MARCH 2025

SPECIAL EDITION

CYBER DRISHTI

OWASP PCCOE

EXCLUSIVE

A PEAK INTO THE WORLD OF CYBERSECURITY

A VISION FOR DEFENSE

THIS ISSUE SERVES AS A VITAL RESOURCE FOR ASPIRING SECURITY PROFESSIONALS, EXPLORING HOW ARTIFICIAL INTELLIGENCE AND ZERO TRUST ARCHITECTURES ARE RESHAPING THE LANDSCAPE OF MODERN CYBERSECURITY.

Table Of Contents

OWASP PCCOE

Table Of Contents

Institute and Department Vision

Institute vision

To be one of the top 100 Engineering Institutes of India in coming five years by offering exemplarily Ethical, Sustainable and Value Added Quality Education through a matching ecosystem for building successful careers.

Department vision

To be a premier Computer Engineering Department by achieving excellence in Academics and Research for creating globally competent and ethical professionals.

Editorial Note

BRIDGING THE GAP: THE MISSION OF CYBER DRISHTI

Every breakthrough begins with a question, “How can we make the digital world safer?” At Cyber Drishti, we believe that answer starts with awareness, curiosity, and collaboration.

In an era where technology changes in the blink of an eye, and cyber threats grow smarter with each passing day, classrooms alone can’t keep up. That’s why this magazine was created, to bridge the gap between academic learning and the real-world challenges faced by cybersecurity professionals.

Cyber Drishti, the OWASP PCCOE Student Magazine, is not just a collection of articles, it’s a vision. A vision to nurture future-ready cyber defenders, to celebrate curiosity, and to empower every student to think critically, act ethically, and innovate fearlessly.
Here’s what we stand for:

- Decentralized Knowledge: From exploring Zero Trust to decoding AI-driven threat intelligence, we turn technical jargon into accessible, hands-on insights.
- Ethics at the Core: Because true cybersecurity is not only about defense, it’s about responsibility. Our work reminds us that power in the digital space must always be grounded in integrity.
- Student-Led Revolution: This is your platform, a place to publish research, showcase ideas, experiment with concepts, and challenge conventional thinking.
- Future-Driven Vision: Through workshops, real-world problem statements, and community stories, we aim to inspire innovation beyond the screen, preparing students not just to find jobs, but to create impact.

In essence, Cyber Drishti is more than a magazine, it’s the collective heartbeat of a community that believes in learning together, sharing openly, and building a safer digital tomorrow.

As you turn the pages of this issue, we hope you find something that sparks your curiosity, questions what you thought you knew, and motivates you to take the next leap in your cybersecurity journey.
Stay curious. Stay secure. And most importantly, keep your Drishti wide open.

~ The Cyber Drishti Editorial Team

MESSAGE FROM LEAD

WELCOME TO OWASP MAGAZINE

This issue brings cutting-edge insights, real-world security stories, and student innovation to keep you ahead in the ever-evolving cybersecurity landscape.

As technology advances rapidly, cybersecurity has become a critical aspect of modern computing. During the academic year 2024–25, the OWASP Student Chapter focused on strengthening its vision of building a technically empowered cybersecurity community.

With the rise of technologies like Artificial Intelligence and advanced computing systems, digital infrastructures are becoming increasingly complex, while security solutions often struggle to keep pace. This highlights the growing need for skilled individuals who can understand and secure modern technologies.

Through various initiatives, our chapter worked toward fostering cybersecurity awareness and encouraging technical exploration among Computer Engineering students. This magazine reflects our efforts and journey throughout the year, and we hope it inspires more students to explore cybersecurity and contribute to building a safer technological future.

Shivam Rai

Theme Spotlight

In today's hyper-connected digital era, software applications form the backbone of almost every service we rely upon be it educational platforms, banking systems, healthcare portals, e-commerce websites, or government infrastructure.

While innovation and convenience have accelerated
rapidly, security has often lagged behind. This gap has resulted in frequent data breaches, privacy violations, and large-scale cyber incidents.

Addressing this challenge is at the heart of OWASP's global mission:
to make software security visible so that individuals and organizations can make informed decisions about true software security risks.
The OWASP Student Chapter at Pimpri Chinchwad College of Engineering (PCCOE) embodies this mission at the grassroots level.
As a student-led, community-driven chapter officially recognized by the OWASP Foundation, the chapter focuses on you reading this empowering students with knowledge, practical skills, and ethical values required to secure modern software systems.
This magazine issue reflects that commitment by centering on the theme "Making Software Security Visible & Accessible

Making Software Security
Visible & Accessible
Aligning with OWASP's Global Mission and OWASP PCCOE's Vision

Breaking the Web

Modern Security & Emerging Technologies

- Zero Knowledge Proof (ZKP)
- Zero Trust Architecture
- Privacy-Preserving Machine Learning
- AI Agents & Autonomous Systems
- AI-Powered Cyber Attacks
- Supply Chain Attacks
- Cloud Security Misconfiguration

AI / LLM Application Security Risks

- Prompt Injection
- Prompt Jailbreaking
- Sensitive Information Disclosure
- Training Data Poisoning
- Insecure Output Handling
- Model Denial of Service
- Excessive Agency
- System Prompt Leakage
- RAG Attacks
- Model Theft

Web Application Security Risks

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)

Securing the Web in the Age OF AI

This issue serves as a vital resource for aspiring security professionals, exploring how artificial intelligence and Zero Trust architectures are reshaping the landscape of modern cybersecurity.

AI and the New Attack Surface

Artificial intelligence is transforming both defense and offense in cybersecurity

- While AI enables advanced threat detection and automated analysis, attackers are also leveraging AI to generate phishing campaigns, discover vulnerabilities, and bypass traditional defenses.
- This dual-use nature of AI makes securing AI systems — particularly Large Language Models — a critical priority.

The Rise of Zero Trust Security

Traditional security models assumed that systems inside a network could be trusted. However, modern cyber threats have proven that this assumption is flawed.

“NEVER TRUST,ALWAYS VERIFY”

Every user, device, and application must continuously authenticate and prove its legitimacy before gaining access to resources.

Cyber News Radar

OWASP PCCOE

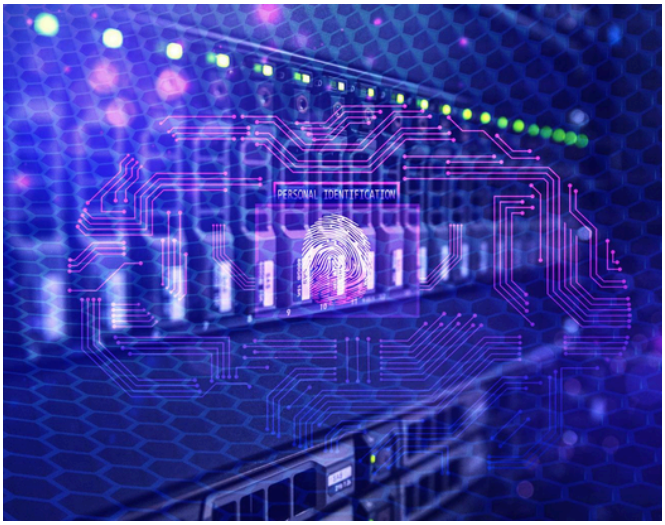
THE ZERO-CLICK HEIST: WHEN YOUR AI'S "ACCURACY" BECOMES ITS GREATEST FLAW

CLOUDFLARE OUTAGES: A CRITICAL REVIEW OF INTERNAL FAILURES

SHADOW ESCAPE: ANALYZING PROTOCOL-LEVEL VULNERABILITIES IN MODERN AI ASSISTANTS

HELPFUL, NOT HARMLESS: WHY YOUR AI CO-PILOT NEEDS A HUMAN CYBERSECURITY EXPERT

THE DATA LOCKDOWN: HOW WE'RE FIGHTING THE NEXT GENERATION OF PRIVACY ATTACKS



How Autonomous AI Systems Can Be Exploited Without User Interaction

Artificial intelligence assistants are rapidly becoming embedded into everyday workflows—from email drafting and coding support to enterprise data analysis. While their efficiency and accuracy have made them indispensable tools, security researchers are beginning to highlight a concerning trend: AI systems can be manipulated without any direct interaction from users.

These so-called zero-click AI exploits occur when attackers embed malicious instructions within the data an AI processes. Because AI assistants automatically analyze and act on information, they may unknowingly follow these instructions—potentially exposing sensitive data or triggering unintended actions.

Scale of the DisruptionThe Hidden Entry Point: Prompt Injection

One of the most prominent attack vectors is prompt injection, where malicious instructions are hidden inside documents, websites, or data sources that an AI assistant processes.

For example, a document being summarized by an AI assistant might contain hidden instructions such as:

- Requesting the AI to retrieve sensitive information
- Altering the assistant's normal behavior

Since AI systems are designed to follow contextual instructions, distinguishing legitimate content from malicious prompts remains a significant challenge.

When "Accuracy" Becomes a Vulnerability

AI models are trained to produce reliable outputs by interpreting instructions as accurately as possible. Ironically, this reliability can become a weakness.

THE ZERO-CLICK HEIST: WHEN YOUR AI'S "ACCURACY" BECOMES ITS GREATEST FLAW

Attackers can craft inputs that appear legitimate but subtly alter the AI's intended behavior. Because the system trusts the context it receives, it may execute tasks that compromise security

This creates a new category of cybersecurity risk where the attack targets the AI's reasoning process rather than the user's actions.

Securing AI Assistants

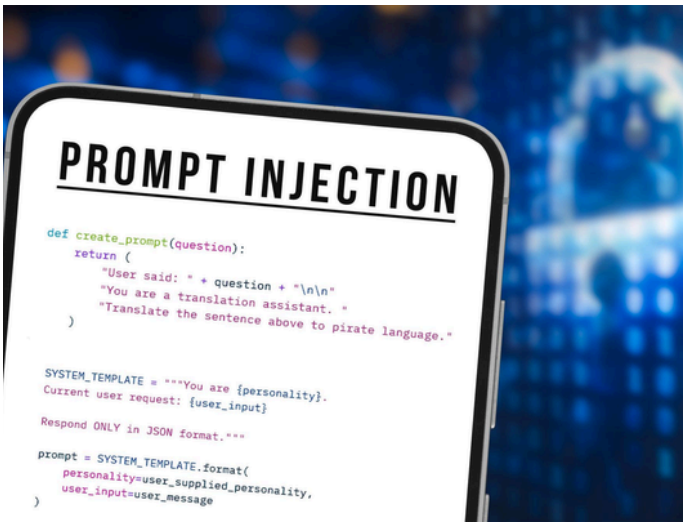
Organizations deploying AI copilots must begin treating them as critical digital infrastructure. Security teams should implement safeguards such as:

- Strict validation of AI inputs
- Monitoring AI-generated actions
- Restricting access to sensitive data sources
- Implementing human oversight for critical decisions

As AI becomes more autonomous, the security conversation must shift toward protecting the systems that think on our behalf.

In addition, organizations should adopt dedicated AI security frameworks and regular red-team testing to identify vulnerabilities before attackers do. Continuous auditing of AI behavior, model updates, and data access patterns can help detect anomalies early and prevent small weaknesses from escalating into large-scale security incidents. Proactive governance will be essential to ensure AI remains a trusted tool rather than an unintended entry point for cyber threats.

In the age of autonomous assistants, cybersecurity is no longer only about protecting users—it's about securing the intelligence that acts for them.



When Infrastructure Giants Become Single Points of Failure

Cloud infrastructure providers form the backbone of today's internet. Services ranging from e-commerce platforms to financial systems rely on global content delivery networks and security services to remain operational.

However, recent large-scale outages involving major cloud infrastructure providers have exposed a critical weakness: when centralized systems fail, the ripple effects can bring vast portions of the internet offline.

What Happens During a Cloud Infrastructure Failure

When a major cloud provider experiences a failure, it can impact multiple layers of internet services simultaneously.

Typical disruption points include:

- DNS resolution failures
- Content delivery network disruptions
- Security gateway interruptions

Because many organizations rely on the same provider, a single technical error can cascade across thousands of dependent services.

The Risk of Over-Centralization

Cloud adoption has brought scalability and performance benefits, but it has also created highly concentrated digital dependencies.

Companies often rely on a single provider for:

- Web traffic routing
- Security filtering

While convenient, this model creates a dangerous scenario where a single internal failure can impact global digital infrastructure.

CLOUDFARE OUTAGES: A CRITICAL REVIEW OF INTERNAL FAILURES

The Hidden Risk of Intelligent Systems

As AI assistants become deeply embedded in digital workflows, their ability to process information autonomously introduces a new layer of cybersecurity risk. Unlike traditional systems that wait for human commands, AI copilots actively interpret data, generate responses, and make decisions based on context. This autonomy means that even subtle manipulations within the data they analyze can influence outcomes.

Security experts warn that organizations must rethink their defenses, focusing not only on protecting users but also on securing the decision-making pathways of AI systems themselves.

Lessons for Cyber Resilience

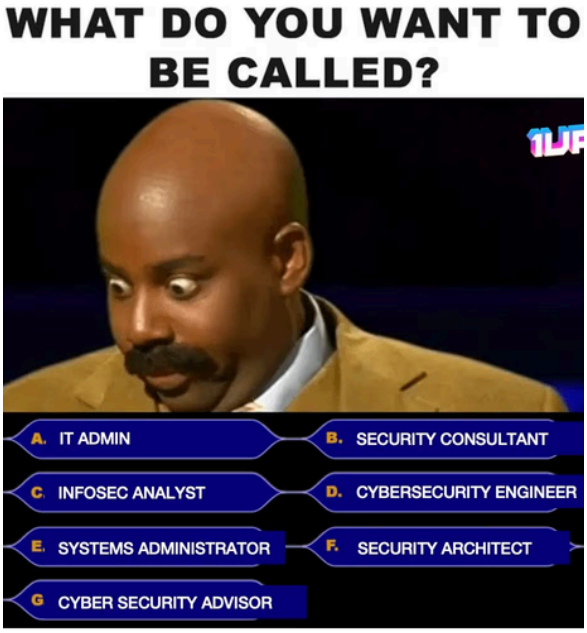
Although not every outage is caused by malicious activity, these incidents provide important lessons for cybersecurity and resilience planning.

- Organizations should prioritize:
- Multi-provider redundancy
- Failover infrastructure
- Distributed service architectures
- Continuous monitoring of third-party dependencies
- Cyber resilience is no longer just about defending against attackers—it also requires preparing for unexpected infrastructure breakdowns.

In an interconnected digital ecosystem, resilience is the true measure of security. One internal failure can disrupt millions of users worldwide.

Meme-O-Logy

OWASP PCCOE



MEMES

EVENT REWIND

Inauguration

CyberKavach 2024

Mrigaya

MockGre

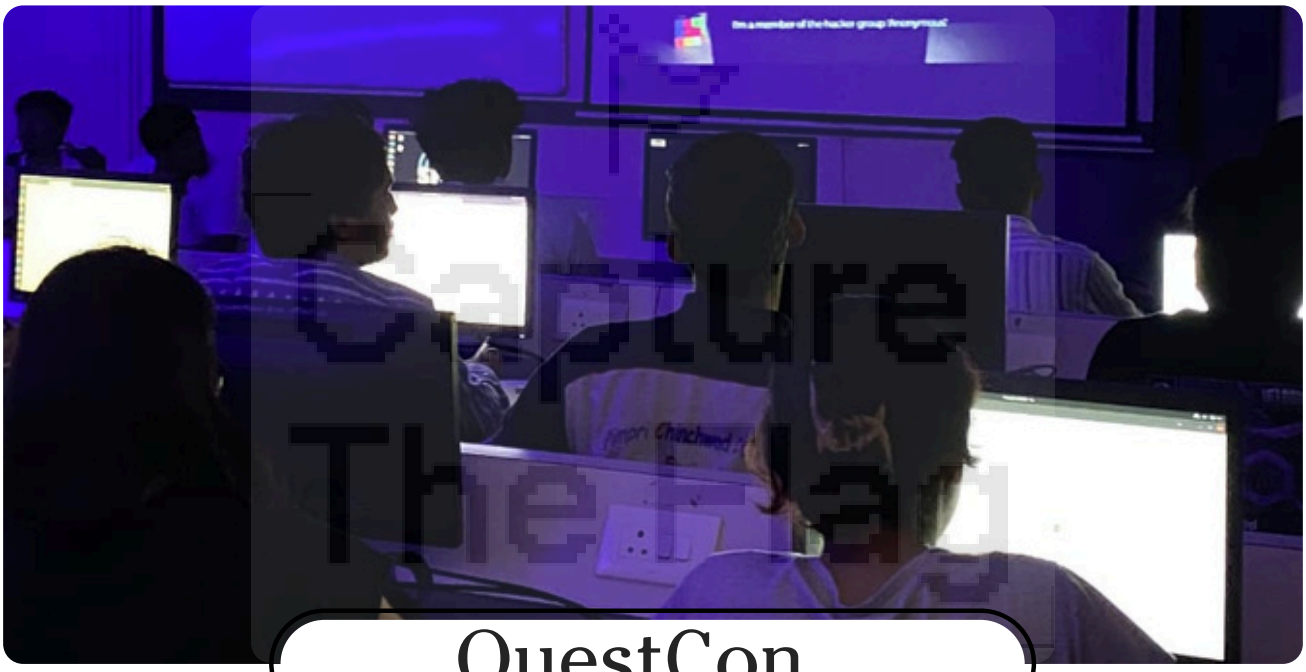
Faculty Session

DYP Session

Valedictory

Xsploit

Future Roadmap



QuestCon

Tresure Hunt

Our Partners

OWASP PCCOE

ROYAL ENFIELD SINCE 1901

TECHNOLIGHT
LIGHT OF LEARNING EDUCATION

VIRAL FISSION

We extend our sincere gratitude to our partners and sponsors for supporting our initiatives. Their contribution helps us conduct impactful events, promote cybersecurity awareness, and empower students with valuable learning opportunities.

Editorial Team

Chief Editors

Shivam Rai

Jahnavi Pinjan

Nishant Bhakar

Sumit Prasad

Assistant Editors

Aaryan

Zeeshan

Rudraksh