Contributors:

Aaditya Rengarajan
Founder, The Eye

Sree Shivesh K
Training Co-Ordinator

Swetha M
Security Researcher, CERT Member and Training Co-Ordinator

Table of Contents

The Eye, a cybersecurity-focused college club, has been actively engaged in promoting awareness and educating members about the importance of cybersecurity since its inception. The club operates under the Computer Science and Engineering Association at PSG College of Technology, catering to students who have an interest in cybersecurity and wish to learn more about it.

Over the past six months, from September 2022 to April 2023, The Eye has undertaken numerous initiatives to fulfill its objectives of promoting cybersecurity awareness and providing a platform for members to learn and practice cybersecurity in their daily lives. Through multiple verticals, such as research and documentation, secure coding, and mock box attacks, The Eye has worked tirelessly to educate and upskill its members in the field of cybersecurity.

Apart from organizing events and conducting activities, The Eye also seeks to foster a community of like-minded individuals who share a passion for cybersecurity. Members are encouraged to collaborate, share knowledge, and engage in discussions to promote a culture of continuous learning.

As the threat landscape continues to evolve, The Eye recognizes the need to stay abreast of emerging threats and challenges. The club has, therefore, prioritized keeping up with the latest trends and technologies in cybersecurity to ensure that its members are well-equipped to face any challenges that come their way.

1 Introduction

The Eye is a college club with a focus on cybersecurity, which operates under the umbrella of the Computer Science and Engineering Association at PSG College of Technology. The club offers various verticals that assist its members in learning and applying cybersecurity practices in their daily lives. The club also hosts events to raise awareness of cybersecurity within the college and conducts research and documentation, secure coding, and mock box attacks as part of its other activities.

2 Club Verticals

The Eye has 8 verticals. A brief introduction to each vertical is given as follows:

1) The **OSINT** (Open Source INTelligence) Team, headed by **Aswath Harish** is responsible for contributing to already-existing open source intelligence projects to improve the world of Cybersecurity.

2) The **Intel** Team, headed by **Ashwant Krishna**, develops cybersecurity solutions for proprietary use within The Eye based on Python and the NMap Scripting Language for already-available tools like Maltego, NMap and other custom tools created by The Eye.

Oculus UI, headed by **Navaneetha Krishnan S** is a secure coding project under the **web development** stream, simplifying the everyday club tasks within The Eye - for internal usage.

The **Bug Bounty Research** Team, coordinated by **Aaditya Rengarajan**, tries to mimic grey hat actors and identify vulnerabilities in the online assets of third-party corporations that provide open bug bounty programmes.

The **Training** Team, coordinated by **Swetha M**, consists of a few core members - who organize self assessment-based cybersecurity training programmes exclusive to all the members of The Eye.

The **Events and Social Media** team, headed by **Dhanush Gowdhaman**, are responsible for ideating and conducting events - like workshops, hackathons and treasure-hunts., as well as handling the Social Media handles of The Eye.

The **Documentation** Team is responsible for writing and creating articles, research-work, and more relevant document-related tasks. There are 3 projects under the documentation team, jointly lead by **Akshayaa Mahesh** and **Aaditya Rengarajan**- namely - the **Case Study** project where the team aims to work on case studies of security incidents worldwide, the **Research Project** where the team aims to perform R&D and write a research paper on something new, and the **Articles Project** where the team aims to write Security Guidelines, Quarterly Reports and Whitepapers for the club.

The **YouTube** Team, headed by **Rohith Sundharamurthy**, works on YouTube videos to be released on the YouTube platform under The Eye.

P.T.O

3 Club Events

A. BREACH 2022

Breach' 22, a 2- day workshop on cybersecurity was held on the 13th and 14th of October 2022. This workshop was held to create awareness on the importance of cybersecurity and organizational network security as well as introduce the basics of it as a part of Cybersecurity Month Celebrations.
The workshop shed light on famous real-world incidents related to cybersecurity. It cultivated awareness among the people through the exploration of the dark web.

The workshop also gave insights into some of the common hacking attacks like XSS and Phishing. The topics covered in the first day are as follows:

Learning Outcomes	Description	Objective
Case studies	Blue whale, Ice salt challenge, science of addiction, body dysmorphia disorder, Alicia Navarro case.	To bring out the importance of cybersecurity as an individual.
Attack on SCADA system	Brief on security operation centre. Bhopal gas disaster– Taking in password credentials from hackers arise website and using them to login into the simulation. Simulated and changed the pressure of tanks to create a virtual accident.	Bring in the cybersecurity point of view to the incident.
Complaint procedure	A brief on the topic.	To bring in the importance of the complaint procedure.
Uber hack and Rockstar hack	An insight into the hacks – how and for what they were hacked i.e., uber – user details and rockstar hack deals with gta 6 production leak. A small talk on the Ukraine power grid Attack.	To bring notice of the recent cybercrimes.

The second day covered the following topics:

Learning Outcomes	Description	Objective
Viruses, ransomware, dark web and proxy.	A brief on the topic as introduction followed by a hands-on session. Piratebay- accessing using normal internet vs tor. Launching VM into systems and accessing dark web radio using tor mode in brave.	To introduce the concepts basic concepts of cybersecurity and dark web. To bring awareness about the dark side of the piracy.
XSS attack	A brief on the same and an insight on how it can be done – using vulweb.	To introduce the concept of XSS.
OSI model layers, TCP/IP protocol	An introduction about the topic , Covering the details of each layer and what vulnerabilities can be found where. A comparison of TCP/IP model to OSI model.	To understand OSI and TCP model layers
Homograph attack, nmap and zphisher tool.	A brief on how links can be used for malicious activities – like gmaii for gmail , instagram with different version of 'a' etc. Demonstration of using zphisher tool for getting user credentials.	To introduce the topic.

P.T.O

Images from Breach 2022 are displayed below.

The event attendees for the Iris software security event were encouragingly high with 40 out of 62 participants attending the event on the first day, and 28 out of 40 on the second day. The event saw a diverse group of participants from different backgrounds and skill levels. The participants came from various colleges across the state, and the event was well received by all. The event was designed to provide a platform for participants to enhance their skills in secure coding and cryptography, and the feedback received from the attendees was overwhelmingly positive. The attendees appreciated the efforts put in by The Eye club members to create a conducive learning environment.

During the event, the general audience feedback was that it was a smooth event. At the beginning, the audience was a bit reserved, but as the workshop progressed, they became more interactive with the organizers. Queries and doubts raised during the sessions were promptly addressed by the organizers to the best of their capabilities. This made the attendees feel more confident in their learning experience, and they appreciated the transparency and openness of the organizers. The attendees also noted that the event was well-organized and had a well-structured curriculum.

In addition to the good turnout, the feedback received from the attendees was equally positive. Some attendees mentioned that the workshop was really good, and they had a great time attending it. They also appreciated the efforts put in by the organizers to create a conducive learning environment. One attendee mentioned that they wished to learn more about ethical hacking and asked if the organizers could suggest some good resources. This shows that the attendees were not only interested in learning during the workshop but also wanted to continue learning after the event.

B. IRIS 2023

Iris was a highly anticipated software security event that took place from March 3 to March 6, 2023. The event consisted of two streams: Secure Coding and a mini-CTF (Capture The Flag).

During the hackathon and CTF phase, participants were required to complete coding challenges related to various topics such as Personal Budget Manager, Retirement Planning Manager, Stock Predictor, Loan Calculator, Tax Filing System, Credit Score Checker, Investment Portfolio Manager, Bill Payment System, Expense Tracker, and Fraud Detection System. Additionally, the CTF phase involved various challenges such as exploiting a buffer-overflow to break a payment system, exploiting a stock portfolio web-app using SQL Injection and XSS Injection, decrypting cryptic texts that were available at an Onion site for Insider Trading in India, finding a password from a malicious EXE file for a banking software, finding the flag in EXIF data of a bank CCTV image capture, finding deleted files in a hard drive image of a banking computer, and extracting banking logs from a simulated mobile device.

The hackathon and CTF phase were held online, and participants were given 48 hours to complete the challenges. The event concluded with an offline final round on March 7, where the participants were given more time to complete harder CTF challenges. Cash prizes worth a total of INR 10,000 were awarded to the top three participants, and the winners were appreciated for their exceptional skills and knowledge in software security.

Overall, the event was a huge success, and the participants had a great time participating in the various challenges and scenarios. The event helped the participants learn and practice software security in their everyday lives and increase their awareness of cybersecurity. The organizing team received positive feedback from the participants, and the event was appreciated for its smooth conduct and excellent execution.

Iris was a significant step towards promoting software security among college students.

Images from Iris 2023 are displayed below.

The top 2 winning teams wrote their feedback and also a CTF writeup on the steps they took to solve the challenges, which is published on our website.

P.T.O

4 Club Activities

A. OSINT Team

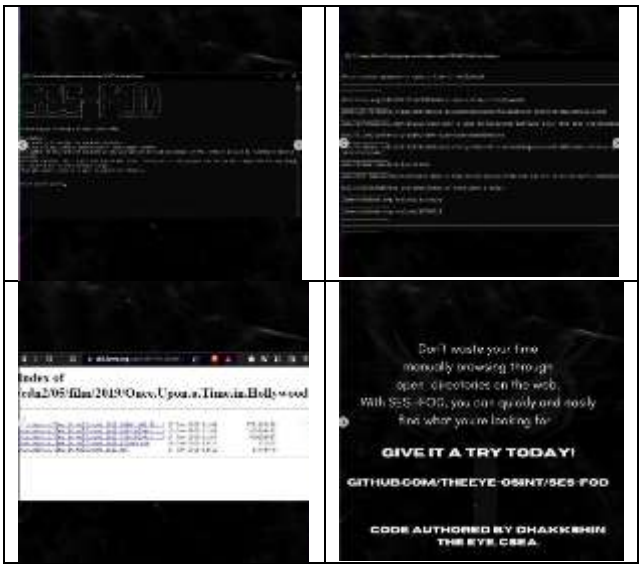
OSINT, or Open Source Intelligence, refers to the collection, analysis, and dissemination of publicly available information. This includes any data that can be gathered from open sources such as social media, public records, news articles, and websites. The OSINT team of The Eye's club has recently released a software tool on GitHub named "SES-FOD" - Search Engine Scraping For Open Directories. This tool is designed to index and search through directories exposed on the web directly from the command line. SES-FOD is easy to use, simply run the executable file and enter your query string. The tool will do the rest, providing you with a comprehensive list of results in no time.

The development of SES-FOD was an initiative of The Eye's club OSINT team, and it was completed in February 2023, thanks to the dedicated efforts of Dhakkshin. This tool can be used for a variety of purposes, including information gathering, threat intelligence, and research. By providing users with quick access to open directories, SES-FOD can help identify potential security risks, data breaches, or other vulnerabilities that may be present on a website or network.

SES-FOD has the potential to be a valuable tool for cybersecurity professionals, researchers, and anyone looking to gather information from open sources. It can also be used by individuals who are interested in learning more about OSINT and how it can be used to gather information online. The release of this tool on GitHub is a testament to the commitment of The Eye's club and its members to promote cybersecurity and encourage the development of open-source software.

Overall, the release of SES-FOD by The Eye's club OSINT team is a significant contribution to the field of cybersecurity and information gathering. With the increasing amount of information available online, tools like SES-FOD are becoming more important in helping individuals and organizations stay informed and protect themselves from potential threats. The ease of use and comprehensive search results provided by SES-FOD make it a valuable addition to any cybersecurity toolkit.

Screenshots of this tool are attached below:



B. Documentation

The Documentation team of The Eye's club is making significant contributions in the field of cybersecurity by undertaking projects that are relevant, informative, and up-to-date. Jointly headed by Akshayaa Mahesh and Aaditya Rengarajan, the team comprises three major projects, each with a specific objective and focus.

The Case Study Project aims to document and analyze various security incidents and data breaches worldwide. The team has successfully completed case studies on AIIMS Delhi Attack, Panasonic In-Flight Entertainment Systems' vulnerabilities, Arrest of BreachForums' Admin and Ukraine Power Grid hacking. These case studies serve as important resources for cybersecurity professionals, students, and enthusiasts alike to understand the security vulnerabilities and loopholes in various systems and how to avoid them.

The Research Project, headed by Aaditya Rengarajan, aims to explore and research new trends and developments in the field of cybersecurity. The team is currently exploring the use of artificial intelligence (AI) to enhance the security of industrial control systems (ICS), which have become a crucial aspect of many industries, including energy, manufacturing, and transportation. This research project aims to identify the potential security threats and risks associated with ICS and how AI can be used to prevent, detect and respond to such threats.

The Articles Project aims to create informative and engaging content in the form of security guidelines, reports, and whitepapers for the club's members and the general public. The team has already released Security Guidelines for handling E-mails, credit cards, and handling stand-alone computers. These guidelines are essential for people who are not familiar with the basics of cybersecurity, helping them protect their personal information and stay safe from cyber threats.

In today's world, where cyber threats are constantly evolving and becoming more sophisticated, it is crucial to have resources like those provided by The Eye's Documentation team. Their projects and contributions serve as important tools for anyone interested in cybersecurity, from beginners to experienced professionals. With their dedication and expertise, the team is making a significant impact on the world of cybersecurity, and their work is highly valued and appreciated by the club's members and the broader community.

C. Social Media

The events organized by The Eye are of great value to those who wish to learn about cybersecurity, and the efforts of the Events and Social Media team in promoting these events are commendable. The Instagram page is not only aesthetically pleasing but also educational, making it an excellent resource for those who want to learn more about cybersecurity.

The Eye's Instagram page is a great resource for anyone interested in cybersecurity. The posts cover a wide range of topics, from case studies of security incidents to specific types of cyber attacks. The posts on XSS, or cross-site scripting attacks, are particularly informative. XSS is a type of attack in which an attacker injects malicious code into a web page, which then runs in the user's browser. This can be used to steal sensitive information, like login credentials or credit card numbers. The Eye's post on Social Engineering Attacks is also very informative. Social engineering attacks are a type of attack that relies on psychological manipulation, rather than technical vulnerabilities. For example, an attacker might pretend to be a bank representative and ask for the victim's login credentials. The Eye's post on Malware Attacks is also worth noting. Malware is a catch-all term for any type of malicious software, like viruses, trojans, or ransomware. The post explains how malware can infect a computer and what steps users can take to protect themselves. Finally, The Eye's post on MITM attacks, or man-in-the-middle attacks, is very informative. MITM attacks occur when an attacker intercepts communication between two parties and can read or modify the messages. This can be used to steal sensitive information, like login credentials or credit card numbers. The post explains how MITM attacks work and what steps users can take to protect themselves.

Overall, The Eye's Instagram page is an excellent resource for anyone interested in cybersecurity, and the Events and Social Media team deserves a lot of credit for creating and maintaining such an informative resource.

D. Oculus UI

The Eye at PSG College of Technology has launched a website named cseatheeye.com that is aimed at promoting cybersecurity awareness and education. The website offers a comprehensive overview of the club and its related work, including documents, research papers, blogs, white papers, security guidelines, and projects

worked upon. The website was developed by a team of members comprising Manojkumar K., Udhith Akash R.R., Anbuselvan M., Lohith S., Arun U.S., Aaditya Rengarajan, and **Navaneetha Krishnan S**, who is the head of the secure coding project under the web development stream named Oculus UI.

The website is a valuable resource for students, faculty members, and anyone interested in learning more about cybersecurity. It also offers two important features, the Cyber-Incident Reporting Form and the Vulnerability Reporting Form. These forms have been designed to ensure that all reports are comprehensive and accurate, allowing the Incident Response Team to handle incidents promptly and effectively. By providing a centralized platform for reporting cybercrime complaints and vulnerability reports, the impact of cyberattacks can be mitigated, and prevention can be enforced.

The Eye's website is special because it offers not only comprehensive information on the club and its activities but also two essential features that allow people to report incidents and vulnerabilities. The website provides a centralized platform for reporting cybercrime complaints, and vulnerability reports, which are then handled promptly and effectively by The Eye's Incident Response Team. This makes the website unique and provides an additional layer of security and protection for the college community.

The website is also given an extra layer for secure access as it is available through The Onion Routing services.

E. Training

The training team of The Eye plays an essential role in upskilling budding cybersecurity enthusiasts through weekly quizzes. The main aim of the team is to promote the importance of cybersecurity and educate individuals about potential cyber threats. By offering weekly quizzes, participants can test their knowledge and gain a better understanding of key cybersecurity concepts. The quiz is usually prepared on Kahoot and contains around 15-20 questions covering a range of topics such as Burp Suite, Malware, Dark Web, and more.

This half-year, the training team has completed four successful training sessions and is eager to continue helping the community to sharpen their knowledge of cybersecurity. The team is dedicated to providing quality training to the participants, ensuring that each quiz is designed to challenge and educate individuals on different aspects of cybersecurity. The topics are as tabulated:

Week	Topics
1	Networking Security, VPNs, Firewalls and TOR
2	Malware
3	Dark Web and TOR
4	BurpSuite

Moreover, the weekly quizzes are designed to be self-paced, allowing individuals to take the quizzes at their own convenience. This flexibility ensures that participants can learn at their own pace, making it easier to fit training into their busy schedules.

In conclusion, The Eye’s training team plays a crucial role in promoting cybersecurity awareness and educating individuals about potential cyber threats. Their weekly quizzes are an excellent way to test knowledge and learn about different aspects of cybersecurity. With their continued efforts, the team will undoubtedly continue to upskill budding cybersecurity enthusiasts and contribute to making the community a safer place.

F. Emergency

The Eye has it's own Incident Response Team (IRT) organized with the following standard operating procedures.

The IRT team's primary goal is to respond to cybersecurity incidents, cyberbullying/abuse incidents, and work as a CERT (Computer Emergency Response Team) for our college by reverting to any vulnerabilities found on the college website.

Cybersecurity incidents refer to any unauthorized access, data breaches, malware attacks, or any other security incidents that can affect the confidentiality, integrity, and availability of information. The IRT team will respond promptly to any such incidents, investigate the source, and take appropriate measures to contain and remediate the situation. The team will also document the incident and provide a report to the relevant college departments and authorities.

Cyberbullying/abuse incidents refer to any malicious and offensive behavior on the internet, such as harassment, bullying, and other types of abuse. The IRT team will investigate any such incidents and take appropriate action to stop the behavior and provide support to the victims. The team will also educate the college community about the dangers of cyberbullying and how to prevent and report it. Working as a CERT for our college means that the IRT team will identify and report any vulnerabilities found on the college website. The team will also provide recommendations and best practices to mitigate and prevent future vulnerabilities.

The IRT team takes its role seriously and strives to maintain the confidentiality, integrity, and availability of all information it handles. Confidentiality means that any information related to incidents or victims must remain private and secure. Integrity means that the team must ensure the accuracy and completeness of all information. Availability means that the team must ensure that information is available to those who need it when they need it.

To ensure the success of our team, we have established some guidelines that must be followed at all times. These guidelines are as follows:

1. Team Goals: Our team's goals are to prevent, detect, respond to, and recover from any cybersecurity incidents that may affect our college. We aim to educate the college community about cybersecurity and to foster a culture of security awareness.
2. Confidentiality of Information: The IRT team must maintain strict confidentiality regarding any information related to cybersecurity incidents. This includes personal information of individuals involved in the incident, technical details, and any other sensitive information.
3. Ensuring CIA Triad: Our team is committed to ensuring the CIA triad of confidentiality, integrity, and availability for all college information systems. This means that we must protect information from unauthorized access, ensure the accuracy and completeness of information, and ensure that information is available when needed.
4. Reporting incidents: Any member of the college community who suspects a cybersecurity incident must report it to the IRT team immediately. The team will investigate the incident and take appropriate action. All team members must document their activities and provide regular updates to the team lead.
5. Collaboration: The IRT team must work collaboratively with other college departments, such as IT, HR, and legal, to respond to incidents effectively. The team must also collaborate with external organizations, such as law enforcement agencies and other CERTs, as needed. All

these collaboration with external must be done through college and faculty only.

6. Training and Development: All IRT team members must receive training on cybersecurity incident response, cybersecurity best practices, and relevant laws and regulations. The team must also engage in ongoing professional development to stay up-to-date with the latest threats and trends in cybersecurity.

The Team has received a form submission and has handled an Incident on Cyber Bullying through an Online Dating Application faced by one of the students of PSG College of Technology. This incident has been summarized in further notes.

Incident summary: The incident took place on when the victim received texts and phone calls from anonymous users claiming that they had shared her number through an online dating game/app available in the google play store in which a fake account has been created in the victim's name and has been used to circulate their phone number and other social media handles to random users across the globe. The incident has been reported to the application's support email and no response or action from the developer side has been received/taken yet.

The IRT Team lead was informed of the incident on March 18, 2023 at 9:15 pm by two students of PSG College of Technology and members of the victim's close circle of friends.

Impact: The cyberbullying incident had a significant impact on the victim, causing them to feel distressed. They reported feeling that the Incident has affected their daily work routine. The victim is a fashion designer who runs their own business that required them to pick up calls from unknown numbers who may be business clients. However, this incident made it hard for them to do so.

Evidence: Screenshots containing the conversations between random people and the account have been provided to the platform administrators through email, as evidence of the cyberbullying incident. A screenshot of the fake account has also been attached and requested to be removed immediately.

Analysis: This incident appears to be an isolated event and does not indicate a larger issue with cyberbullying on the platform. However, it does highlight the need for stricter enforcement of platform policies to prevent such incidents in the future.

Response: The platform administrators were notified of the incident by the club. However, no response or action from the application's support system had been receive. The victim has also been provided with the information about support services available to victims of cyberbullying, including resources for reporting incidents to law enforcement if necessary.

Recommendations: We recommend that platform administrators take swift action to remove any instances of cyberbullying and provide support to victims of such incidents. We also recommend that the platform considers implementing stricter policies and procedures to prevent cyberbullying. The app being an online dating app must include verification protocols to verify the originality of their users and also improve their support systems to provide a faster response. Victims must also be made aware of the procedure to file a legal complaint on cyber bullying if needed.

Complaints can be filed at the local police station under relevant sections of the Indian Penal Code (IPC) such as

• Section 354D (Stalking): Section 354D of the Indian Penal Code (IPC) deals with the offense of stalking. It defines stalking as a person following or contacting someone repeatedly, causing them fear or distress, despite their expressed desire to cut off communication. The section provides for punishment up to three years imprisonment and/or fine for the first offense, and for subsequent offenses,

punishment can extend up to five years of imprisonment and/or fine.

• Section 499 (Defamation): Section 499 of the IPC defines defamation as any act of making a false statement that harms the reputation of a person, entity, or organization. It can be done through spoken or written words, signs, or gestures. The section provides for punishment of up to two years imprisonment and/or fine for the offense of defamation. However, in cases where the defamation is against a public figure, the burden of proof lies with the plaintiff to prove the statement as false.

• Information Technology (IT) Act, 2000: The IT Act, 2000, is an Indian law that deals with various aspects of online activities, including electronic transactions, data protection, and cybercrimes. The act was amended in 2008 to include new provisions related to cybercrime, such as hacking, phishing, identity theft, and cyberstalking. The act also provides for punishment for offenses related to cybercrime, including imprisonment for up to three years and/or fine. Additionally, the act provides for the establishment of the Cyber Appellate Tribunal to hear appeals against the orders of the Controller of Certifying Authorities.

The incident has been reported to two email addresses provided by the application's support page. The company or the support team has not reverted back yet.

The victim was given emotional support throughout this incident by our IRT. The victim had, through personal interest, approached the local police cell – ever since which this incident was successfully curbed.