

# Programmazione Sicura



Presentazione  
del corso  
**a.a. 2024/2025**



**Barbara Masucci**  
UNIVERSITÀ DEGLI STUDI DI SALERNO  
**DIPARTIMENTO DI INFORMATICA**  
**DIPARTIMENTO DI ECCELLENZA**

# Docente

Barbara Masucci, Professore Associato

- <https://docenti.unisa.it/005096/home>
- bmasucci@unisa.it
- Dipartimento di Informatica
  - Studio 43, quarto piano, stecca 7



## Ricevimento Studenti

- Richiedere appuntamento via e-mail



# Docente

Barbara Masucci, Professore Associato

- Afferente al Dipartimento di Informatica dal 2002 (fino al 2019 come Ricercatore)
- Corsi insegnati per la Laurea Triennale in Informatica
  - Sicurezza su Reti (dal 2002 al 2012)
  - Programmazione II (dal 2002 al 2004 e dal 2011 al 2016)
  - Complementi di Sicurezza su Reti (dal 2007 al 2009)
  - Architettura degli Elaboratori (dal 2017)
- Corsi insegnati per la Laurea Magistrale in Informatica
  - Elementi di Crittografia (2015)
  - Programmazione Sicura (dal 2017)



# Informazioni sul Corso

➤ Il corso fa parte dell'offerta formativa dei seguenti curricula della Laurea Magistrale in Informatica

- Sicurezza Informatica (SI)
- Software Engineering and IT Management (SE)



➤ Orario lezioni:

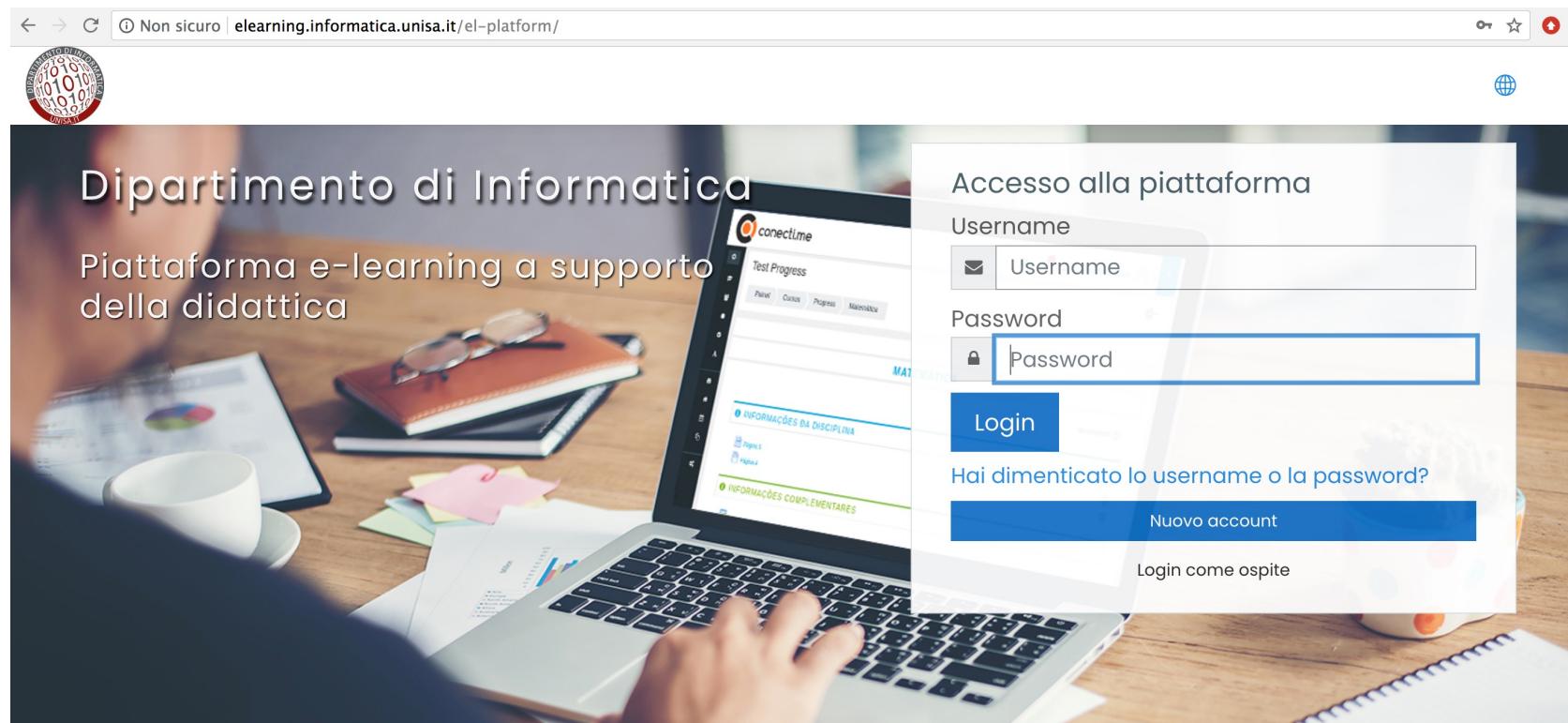
- Lunedì: 9:00 - 11:00, P6
- Martedì: 9:00 - 11:00, F5



# Home Page del Corso

Piattaforma e-learning del Dipartimento di Informatica

➤ <http://elearning.informatica.unisa.it/el-platform/>



# Home Page del Corso

- Piattaforma e-learning del Dipartimento di Informatica
  - <http://elearning.informatica.unisa.it/el-platform/>
- La piattaforma verrà utilizzata per
  - Slide
  - Materiale integrativo
  - Approfondimenti
  - Informazioni
  - Comunicazioni
  - Avvisi



# Obiettivi Formativi

Il corso introduce i concetti fondamentali della  
**Programmazione Sicura**  
ed approfondisce le metodologie e  
le tecniche necessarie per la  
valutazione della **sicurezza di un programma**



# Obiettivi Formativi

➤ Perché ci interessa la **sicurezza dei programmi**?

➤ Essendo i programmi residenti su computer connessi in rete, essi sono oggetto di **continui attacchi**



➤ E' importante saper valutare le **debolezze** e le potenziali **vulnerabilità** di un programma

➤ Si vuole evitare che esse vengano sfruttate per la realizzazione di un **exploit** da parte di un attaccante



➤ E' importante saper fornire **mitigazioni** per le debolezze individuate



# Programmi Insicuri

## ➤ Perché gli sviluppatori scrivono **programmi insicuri**?

- Non pensano che i loro programmi potrebbero essere oggetto di attacco
- Hanno la certezza che i committenti non saranno in grado di valutare la sicurezza dei programmi loro commissionati
- Non tendono ad imparare dagli errori degli altri
  - Molte vulnerabilità sono state causate dagli stessi errori ripetuti negli ultimi 40 anni!
- Non hanno informazioni adeguate
  - Esistono pochi corsi, di tipo specialistico, focalizzati sulla problematica



# Storia del Corso

- Il corso è stato attivato nell'a.a. 2017/2018, con 22 studenti frequentanti



Party di fine corso, Maggio 2018

- Negli anni, il numero di studenti è cresciuto, fino a quintuplicarsi per l'a.a. 2021-2022



# Storia del Corso

Maggio 2019 (58 studenti)



Maggio  
2020  
(79 studenti)



Maggio  
2021  
(68 studenti)



# Storia del Corso



Maggio  
2022  
(111 studenti)

Maggio  
2023  
(71 studenti)



# Storia del Corso



Maggio 2024  
(94 studenti)



Maggio 2025: 81 studenti

# Gradimento del Corso



Salve professoressa, ora che ho completato l'esame di PS e ho confermato il voto, posso dirle che il suo corso è stato tra quelli più interessanti che io abbia mai seguito sia della triennale che della magistrale, senza nulla togliere ad altri corsi.



mi sento di farle i miei complimenti per le spiegazioni e le slide che hanno permesso anche ad un neofita come me (di questi argomenti) di capire a fondo cose che non sapevo nemmeno esistessero.

Peccato non aver scoperto durante la triennale questi argomenti, perché sarebbe stata una buona occasione per partecipare alle sfide ctf che sicuramente avrebbero permesso di approfondire le conoscenze, e forse oggi seguire un curriculum diverso della magistrale.



Mi auguro per i colleghi della triennale di ritrovarsi prima o poi "programmazione sicura 1" al terzo anno, perché è fondamentale per diventare un bravo programmatore, e può aiutare nella scelta del curriculum giusto alla magistrale per chi scopre di essere appassionato a queste tematiche.  
Grazie di tutto.



## Sfatiamo certi miti: le donne? Più brave anche nell'Information Technology

Intervista VIP con Barbara Masucci Professore  
Associato di Informatica, Dipartimento di Informatica  
dell'Università di Salerno.



UNIVERSITÀ DEGLI STUDI DI SALERNO

Professoressa, "Programmazione Sicura" oltre ad essere la denominazione del corso che la vede impegnata presso l'Università di Salerno è un tema cruciale per lo sviluppo dell'Information Society. Può trarre vantaggio in sintesi i contenuti formativi di questa iniziativa?

Il corso di "Programmazione Sicura" è stato introdotto tra gli insegnamenti offerti dal Corso di Laurea Magistrale in Informatica presso l'Università di Salerno nell'a. a. 2017-2018 ed è giunto alla sua quarta edizione. Dapprima proposto tra gli insegnamenti a scelta offerti dall'indirizzo "Sicurezza Informatica" della Laurea Magistrale, negli anni successivi è stato inserito anche negli indirizzi "Sistemi Informatici e Tecnologie del Software" e "Data Science e Machine Learning", coinvolgendo un numero sempre maggiore di studenti.

L'insegnamento introduce i concetti fondamentali della Programmazione Sicura ed approfondisce le metodologie e le tecniche necessarie per la valutazione



della sicurezza di un programma. L'obiettivo dell'insegnamento è quello di fornire agli studenti un insieme di linee guida per scrivere programmi sicuri; tali linee guida sono sviluppate come un insieme di lezioni apprese da casi di studio e riguardano vari linguaggi di programmazione e di scripting e diversi sistemi operativi, con particolare enfasi sui sistemi Unix-like. In particolare, il corso offre agli studenti la possibilità di studiare in profondità alcune tipologie di vulnerabilità, allo scopo di comprendere sotto quali ipotesi esse si verificano, che conseguenze determinano e quali sono le soluzioni più idonee a prevenire.

Quali sono le ragioni del successo crescente, registrato in questi anni? La forte connotazione pratica della metodologia di insegnamento, mirata a stimolare la curiosità degli studenti mediante la proposta di "sfide" che essi

devono tentare di risolvere, è probabilmente una delle ragioni principali per cui un numero sempre maggiore di studenti, anche iscritti ad indirizzi non necessariamente legati alla Sicurezza Informatica, ha deciso di inserire l'insegnamento di "Programmazione Sicura" nel proprio Piano di Studi.

Il corso di "Programmazione Sicura" si fonda su un metodo innovativo. CTF è l'acronimo che racchiude la sfida dal profilo forse più innovativo. Possiamo spiegare di che cosa si tratta?

CTF è l'acronimo di "Capture The Flag" (cattura la bandierina) e viene utilizzato, a livello internazionale, per indicare una categoria di competizioni di Sicurezza Informatica in cui lo studente è messo alla prova, allo scopo di raggiungere uno specifico obiettivo (la bandierina) che indica che la sfida è stata vinta. Durante il corso di "Programmazione Sicura", vengono proposte sfide CTF relative a diverse tematiche, quali l'iniezione locale e remota di codice arbitrario e l'alterazione della memoria, mettendo a disposizione degli studenti diverse macchine virtuali su cui fare prove in piena autonomia e libertà.



La prima categoria di sfide (iniezione locale) presuppone che gli studenti abbiano a disposizione una shell sulla macchina vittima per l'immissione diretta di comandi; la sfida si conclude con la cattura della bandierina nel momento in cui gli studenti riescono ad eseguire un certo programma, per il quale non dispongono dell'autorizzazione necessaria, iniettandone direttamente il codice all'interno dell'eseguibile del programma vulnerabile residente sulla macchina vittima. La seconda categoria di sfide (iniezione remota) presuppone che gli studenti non abbiano un accesso

locale alla macchina vittima, ma debbano utilizzare un vettore di attacco remoto per la cattura della bandierina. Infine, nella terza categoria di sfide (alterazione della memoria), gli studenti catturano la bandierina se riescono ad alterare il contenuto della memoria in uso da un programma, allo scopo di modificarne il flusso di esecuzione o di eseguire codice arbitrario.



L'Information Security è un ambito che siamo abituati a considerare come prettamente maschile. Sta cambiando qualche cosa in questo senso?

E' un argomento delicato, che non riguarda solo il mondo della Sicurezza Informatica, ma quello della Computer Science in generale. Attualmente, la percentuale di studentesse iscritte al Corso di Laurea Magistrale in Informatica presso l'Università di Salerno è di circa il 10% del numero totale, ed essa riflette quello che accade anche al Corso di Laurea (triennale) in Informatica. Per incrementare queste percentuali, il Dipartimento di Informatica dell'Università di Salerno è impegnato nella realizzazione di una serie di iniziative volte a incoraggiare il sesso femminile ad intraprendere gli studi in ambito informatico. Credo, più in generale, che sia necessario sfatare il mito che l'informatica sia una disciplina più affine all'universo maschile che a quello femminile ed incoraggiare le donne, in particolare coloro che dimostrino una spiccata propensione verso le materie scientifiche, ad intraprendere gli studi e quindi la professione in questo ambito, contribuendo con la loro sensibilità, creatività, intuito e talento all'innovazione digitale per il futuro della nostra società.

Vi sono dei progetti orientati a far maturare un salto culturale orientato a riconoscere alle donne il ruolo e l'importanza che meritano?

Tra le iniziative a cui il Dipartimento di Informatica partecipa, va ricordato il progetto Coding Girls, proposto dalla Fondazione Mondo Digitale e dall'Ambasciata degli Stati Uniti in Italia. Lo scopo del progetto è quello di agevolare il raggiungimento della parità di genere nel settore scientifico e tecnologico, agendo su diversi fronti, tra i quali la lotta a pregiudizi e stereotipi di genere, la formazione paritaria e l'orientamento alle carriere del futuro, e proponendo diverse iniziative mirate a stimolare nelle ragazze delle Scuole Medie e Superiori la curiosità verso le scienze informatiche, evidenziandone aspetti particolarmente consoni all'intelletto femminile.

Il programma CyberChallenge.it



La sua Università partecipa all'edizione italiana della Cyberchallenge, che ha la finalità di attrarre nuovi talenti. Un compito arduo non crede?

CyberChallenge.it è un programma di formazione, organizzato dai Laboratori Nazionali di Cybersecurity del CINI, che coinvolge diverse sedi in tutta Italia, tra cui l'Università di Salerno. Il programma, indirizzato agli studenti di età compresa tra i 16 e i 23 anni



# Cybersecurity Trends

## parla di Noi

ed iscritti presso Scuole Superiori o Università italiane, mira ad incuriosire ed identificare giovani talenti, incentivando il loro interesse per le discipline informatiche, oltre che a mostrare loro le opportunità professionali offerte dall'iniziativa. L'auspicio è quello che i giovani talenti individuati possano costituire la prossima generazione di professionisti nell'ambito della Cybersecurity, indispensabile per garantire la sicurezza del nostro Paese. Si tratta, senza dubbio, di un compito arduo ma la particolare tipologia dell'offerta formativa, basata sull'alternanza di didattica tradizionale e proposta di accattivanti sfide CTF, unita alle possibilità per gli studenti di incrementare la propria visibilità presso aziende e istituzioni italiane ed internazionali, ha riscosso un successo crescente negli anni.

### Quali sono le tappe principali di CyberChallenge.IT?

Il percorso formativo si conclude con la formazione di TeamItaly, la Squadra Nazionale di Cyberdefender, della quale vengono chiamati a far parte i ragazzi che hanno avuto maggior successo sia a livello individuale che come gioco di squadra, durante le varie fasi di CyberChallenge.IT. La squadra TeamItaly rappresenta l'Italia alla European Cyber Security Challenge (ECS), la competizione internazionale organizzata ogni anno dalla European Union Agency for Cybersecurity (ENISA) con lo scopo di favorire lo scambio di conoscenza e talenti in tutta Europa.

*Le minacce si stanno sempre più evolvendo, anche gli hacker hanno cambiato pelle rispetto alle prime celebri "apparizioni". Di quali competenze hanno bisogno le aziende per affinare strategie di governance del rischio e di individuazione delle vulnerabilità che siano al passo con i tempi?*

Le competenze richieste per essere al passo con i tempi sono quelle che si acquisiscono in corsi specializzati, quali ad esempio quelli offerti dal curriculum "Sicurezza Informatica" del Corso di Laurea Magistrale in Informatica presso l'Università di Salerno. Non dimentichiamoci che il

termine "hacker" ha cambiato radicalmente significato nel tempo. Oggi, esso viene utilizzato con un'accezione prevalentemente negativa, per indicare coloro che fanno uso delle proprie competenze per violare sistemi informatici, rendere inutilizzabili risorse, rubare e divulgare dati sensibili, al fine di ottenere un vantaggio economico o politico. Ma il significato originario del termine aveva invece un'accezione totalmente positiva e iniziò a circolare all'inizio degli anni Sessanta tra i membri del Tech Model Railroad Club del Massachusetts Institute of Technology (MIT) di Cambridge, per identificare coloro che, inizialmente accomunati dalla passione per il modellismo ferroviario, amavano esplorare i dettagli dei sistemi informatici e i modi con cui estenderne le capacità. Non è un caso che molti dei membri del club abbiano rivestito un ruolo di primaria importanza nella storia della Computer Science.

### Senza formazione non ci può essere sicurezza

*Vi sono minacce che dobbiamo temere in modo particolare?*

Al giorno d'oggi, i pericoli che possono derivare agli utenti in seguito a un cyber-attacco sono numerosi e possono avere effetti disastrosi, cosicché appare evidente la crescente necessità delle aziende di affinare strategie di gestione dei rischi e di individuazione delle vulnerabilità, allo scopo di difendersi nel miglior modo possibile. Pertanto, è necessario avere una profonda conoscenza

### BIO

Barbara Masucci è nata a Salerno il 27/11/1972. Nel 1996 ha conseguito la Laurea in Scienze dell'Informazione, con votazione di 110/110 e lode, presso l'Università di Salerno e nel 2001 il titolo di Dottore di Ricerca in Informatica, presso la stessa università. Durante il Dottorato di Ricerca ha svolto periodi di studi e ricerca all'estero: da Settembre 1999 ad Aprile 2000 presso il Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, Ontario, Canada, e nel Luglio 2001 presso il Departament de Matemática Aplicada IV, Universitat Politècnica de Catalunya, Barcellona, Spagna. Dal 2019 è Professora Associata di Informatica presso il Dipartimento di Informatica dell'Università di Salerno. Dal 2002 al 2019 è stata Ricercatore Universitario presso lo stesso dipartimento. I suoi interessi di ricerca riguardano la Crittografia e la Sicurezza Informatica, ed in particolare l'analisi e la progettazione di protocolli crittografici efficienti e sicuri.

relativa al modo di agire degli attaccanti, focalizzandosi su come le stesse metodologie e tecniche da essi utilizzati per effettuare gli attacchi possano diventare strumenti per proteggere i sistemi informatici. Una volta acquisiti il background tecnico e metodologico tipico di un attaccante, sarà possibile valutare lo stato e i fabbisogni, in termini di sicurezza, di sistemi complessi.

*In Inghilterra esiste un programma di Cyberchallenge per le donne. I Italia è percorribile una strada simile?*

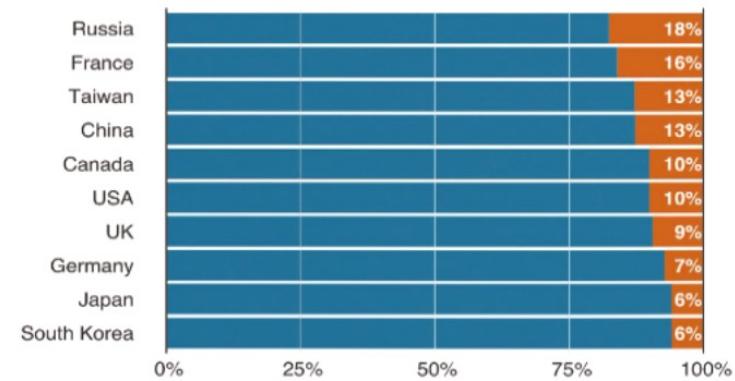
Per quanto riguarda l'Italia, CyberChallengeIT è giunto alla sua quinta edizione: per il 2020 sono stati 4452 i giovani iscritti, di cui solo il 13,6% c'è sesso femminile, e 560 i ragazzi selezionati. Un dato incoraggiante, se pensa che nelle edizioni precedenti la percentuale di presenze femminili tra gli iscritti oscillava tra il 9% e l'11%. Dall'analisi dei dati relativi alle diverse edizioni del programma formativo, si evidenzia, purtroppo, il gender gap di cui abbiamo parlato prima. Secondo il rapporto "Cracking the Code: Girls and women's education in Science, Technology, Engineering and Mathematics (STEM)", pubblicato dall'UNESCO, la disparità di genere nello studio delle STEM deriva dal contesto culturale e sociale in cui le donne vivono.

*In conclusione: quali sono a suo avviso i principali ostacoli da rimuovere?*

La convinzione che l'informatica sia una disciplina più affine all'universo maschile che a quello femminile è ancora troppo radicata nella collettività: e con essa l'idea che lo stereotipo del professionista informatico sia quello di un nerd che svolge un lavoro non adatto ad una donna. Credo che si necessario impegnarsi al più presto a favorire le iniziative volte a colmare questa disparità di genere e ad educare, sin dall'infanzia, il sesso femminile a prediligere attività di tipo tecnologico e scientifico. ■

### Russia has higher share of women inventors

Proportion of men and women in patent applications, 1998-2017



Source: IPO analysis of PATSTAT data

BBC



# Cybersecurity

Trends

# parla di Noi



**Prof.ssa Barbara Masucci - Il valore della leadership femminile nella cyber security**



# Scopo del Corso

- Fornire un insieme di **linee guida** per scrivere **programmi sicuri**
- Le linee guida sono sviluppate come **insieme di lezioni apprese da casi di studio** e riguardano
  - Diversi linguaggi di programmazione e di scripting, tra cui C, Perl, PHP, Python
  - Diversi sistemi operativi, con particolare enfasi sui sistemi Unix-like



# Casi di Studio

- Durante il corso studieremo in profondità alcune **tipologie di vulnerabilità**
  - Sotto quali ipotesi si verificano?
  - Quali conseguenze hanno?
  - Come si possono mitigare?
- L'indagine avrà una **forte connotazione pratica**
  - Avremo a disposizione diverse **macchine virtuali** su cui fare prove, in piena autonomia e libertà



# Capture the Flag!

- Le macchine virtuali che useremo propongono **sfide CTF** relative a diverse tematiche
- CTF: "**Capture The Flag**" (cattura la bandierina)
  - Competizioni di **Sicurezza Informatica** in cui sarete messi alla prova allo scopo di raggiungere un obiettivo specifico (la bandierina)
  - Solo alcune sfide saranno risolte in aula (le altre saranno proposte come progetti da svolgere in piccoli gruppi)



# CyberChallenge.IT

- Il Dipartimento di Informatica partecipa a **CyberChallenge.IT** dal 2021
- Progetto di formazione organizzato dal **Laboratorio Nazionale di Cybersecurity** del CINI



# CyberChallenge.IT

- Per il 2024, le sedi partecipanti al progetto sono 40



- Al termine del periodo di formazione (Marzo-Maggio) è prevista una gara CTF locale, seguita da una gara CTF nazionale a squadre
  - Gara locale: 28 Maggio 2025 (UNISA)
  - Gara nazionale: 6 Luglio 2025 (Torino)



# CyberChallenge.IT

Squadra UNISA 2023



# TeamItaly

I migliori studenti delle varie edizioni di  
**CyberChallenge.IT** entrano a far parte di TeamItaly



Nazionale Italiana di Cyberdefender



# TeamItaly

- La squadra è formata da 20 ragazzi di età compresa tra 16 e 24 anni, partecipanti alle passate edizioni di [CyberChallenge.IT](#)



- Ogni anno la squadra partecipa all' **European Cyber Security Challenge (ECSC)**

- L'edizione 2025 si terrà in Polonia dal 6 al 10 Ottobre
- Nelle edizioni del 2018, 2019 e 2021, TeamItaly ha conquistato il podio



# Capture the Flag with Google

- Anche Google propone ogni anni una competizione basata su sfide Capture the Flag
  - <https://capturetheflag.withgoogle.com>
- L'ultima competizione si è tenuta dal 21 al 23 Giugno 2024, ma le sfide sono ancora online e quindi è possibile provare a risolverle
- Alcune delle sfide sono relative a tematiche affrontate in questo corso



# Risultati Attesi

- Al termine del corso sarete in grado di
  - **Valutare le debolezze e le potenziali vulnerabilità** all'interno di un programma, al fine di evitare che esse forniscano le basi per un exploit
  - **Saper progettare le soluzioni più idonee a prevenire** possibili attacchi



# Prerequisiti

- Conoscenza dei **contenuti di base** relativi ad alcuni insegnamenti fondamentali della triennale
  - Programmazione I
  - Sistemi Operativi
  - Reti di Calcolatori
- La conoscenza dei contenuti di esami del percorso **Sicurezza** è preferibile ma non indispensabile



# Modalità di Esame

- Il raggiungimento degli obiettivi del corso è testato mediante un **esame orale**
- Inoltre è richiesta la preparazione di un progetto di gruppo che può consistere in
  - Analisi e soluzione di sfide **Capture the Flag!** non trattate a lezione
  - Studio approfondito di specifiche vulnerabilità



# Discussione Progetti

I progetti saranno discussi sotto forma di seminari  
nell'ultima parte del corso (**5-27 Maggio 2025**)



# Date di Esame

- Sono previsti i seguenti **appelli**:
  - Preappello: 10 Giugno 2025
  - Primo appello: 30 Giugno 2025
  - Secondo appello: 16 Luglio 2025
  - Terzo appello: 15 Settembre 2025
  - Quarto appello: Gennaio 2026
  - Quinto appello: Febbraio 2026



# Programma del Corso

## ➤ Introduzione

- Cenni storici
- Terminologia, obiettivi e tipi di attacchi
- Vulnerabilità e debolezze del software



## ➤ Panoramica sulle caratteristiche di sicurezza dei sistemi Unix-like

- Gestione del controllo degli accessi
- Esecuzione con privilegi elevati
- Abbassamento e ripristino dei privilegi



## ➤ Casi di studio

- Tecniche per l'iniezione locale di codice
- Tecniche per l'iniezione remota di codice
- Tecniche per la corruzione della memoria
- Tecniche per l'analisi di file binari e per il Reverse Engineering

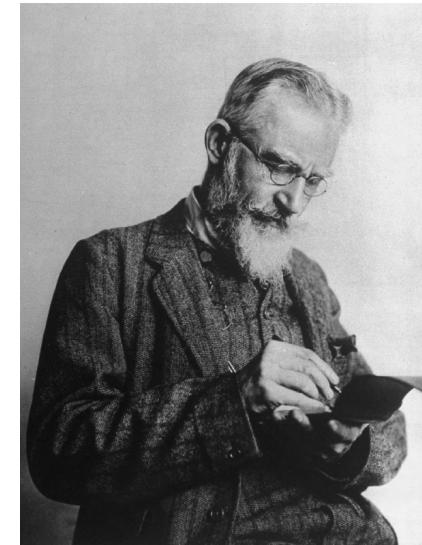


# Cenni Storici

"If history repeats itself, and the unexpected always happens, how incapable must Man be of learning from experience"

George Bernard Shaw (1856 - 1950)

Scrittore, drammaturgo, linguista,  
critico musicale



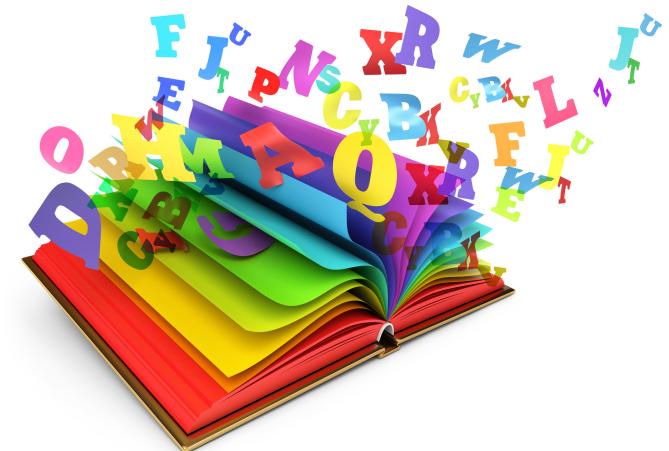
- Vedremo alcuni **esempi di incidenti** che si sono ripetuti negli anni
- Ciascun incidente mette in luce una **vulnerabilità** e ha comportato **conseguenze** di tipo diverso



# Terminologia

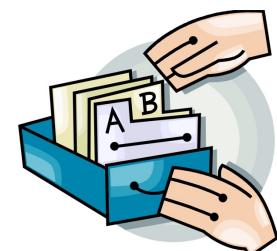
Introdurremo la **terminologia** necessaria per analizzare la sicurezza di un programma

- Asset
- Minacce
- Attaccanti
- Bug, difetti, debolezze
- Vulnerabilità
- Exploit
- Vettore di attacco
- Politiche di sicurezza
- Analisi dei rischi
- Meccanismi di sicurezza



# Vulnerabilità e Debolezze

- Analizzaremos il ciclo di vita delle **vulnerabilità del software**
- Descriveremo diversi sistemi di catalogazione delle **vulnerabilità e delle debolezze**
  - CVE (Common Vulnerability Exposures)
  - CVSS (Common Vulnerability Scoring System)
  - CWE (Common Weaknesses and Exposures)
  - CWSS (Common Weaknesses Scoring System)



# Controllo degli Accessi nei Sistemi Unix-like

- Descriveremo la politica di controllo degli accessi nei sistemi Unix-like
  
- L'accesso ai file è regolato da permessi, definiti come tre terne di azioni
  - Azioni: Read, Write, eXecute
  - Tipologie di utenti: proprietario, gruppo di lavoro, altri utenti



# Esecuzione con Privilegi Elevati

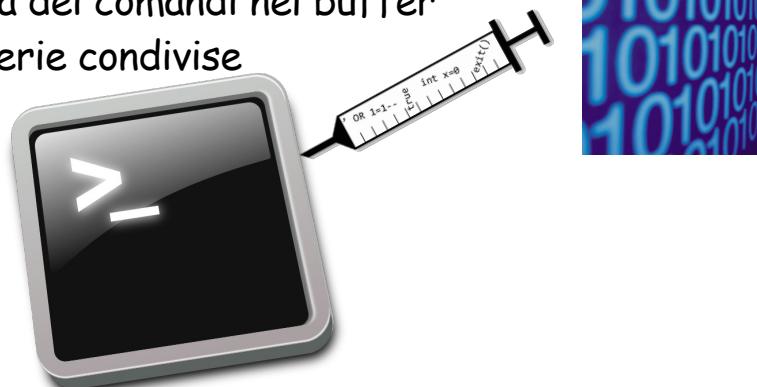
- Analizzeremo in dettaglio il problema dell'esecuzione di programmi con **privilegi elevati** nei sistemi UNIX
- Un esempio
  - Il comando `passwd` necessita dei permessi di `root` per modificare il file `/etc/passwd`
  - L'**elevazione automatica dei privilegi** consente all'utente di ottenere i privilegi di `root` per l'esecuzione del comando `passwd`
- L'elevazione automatica dei privilegi è una funzionalità interessante offerta da UNIX
  - Tuttavia, se il programma è scritto in modo scorretto, tale funzionalità può avere **conseguenze devastanti**



# Casi di Studio

## ➤ Iniezione locale di codice

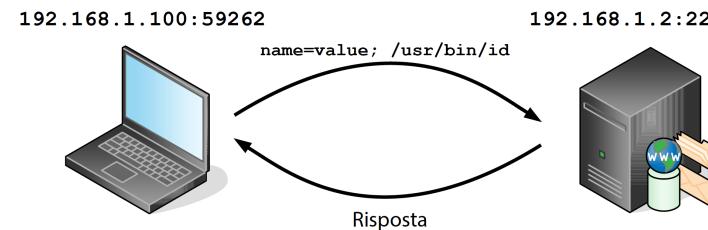
- L'utente ha a disposizione una shell sulla macchina vittima per l'immissione diretta di comandi
- Lo scopo è eseguire un certo programma (per il quale l'utente non è autorizzato) **iniettandone** direttamente il codice all'interno dell'eseguibile del programma vulnerabile fornito dalla sfida
- Vedremo **diverse tecniche** per farlo
  - Manipolazione di variabili di ambiente
  - Manipolazione diretta dei comandi nel buffer
  - Manipolazione di librerie condivise



# Casi di Studio

## ➤ Iniezione remota di codice

- L'utente non ha a disposizione una shell sulla macchina vittima per l'immissione diretta di comandi
- Lo scopo è eseguire un certo programma **iniettandone** il codice all'interno dell'eseguibile del programma vulnerabile mediante un **vettore di attacco remoto**



## ➤ Vedremo diverse tecniche per farlo

- SQL Injection
- Cross Site Scripting
- Cross Site Request Forgery



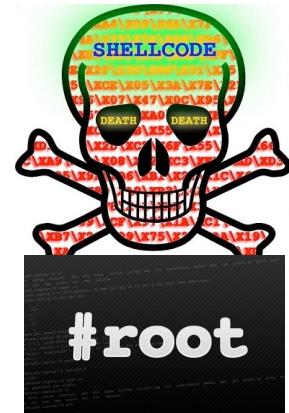
# Casi di Studio

## ➤ Corruzione della memoria

- Consiste nell'alterare il contenuto della memoria in uso da un programma
- Lo scopo può essere quello di modificare il flusso di esecuzione del programma o addirittura di eseguire codice arbitrario

## ➤ Stack-based buffer overflow

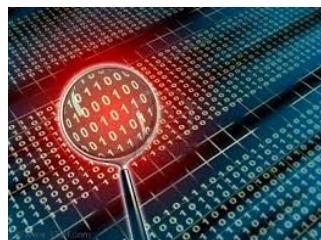
- E' una tecnica di corruzione della memoria che consiste nel riempire lo **stack** (porzione di memoria) oltre i limiti consentiti
- Può avere conseguenze disastrose, come consentire all'attaccante di ottenere una shell di root sulla macchina vittima mediante la costruzione di uno shellcode



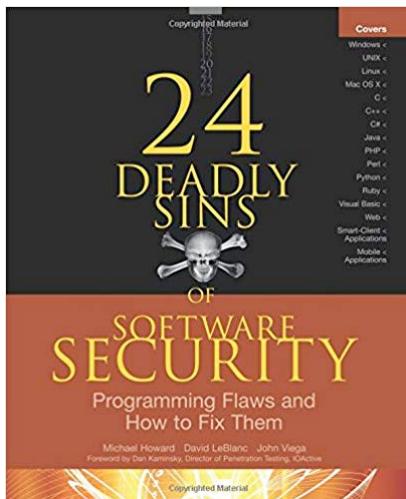
# Casi di Studio

## ➤ Analisi file binari

- Dato un file binario, possiamo **determinare eventuali punti deboli** nel codice mediante l'uso di **tecniche statiche** (non richiedono l'esecuzione del file) o **dinamiche** (richiedono l'esecuzione del file)
  - Ad esempio, possiamo controllare per quale architettura è stato compilato il file, collezionare simboli e stringhe, identificare nomi di funzioni e librerie...
- Un'analisi più profonda può essere effettuata mediante tecniche di **Reverse Engineering**
  - L'uso di **disassemblatori e decompilatori** consente l'analisi del codice assembly e del sorgente corrispondente a un file binario eseguibile
  - Tra i vari tool disponibili, useremo Ghidra, un software open-source rilasciato nel 2019 dalla NSA
  - Le sfide CTF analizzate fanno parte del percorso Cyberchallenge.IT



# Testi di Riferimento



Michael Howard, David Le Blanc **24  
Deadly Sins of Software  
Security: Programming Flaws and How to  
Fix Them**  
McGraw Hill, 2009 , ISBN: 0071626751

Michael Howard, David LeBlanc  
**Writing Secure Code: Practical Strategies and  
Proven Techniques for Building Secure  
Applications in a Networked World**  
Microsoft Press, 2002, ISBN: 0735617228

