europass

# Harsh Kumar

**Data di nascita:** 13/12/2007 | **Nazionalità:** Italiana | **Sesso:** Maschile | **Numero di telefono:** (+39) 3886955182 (Cellulare) | **Indirizzo e-mail:** fyo9329@gmail.com | **LinkedIn:** https://www.linkedin.com/in/harsh-kumar-257a55219/ | **LinkedIn:** https://www.linkedin.com/in/security-h-2081ba21b/ | **Indirizzo:** Via Pantanelle 1, 04011, Aprilia, Italia (Abitazione)

## PRESENTAZIONE

Salve sono lieto di presentarmi, mi chiamo ***Harsh Kumar***, sono un ***giovane ragazzo*** esperto in sicurezza informatica e devo ammettere che mi sento come un bambino in un negozio di caramelle quando si tratta di ***hacking etico*** e ***sicurezza informatica***.
Insomma, sono un vero poliedrico della sicurezza informatica, e come diceva il grande filosofo ***Alan Kay***:"La tecnologia è solo un pezzo di legno. Ciò che conta è il fuoco nell'anima dell'artista." E di sicuro, il fuoco nella mia anima brilla come un server in una stanza fredda.

## ISTRUZIONE E FORMAZIONE

2023
**COMPTIA SECURITY+** Istituto Volta

2023
**CISCO CCNA** Istituto Carlo E Nello Rosselli

2023
**EC-COUNCIL ETHICAL HACKING ESSENTIALS (EHE)** Istituto Volta

15/03/2023 – 07/06/2023
**CORSO IOT** Istituto Carlo E Nello Rosselli

05/03/2022 – 25/03/2023
**CORSO DI SICUREZZA INFORMATICA** Istituto Volta

1. Reti e Protocolli;
2. Malware, Vulnerabilità e Hardering dei Sistemi;
3. Ethical Hacking, Footprinting, Enumerazione e Analisi delle Vulnerabilità;
4. Hacking dei Sistemi ed Attacchi;
5. Attacchi alle Applicazioni WEB, Attacchi Wireless;
6. Crittografia e Deep Web.

03/09/2023 – 11/11/2023
**CORSO DI WEB APPLICATION PENETRATION TESTING**

2021 – ATTUALE
**FREQUENZA INDIRIZZO DI STUDIO: INFORMATICO** Istituto Carlo E Nello Rosselli

## COMPETENZE LINGUISTICHE

Lingua madre: **ITALIANO**

Altre lingue:

| | COMPRENSIONE | | ESPRESSIONE ORALE | | SCRITTURA |
|---|---|---|---|---|---|
| | Ascolto | Lettura | Produzione orale | Interazione orale | |
| **INGLESE** | B1 | B2 | B1 | B1 | B1 |
| **SPAGNOLO** | A2 | B1 | A2 | A2 | A2 |
| **PANJABI; PUNJABI** | B2 | A1 | B1 | B1 | A1 |

*Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato*

## COMPETENZE DIGITALI

**Linguaggi di Programmazione:**

Conoscenza base di Flutter e Dart | Python | Conoscenza base di SQL | Go | CSS | Javascript | HTML | BASH | C++ | C

**Conoscenza delle Distribuzioni:**

BlackArch Linux | Parrot OS | Kali Linux

**Conoscenze:**

OSSTMM | NIST | Sicurezza informatica | OWASP | Conoscenza dei principi di AI | Network e relativi protocolli | Malware Investigation (Malware Analysis) | cloud security | Reverse Engineering | Mobile Security | Exploit Database | SICUREZZA IOT | Mitre CVE | Padronanza del Pacchetto Office (Word Excel PowerPoint ecc)

**Software:**

Linux | Android | Metasploit | Wireshark | Google Dork | Nmap | Hydra | Nessus | Burp Suite | Windows

## ULTERIORI INFORMAZIONI

### COMPETENZE ORGANIZZATIVE

**Competenze Organizzative**
***Pianificazione strategica:*** Capacità di definire una visione e un piano d'azione per raggiugnere gli obiettivi dell'organizzazione.
***Gestione del tempo:*** Capacità di organizzare le proprie attività e quelle del team in modo efficiente, rispettando le scadenze.
***Risoluzione dei problemi:*** Capacità di identificare i problemi, analizzarli e trovare soluzioni efficaci.

### HOBBY E INTERESSI

**Hobby e Interessi**
1. Ascoltare la musica;
2. Passeggiare all'aria aperta;
3. Leggere articoli e libri sulla sicurezza informatica e sulla programmazione;
4. Giocare a Calcio;

### COMPETENZE COMUNICATIVE E INTERPERSONALI

**Competenze e Interpersonali** ***Leadership:*** Capacità di motivare e guidare le persone che stanno accanto a me, per raggiungere gli obiettivi prefissati.
***Capacità di apprendere in modo continuo ed autonomo:*** Capacità di acquisire nuove competenze e di rimanere aggiornati sulle ultime tendenze del settore.

### VULNERABILITÀ SCOPERTE

**Scoperta di vulnerabilità multiple dentro: NASA, Sky, Stanford, Unesco (Con relative menzioni ed HOF)**

Dopo aver completato con successo ***il corso di Web Application Penetration Testing***, ho immediatamente messo in pratica le competenze acquisite con risultati significativi.
Inizialmente, ho individuato una vulnerabilità all'interno della ***NASA*** utilizzando raffinate ***Google dork***, permettendomi di accedere a un file che conteneva informazioni sensibili, inclusi nomi utente.
Questo accesso privilegiato mi ha consentito di penetrare un server completo, rivelando dettagli critici sulle missioni e documenti riservati, oltre a informazioni sensibili come indirizzi email e numeri di telefono.
Per quanto riguarda ***Sky***, ho scoperto una vulnerabilità ancora da risolvere, della quale non posso divulgare i dettagli conformemente alle pratiche etiche.
Nel contesto accademico, ho eseguito con successo un ***subdomain takeover*** presso ***Stanford***, prendendo il controllo di un sottodominio in modo impeccabile.
Altrettanto significativa è stata la scoperta di una vulnerabilità ***CSRF*** presso ***l'UNESCO***, che mi ha consentito di condurre attacchi ***XSS e ATO (account takeover)***, risultando nell'acquisizione dell'account amministratore del sito. In aggiunta, ho recentemente identificato ***un rate limit sul recupero password***, dimostrando la mia attenzione ai dettagli e la capacità di individuare potenziali vulnerabilità.
La mia esperienza nel ***penetration testing si caratterizza per la capacità di individuare e risolvere criticità nei sistemi informatici più complessi.*** Il mio approccio, improntato alla professionalità e all'etica, riflette un impegno costante nel garantire la sicurezza delle reti digitali.
Una parte delle vulnerabilità le vado a pubblicare su questo profilo: https://www.linkedin.com/in/security-h-2081ba21b/

---