CYBERSECURITY NATIONAL LABORATORY

Abstract
2021 Best Practice in Education Award "Cybersecurity"

Index

1. Names and addresses of the applicant or applicants

CINI Cybersecurity National Laboratory
https://cybersecnatlab.it/

2. Indication of whether the submission is on behalf of an individual or a group

The submission is on behalf of a group

3. Description of the achievements (max 5 pags)

CyberChallenge.IT is a training program for young talents that aims to significantly reduce the current shortage of the IT workforce, being the main Italian initiative aiming at identifying, attracting, recruiting and placing the next generation of IT security professionals. In the 2021 edition CyberChallenge.IT involved 4,900 of the best students in Italy and encourage them to fill the ranks of future cybersecurity professionals, thus making their skills available to the country system.
The project aims to create and grow the cyber defender community by investing in young people. In particular, it aims at:

- stimulating interesting technical-scientific subjects and, in particular, in information technology topics;
- presenting the professional opportunities offered by the training courses on information security;
- putting young people in direct contact with companies, also thanks to the challenges they will have to face;
- identifying young cyber talents and contributing to their orientation and professional training.

The program combines traditional training activities with a gamification-oriented approach that translates into participation in competitions in virtual arenas where different scenarios of networks and real work environments are simulated. The proposed model is unique on the international scene; in fact, it exploits not only gaming as an instrument for attracting young people, but offers a significant multidisciplinary training, as well. The course focuses on technical, scientific and ethical issues related to information security, alternating theoretical lectures and hands-on experiences on various topics such as cryptography, malware analysis, and web security.
The syllabus for the whole training course includes:

- Software Security:
    - Secure programming
    - Program analysis, static analysis, debugging and tracing
    - Memory management, allocation and buffer overflow
    - Format-string vulnerabilities

  - Code reuse attack: return-to-libc attack, return-oriented programming, jump-oriented programming, shellcode
  - Attack mitigations and countermeasures: stack canaries, ASLR, NX
- Cryptography:
  - Historical cyphers
  - Perfect secrecy: One-time-pad
  - Symmetric encryption and block ciphers: DES, AES, block cipher mode of operations
  - Asymmetric encryption: RSA, Diffie-Hellman
  - Key exchange protocols
  - Message authentication
  - Digital Signature
  - Hash functions and steganography
  - Random number generation
  - Protocols attack: replay attack, man-in-the-middle attack, reflection attack, type flaw attack
  - Needham-Schroeder: public key authentication protocol and shared-key protocols
  - Kerberos protocol
- Web Security:
  - HTTP protocol
  - File disclosure and path traversal attacks
  - Service-Side request forgery
  - Command and code injections
  - SQL injections vulnerabilities: union-based, blind time-based
  - Client-side security: SOP, Cross-Site Scripting, Cross-Site Request Forgery
- Network Security:
  - Network analysis and monitoring
  - Strategies and policies for securing internet communications
- Access Control:
  - Access control principles, DAC, MAC, ACL
  - UNIX file permission
  - Privilege escalation
  - Race conditions
- Hardware Security:

- Hardware-based Security
- Hardware vulnerabilities
- Hardware Trojan
- Hardware attacks exploiting Test infrastructures
- IoT security

During the fifth editions of the CyberChallenge.IT project we acquired a significant expertise in challenge development, both for training and for final competitions, as outlined in the sequel:
Challenges developed for Training:

- Cyberchallenge.IT 2020 – National training – 80 challenges
- CyberChallenge.IT 2021 - National training – 84 challenges

Challenges developed for final competitions:

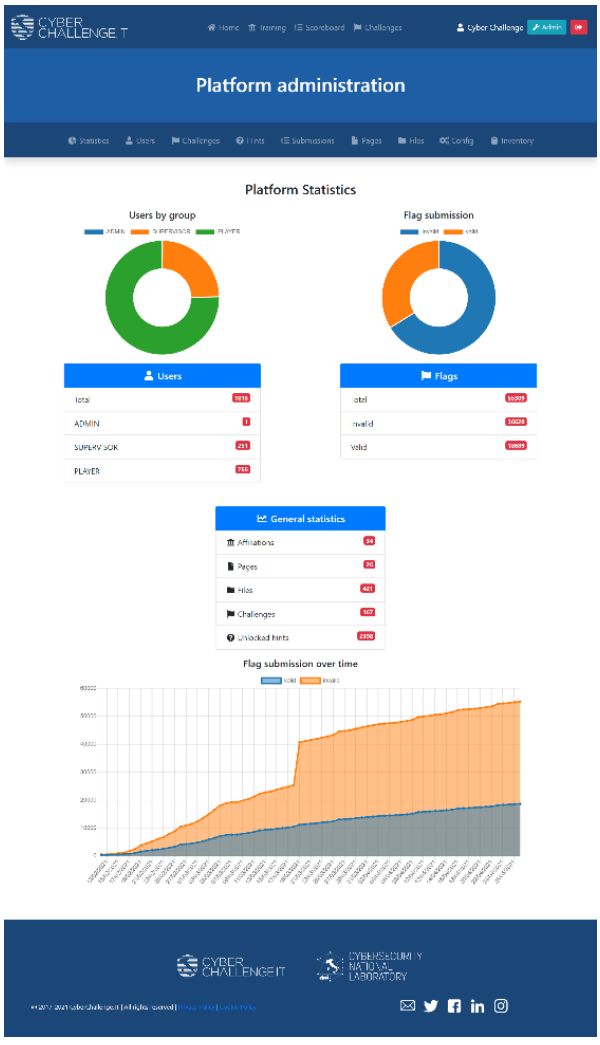
- CyberChallenge.IT 2018 – CTF Jeopardy – 12 challenges
- CyberChallenge.IT 2018 – CTF Attack/Defense – 4 challenges
- CyberChallenge.IT 2019 – CTF Jeopardy – 12 challenges
- CyberChallenge.IT 2019 – CTF Attack/Defense – 4 scenarios
- CyberChallenge.IT 2020 – CTF Jeopardy – 22 challenges
- CyberChallenge.IT 2020 – CTF Attack/Defense – 6 scenarios
- CyberChallenge.IT 2021 – CTF Jeopardy – 24 challenges
- CyberChallenge.IT 2021 – CTF Attack/Defense - 4 scenarios (in development)

Peer-review
In particular all the training challenges and all the Attack/Defense scenarios prepared during the CyberChallenge.IT editions were reviewed by at least 2 experts not involved in the development phase.
All the reviews have been carried out using a single-blind peer review system.

3.1 Training platform

Start from the 2020 edition of CyberChallenge.IT we have setup an online infrastructure to deliver lessons and exercises remotely, also strengthened by limitations imposed in Italy by COVID-19.
The training platform is a brand-new learning and competition platform in order to meet the needs of the CyberChallenge.IT project. The training platform has been, and is still used for more than 4 months by more than 1.000 students and 250 instructors among 33 Italian university and cyber security centers. Currently it contains more than 170 challenges, tens of hours of training video, slides and lectures and external materials.


CYBER CHALLENGE.IT
Challenges
CyberChallenge.IT 2021 - Training challenges
Web Security 1
WS_1.01 - BasicRCE
WS_1.02 - PHPisLovePHPisLife
WS_1.03 - ZipZap - level 1
WS_1.03 - ZipZap - level 2
WS_1.04 - plottyboy
WS_1.05 - ssrf basics - level 1
WS_1.05 - ssrf basics - level 2
WS_1.05 - ssrf basics - level 3
WS_1.05 - ssrf basics - level 4
WS_1.06 - 302camo
WS_1.07 - basic lfi
WS_1.08 - not a bug
Web Security 2
WS_2.01 - SQL Injection tutorial - Level 1
WS_2.01 - SQL Injection tutorial - Level 2
WS_2.01 - SQL Injection tutorial - Level 3
WS_2.01 - SQL Injection tutorial - Level 4
WS_2.02 - filtered
WS_2.03 - NoSQLInjection Here
WS_2.04 - yet another blog
WS_2.05 - Faas
WS_2.06 - NF(Lag)T


Platform administration
Platform Statistics
Users by group
Flag submission
Users
Flags
General statistics
Flag submission over time

3.2 Documentation & Training material

For each module of the training course, the following teaching materials are available:

- Prerequisites and Learning Outcomes
- Preparatory material
- Tutorial(s) on the use of the tools/environments to be used within the Module
- 2 hours of theoretical lessons, prerecorded
- Detailed presentation of the proposed Challenge
- Challenges to solve in the 4 hours of Hands-on-Experience
- Additional in-depth material
- Detailed Challenge write-ups (for the instructors, only)

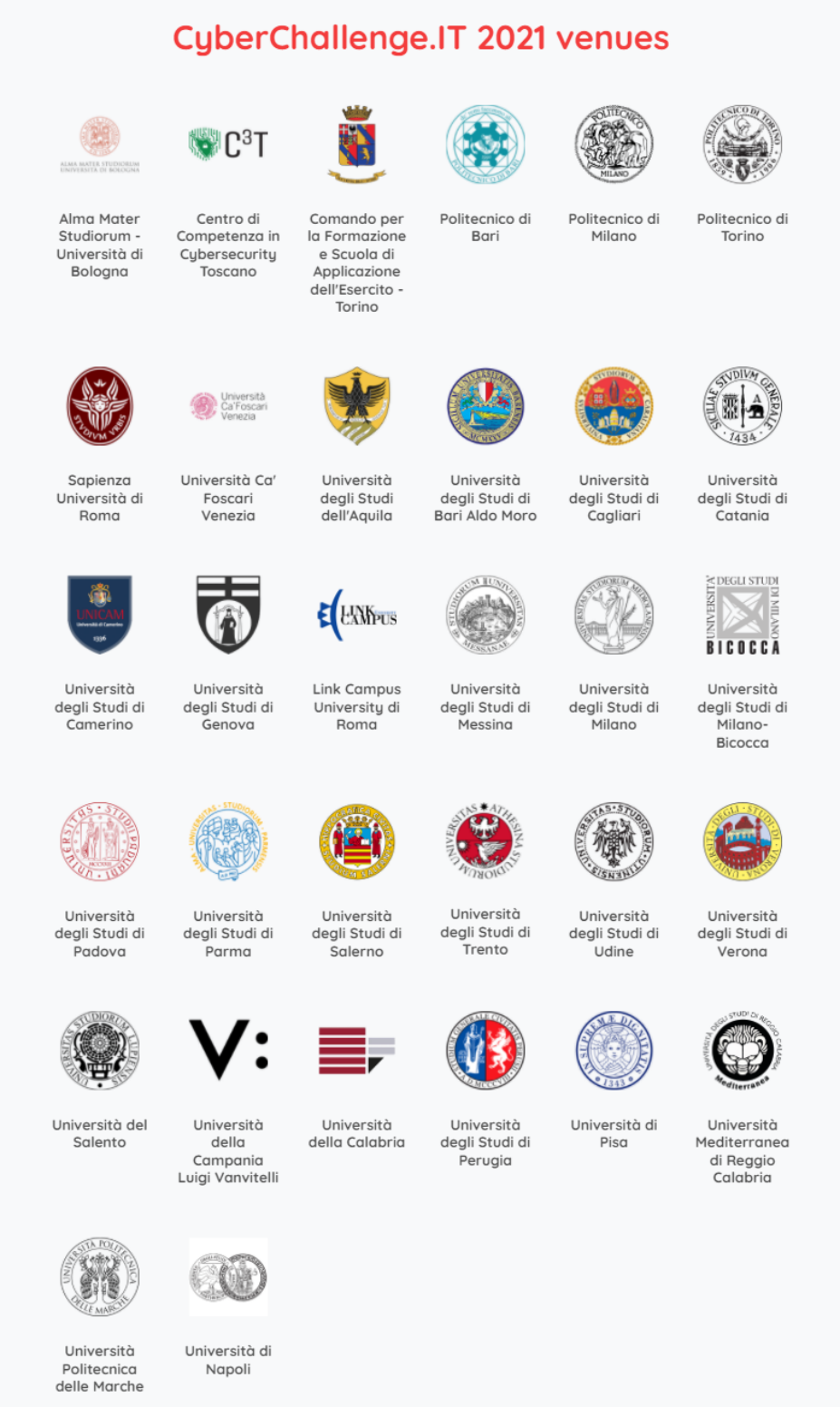
3.3 Detailed Challenge write-ups

For each of the training challenges and the competition-oriented ones prepared during the CyberChallenge.IT 2020/2021 a detailed write-up is available.
A write-up contains all the information to understand, run and teach the solution of the challenge, in particular the following information are available:

- A private description of the challenge, with the difficulty rate and the flag
- A list of prerequisites needed to solve the challenge
- A list of outcomes learned after solving the challenge
- A public description available for the students with the information to download or connect to the challenge
- A list of unlockable hints that lead to the challenge solution
- A detailed solution of the challenge with all the instruction needed to solve it
- All the instruction needed to run the challenge in a local machine

4. Evidence of availability of the outcomes of the initiative to the teaching community

The project after 5 edition involved more than 30 Italian universities and 250 between full professors and cybersecurity researcher.



5. Evidence of impact

General stats

Year	Venues	Schools	Participating students								
			Signed in							Admitted	
			Total	Gender		Origin					
				M	F	Schools		Universities			
			#	#	#	#	%	#	%	#	%
2017	1	-	683	603	80	57	8.3	626	91.7	20	2.9
2018	8	-	1866	1698	168	583	31.2	1283	68.8	160	8.6
2019	18	19	3203	2830	373	1341	41.9	1862	58.1	360	11.2
2020	28	114	4452	3848	604	1960	44.0	2492	56.0	560	12.5
2021	33	184	4896	4255	641	2262	46.2	2634	53.7	671	13.7

https://cyberchallenge.it/stats

CTF Teams

Italian teams linked to CyberChallenge.IT

https://cyberchallenge.it/ctf-teams

6. A reference list (which may include URLs of supporting material)

- https://cyberchallenge.it/
- https://teamitaly.eu/
- https://olicyber.it/
- https://cybersecnatlab.it/news/

7. One or two letters of support. The letters of support may come for example from school or university management, associations, or colleagues in the same or another institution:

- Prof. Rocco De Nicola, Professor IMT School for Advanced Studies Lucca, Director C3T - Centro di Competenza Cybersecurity Toscano