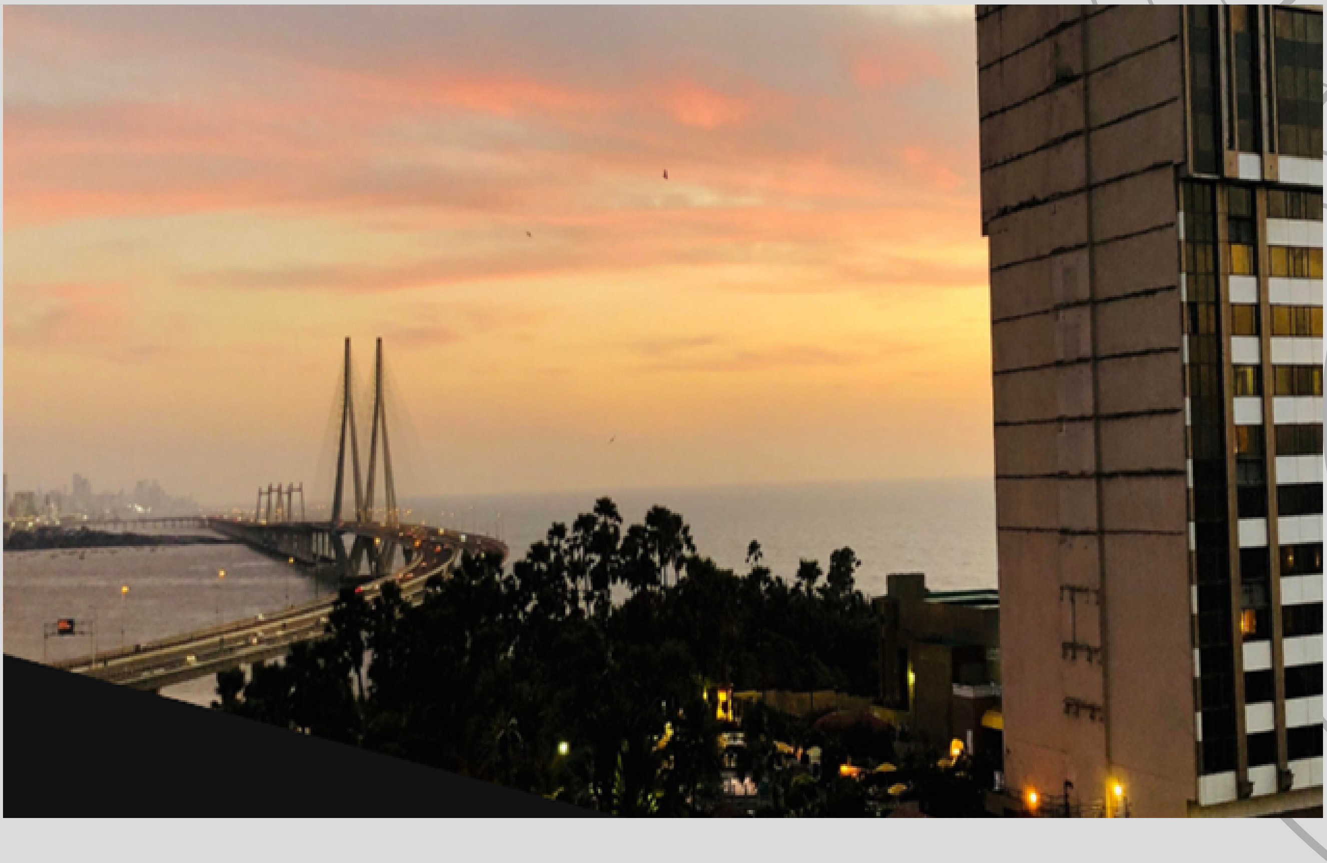
Latest information and analysis on the security of digital systems and networks!

HAWK-I CRCE

TRINETRA

TIME TO SECURE!

2022-2023



About College

Located in a picturesque environment in the heart of Mumbai city, Fr. Conceicao Rodrigues College of Engineering (FR.CRCE) is one of the renowned, premier, and sought-after private Engineering colleges. This Institute is dedicated to making a difference in Engineering education, with its exclusive approach towards the ongoing momentum of trends in technology and holistic development.

Beginning with an Orphanage (BalBhaven) and a trade school in carpentry, the Agnel Ashram (set up in 1957 at Bandra, Mumbai) has today grown into a full-fledged Technical Complex. The Institute today proudly bears the founder's name as a fighting tribute to his impassioned faith in highly-qualified and fully-trained Engineers and Technicians in the service of the Nation.

EXECUTIVE COMMITTEE 2022-2023

Mr. Unik Lokhande
Assistant Professor

As an Assistant Professor in the field of Computer Engineering at Fr. Conceicao Rodrigues College of Engineering, I am also honored to serve as the teacher-in-charge of the college's cybersecurity club, HAWK-i. The club's goal is to provide opportunities for students to gain valuable industry experience through outside-of-class activities such as seminars and workshops. Our aim is to enhance our understanding of cybersecurity and information security through hands-on learning and direct engagement with professionals in the field.

India's Prime Minister Mr. Narendra Modi has spoken about his vision of a "Digital India" where cybersecurity is a fundamental aspect of national security. However, as per India's cybersecurity policy, the country currently faces a shortage of cybersecurity professionals with a requirement of 500,000 professionals while only having 65,000. The **HAWK-i CRCE COMMUNITY/CLUB** is committed to addressing this skill gap by providing students with the skills and knowledge required to excel in this field.

I extend my sincere appreciation to each member of the HAWK-i CRCE team for their invaluable contributions to creating the club's magazine, "**TRINETRA**". I am impressed by the dedication and hard work of the students and would like to extend my congratulations on this outstanding accomplishment.

EXECUTIVE COMMITTEE 2022-2023

Upmanyu Jha
Team Caption, Bug Hunter
Founder
(BE COMPS)

Prathamesh Adake
Pentester
Co-Founder
(BE COMPS)

Harshala Athani
Web Developer Lead
Co-Founder
(BE COMPS)

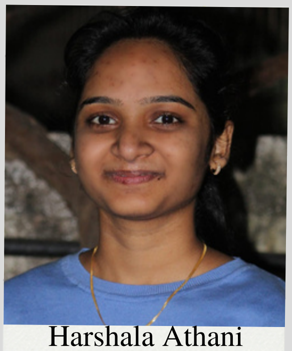
Before 2021, there was no CyberSecurity Community or Club at our College. Additionally, we had only recently begun working on cybersecurity, bug hunting, and playing CTF; therefore, we reasoned that it would be a good idea to establish a group of like-minded individuals that enjoy hacking, pentesting, bug hunting, cybersecurity, etc., and are ready to learn more about it.

As a result, at the end of our third year, we established the **HAWK-i CRCE COMMUNITY/CLUB**, a cybersecurity community that consistently inspired others by offering and disseminating cybersecurity information. We are thrilled to work with such a motivated group of people. We are pleased to report that the publication of our magazine, "**TRINETRA**," is the outcome of our efforts. Our publication delves deep into the subject of cybersecurity. We hope HAWK-i CRCE continues to achieve greater heights in the future as well.

EXECUTIVE COMMITTEE 2022-2023

Upmanyu Jha
Bug Hunter, Founder
(BE COMPS)

Prathamesh Adake
Pentester,Co-Founder
(BE COMPS)

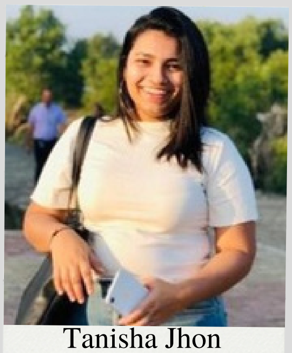


Harshala Athani
Web Developer Lead,Co-Founder
(BE COMPS)

Sachi Verma
Platform Engineer
(BE COMPS)

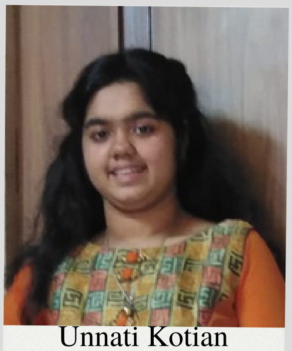
Natasha Lobo
Documentation Lead
(BE COMPS)

Nicole Dias
Management Lead
(BE COMPS)



Tanisha Jhon
Public Relation Lead
(BE COMPS)

Amogh Hegde
Graphic Designer
(TE ECS)



Unnati Kotian
Web & API Security Lead
(TE COMPS)

Oswin Lopes
Web & API Security Lead
(TE AIDS)

https://hawkicrce.com

/@hawki_crce

EXECUTIVE COMMITTEE 2022-2023

Dhruvin Barot
Documentation Co-Lead
(SE)

Joel Varghese
Boys SE Representative
(SE)

Ratan Singh
Boys SE Representative
(SE)

Nivedita Kokane
Girls SE Representative
(SE)

Shubham Shanbhag
Boys SE Representative
(SE)

Namrata Joshi
Design Master
(SE)

Pranav Jakkani
Marketing Associate
(SE)

Jaya Sahani
Public Relation Associate
(SE)

Jerry Jacob
Boys SE Representative
(SE)

Prathamesh Doifode
Public Relation Associate
(SE)

Dylan D'silva
Boys SE Representative
(SE)

Girish Nhavkar
Design Master
(SE)

About Us

HAWK-i CRCE is a One-Stop Platform for Students who are just considering a career in cybersecurity, people who want to compete via CTF challenges, or experienced leader in the cybersecurity workforce who gets an opportunity to inculcate/Collaborate and have a hands-on learning Experience with Real World Bugs & Vulnerabilities, which provides tangible benefits and a supportive community to get guidance from industries best Hackers, Pentesters, Bug Hunters, Researchers, Enthusiasts & Content Creators on a global scale, to comprehend the significance of Cybersecurity in the upcoming era of cyberspace.

HAWK-i Summer Conference is an excellent opportunity for companies to meet with students and professional candidates in order to hire them for cybersecurity roles! More than half of the attendees are students looking for opportunities who have been enrolled through the HAWK-i scholarship program, which is supported by sponsorships.

DEPARTMENT VISION

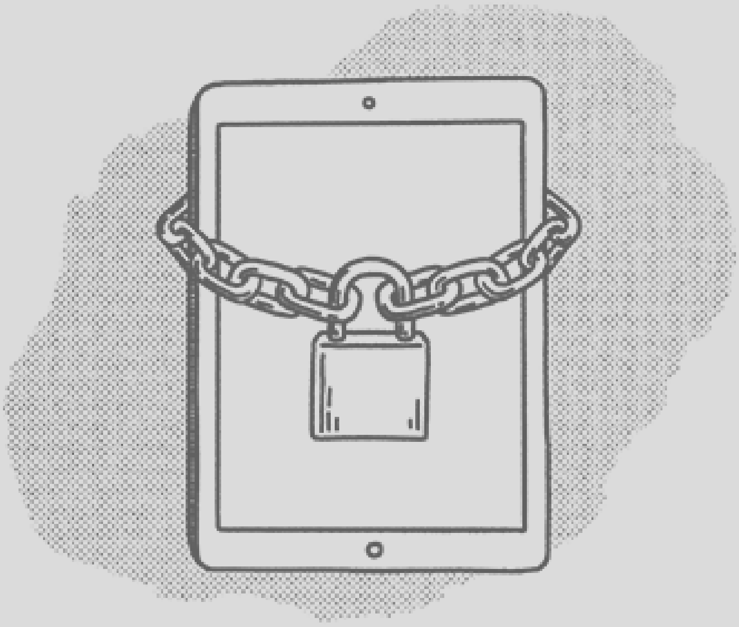
VISION

To be a center of excellence in Computer Engineering education that will produce self-motivated, and globally competent individuals through holistic development.

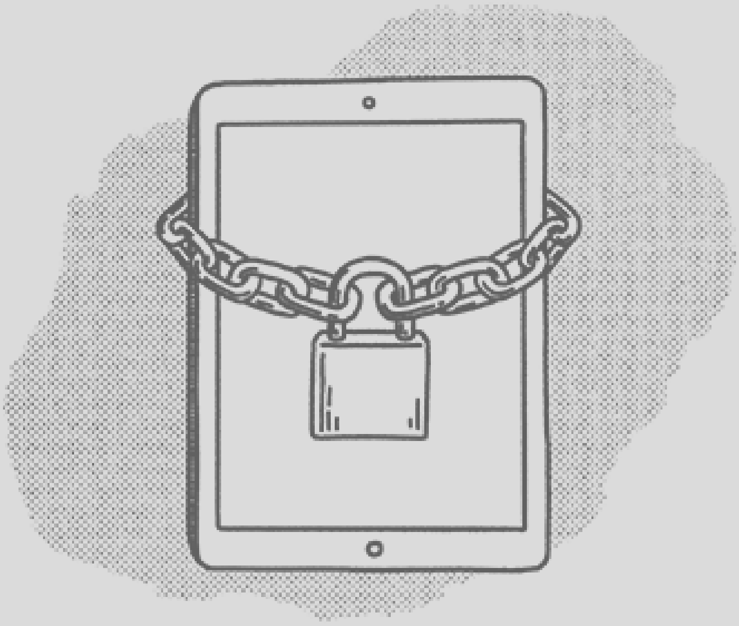
MISSION

- Build state-of-the-art infrastructure that can accommodate cutting-edge technology and is constantly updated in response to the needs.
- To emphasize experiential learning in order to pursue academic excellence and inculcate research aptitude through high-quality research publication
- Enable the students to foster innovative ideas in pace with emerging technologies.
- Encourage faculty members to pursue higher education/research and stay abreast with the latest technology.

TABLE OF CONTENT



ARTICLES



ChatGPT changing the way cybersecurity practitioners look at the potential of AI

ChatGPT, a large language model developed by OpenAI, is revolutionizing the field of cybersecurity by providing practitioners with a powerful tool for detecting and responding to cyber threats. With its advanced natural language processing capabilities, ChatGPT is able to analyze and understand large amounts of text data, including emails, social media posts, and other forms of online communication. This enables it to identify patterns and anomalies that may indicate the presence of a cyber attack, making it an invaluable tool for cybersecurity professionals.

One of the key ways in which ChatGPT is changing the way cybersecurity practitioners look at the potential of AI is by enabling them to detect and respond to phishing attempts. Phishing is a common form of cyber attack in which attackers use social engineering tactics to trick victims into providing sensitive information or access to their systems. Traditional anti-phishing solutions, such as spam filters, are often ineffective against these attacks because they rely on identifying known patterns or specific keywords. ChatGPT, on the other hand, is able to understand the context of emails and social media posts, allowing it to detect more subtle phishing attempts that would otherwise go unnoticed.

Another way in which ChatGPT is changing the way cybersecurity practitioners look at the potential of AI is by providing them with a more effective means of analyzing and responding to cyber threats. With its ability to process large amounts of text data, ChatGPT With its ability to process large

ChatGPT changing the way cybersecurity practitioners look at the potential of AI

amounts of text data, ChatGPT can quickly identify patterns and anomalies that may indicate a cyber attack, allowing cybersecurity professionals to respond more quickly and effectively. Additionally, ChatGPT's ability to understand natural language makes it possible to analyze unstructured data such as social media posts, which can provide valuable insights into potential cyber threats.

ChatGPT is also changing the way cybersecurity practitioners look at the potential of AI by enabling them to better understand the motivations and tactics of cyber attackers. By analyzing the language used in emails, social media posts, and other forms of online communication, ChatGPT can help cybersecurity professionals identify the specific tactics and motivations of attackers, allowing them to develop more effective countermeasures.

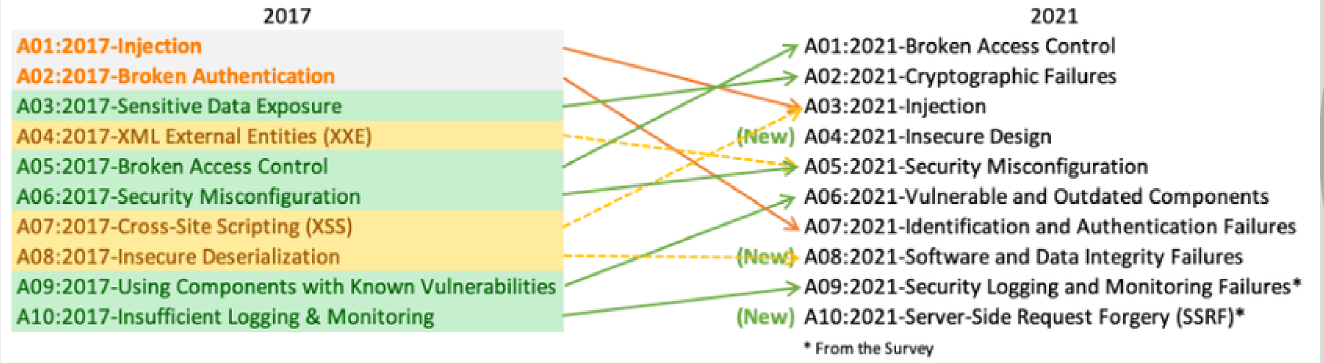
In conclusion, ChatGPT is changing the way cybersecurity practitioners look at the potential of AI by providing them with a powerful tool for detecting and responding to cyber threats. With its advanced natural language processing capabilities, ChatGPT is able to analyze and understand large amounts of text data, enabling it to identify patterns and anomalies that may indicate the presence of a cyber attack. This makes it an invaluable tool for cybersecurity professionals and a powerful tool for the future of AI in cybersecurity.

OpenAI

-by UPMANYU JHA

OWASP TOP 10 VULNERABILITIES

Image credit to OWASP



2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure	A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New) A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New) A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities	A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

The OWASP Top 10 is a list of the most critical web application security risks, as determined by the Open Web Application Security Project (OWASP). The list is updated every three years and is widely used as a benchmark for web application security. The latest version, OWASP Top 10 - 2021, was released in November 2021, and includes the following vulnerabilities:

- **Broken Access Control** The category of Broken Access Control has moved to the top of the web application security risk rankings, with data indicating that on average, 3.81% of tested applications have one or more Common Weakness Enumerations (CWEs) in this category, with over 318,000 occurrences.

- **Cryptographic Failures** were previously known as **A3:2017-Sensitive Data Exposure** which has moved up one position to second place, they focus on failures related to cryptography and often lead to sensitive data exposure or system compromise.

OWASP TOP 10 VULNERABILITIES

- **Injection** has moved down to the third place, with data showing that 94% of applications were tested for some form of injection, with an average incidence rate of 3.37%. Additionally, the 33 CWEs mapped to this category have the second most occurrences in applications with 274k occurrences. Cross-site scripting is now part of this category in this edition.

- **Insecure Design** is a new category added in 2021 that focuses on risks related to design flaws and emphasizes the need for threat modeling, secure design patterns and principles, and reference architectures in order to address these issues. It highlights that an insecure design cannot be resolved by a perfect implementation as needed security controls were never created to defend against specific attacks.

- **Security Misconfiguration** has moved up from 6th place in the previous edition, with data showing that 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.5% and over 208k occurrences of CWEs mapped to this category. With the increased use of highly configurable software, it's not surprising to see this category move up. The former category for **A4:2017-XML External Entities (XXE)** is now part of this risk category.

- **Vulnerable and Outdated Components** previously known as Using Components with Known Vulnerabilities has moved up from 9th place in 2017 and is now #2 in the Top 10 community survey.

OWASP TOP 10 VULNERABILITIES

This category is a known issue that is difficult to test and assess risk for. It is the only category without any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

- **Identification and Authentication Failures**, previously known as Broken Authentication, have moved down from the second position and now include CWEs that are more related to identification failures. Despite this slide down, this category is still a significant part of the Top 10 and the increased availability of standardized frameworks seems to be helping to mitigate the risk.

- **Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. **A8:2017-Insecure Deserialization** is now a part of this larger category.

- **Security Logging and Monitoring Failures** previously known as **A10:2017-Insufficient Logging & Monitoring** have moved up from 10th place previously and are now added to the Top 10 community survey (#3). This category has been expanded to include more types of failures, and it is challenging to test for and is not well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

OWASP TOP 10 VULNERABILITIES

- **Server-Side Request Forgery** has been added to the Top 10 community survey (#1). The data shows a relatively low incidence rate with above-average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are indicating that it is important, even though it's not illustrated in the data at this time.

It is important to note that these vulnerabilities are not specific to web applications only, they are also common in mobile, IoT, and other types of applications. These vulnerabilities are also not limited to a specific technology or platform, they can occur in any application that processes user input. By regularly testing and monitoring web applications for these vulnerabilities, organizations can reduce their risk of a data breach and maintain the security of their sensitive data.

-by GLEN RODRIGUES

CLOUD SECUIRTY

Cloud security refers to the protection of data and resources stored in the cloud from unauthorized access, use, disclosure, disruption, modification, or destruction. As more & more organizations move their data & applications to the cloud, it has become increasingly important to ensure that these resources are protected from cyber threats.

One of the key challenges of cloud security is the shared responsibility model. Under this model, the cloud provider is responsible for the security of the infrastructure and the underlying hardware, while the customer is responsible for securing their own data and applications. This requires organizations to implement robust security measures to protect their resources in the cloud.

One real-life example of cloud security is the case of Capital One. In 2019, a hacker was able to gain access to the personal information of over 100 million Capital One customers through a misconfigured firewall in the company's cloud environment. This data included sensitive information such as social security numbers and bank account numbers. The incident highlights the importance of proper security configurations and monitoring in the cloud.

CLOUD SECUIRTY

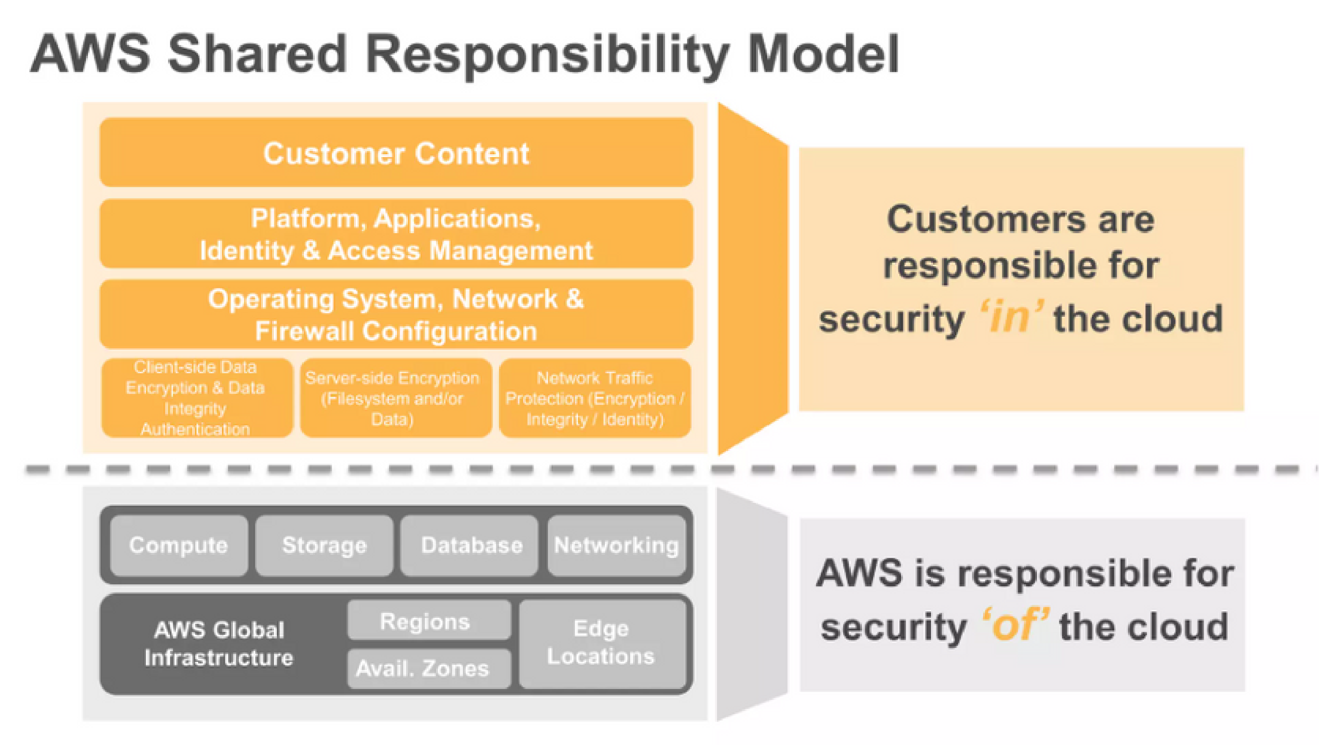
To prevent similar incidents, organizations need to implement robust security measures to protect their resources in the cloud. These measures include:

- Implementing multi-factor authentication to prevent unauthorized access to cloud resources
- Regularly monitoring cloud environments for suspicious activity
- Encrypting sensitive data to protect it from unauthorized access
- Regularly backing up data to protect against data loss
- Implementing security policies and procedures to ensure compliance with industry regulations

In conclusion, cloud security is crucial to protect data and resources stored in the cloud from unauthorized access, use, disclosure, disruption, modification, or destruction. The Capital One incident highlights the importance of proper security configurations and monitoring in the cloud, and organizations should implement robust security measures to protect their resources.

-by UPMANYU JHA

AWS CLOUD SECURITY


AWS Shared Responsibility Model
Customer Content
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (Filesystem and/or Data)
Network Traffic Protection (Encryption / Integrity / Identity)
Customers are responsible for security 'in' the cloud
Compute
Storage
Database
Networking
AWS Global Infrastructure
Regions
Avail. Zones
Edge Locations
AWS is responsible for security 'of' the cloud

AWS Cloud Security refers to the measures and procedures that are put in place to protect Amazon Web Services (AWS) environments from unauthorized access, use, disclosure, disruption, modification, or destruction.
AWS provides a number of built-in security features and services that customers can use to secure their environments, including:

- Identity and Access Management (IAM): IAM allows customers to create and manage users, groups, and permissions for their AWS resources.
- Virtual Private Cloud (VPC): VPC allows customers to create a logically isolated section of the AWS cloud where they can launch AWS resources in a virtual network that they define.

AWS CLOUD SECURITY

- Security Group: Security groups act as a virtual firewall for Amazon Elastic Compute Cloud (EC2) instances and control the inbound and outbound traffic.
- Elastic Block Store (EBS) encryption: EBS encryption allows customers to encrypt their data at rest on EBS volumes.
- CloudTrail: CloudTrail is a web service that records AWS API calls for an account and delivers log files to an S3 bucket.
- Amazon Inspector: Inspector is an automated security assessment service that helps customers identify and fix security vulnerabilities in their environment.

In addition to these built-in security features, customers can also use third-party security solutions and services from AWS partners to further secure their environments.

It is important to note that while AWS provides a secure infrastructure and a wide range of security features, the responsibility for securing data and applications in the cloud ultimately lies with the customer. This means that customers must implement security best practices, such as regular backups, regular security assessments, and the use of multi-factor authentication, in order to fully secure their environments in the cloud.

Overall, AWS Cloud Security is an ongoing process that requires customers to continuously monitor and improve their security measures in order to protect their data and applications from unauthorized access and other security threats.

Securing Smart Contracts in a Blockchain Network

Blockchain technology has the potential to revolutionize a wide range of industries by providing a secure and decentralized way of storing and transferring data. One of the key components of blockchain technology is the use of smart contracts, which are self-executing contracts with the terms of the agreement written directly into the code.

However, as with any technology, blockchain, and smart contracts are not immune to security threats. In fact, the immutability of the blockchain means that once a contract is deployed, it cannot be modified or deleted, which can make it difficult to address security vulnerabilities.

One of the biggest security threats to smart contracts is the potential for errors in the code. These errors can lead to unintended consequences and potentially result in the loss of funds. To mitigate this risk, it is important to thoroughly test and audit smart contract code before deployment.

Another security threat is the potential for malicious actors to exploit vulnerabilities in the smart contract code to gain unauthorized access to funds or information. To address this threat, it is essential to use secure coding practices and to keep the smart contract code and any associated libraries up-to-date.

To enhance the security of smart contracts, blockchain networks can use technologies like formal verification, which

Securing Smart Contracts in a Blockchain Network

mathematically prove the correctness of smart contract code, and access control mechanisms that limit the actions that can be performed by different actors on the network.

Another crucial aspect of securing a smart contract is to keep the blockchain network updated with the latest security patches and upgrades. This can be done by using permissioned blockchain network where only authorized parties can participate in the network and can be controlled by the network administrator.

In addition, it is important to have a proper incident response plan in place in case of security breaches. This plan should include procedures for identifying and containing a security incident, as well as steps for restoring normal operations and minimizing the potential impact of the incident.

In conclusion, securing smart contracts in a blockchain network is a critical task that requires a multi-layered approach. By combining thorough code testing and auditing, secure coding practices, access control mechanisms, and incident response plans, organizations can minimize the risk of security breaches and ensure the integrity of their smart contract.

-by HAWK-i CRCE

Preventing IoT Device Hacking: Best Practices and Security Measures

The Internet of Things (IoT) refers to the interconnectedness of everyday devices, such as smartphones, home appliances, and vehicles, through the internet. While this interconnectedness has brought about many benefits, it has also created new security risks, as IoT devices can be vulnerable to hacking.

One of the biggest security risks to IoT devices is their use of default or weak passwords. Many IoT devices come with pre-configured passwords that are easily guessable or available online, making them vulnerable to brute-force attacks. To prevent this, it is important to change the default passwords on all IoT devices to strong, unique passwords, and to regularly update them.

Another security risk to IoT devices is the lack of software updates. As with any software, IoT devices are vulnerable to security vulnerabilities that can be exploited by hackers. To address this risk, it is important to ensure that all IoT devices have the latest software updates and security patches installed. Additionally, IoT devices are also vulnerable to man-in-the-middle (MitM) attacks, in which a hacker intercepts communication between a device and the internet. To prevent this, it is important to use secure communication protocols, such as HTTPS, and to verify the authenticity of any software or firmware updates before installing them.

Another way to secure IoT devices is by using a VPN (Virtual Private Network) to encrypt all communication between the

Preventing IoT Device Hacking: Best Practices and Security Measures

devices and the internet, which makes it difficult for attackers to intercept or tamper with the data.

Another way to ensure the security of IoT devices is to limit their access to the internet, this can be done by using firewalls, VLANs, and other network segmentation techniques that restrict access to only the necessary ports and protocols.

Lastly, it is important to monitor IoT devices for any unusual activity or communication patterns. This can be done by using security software and tools that can detect and alert potential security breaches.

In conclusion, securing IoT devices requires a multi-layered approach that includes strong and unique passwords, regular software updates, secure communication protocols, network segmentation, and monitoring. By implementing these best practices and security measures, organizations can minimize the risk of IoT device hacking and protect their data and devices.

-by HAWK-i CRCE

Preventing Car Hacking:
A Guide to Securing Modern Vehicles

As cars become increasingly connected and autonomous, the risk of car hacking is becoming a major concern for manufacturers, owners, and government agencies. Car hacking refers to the unauthorized access, use, disclosure, disruption, modification, or destruction of a car's electronic systems.

One of the main vulnerabilities of modern cars is their use of onboard computers and networks. These systems control everything from the car's engine and transmission to its entertainment and navigation systems. They also connect to the internet, which allows hackers to remotely access the car's systems.

One of the most common ways that hackers can gain access to a car's systems is through the use of malware. This can be delivered to the car through a USB drive or even over the internet through a connected device like a smartphone or tablet. Once the malware is installed, it can give the hacker access to the car's systems and control over its functions.

Another way that hackers can gain access to a car's systems is through the use of wireless networks and communication protocols. Many cars use wireless technologies like Bluetooth, Wi-Fi, and cellular networks to connect to the internet and other devices. If these systems are not properly secured, hackers can use them to gain access to the car's systems and control over its functions.

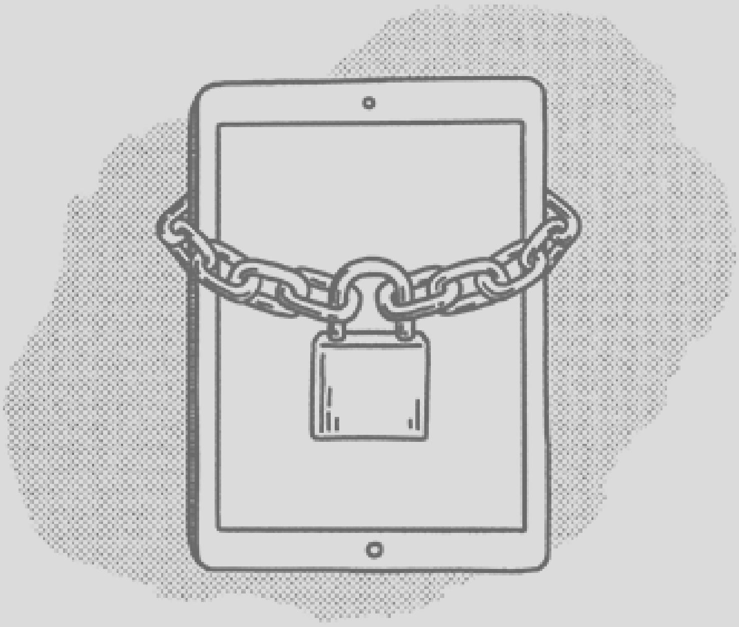
Preventing Car Hacking:
A Guide to Securing Modern Vehicles

To prevent car hacking, manufacturers and owners should take a multi-layered approach to security. This includes implementing security measures such as firewalls, encryption, and secure communication protocols to protect the car's onboard networks and systems. Additionally, software and firmware updates should be regularly installed to address any known vulnerabilities.

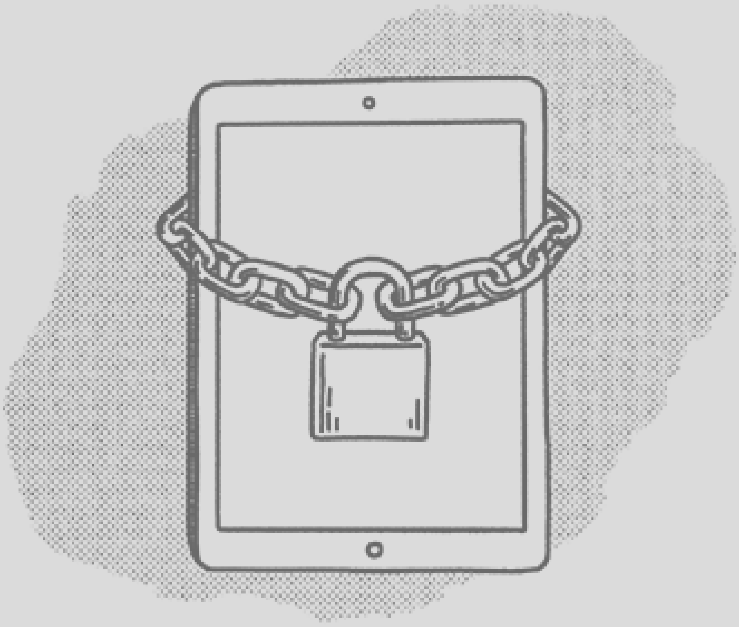
Another way to prevent car hacking is by using intrusion detection and prevention systems that can detect and alert any suspicious activity or communication patterns. It is also important for car owners to be aware of their car's cybersecurity features and to use them properly. For instance, owners should be careful when connecting their smartphones or other devices to the car's systems and should only use trusted and verified apps. Finally, it is essential for manufacturers and government agencies to work together to establish industry-wide standards and regulations for car cybersecurity. This will help ensure that all cars on the road are secure and that consumers can trust in the safety and security of their vehicles.

In conclusion, car hacking is a serious issue that requires a comprehensive approach to security. By implementing the right security measures, staying aware of the latest vulnerabilities, and following best practices, manufacturers and car owners can help protect their vehicles from unauthorized access and control.

-by HAWK-i CRCE



WORKSHOPS
&
SEMINARS



Annual WorkShops / Seminars 2022

CHECKOUT LIST OF 2022 WORKSHOP's

Which attracts a varied group of students and Newbies from various colleges (especially Tier 1, Tier 2 & Tier 3 Colleges).

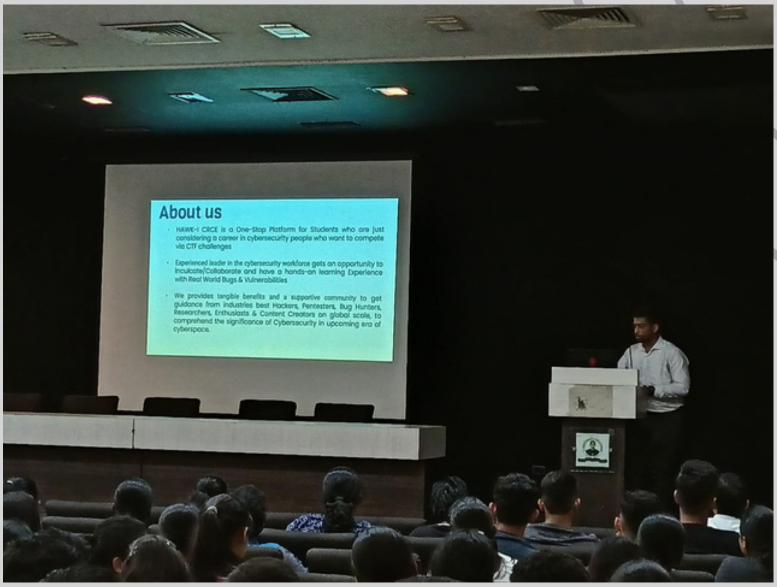
Targeted Cumulative Stats:

40 - 170 participants per workshop.

HAWK-i CRCE
WORKSHOP/SEMINAR

Bug Bounty WorkShop

HAWK-i Introductory Session on Cybersecurity



About us

- HAWK-I CRCE is a One-Stop Platform for Students who are just considering a career in cybersecurity people who want to compete via CTF challenges
- Experienced leader in the cybersecurity workforce gets an opportunity to Inculcate/Collaborate and have a hands-on learning Experience with Real World Bugs & Vulnerabilities
- We provides tangible benefits and a supportive community to get guidance from industries best Hackers, Pentesters, Bug Hunters, Researchers, Enthusiasts & Content Creators on global scale, to comprehend the significance of Cybersecurity in upcoming era of cyberspace.

Web Application VDP

HAWK-i CRCE
WORKSHOP/SEMINAR

Annual WorkShops / Seminars 2023

CHECKOUT LIST OF Upcoming 2023 WORKSHOP's
This Year We are Aiming for quality than quantity as this will be our 2nd year from the day we started.

Targeted Cumulative Stats:

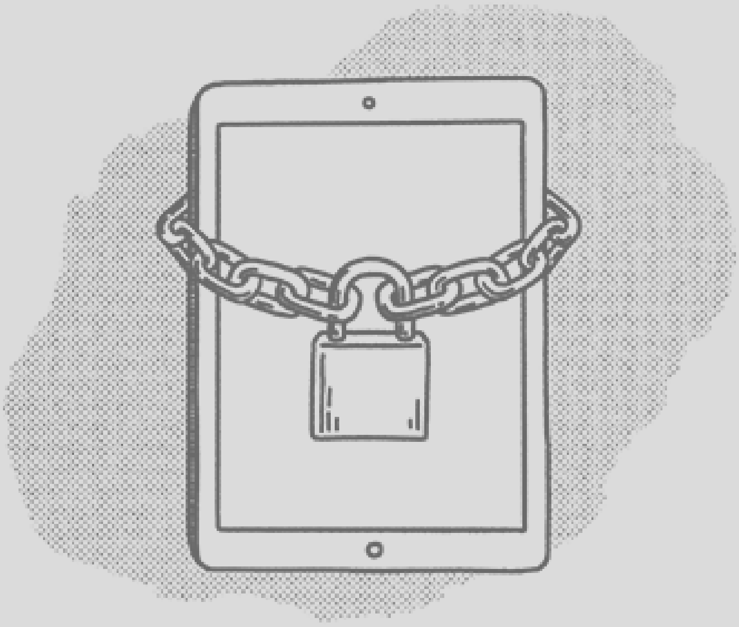
80 - 250 participants per workshop.

LIST OF 2023 WORKSHOP

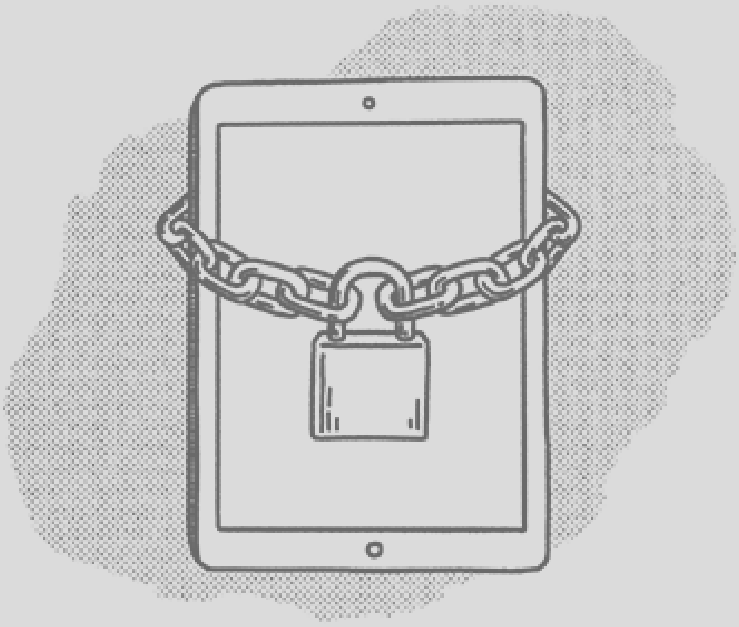
- AWS CLOUD SECURITY
- BLOCKCHAIN SECURITY
- MOBILE and API SECURITY
- Data Privacy Day
- SECURE CODING FOR E-COMMERCE WEBSITE

https://hawkicrce.com

/@hawki_crce



EVENTS



Virtual Pirate CTF

Virtual Pirate CTF is one of our major events that are in a **Jeopardy-style + offline in form of a Virtual Treasure Hunt-based CTF** that is organized mostly during the **Fr. CRCE SYNERGY in collaboration with GDSC**.

This is a beginner-level CTFs that gives players the feel of a treasure hunt and it has a variety of well-written challenges, each with an easy-to-follow path.

Targeted Cumulative Stats:

Only best 15 Teams from Fr.CRCE gets to participate in this CTF with 2-4 participants in each team.

Winning Teams that participated in the event.

Website for the CTF:
https://ctf.hawkicrce.com

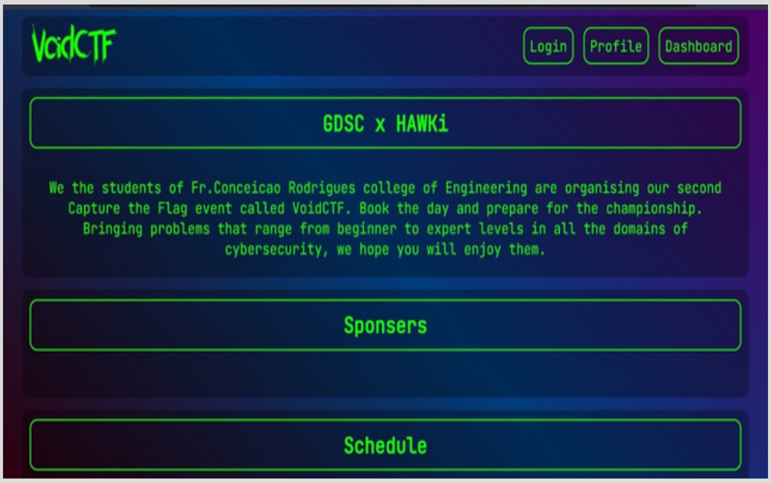
VOID CTF (Upcoming Event)

VOID CTF is another **MAJOR EVENT** that is also in **jeopardy-style but a beginner-level CTF** which is also conducted in collaboration with **GDSC** (**Google Developer Student Clubs**) **on a National Level**.

This is one of the 1st National Level CTF organized by our college which is mostly conducted in January/February. This CTF also has a variety of well-written challenges, each with an easy-to-follow path.

Targeted Cumulative Stats:

Min 100 Teams which have 2-4 participants each for This CTF.



GDSC x HAWKi

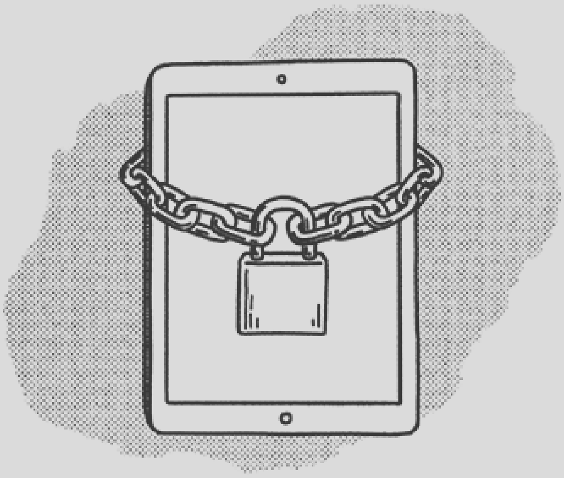
We the students of Fr.Conceicao Rodrigues college of Engineering are organising our second Capture the Flag event called VoidCTF. Book the day and prepare for the championship. Bringing problems that range from beginner to expert levels in all the domains of cybersecurity, we hope you will enjoy them.

Sponsers

Schedule

Glimpse of our event website

The website for Void CTF will be updated Soon on:
https://hawkicrce.com



IMPACT CTF/HACKATHON (Upcoming Event)

IMPACT CTF/HACKATHON is a two-phase Event where in **Phase 1**: Teams will Participate in a **HACKATHON** where teams will be given one flag and their task is to make the application and then hide the given flag in that application.

Then in **Phase 2 i.e in CTF Phase:** The top projects made by various teams in Phase 1 will be taken as the problem for Phase 2 where other teams apart from the ones who made the application will try to break that application and find the hidden flag which was hidden in phase 1.

MOTIVE:

- The Main Motive of this Event is to test the skills of developers as well as CTF Players.
- To Check how well-aware developers are with security while making any application.

Targeted Cumulative Stats:

In **Phase one min 80 Teams** with 2 to 4 members per team will participate

Then in **Phase Two** top 50 Teams from **Phase One will be taken for the Pase 2 Challenge.**

SUMMER CON (Upcoming Event)

BRIEFING:

SUMMER CON 2023 provides security professionals with a place to learn the very latest in information security risks, research, and trends. Leading security researchers from around the globe present their most recent findings and vulnerabilities in a friendly, vendor-neutral setting. Attendees will learn about cutting-edge research on a variety of subjects, from flaws in common consumer electronics to risks to vital global infrastructure, and everything in between.

TRAINING:

HAWK-i's SUMMER CON Trainings provide attendees with individualized technical courses on a variety of subjects, including the most recent advancements in penetration testing, and web application exploitation. These hands-on attack and defense courses, which are frequently created expressly for Cybersecurity enthusiasts, are instructed by subject matter and industry experts from around the world with the aim of defining and protecting tomorrow's information security landscape.

ATTRACTING TOP TALENT AND RESEARCH:

Summer Con will be proud of the depth of research and vulnerability disclosures being revealed at each of its events. We strongly support and encourage responsible disclosure. We hope that Summer Con will be the ideal setting for new and future cybersecurity professionals to begin their careers. In order to support the cutting-edge research and vulnerability disclosure that participants have come to know and appreciate, HAWK-SUMMER i's CON is committed to upholding free speech and privacy rights.

SUMMER CON (Upcoming Event)

WHO SHOULD ATTEND:

- **Security Practitioners**
  - (IT Specialists, Security Analysts, Risk Managers, Security Architects/Engineers, Penetration Testers, Security Software Developers, Cryptographers, Programmers, and Government Employees)
  - Hone your skills with the latest tools and techniques throughout the industry with Summer Con's intensely technical and relevant Briefings and Training. Explore challenges and successes others in the field are experiencing while collaborating on uses for emerging platforms, development models, and best practices.

- **Security Executives, Business Developers, and Venture Capitalists**
  - (CISOs, CEOs, Presidents, Directors, VPs, Consultants)
  - Take advantage of a multi-billion-dollar industry by networking with other top information security executives, practitioners, and potential investors. Gain knowledge of opportunities in the growing information security industry, while engaging with the community that is molding the future of the field and trailblazing new ventures.

- **Vendor Companies and Sponsors**
  - (Hardware, Software, Middleware, Services)
  - Summer Con is aiming to attract the world's most renowned security experts, executives, and attendees, which creates the industry's most dynamic & concentrated information security community. Unveil your latest and greatest innovations, expertise, services, and products over the course of two days.

SUMMER CON (Upcoming Event)

WHO ELSE SHOULD ATTEND AS WELL:

- **Career Seekers and Recruiters**
  - (Seasoned Veterans, Students, Schools, Expanding Companies)
  - SummerCon offers the opportunity to network with the best new and seasoned talent in the industry. Meet face-to-face with top international experts committed to defining and defending the future of security. Job seekers can meet with the most influential companies and recruiters looking for new hires.

- **Academia**
  - (Professors, Students Aged 18+)
  - SummerCon provides students with opportunities to interact with and learn from top industry professionals through conference sessions, networking activities, Business Hall Sessions, and more. Take advantage of the academic rate for students and full-time university professors interested in attending.

START A CAREER IN CYBERSECURITY

Cybersecurity is a rapidly growing field, as the world becomes increasingly dependent on technology.

With the constant threat of cyberattacks, companies & organizations need professionals who can protect their systems and data.

Starting a career in cybersecurity can be challenging, but it can also be highly rewarding. In this article, we will discuss the steps you can take to start a career in cybersecurity.

- **Get educated**: A strong educational foundation is crucial for a career in cybersecurity. **A bachelor's degree in computer science, information technology, or a related field** is a good starting point. Many universities now offer cybersecurity-specific programs, which can provide a more in-depth education in the field. These programs usually cover topics such as **network security, cryptography, and computer forensics.**

- **Gain hands-on Training**: Along with getting a degree you also need to start learning in-depth via PenteserLab Challenges, TryHackMe Rooms/Paths, PortSwigger Lab, and academic training via TCM Security Courses, TaggartInstitute Courses, API Security University Courses,

START A CAREER IN CYBERSECURITY

& lastly watch podcasts by NahamSec, Tib3rius, Alh4zr3d & YT Videos by Jhaddix, John Hammond, InsiderPhD, Husky-Hack, CybersecMeg, InsiderPhD, and Farah Hawa.

- **Gain hands-on experience (Mostly Play CTF on HTB)**: Many cybersecurity positions require practical experience. You can gain this experience through internships, volunteering, or participating in cybersecurity competitions and Playing CTFs on TryHackMe, HackTheBox, and CTF Times. These opportunities will give you a chance to apply the knowledge you've gained in your education and develop real-world skills.

- **Get certified**: Many employers prefer to hire professionals with industry-recognized certifications. These certifications demonstrate to employers that you have a certain level of knowledge and skills in the field. Some popular certifications include CompTIA Security+, Certified Information Systems Security Professional (CISSP), Practical Network Penetration Tester (PNPT), eLearnSecurity Junior Penetration Tester (eJPT), Offensive Security Certified Professional(OSCP) and Certified Ethical Hacker (CEH).

- **Network especially on socials like Twitter/LinkedIn/Instagram**: Cybersecurity is a field that is constantly changing, and staying current with the latest trends and developments is crucial. Networking with other professionals in the field can help you stay informed and provide opportunities for advancement. Joining cybersecurity professional organizations and attending

START A CAREER IN CYBERSECURITY

industry conferences and events can be great ways to meet other professionals and learn about new developments in the field.

- **Continuously improve**: Keep learning and expanding your skillset. Cybersecurity is a field that is constantly evolving, so it's important to stay current with new technologies and best practices. Taking additional courses, attending workshops, and earning additional certifications can help you stay competitive in the job market and advance in your career.

In summary, a career in cybersecurity requires a combination of education, experience, certification, networking, and continuous improvement. It's a challenging field, but with dedication and hard work, you can land a fulfilling and high-paying job. Keep in mind that the field is vast and diverse, it's important to explore different areas of cybersecurity, and find the one that interests you the most. Some of the popular areas are Network Security, Application Security, Cloud Security, and Incident Response, Red Teamer, Pentester, Bug Bounty Hunter to name a few.

If you're passionate about technology and want to make a difference in the world, a career in cybersecurity may be the perfect fit for you. With the right education, experience, and certifications, you can secure your place in this exciting field and make a real impact in the fight against cybercrime.

-by UPMANYU JHA

HAWK-i
CRCE

As a team, we are 28 players + 100 Volunteers with one heartbeat who take pride in being the voice and strength of a community of 1000+ students. We don't look for a reason to help others. We work for a cause, not applause .

- HAWK-i COMMUNITY

CONTACT US

Team Lead

UPMANYU JHA (+91 7303969321)

PR and Social Media

Tanisha John (+91 93244 73394)

Head of Operations

Nicole Dias (+91 87794 60422)

Visit Our Website

https://hawkicrce.com

Sociak Media Handels

Instagram: @hawki_crce

Twitter: @Hawki_Crce

YouTube: @hawki_crce

✉ hawkicrce@gmail.com