



Buletin informativ

August 2026

Scenarii de învățare bazate pe provocări pentru studii în laborator și integrare în programul de studiu

Învățarea bazată pe provocări oferă un cadru eficient și eficace pentru învățare, rezolvând în același timp provocări din lumea reală. Poate fi utilizată de fiecare parte interesată din școală pentru a dezvolta planificare strategică, a conecta practicile actuale, a consolida asumarea responsabilității și personalizarea și a crea persoane care învață pe tot parcursul vieții. În loc să concureze cu alte abordări, aceasta urmărește să stabilească conexiuni și să ajute toate părțile interesate să co-creeze experiența de învățare.

Obiectivul general al CYBERCHALLENGE este de a crește disponibilitatea conținutului digital, a tehnologiilor și a practicilor prin dezvoltarea unui curriculum de cibersecuritate, inclusiv un Laborator Federativ de Cibersecuritate bazat pe un sandbox de instrumente și utilizând o metodologie CBL.

Unul dintre principalele obiective ale proiectului este de a stimula practici inovatoare de învățare și predare pentru a spori motivația elevilor, gândirea critică și abilitățile de rezolvare a problemelor. În acest sens, proiectul implică, de asemenea, adăugarea unor scenarii CBL la programele de învățământ dezvoltate.

CBL în studiile universitare nu este doar o altă metodă de predare - este o schimbare în filosofia studiilor, de la acumularea de cunoștințe teoretice la crearea de efecte reale.

CBL este o parte integrantă a modului de studiu, procesul de studiu fiind transformat de la „ascultare și îndeplinire a sarcinilor” la „cercetare, rezolvare și implementare”. Integrarea CBL transformă modulul de studiu nu într-un set static de cunoștințe, ci într-un ecosistem dinamic. La nivel de master, un astfel de model este extrem de eficient, deoarece simulează un mediu profesional real, în care un expert trebuie nu doar să „știe”, ci și să „acționeze” în fața incertitudinii. Modelul dezvoltat al modului de studiu cu integrarea CBL arată cum fiecare parte se completează reciproc.

Unul dintre principalele obiective ale proiectului este stimularea practicilor inovatoare de învățare și predare pentru a spori motivația studenților, gândirea critică și abilitățile de rezolvare a problemelor. În acest sens, proiectul implică și adăugarea unor scenarii CBL la programele de învățământ dezvoltate.

În timpul implementării proiectului, au fost create patru scenarii CBL, câte unul pentru fiecare modul: Fundamentele securității cibernetice, Managementul identității și accesului, Atacuri cibernetice și apărări cibernetice și Managementul securității cibernetice.

Fundamentele securității cibernetice: Securitatea sistemelor de casă inteligentă

Ideea principală: Securitatea sistemelor de casă inteligentă.

Provocarea principală (Problema specifică): Problemele de securitate din sistemele de casă inteligentă sunt adesea legate de defectele de securitate din protocoalele de comunicare. Defectele de securitate la nivel de protocol sunt adesea mai sistemice și dificil de remediat pentru o persoană nespecializată.

Casele conectate oferă confort, dar introduc și riscuri semnificative de securitate. Cum putem proiecta sisteme care rămân sigure chiar dacă un atacator obține acces la rețeaua internă?

Managementul identității și accesului

Ideea principală: Propunere de proiect orientată spre provocare: „Acces și identitate securizate într-un ecosistem federat”.

Proiectați și implementați un sistem federat de autentificare și control al accesului care combină managementul identității care păstrează confidențialitatea (folosind acreditări verificabile și



CYBERCHALLENGE - Challenges Solving in Cybersecurity Study Program No. 2024-1-LT01-KA220-HED-000252504

principii de identitate descentralizate) cu mecanisme de control al accesului detaliate (delegare RBAC, ABAC și OAuth 2.0).

Studentii trebuie să simuleze un mediu real - de exemplu, o platformă de servicii digitale (cum ar fi e-Guvernare, asistență medicală sau sistem universitar) - care necesită o gestionare sigură a identității, respectând confidențialitatea, și un control al accesului bazat pe politici.

Provocarea principală (Problema specifică): Cum putem proiecta un sistem care să permită accesul securizat și verificarea identității cu respectarea confidențialității în mai multe servicii, utilizând autentificarea federativă (SSO) și autorizarea delegată (OAuth 2.0), aplicând în același timp politici de control dinamic al accesului (RBAC/ABAC)?

Subprobleme cheie:

- Gestionarea în siguranță a identităților digitale și a acreditărilor.
- Păstrarea confidențialității utilizatorilor și minimizarea expunerii la date.
- Implementarea autentificării interoperabile prin acreditări verificabile (aliniată cu eIDAS).
- Aplicarea principiilor de control al accesului (privilegiu minim, separarea sarcinilor).

Atacuri cibernetice și apărare cibernetică

Ideea principală: Îmbunătățirea infrastructurii unei companii partenere prin simularea diferitelor tipuri de

Provocarea principală (Problema specifică): Universitatea Transilvania, prin programul său de masterat în Securitate Cibernetică și în calitate de membru fondator al Brașov CyberHub, colaborează cu diverse instituții și companii pentru a îmbunătăți și promova securitatea cibernetică în rândul tuturor părților interesate. Pe baza acestui acord de parteneriat, studenții Cyberchallenge pot participa la evaluări de securitate:

Subiectul 1. Testarea rezistenței companiei la atacurile de phishing.

Subiectul 2. Verificarea rețelei instituției pentru vulnerabilități cunoscute

Subiectul 3. Evaluarea securității aplicațiilor web.

Managementul securității cibernetice

Ideea principală: Managementul riscurilor de securitate în infrastructura inteligentă, în special în sistemul de ride-hailing pentru scutere.

Provocarea principală (Problema specifică): Problemele de management al riscurilor de securitate în sistemele de ride-hailing sunt legate de proiectarea sistemului, inclusiv validarea și reprezentarea intrărilor, abuzul API, caracteristicile de securitate, managementul timpului și al stării, gestionarea erorilor, calitatea codului și preocupări similare. Conectarea componentelor sistemului și dezvoltarea unei infrastructuri inteligente sunt activități provocatoare care ar putea introduce riscuri de securitate. Provocarea constă în a anticipa aceste riscuri înainte de implementarea sistemului, a le estima și a raționa sistematic și a introduce contramăsuri pentru acestea.

PROJECT COORDINATOR



PROJECT PARTNERS



<https://www.cyberchallenge-erasmus.eu/>

Kaunas University of Technology

Faculty of Informatics

Studentu str. 50, Kaunas, Lithuania