

Secure your Students' Future

with CyberEDU for Universities





CyberEDU for you

Give your students a space to grow and develop their skills, with CyberEDU's industry-standard aligned cybersecurity gym. We'll create a dedicated space for you to host cybersecurity labs and practical sessions for your budding hackers.

What is CyberEDU

CyberEDU's mission is to increase and improve cybersecurity skills worldwide, by providing a space for people to learn, and practice cybersecurity skills using real-world inspired exercises and challenges.

CyberEDU caters to novices, experts, and everyone in between, with our "Beginner to Pro" capability skilling, suitable for individuals and companies around the world. For schools, colleges, training institutes and universities, we enrich the traditional cybersecurity curricula, by providing a "gym" with hundreds of exercises for your students to build and test their skills.

We uniquely bridge the gap between cybersecurity theory and practice through:



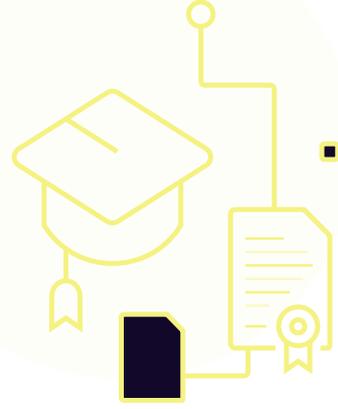
- an always growing content library of cybersecurity exercises and challenges mapped against internationally-recognised industry standards;
- our highly-engaging gamified user experience, replicating real-world scenarios; and
- our AI-driven personalized training and career path advice, tailored to our users' needs and skills.

Who are we

We are a team of dedicated infosec professionals who have been creating educational cybersecurity content and running competitions for the last decade. Our team has over 30 years experience in cybersecurity, and our core belief is that education and knowledge, honed through practice, are essential to building world-class cybersecurity expertise. We've discovered that our hands-on approach to applying cybersecurity skills is highly effective for learning, and we're building CyberEDU based on this discovery.

We hold the most prestigious professional certificates in the field, and as a team we are committed to continually increasing our own expertise -- so that we can pass our knowledge along to you!

Why choose CyberEDU for your students?



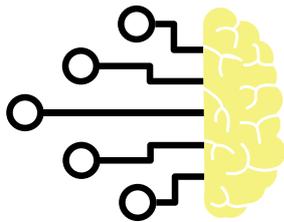
Build reputation

Reputation matters. Students are looking for universities and teaching institutions that have the edge in cybersecurity.

Students expect effective learning journeys, based on real life situations. Position your course, and your university as a top generator of highly-skilled future cybersecurity experts and host cybersecurity competitions to test and assess student performance.

Make an impact

Increase student engagement and retention with realistic hands-on cyber scenarios that sharpen individual skills while cultivating critical thinking, and encouraging collaborative team play.

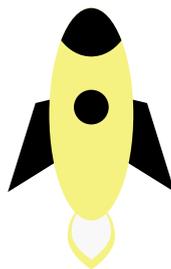


Learning flexibility

Have an “always on” cybersecurity practice playground for your students. The learning journey for students can be tailored as the CyberEDU platform provides access 24/7 with technical support on demand.

Enriched curricula

Bridge the gap between cybersecurity theory and practice, and document student mastery of industry standards, with ease. CyberEDU provides you with fresh content on a regular basis together with write-ups and other support materials.



Cost effective

A subscription for CyberEDU will be cost effective compared to building your own practice playground. CyberEDU supports your teaching curricula with fresh content based on real life scenarios to explain concepts for your students.



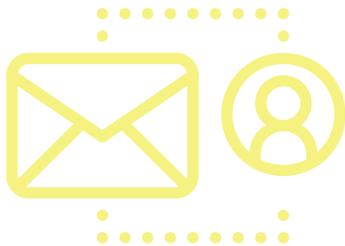
Note: For advanced activities, we can host red team - blue team scenarios to teach students how to identify misconfigurations and coverage gaps in existing security products.

Cyber security labs and exercises available on CyberEDU include topics like ethical hacking, biometrics, forensics, steganography, intelligence systems, mobile system security, smart grid security, PWN and reverse engineering.

All scenarios are based on real life situations with strong ties to industry leaders with a proven track record for actively touching base with all these in their daily activity.

Let's have a talk!

For a conversation about how CyberEDU can become part of your course, please send an email to:



Florina DUMITRACHE

Project Manager

CyberEDU

florina@bit-sentinel.com



Contact us

Phone: +40 755 751 544

Email: contact@cyberedu.ro



Snapshots from the platform

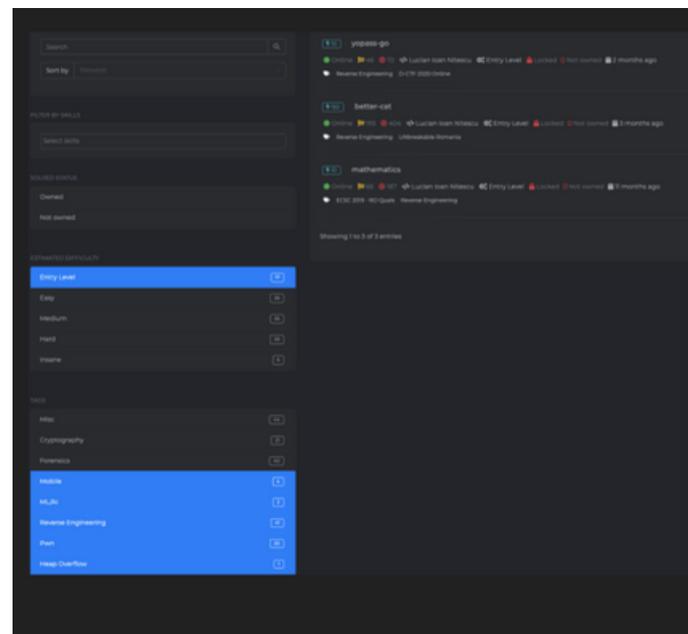
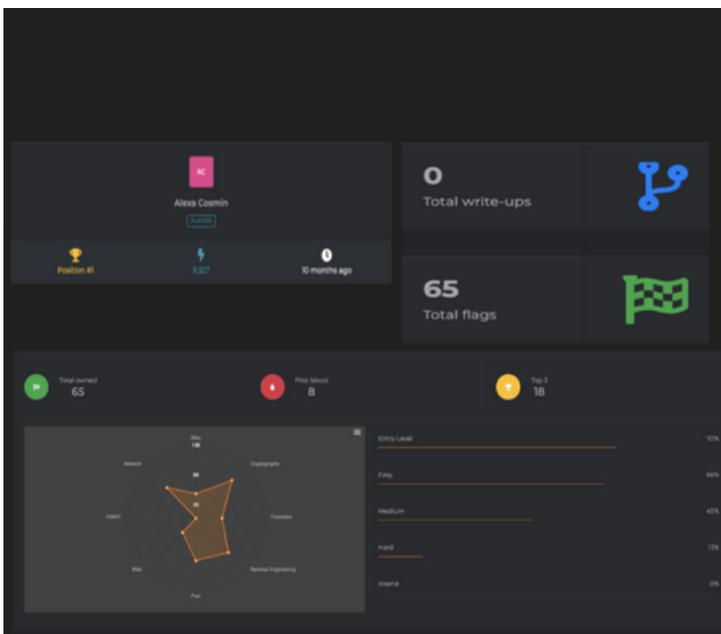
MITRE ATT&CK® CWE™ OWASP WSTG

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: 0% 100%

Information Gathering	Configuration and Deploy Management Testing	Identity Management Testing	Authentication Testing	Authorization Testing	Session Management Testing	Data Validation Testing	Error Handling
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-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-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-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-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-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-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-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 Puddling	WSTG-INPV-08: Testing for SSI Injection	
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-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-CONF-11: Test Cloud					WSTG-INPV-11: Testing for	



See more on: <https://cyberedu.ro>