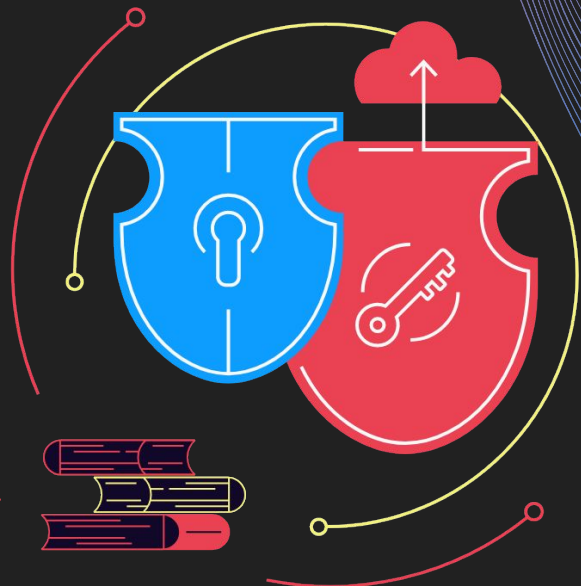




**Next-gen cybersecurity hands-on
learning for students and
infosec professionals**



Cybercrime | Data loss | Cyberattacks

Supply chain attacks grew **420% in just 12 months**

Almost **90% of web applications are vulnerable to exploits**

1 attack happens **every 40 seconds**

Roughly **1 million new pieces of malware** are made each day

280 days on average to contain a data breach in 2020



Cybercrime is on the rise, both operations and impact: by 2025, the number of **ransomware attacks will increase by 700%**

Attack **tactics are more sophisticated** while user behavior and IT personnel isn't changing towards a proper cyber hygiene

Cybersecurity professionals need **more hands-on training** to identify new methods and approaches to counteract these threats

The **unemployment rate in cybersecurity has been 0** since 2011 and every year the shortage deepens



Who are we?



Florina Avadanei

Co-founder and CEO

More than 12 years of experience in marketing, communication and project management. Active in the cybersecurity industry since 8 years, founded Ladies in Cybersecurity - an initiative that encourages women to choose a career in cybersecurity.



Andrei Avadanei

Co-founder and CTO

More than a decade working in tech and cybersecurity. Founded DefCamp in 2011 and was nominated in Forbes 30Under30 and in New Europe 100 for results during his career.



Meet the Co-founders

Introducing CyberEDU



The **special secure environment that leverages cyber-range-as-a-service technology.**

It offers individuals the possibility to reach the next level of mastery in ethical hacking, offensive or defensive cybersecurity.

Nov 2019

First line of code

Apr 2020

Soft launch

Sept 2020

Accepted in Impact EdTech
Programme stage 1 & 2
5k registered users

Mar 2022

over 60 competitions
10k registered users

Mar 2023

new features release: create your own competition, better stats & reporting
over 50 available training courses
over 15k registered users

How it began

- Organising cybersecurity competitions since 2011
- Organising DefCamp - largest cyber security conference from CEE
- Technical coordinators and coaches for the European Cyber Security Challenge in 2019



Important milestones

- validation of product for companies and academias
- accelerated in the European Impact EDEch Accelerator program - stage 1 and stage 2
- selected in Orange Fab Accelerator
- over 80 international competitions and activities organized or hosted on the platform
- 15k+ registered users
- over 50 available training courses
- successful initiatives: UNbreakable Romania, Caucasus University pilot, Romanian Cyber Security Challenge
- awarded as the Education Program of the Year with UNbreakable Romania by ANIS Romania in 2022



CyberEDU is...

- a **safe cybersecurity practice and learning space** that serves the worldwide ethical hacking community
- a **software-as-a-service** with no installation of further setup requirements needed
- a **way to "learn by doing" in a variety of classes**: digital forensics, penetration testing, threat intelligence, threat hunting, security monitoring, web security
- an **"always on" place to practice cybersecurity** through hundreds of practical exercises based on real life scenarios, mapped against industry standards
- a **competitive environment** where you assess your current level of knowledge and learn to move on to the next level

On CyberEDU, you can...

3y+

- access 350+ labs, exercises and training sessions on cybersecurity topics
- participate in CTF competitions
- join large scale challenges based on complex infrastructures
- join attack / user / network traffic simulations and tabletop exercises
- join Attack / Defense competitions: Red vs Blue, Blue only, Red only, Purple
- create your own CTF competition
- launch cloud-based or on-premise, on-demand, hands-on cybersecurity labs
- manage unlimited number of cyber enthusiasts in private spaces
- screen talent and track performance in a gamified environment
- upload your own challenge stack
- review challenges
- upload write-ups for current challenges
- certify acquired knowledge with a diploma

CyberEDU is developed for...

COMPANIES

- improve your security team's performance and collaboration
- build and test your team's cybersecurity skills

UNIVERSITIES, SCHOOLS, COLLEGES AND TRAINING INSTITUTES

- enrich your student's curriculum with practical cybersecurity labs to let them gain real practical experience
- you stay up-to-date with the latest developments in cybersecurity

INDIVIDUALS

- keep your skills and mind sharp
- get creative for emerging cyber risks and threats

Our ambition



To be an **active booster in increasing and improving cybersecurity skills worldwide**, by providing a safe space for people **to learn and practice cybersecurity skills using real-world inspired scenarios.**

Partners & Customers of CyberEDU



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



... and more than 150 universities, high schools and organisations

User view of the OWASP skills taxonomy



MITRE ATT&CK® CWET™ OWASP WSTG

OWASP WSTG

The Web Security Testing Guide (WSTG) [Project](#) produces the premier cybersecurity testing resource for web application developers and security professionals. The framework below shows your progress through the mapped labs and techniques against OWASP WSTG.

Your progress



Information Gathering	Configuration and Deploy Management Testing	Identity Management Testing	Authentication Testing	Authorization Testing	Session Management Testing	Data Validation Testing	Error Handling	Cryptography	Business logic Testing	Client Side Testing	API Testing
WSTG-INFO-01: Conduct Search Engine Discovery Reconnaissance for Information Leakage	WSTG-CONF-01: Test Network Infrastructure Configuration	WSTG-IDNT-01: Test Role Definitions	WSTG-ATHN-01: Testing for Credentials Transported over an Encrypted Channel	WSTG-ATHZ-01: Testing Directory Traversal File Include	WSTG-SESS-01: Testing for Session Management Schema	WSTG-INPV-01: Testing for reflected Cross Site Scripting	WSTG-ERRH-01: Testing for Improper Error Handling	WSTG-CRYP-01: Testing for Weak Transport Layer Security	WSTG-BUSL-01: Test Business Logic Data Validation	WSTG-CLNT-01: Testing for DOM-Based Cross Site Scripting	WSTG-APIT-01: Testing GraphQL
WSTG-INFO-02: Fingerprint Web Server	WSTG-CONF-02: Test Application Platform Configuration	WSTG-IDNT-02: Test User Registration Process	WSTG-ATHN-02: Testing for Default Credentials	WSTG-ATHZ-02: Testing for Bypassing Authorization Schema	WSTG-SESS-02: Testing for Cookies Attributes	WSTG-INPV-02: Testing for Stored Cross Site Scripting	WSTG-ERRH-02: Testing for Stack Traces	WSTG-CRYP-02: Testing for Padding Oracle	WSTG-BUSL-02: Test Ability to Forge Requests	WSTG-CLNT-02: Testing for JavaScript Execution	
WSTG-INFO-03: Review Webserver Metafiles for Information Leakage	WSTG-CONF-03: Test File Extensions Handling for Sensitive Information	WSTG-IDNT-03: Test Account Provisioning Process	WSTG-ATHN-03: Testing for Weak Lock Out Mechanism	WSTG-ATHZ-03: Testing for Privilege Escalation	WSTG-SESS-03: Testing for Session Fixation	WSTG-INPV-03: Testing for HTTP Verb Tampering		WSTG-CRYP-03: Testing for Sensitive Information sent via Unencrypted Channels	WSTG-BUSL-03: Test Integrity Checks	WSTG-CLNT-03: Testing for HTML Injection	
WSTG-INFO-04: Enumerate Applications on Webserver	WSTG-CONF-04: Review Old Backup and Unreferenced Files for Sensitive Information	WSTG-IDNT-04: Testing for Account Enumeration and Guessable User Account	WSTG-ATHN-04: Testing for Bypassing Authentication Schema	WSTG-ATHZ-04: Testing for Insecure Direct Object References	WSTG-SESS-04: Testing for Exposed Session Variables	WSTG-INPV-04: Testing for HTTP Parameter Pollution		WSTG-CRYP-04: Testing for Weak Encryption	WSTG-BUSL-04: Test for Process Timing	WSTG-CLNT-04: Testing for Client Side URL Redirect	
WSTG-INFO-05: Review Webpage Content for Information Leakage	WSTG-CONF-05: Enumerate Infrastructure and Application Admin Interfaces	WSTG-IDNT-05: Testing for Weak or unenforced username policy	WSTG-ATHN-05: Testing for Vulnerable Remember Password		WSTG-SESS-05: Testing for Cross Site Request Forgery	WSTG-INPV-05: Testing for SQL Injection			WSTG-BUSL-05: Test Number of Times a Function Can be Used Limits	WSTG-CLNT-05: Testing for CS Injection	
WSTG-INFO-06: Identify application entry points	WSTG-CONF-06: Test HTTP Methods		WSTG-ATHN-06: Testing for Browser Cache Weaknesses		WSTG-SESS-06: Testing for Logout Functionality	WSTG-INPV-06: Testing for LDAP Injection			WSTG-BUSL-06: Testing for the Circumvention of Work Flows	WSTG-CLNT-06: Testing for Client Side Resource Manipulation	
WSTG-INFO-07: Map execution paths through application	WSTG-CONF-07: Test HTTP Strict Transport Security		WSTG-ATHN-07: Testing for Weak Password Policy		WSTG-SESS-07: Testing Session Timeout	WSTG-INPV-07: Testing for XML Injection			WSTG-BUSL-07: Test Defenses Against Application Mis-use	WSTG-CLNT-07: Test Cross Origin Resource Sharing	
WSTG-INFO-08: Fingerprint Web Application Framework	WSTG-CONF-08: Test RIA cross domain policy		WSTG-ATHN-08: Testing for Weak Security Question Answer		WSTG-SESS-08: Testing for Session Puzzling	WSTG-INPV-08: Testing for SSI Injection			WSTG-BUSL-08: Test Upload of Unexpected File Types	WSTG-CLNT-08: Testing for Cross Site Flashing	
WSTG-INFO-09: Fingerprint Web Application	WSTG-CONF-09: Test File Permission		WSTG-ATHN-09: Testing for Weak Password Change or Reset Functionalities		WSTG-SESS-09: Testing for Session Hijacking	WSTG-INPV-09: Testing for XPath Injection			WSTG-BUSL-09: Test Upload of Malicious Files	WSTG-CLNT-09: Testing for Clickjacking	
WSTG-INFO-10: Map Application Architecture	WSTG-CONF-10: Test for Subdomain Takeover		WSTG-ATHN-10: Testing for Weaker Authentication in Alternative Channel			WSTG-INPV-10: Testing for IMAP SMTP Injection				WSTG-CLNT-10: Testing WebSockets	
	WSTG-CONF-11: Test Cloud Storage					WSTG-INPV-11: Testing for Code Injection				WSTG-CLNT-11: Test Web Messaging	

Organize exams, events and competitions

Cyber Security Competitions & Hacking Tournaments

Grow your offensive and defensive skills by competing in our exciting hacking & Capture the Flag competitions. Contact us if you plan to organize a corporate event, a competition in your University or your Highschool. You can design your own challenges or you can let us manage your event.

Upcoming / Live (1) Past events (31) My events (44) [CREATE EVENT](#)



Campionatul European de Securitate Cibernetică

ROCSC 2022 - Qualification

Start date: 2022-07-22 09:00:00 UTC
End date: 2022-07-23 19:00:00 UTC
210 players joined

ENDED INDIVIDUAL MODE JEOPARDY 50



UNbreakable Romania

UNbreakable Romania Echipa - Editia 2022

Start date: 2022-05-20 09:00:00 UTC
End date: 2022-05-22 09:00:00 UTC
82 teams joined

ENDED TEAM MODE JEOPARDY 50



UNbreakable Romania

UNbreakable Romania Individual - Editia 2022

Start date: 2022-05-06 09:00:00 UTC
End date: 2022-05-08 09:00:00 UTC
793 players joined

ENDED INDIVIDUAL MODE JEOPARDY 50



UNbreakable Romania

UNbreakable Romania Bootcamp - Editia 2022

Start date: 2022-04-04 00:00:00 UTC
End date: 2022-05-31 00:00:00 UTC
792 players joined

ENDED INDIVIDUAL MODE JEOPARDY 25



Brasov CyberARENA Contest #1

Start date: 2022-02-04 09:00:00 UTC
End date: 2022-02-06 15:00:00 UTC
61 players joined

ENDED INDIVIDUAL MODE JEOPARDY 10



UNbreakable Romania

UNbreakable Romania Echipa - Editia 2021 S2

Start date: 2021-12-10 14:00:00 UTC
End date: 2021-12-12 14:00:00 UTC
70 teams joined

ENDED TEAM MODE JEOPARDY 50



Brasov CyberARENA

Start date: 2021-12-08 23:59:00 UTC
End date: 2022-02-03 00:00:00 UTC
59 players joined

ENDED INDIVIDUAL MODE JEOPARDY 10



DefCamp HV 2021 - Defend the Castle

Start date: 2021-12-06 09:00:00 UTC
End date: 2021-12-15 09:00:00 UTC
31 players joined

ENDED INDIVIDUAL MODE JEOPARDY 10

Host hands-on trainings

cyber
EDU

Bit-Sentinel

RulesReport a bugFAQLogout

Main

Trainings, Workshops & Career Paths

Grow your offensive and defensive skills by competing in our exciting hacking & Capture the Flag competitions. Contact us if you plan to organize a corporate event, a competition in your University or your Highschool. You can design your own challenges or you can let us manage your event.

Search


Q

STATUS

Not started

DIFFICULTY

Beginner




Cybersecurity is easy when you write "TOP SECRET" on everything.

Introducere in securitate cibernetica

"Securitatea cibernetica" este o preocupare majora in domeniul informatic si este esentiala pentru [...]

Progress 0%

[FREE](#) [9 HOURS](#) [9 MODULES](#) [NOT STARTED](#)




Linux

Introducere in Linux

Este important sa cunoastem Linux, deoarece ne ofera o alternativa la sistemele de operare comercial [...]

Progress 0%

[FREE](#) [3 HOURS](#) [3 MODULES](#) [NOT STARTED](#)




PYTHON PROGRAMMERS
PYTHON PROGRAMMERS
EVERYWHERE

Introducere in Python

Exista mai multe motive pentru care este important sa cunoastem Python in securitatea cibernetica [...]

Progress 0%

[FREE](#) [7 HOURS](#) [7 MODULES](#) [NOT STARTED](#)




DON'T HAVE TO WORRY ABOUT PRIV ESC
IF ALL USERS HAVE ROOT ACCESS

Introducere in Securitatea si Exploatarea Vulnerabilitatilor in Aplicatii Web

Securitatea aplicatiilor web este o preocupare majora in domeniul informatic si este esentiala pentru [...]

Progress 0%

[FREE](#) [3 HOURS](#) [3 MODULES](#) [NOT STARTED](#)




NO ENCRYPTION?

Introducere in Criptografie si Algoritmi de Criptare, Encodare sau Hashing

Algoritmi de criptare sunt indispensabili cand vine vorba despre protejarea informatiilor confiden [...]

Progress 0%

[FREE](#) [19 HOURS](#) [19 MODULES](#) [NOT STARTED](#)




EVIDENCE?

Introducere in Analiza Capturilor de Date, Trafic de Rețea, Memorie sau Hard Disk (forensica)

Criminalistica digitala reprezinta un proces important deoarece infractionalitatea si activitatea [...]

Progress 0%

[FREE](#) [1 HOURS](#) [1 MODULES](#) [NOT STARTED](#)



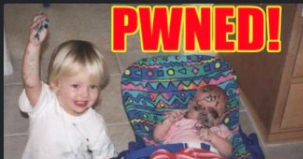
REVERSE ENGINEER

Introducere in Inginerie Inversa pentru aplicatii executabile, scripturi sau documente

Identificarea vulnerabilitatilor de securitate; ingineria inversa poate fi folosita pentru a identifica [...]

Progress 0%

[FREE](#) [17 HOURS](#) [17 MODULES](#) [NOT STARTED](#)



PWNED!


Introducere in exploatarea aplicatiilor binare

Exploatarea binara functioneaza pe principiul transformarii unei vulnerabilitati existente intr-un [...]

Progress 0%

[FREE](#) [1 HOURS](#) [1 MODULES](#) [NOT STARTED](#)


Training example



Bit-Sentinel

Main

Personal



Cybersecurity is easy when you write "TOP SECRET" on everything.

Introducere in securitate cibernetica

Progress0%

FREE

9 HOURS

9 MODULES

IN PROGRESS

Skills in this course

MITRE ATT&CK®

7

Common Weakness Enumeration: CWE™

6

Introducere in securitate cibernetica

Overview

Course

Performance

Overview

Securitatea cibernetică este o preocupare majoră în domeniul informatic și este esențială pentru protejarea datelor utilizatorilor și a sistemelor informatice în general.

În prezentul nostru, serviciile digitalizate sunt folosite tot mai des pentru a oferi suport și a interacționa cu utilizatorii, iar securitatea acestora devine o prioritate absolută.

Acest curs oferă participanților cunoștințele de bază ce sunt necesare pentru a începe o cariera în securitate cibernetică și pentru participarea la concursurile de tip CTF.

Objectives

- Învățați despre principalele obiective ale securității cibernetice
- Învățați cum să vă pregătiți pentru concursurile de tip CTF

Recommended skillset

- Competențe de analiză
- Competențe de configurare a unei stații de lucru
- Competențe de identificare și analiză a activităților rău intenționate

Track students performance

SOC Analyst - Level 2

Progress: 0%

START COURSE

Skills in this course

- OWASP Web Security Testing Guide (WSTG)
- MITRE ATT&CK
- Common Weakness Enumeration (CWE)

2,510 points **27%**

Skills Completion Rate(%)

- 80.2% - 1136/Expectation for Privilege Escalation
- 50.2% - 1136/Expectation for Privilege Escalation
- 50.2% - 1136/Expectation for Privilege Escalation

Common Weakness Enumeration (CWE)

Skills Completion Rate(%)

- 100% - WSTG-AT&CK-06: Testing for Cross Site Request Forgery

ROCSC 2022 - Qualification

Friday, July 22, 2022 at 9:00 AM UTC Saturday, July 23, 2022 at 1:00 PM UTC

Statistics

- Total Participants: 210
- Participants with Positive Score: 97
- Total Tasks: 23
- Total Categories: 9
- Most Popular Category: Forensics (77 solved)
- Least Popular Category: Reverse Engineering (35 solved)
- Most Popular Task: weird-noise (77 solved)
- Least Popular Task: cryptofun (1 solved)

Solved by Category

Category	Solved
Network 101	100%
Forensics	77%
Reverse Engineering	35%
Other	0%

Solved by Difficulty

Donut chart showing solved tasks by difficulty: Easy (blue), Medium (orange), Hard (red), Insane (green).

ROCSC 2022 - Qualification

Leaderboard

Rank	Participant	Points	Solved	Top 3	Final Score	Weight	Accuracy	Category
1	Youssef Alkhatib	1136	30/30	1st	100%	100%	100%	Junior
2	Ali	1136	30/30	2nd	100%	100%	100%	Senior
3	Youssef Alkhatib	1136	30/30	3rd	100%	100%	100%	Senior
4	Ali	1136	30/30	4th	100%	100%	100%	Junior
5	Ali	1136	30/30	5th	100%	100%	100%	Junior
6	Ali	1136	30/30	6th	100%	100%	100%	Junior
7	Ali	1136	30/30	7th	100%	100%	100%	Senior
8	Ali	1136	30/30	8th	100%	100%	100%	Senior
9	Ali	1136	30/30	9th	100%	100%	100%	Senior
10	Ali	1136	30/30	10th	100%	100%	100%	Senior

KALI IN BROWSER INSTANCE

Open Kali Desktop

Extend 1 hour

Open Kali SSH

Destroy Instance

USE CASE - Develop a national program for students



the end-to-end cybersecurity educational program for high schools and university students from Romania.

Through its activities, UNbreakable provides an x-ray and visualisation of the level of cybersecurity skills nationally.

Inspired by: the US The National Cyber League

An infographic titled "Why UNbreakable Romania?" presented as a scroll with five lightbulb icons at the top. It features three quotes from experts in the field.

Why UNbreakable Romania?

This competition uncovers many paths for young people, as they can practice their individual skills, but also their cooperative skills.

Anton Rog
Director for CyberInt National Centre

This type of competition is a fantastic foundation to extremely quickly accumulate knowledge and information that increases your professional value.

Dan Cimpean
DNSC Director (National Directorate for Cyber Security)

UNbreakable is a vehicle, getting you from point A to point B. Point B can be a career in cybersecurity.

Ioan Constantin
Cyber Security Expert Orange Romania

unbreakable.ro

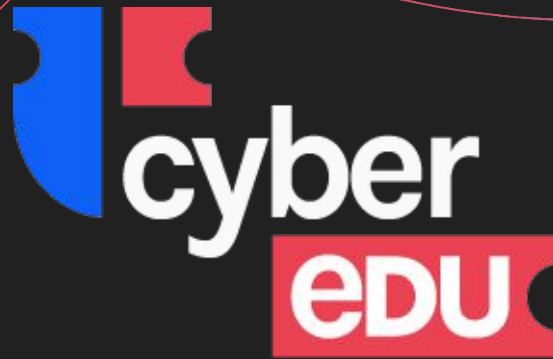
An illustration of a person with blonde hair, wearing a green shirt and black pants, sitting on a large orange question mark. The person is holding a laptop. A speech bubble is next to them.

Source: unbreakable.ro/UNR-2021-S2-RO.pdf

What we are looking for?

- Strategic partnerships
- Reselling partners (Europe, Middle East)





Florina Avadanei
CEO CyberEDU
florina@bit-sentinel.com

