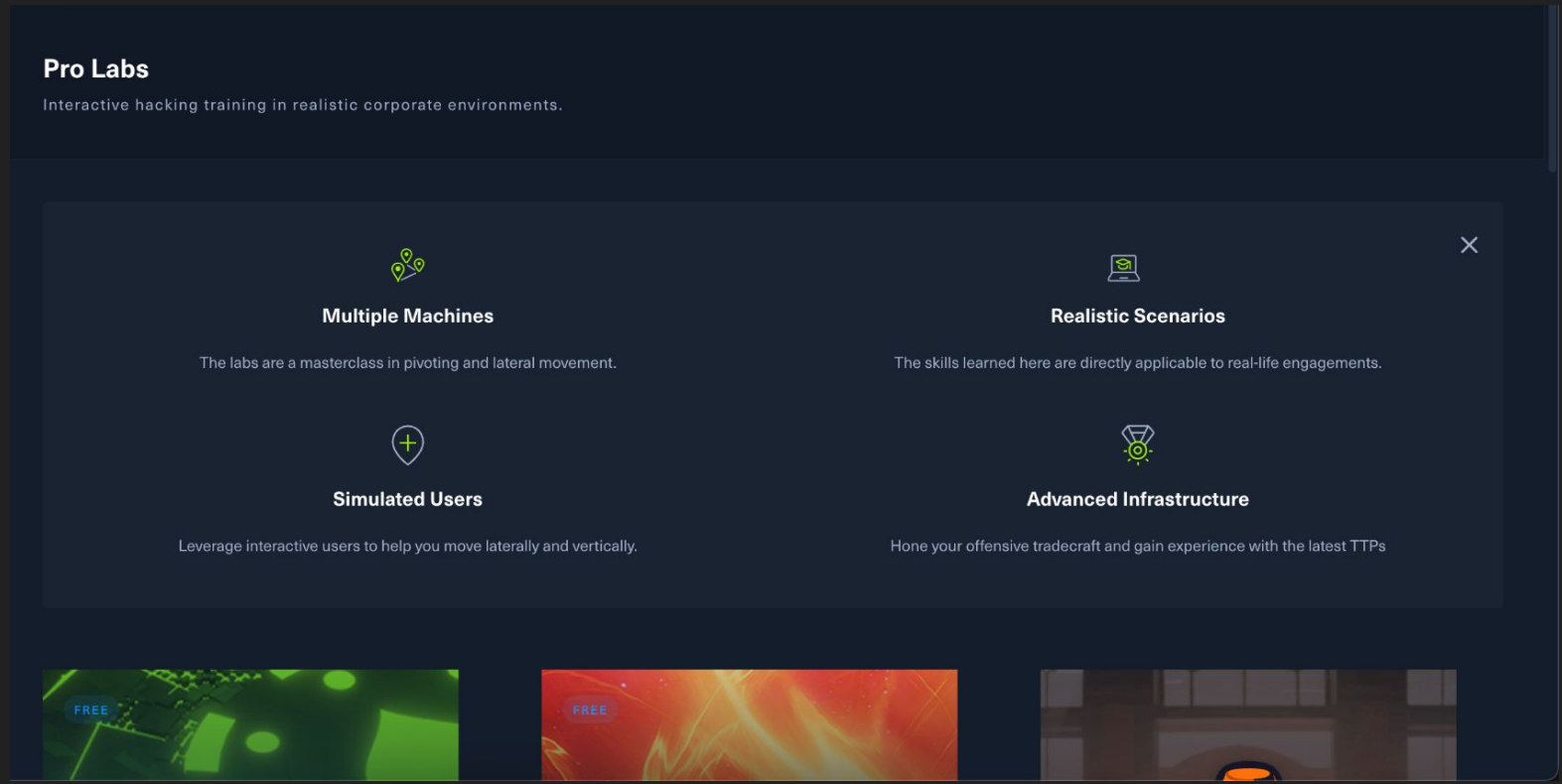
IPPSEC

Twitter • My Contributions • Youtube • Stream Calendar

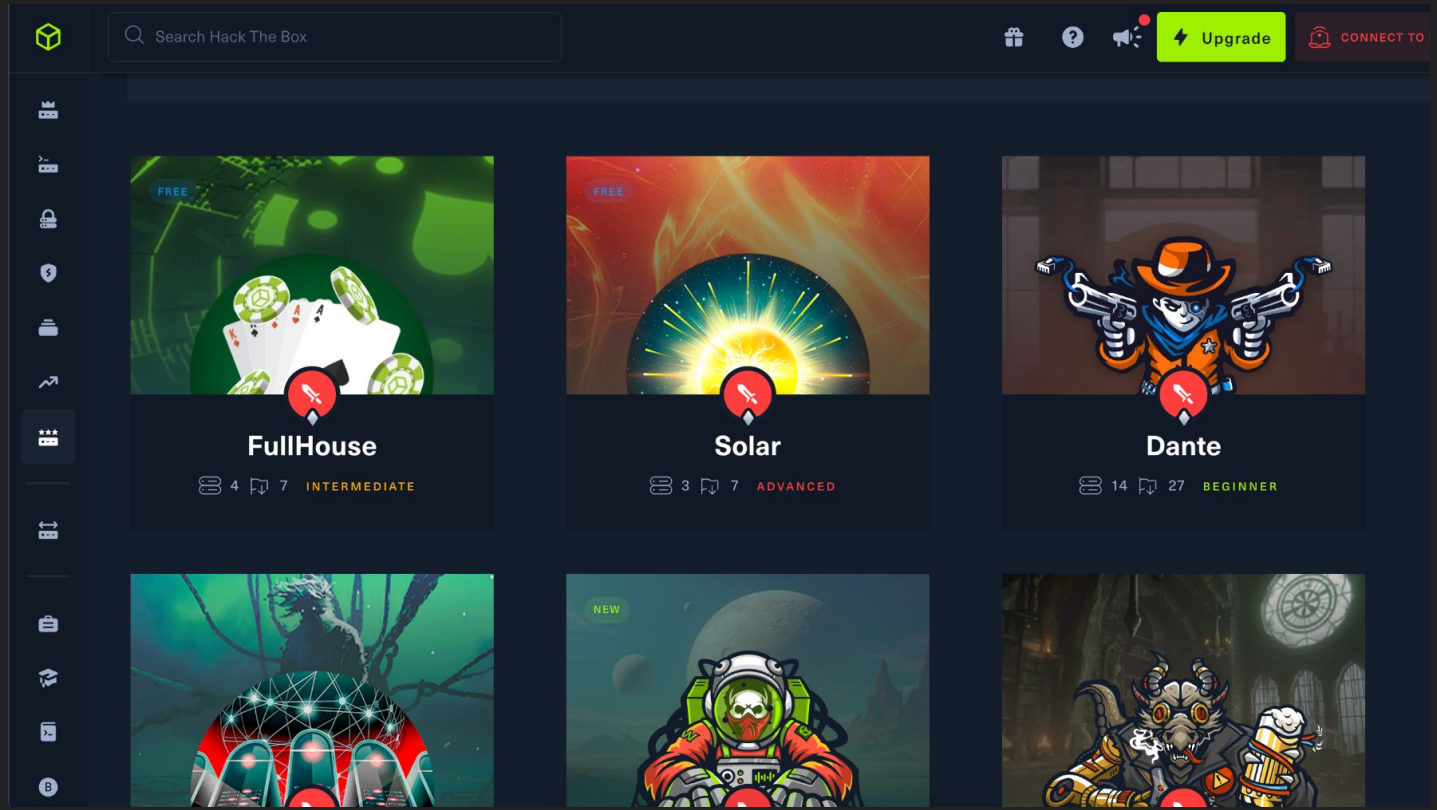
smb

Video/Course	Description
Mist	Having troubles with impacket writing to our SMB Server, writing it to the SYSVOL then copying it to the webserver
SolarLab	Discovering Guest can read files on SMB, using mount to copy all the files
Rebound	Start of nmap then checking SMB Shares
Authority	Using NetExec to search for file shares and discovering the Development share is open. Using smbclient to download everything
Gofer	Enumerating SMB to find a note which gives an email address to send a malicious document to and hints at HTTP Methods being filtered
Escape	Accessing the Public Share, downloading a PDF File and finding credentials in it, using CME again and using CME to test smb, winrm, and mssql

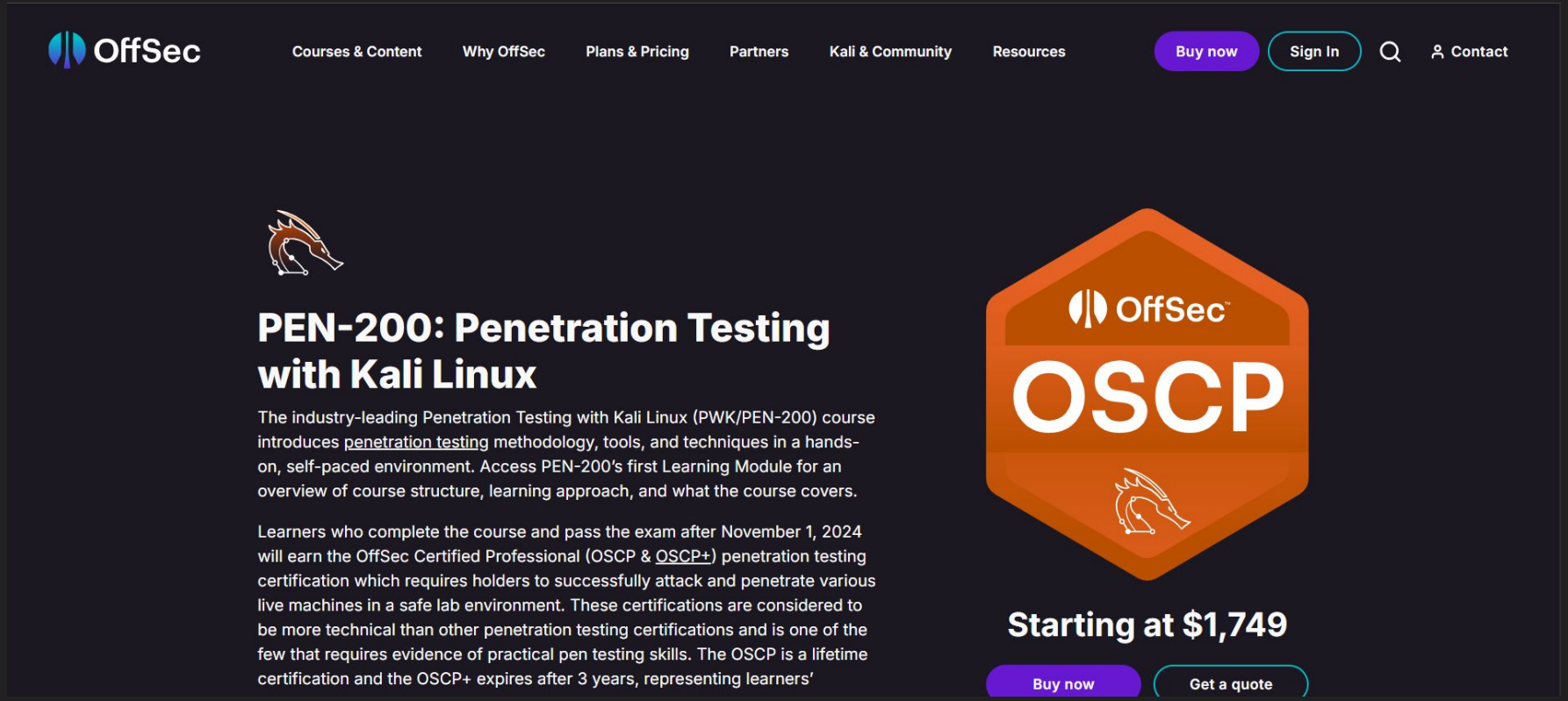
HackTheBox - Pro Labs



HackTheBox - Pro Labs



Apenas pela visibilidade



OSCP

Penetration Testing with Kali Linux Syllabus

- Introduction to Cybersecurity
- Report Writing for Penetration Testers
- Information Gathering
- Vulnerability Scanning
- Introduction to Web Applications
- Common Web Application Attacks
- SQL Injection Attacks
- Client-Side Attacks
- Locating Public Exploits
- Fixing Exploits

Red Team ou App Sec?

Red Team

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Blog | Search

ATT&CK v17 has been released! Check out the blog post for more information.

ATT&CK®

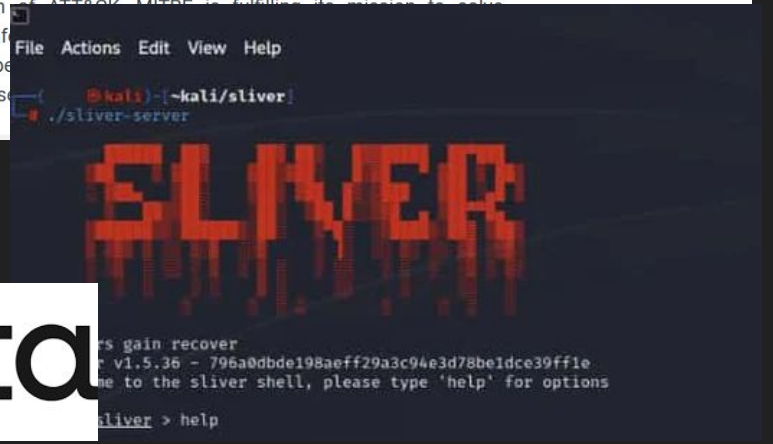
Get Started | Take a Tour

Contribute | Blog

FAQ | Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

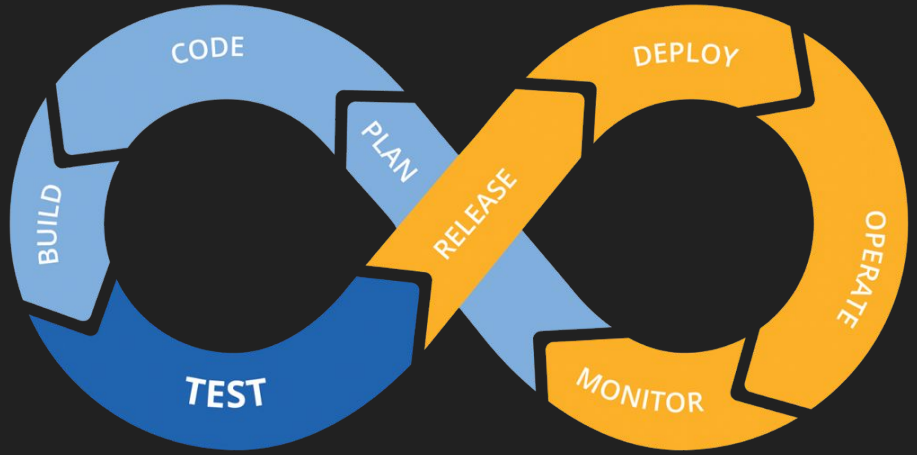
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safe... more effective cybe... organization for use...

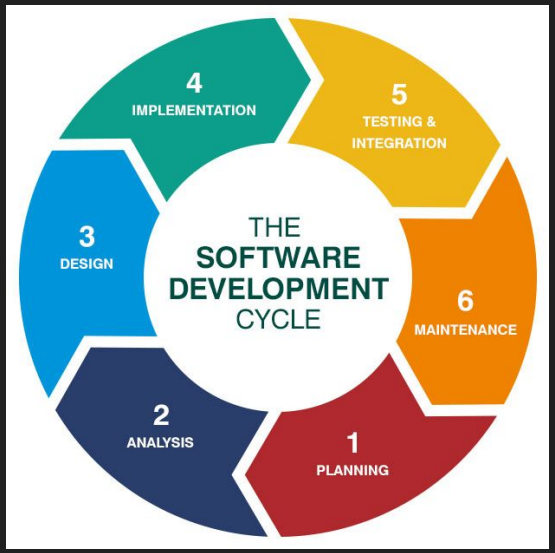


Microsoft Active Directory

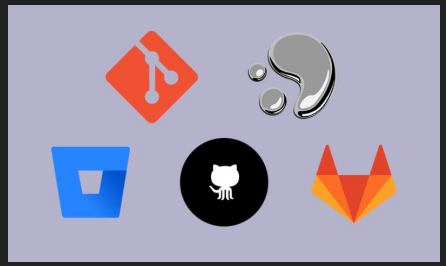
okta

App Sec

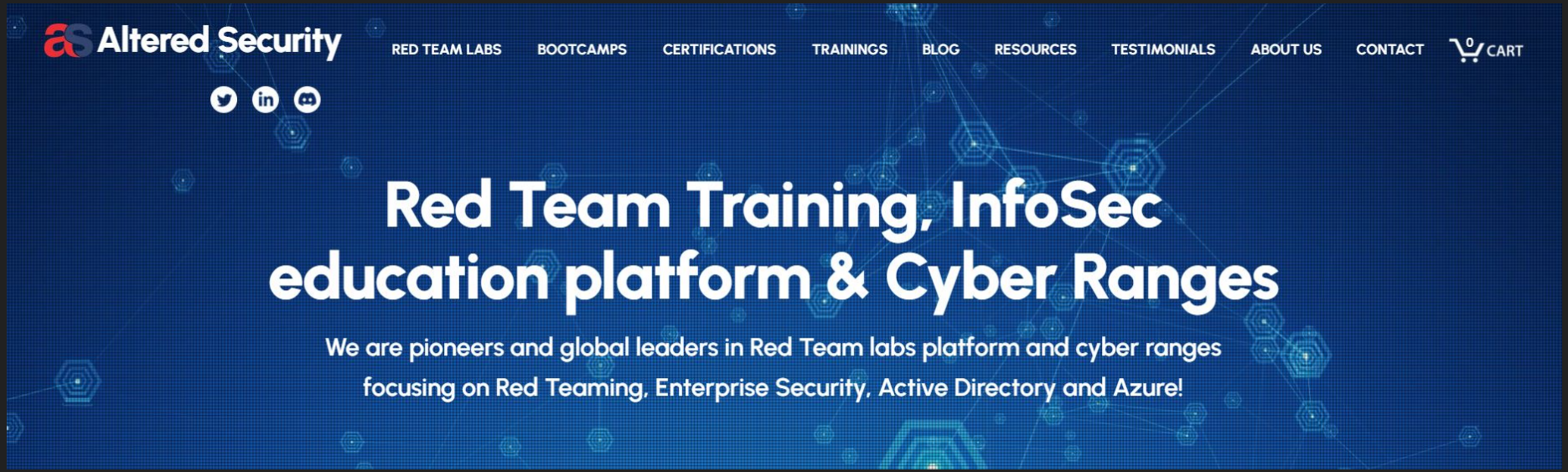




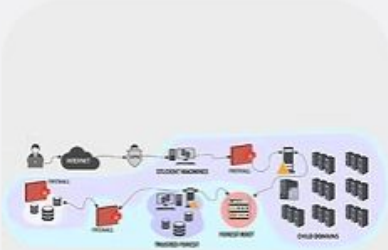
sonarqube



Red Team


Altered Security
RED TEAM LABS
BOOTCAMPS
CERTIFICATIONS
TRAININGS
BLOG
RESOURCES
TESTIMONIALS
ABOUT US
CONTACT
0 CART
Red Team Training, InfoSec education platform & Cyber Ranges
We are pioneers and global leaders in Red Team labs platform and cyber ranges focusing on Red Teaming, Enterprise Security, Active Directory and Azure!

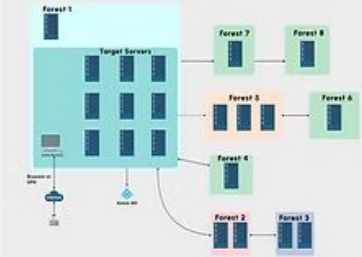
Altered Security - Trilha



Attacking & Defending Active Directory Lab

Earn the CRTP Certification

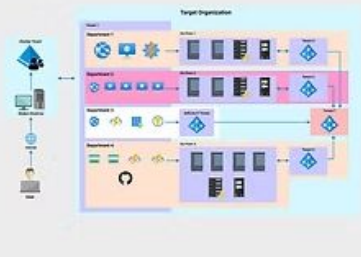
Check Now



Advanced Red Team Lab

Earn the CRTE Certification

Check Now

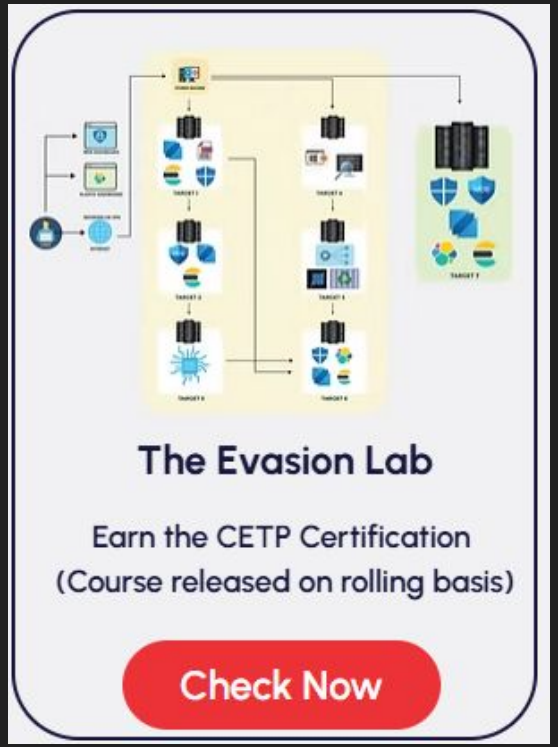


Cloud Red Team Tactics for Attacking & Defending Azure - Beginners

Earn the CARTP Certification

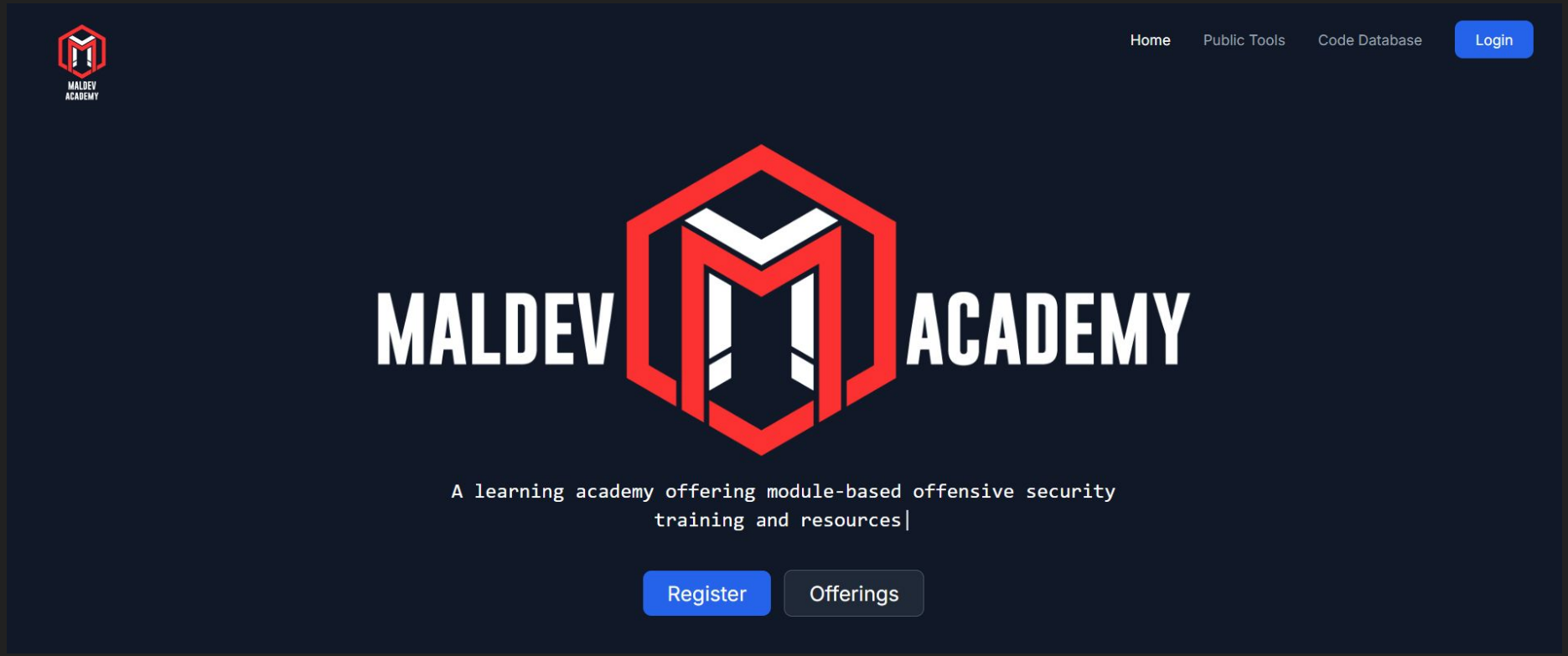
Check Now

Altered Security - Trilha



Altered Security - CRTP

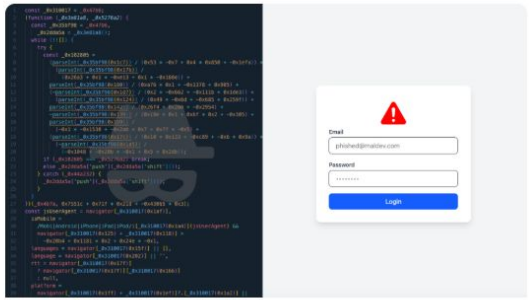
Malware Dev


MALDEV ACADEMY
Home
Public Tools
Code Database
Login
MALDEV ACADEMY
A learning academy offering module-based offensive security training and resources
Register
Offerings

MalwareDev

Maldev Academy Offerings

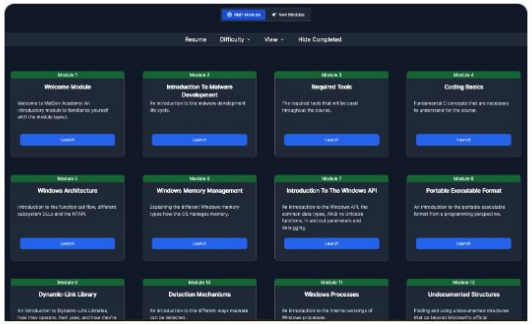
Courses & services we offer to cyber security professionals



Offensive Phishing Operations Course

A continuously updated module-based phishing operations course with over 80 learning modules.

More Info | Pricing | FAQ



Malware Development Course

A continuously updated module-based malware development course with over 195 learning modules and challenges.

More Info | Pricing | FAQ

Malware Development Database

Maldev Academy Database is a continuously growing database of malware code snippets.

More Info | Pricing | FAQ

Malware Development Course

Lifetime

Lifetime access to the malware development course

$499 USD

- ✓ Course access for life
- ✓ Access & download course code
- ✓ Access to module objectives
- ✓ Access to course challenges
- ✓ Occasional course updates
- ✓ Access to new course modules
- ✗ Malware development database access for life

Get started

Bundle

Lifetime access to the malware development course and database

$699 USD

- ✓ Course access for life
- ✓ Access & download module code
- ✓ Access to module objectives
- ✓ Access to course challenges
- ✓ Occasional updates
- ✓ Access to new modules
- ✓ Malware development database access for life

Get started

Pavel

Windows Internals and Programming

Windows Internals

$390 or 4 monthly payments of $99

COM Programming 1

Course • 58 Lessons • Discord access

COM provides an abstraction and supporting runtime for creating component-based systems, leveraging loose coupling and independence of

$99

COM Programming 2

Course • 36 Lessons • Discord access

Continuing from where "COM Programming 1" left off, this course teaches COM automation, EXE Servers, and COM Threading and Apartments.

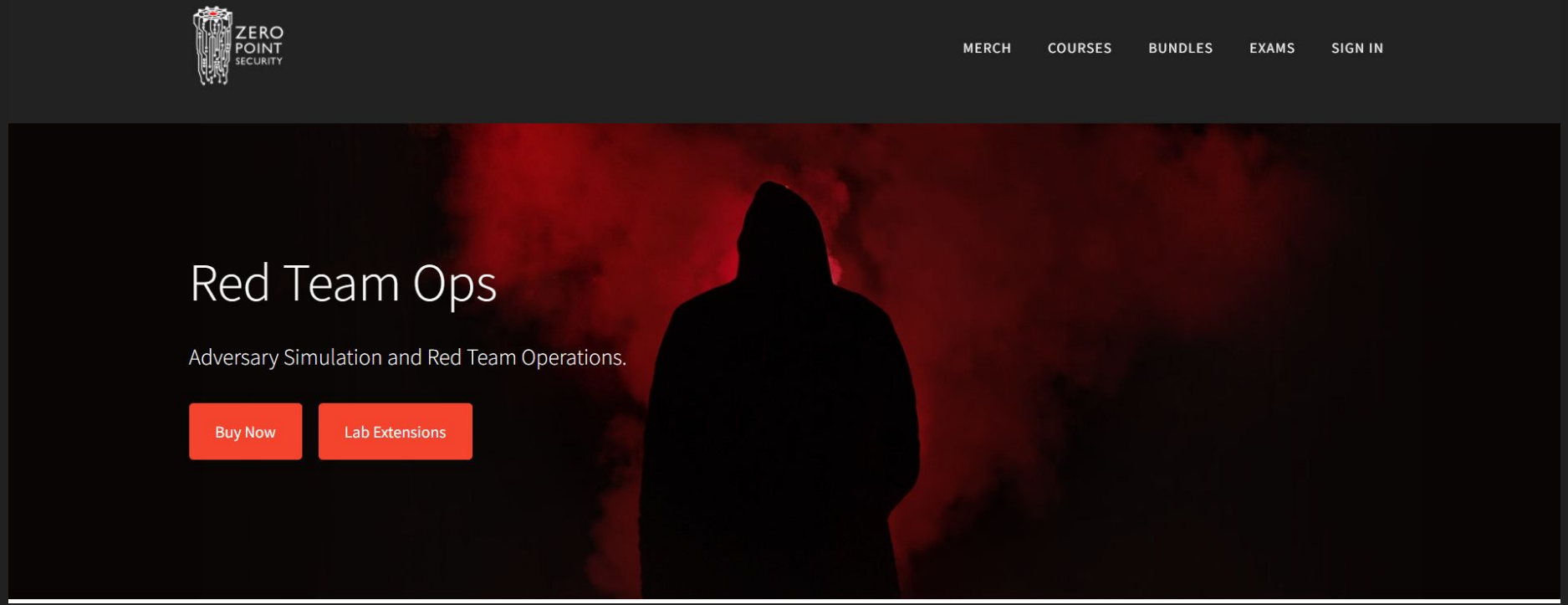
$890 or 6 monthly payments of $150

Malware Analysis and Development

Course • 106 Lessons • Discord access

Learn advanced analysis techniques from real-world malware and harness this knowledge to craft your own malware, understanding attacker strategies.

Apenas para visibilidade



CRTO

ZERO POINT SECURITY

MERCH COURSES BUNDLES EXAMS SIGN IN

- Getting Started
- Command & Control
- External Reconnaissance
- Initial Compromise
- Host Reconnaissance
- Host Persistence

Show more

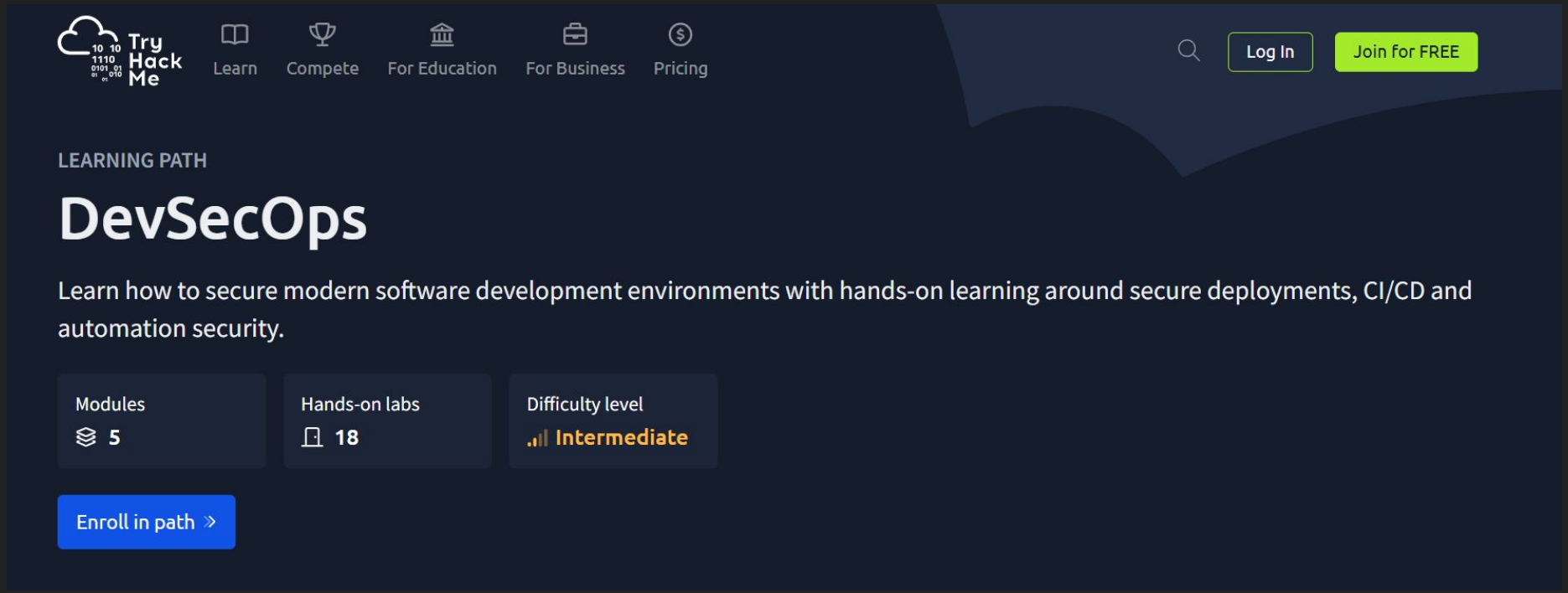
About this course

£365.00

180 lessons

2 hours of video content

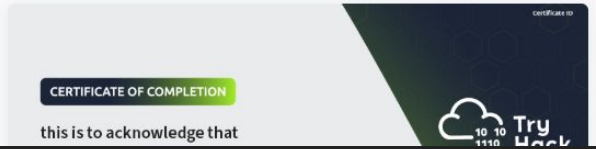
App Sec


Try Hack Me
Learn
Compete
For Education
For Business
Pricing
Log In
Join for FREE
LEARNING PATH
DevSecOps
Learn how to secure modern software development environments with hands-on learning around secure deployments, CI/CD and automation security.
Modules
5
Hands-on labs
18
Difficulty level
Intermediate
Enroll in path

TryHackMe

Acquire specialization in DevSecOps or broaden your understanding of product security.

- Hands-on CI/CD Pipeline Security
- Introduction to Securing IaC
- Containerisation Security
- Applications of DevSecOps Frameworks



Introduction

TryHackMe's DevSecOps Learning Path focuses on securing pipelines and introducing Infrastructure as Code (IaC) and Containerisation security techniques. You'll learn the tools and practices to ensure robust development processes and secure software deployment workflows. From fortifying pipelines to automating infrastructure management, you will gain practical insights into modern DevSecOps methodologies.

SECTION 1

Secure Software Development

 Introduction to DevSecOps

 SDLC

 SSDLC

SECTION 2

Security Of The Pipeline

TryHackMe

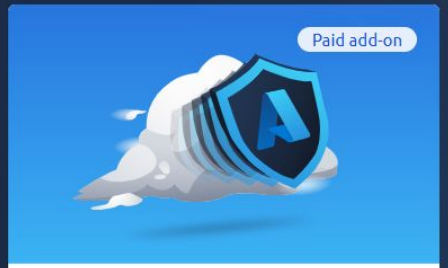
Cloud training

Get hands-on experience with Amazon Web Services (AWS) and Microsoft Azure. Learn how attackers target and exploit cloud environments, and explore the mitigation strategies to prevent security breaches.

Buy Cloud License

What's included

- Full access to AWS & Azure learning paths
- Sandboxed Cloud environments
- Azure security tooling and KQL
- Identity and Access Management
- AWS privilege escalation & security misconfiguration



Defending Azure

Master Azure security with hands-on exercises covering Azure-native security tooling.

Intermediate

Attacking and Defending AWS

Learn how attackers compromise AWS environments.

Intermediate

GitLab University - Free

GitLab | University

All Content Topics Private Training Public Training Certificati

GitLab Security Essentials

In today's software landscape, ensuring application security is critical. This course focuses on using GitLab to integrate security practices into the development lifecycle. By understanding the importance of these practices, exploring GitLab's security and governance features, and learning to effectively implement them, you will be equipped to create and manage secure, high-quality applications that protect end-users and your organization.

Course Details

GitLab University - Free

Learning Objectives

Upon completion of this self-paced course, learners will be able to:

- Describe why security needs to be incorporated into the software development lifecycle and the role GitLab plays in facilitating this process.
- Explain how GitLab's security and governance features are organized, and where they fit in the SDLC.
- Configure and use Static Application Security Testing (SAST) to identify vulnerabilities in source code.
- Implement Secret Detection to identify and prevent accidental expose of sensitive data in the codebase.
- Set up and execute Dynamic Application Security Testing (DAST) to discover and remediate potential vulnerabilities in running applications.
- Use Dependency Scanning to identify and manage vulnerabilities in project dependencies and third-party libraries.
- Configure and perform Container Scanning to detect security vulnerabilities in Docker images and container environments.
- Implement License Compliance to ensure software licenses are properly managed and tracked throughout the development process.
- Execute and interpret Fuzz testing results to identify problems in application code that may be missed by traditional testing methods.

GitLab University - Free

Learning Objectives

Upon completion of this self-paced course, learners will be able to:

- Describe why security needs to be incorporated into the software development lifecycle and the role GitLab plays in facilitating this process.
- Explain how GitLab's security and governance features are organized, and where they fit in the SDLC.
- Configure and use Static Application Security Testing (SAST) to identify vulnerabilities in source code.
- Implement Secret Detection to identify and prevent accidental expose of sensitive data in the codebase.
- Set up and execute Dynamic Application Security Testing (DAST) to discover and remediate potential vulnerabilities in running applications.
- Use Dependency Scanning to identify and manage vulnerabilities in project dependencies and third-party libraries.
- Configure and perform Container Scanning to detect security vulnerabilities in Docker images and container environments.
- Implement License Compliance to ensure software licenses are properly managed and tracked throughout the development process.
- Execute and interpret Fuzz testing results to identify problems in application code that may be missed by traditional testing methods.

Pwned Labs


PWNED LABS
Sign in
Sign up
Real-World Cloud Security Labs
Go from Zero to Hero with our byte-sized content.
aws
GET PWNING!

OSWE

OffSec Courses & Content Why OffSec Plans & Pricing Partners Kali & Community Resources Buy now Sign In Contact

WEB-300: Advanced Web Attacks and Exploitation

OffSec's Advanced Web Attacks and Exploitation (WEB-300) course dives deep into the latest web application penetration testing methodologies and techniques. Learners gain extensive hands-on experience in a self-paced environment, designed to elevate their skills in ethical hacking, vulnerability discovery, and exploit development.

Successful completion of the online training course and challenging exam earns the OffSec Web Expert (OSWE) certification. This web application security certification validates expertise in advanced web application security testing, including bypassing defenses and crafting custom exploits to address critical vulnerabilities, making certified professionals an asset for securing any organization against web-based threats.

Starting at $1,749

Buy now Get a quote

API Sec University

Our Courses

APIsec University courses provide actionable, hands-on training to help you keep APIs secure.

API Penetration Testing

Learn how to hack APIs like a professional penetration tester and find vulnerabilities.

Advanced **Free**

API Security Fundamentals

If you're new to API security, this is the place to start. Learn about the OWASP API Top 10, real-world API breaches and more.

Foundation **Free**

OWASP API Top 10 & Beyond!

Build your API security foundation with a strong understanding of the OWASP API Top 10.

Foundation **Free**

Adicionais

Desenvolvimento de Exploits – 32 bits extended

Aprenda do zero ao avançado as técnicas de exploração de vulnerabilidades através de Buffer Overflow em Windows e Linux, como de sobrescrever os dados do registrador EIP, da estrutura de SEH, construção de backdoors em aplicação legítima, ocultação de código malicioso, Egghunter e muito mais.

Dificuldade
● ● ● ○ ○

Carga horária
40 horas

Disponibilidade
Gravado para download

Idioma
Português

Próximas turmas

Disponibilidade:	Imediata
Metodologia:	Gravado
Investimento:	R$ 529,00

Inscreva-se aqui

Sobre o treinamento | **Habilidades** | **Requisitos**

Versão gravada e ampliada do treinamento de Desenvolvimento de Exploits. Este treinamento é destinado aos profissionais da segurança da informação que desejam aprimorar seus conhecimentos em testes de invasão, conhecendo a fundo o processo de criação e desenvolvimento de Exploit com Buffer Overflow.

Durante o treinamento serão abordados temas avançados de segurança ofensiva como exploração de vulnerabilidades através de Buffer Overflow em Windows e Linux, com algumas das principais técnicas do mercado como de sobrescrever os dados do registrador EIP, da estrutura de SEH, construção de backdoors em aplicação legítima, ocultação de código malicioso, Egghunter, criação

Programa de estudos

1. Introdução a arquitetura de computadores
2. Introdução a linguagem assembly
3. Principais instruções assembly
4. Introdução ao Buffer Overflow

Considerações Finais