⚙️ INNOVATEX 4.0 – Presidency University

MakerSpace Cluster | Standard Rule Book Format

🧠 Event Overview

Field	Details
Event Name	Patch OR Perish
Cluster	Secure Coding Challenge
Event Type	Secure Coding Challenge
Mode	Offline
Team Size	Team of 2-4 Members
Duration	4 Hours

🎯 Event Task / Objective

1. To analyze a given vulnerable software application and **identify critical security vulnerabilities** aligned with the OWASP Top 10.
2. To **implement secure coding fixes** that eliminate vulnerabilities while maintaining the application's intended functionality.
3. To **document and communicate** the identified issues, their impact, and the remediation steps clearly and professionally.
4. To **encourage a security-first mindset** and practical understanding of real-world application security and secure software development practices

---

⚙️ Design / Technical Specifications

Application Environment:
Participants are provided with a pre-configured, intentionally vulnerable software application developed using common web technologies (such as HTML, CSS, JavaScript, backend scripting, and a relational database). The application simulates real-world use cases and security flaws.

Vulnerability Scope:
The challenge includes security issues aligned with the **OWASP Top 10**, such as SQL Injection, Cross-Site Scripting (XSS), insecure authentication, broken access control, insecure file handling, and improper input validation.

Fix Implementation Requirements:
All remediations must follow secure coding best practices, maintain original application functionality, and avoid introducing new vulnerabilities. Automated exploitation tools and unauthorized scripts are prohibited.

Submission Specifications:
Each team must submit the updated source code along with a concise document describing identified vulnerabilities, their impact, and the remediation techniques applied.

🧩 General Guidelines

1. Participation is **team-based**, with a maximum of **four members per team**. All team members must be registered before the event begins.
2. Participants must use **only the source code and resources provided by the organizers**. Any modification outside the defined scope is strictly prohibited.
3. Each team is required to **identify, analyze, and securely fix vulnerabilities** in the given application while preserving its intended functionality.
4. Submissions must include:
    - Updated source code
    - A brief explanation of identified vulnerabilities
    - Description of remediation steps taken
5. Participants must strictly adhere to the **event timeline and submission deadlines**.
6. Judges' decisions regarding **evaluation, scoring, and results** are final and binding.
7. The organizers reserve the right to **modify rules or disqualify teams** to ensure fair play and smooth conduct of the event.

🔋 Safety Rules

1. All equipment must comply with safety regulations (battery, wiring, mechanical setup).
2. Participants must follow event venue safety instructions.
3. No flammable, high-voltage, or hazardous materials allowed.
4. Spectators must remain outside designated operational areas.
5. **Sharing solutions, discussing vulnerabilities with other teams, or accessing external write-ups** is strictly prohibited.
6. Use of **automated exploitation tools, malicious scripts, or any software that may disrupt the competition environment** is not allowed.
7. **Plagiarism or code sharing** between teams will result in immediate disqualification.

8. Teams must **not attempt to attack or interfere with the infrastructure, servers, or systems** of other participants or the organizers.

9. Any form of **misconduct, unethical behavior, or violation of cybersecurity ethics** will lead to immediate disqualification.

10. Participants must operate **only within the provided challenge environment** and avoid actions that could cause data loss or service disruption

---

🧱 Event Rounds / Structure

Round	Description	Duration
Solving	Fix the Code	3Hours
Presentation	Presentation	30Mins
Final Evaluation	Results	30Mins

🧾 Submission Guidelines

✅ A Working Prototype.

✅A 2-3 minute video demonstration of the project.

✅ A short presentation (Powerpoint or PDF) explaining the project.

🧑‍⚖️ Judging Criteria

Parameter	Weightage
Score from Automated tools	75%
Presentation & Communication	25%

💰 Scoring Overview

Parameter	Weightage

Score from Automated tools	75
Presentation & Communication	25

Total : 100

🚫 Penalties & Disqualifications

Violation	Penalty
Late Submission	-10% Points
Unsafe Operation	Immediate Disqualification
Violation of Safety Zone	Disqualification
Misconduct or Unethical Practice	Permanent Ban

🏆 Awards & Recognition

Category	Prize	Remarks
1st Prize	₹30,000	Winner
2nd Prize	₹20,000	Runner-up
3rd Prize	₹10,000	Technical Merit

🧭 Event Team

Role	Name	Department / Club	Contact
Faculty Coordinator	Ms.Sterlin Minish T N	CSE	sterlinminish@presidencyuniversity.in
Event Lead	Piyush Tripathi	Hackeye Club	Piyush.2023CCS0092@presidencyuniversity.in
Technical Mentor	Robin Ponnama	Hackeye Club	ROBIN.20241CCS0106@presidencyuniversity.in
Logistics Lead	Ayush Kumar	Hackeye Club	AYUSH.20231CCS0065@presidencyuniversity.in

Media Lead	Gagan Dharmgond	Hackeye Club	GAGAN.20241CCS0117@presidencyuniversity.in

---

📋 General Instructions

- Follow all university and MakerSpace cluster policies.
- Respect judges, peers, and staff.
- Any form of plagiarism or code reuse will lead to disqualification.
- Decisions of the judges are final and binding.
- Certificates will be awarded to all valid participants.

⚡ Official Note

This Rule Book serves as the official guideline for all MakerSpace Cluster events under INNOVATEX 4.0, Presidency University.
Any updates or clarifications will be communicated officially via the MakerSpace WhatsApp community and notice board.