MARCH EVENTS

MAR 4
ACADEMY UP: CLOUD FOUNDATIONS
6:00pm to 8:00m
Kenneth C Rowe Management Building

MAR 4
SHIFTKEY LOUNGE: ENTREPRENEURSHIP
6:00pm-7:00pm
Goldberg Computer Science Building

MAR 5
ACADEMY UP: PRACTICAL CYBERSECURITY
6:00pm to 8:00pm
Kenneth C Rowe Management Building

MAR 6
WOMEN'S EXCELLENCE GALA
5:00pm to 7:00pm
Dalhousie Student Union Building

MAR 12
INDUSTRY SHOWCASE: AVANADE
4:00pm to 5:30pm
Goldberg Computer Science Building

MAR 12
ACADEMY UP: PRACTICAL CYBERSECURITY
6:00pm to 8:00pm
Kenneth C Rowe Management Building

MAR 13
INDUSTRY SHOWCASE: RBC
4:00pm to 5:30pm
Goldberg Computer Science Building

MAR 15
SNOWBALL AWARDS
5:00pm to 11:30pm
The Westin Nova Scotian

MAR 17
HAPPY SAINT PATRICK'S DAY

MAR 18
SHIFTKEY LOUNGE: FINTECH
6:00pm to 7:00pm
Goldberg Computer Science Building

MAR 19
ACADEMY UP: PRACTICAL CYBERSECURITY
6:00pm to 8:00pm
Kenneth C Rowe Management Building

MAR 20
SPEECH CRAFT WORKSHOP
5:30pm to 8:30pm
Goldberg Computer Science Building

MAR 22
CONSULTING 101 WORKSHOP
1:00pm to 5:00pm
Goldberg Computer Science Building

MAR 24
ALUMNI SPEAKS: ANDRES COLLART
4:00pm to 5:30pm
Goldberg Computer Science Building

MAR 26
ACADEMY UP: PRACTICAL CYBERSECURITY
6:00pm to 8:00pm
Kenneth C Rowe Management Building

MAR 28
INDUSTRY SHOWCASE: VOLTA
4:00 pm to 5:30pm
Goldberg Computer Science Building

Tell us what you think

Practical Cybersecurity

Instructor – Aman Bhalla

WEEK 3 LEARNING OBJECTIVES

Understand OWASP & Web Application Security

- Learn about **OWASP Top 10 threats** and how they impact applications.
- Discover **how the OWASP list is maintained and updated**.

Explore Advanced Cyber Threats

- Understand **zero-day exploits, supply chain attacks, and injection vulnerabilities**.
- Learn **real-world examples of application security failures**.

Dive Deep into Incident Response

- Explore the **6 phases of incident response** and how organizations handle cyberattacks.

Engage in a Hands-On Threat Hunting Activity

- Identify **Indicators of Compromise (IoCs)** and map attack tactics.

WHAT IS APPLICATION SECURITY?

Definition: Application security refers to **practices that prevent security vulnerabilities in software applications**.

Why is it Important?

- **80%** of cyberattacks target **web applications**.
- Attackers **exploit flaws in code** to steal data, hijack accounts, or inject malicious scripts.
- **Proactive security** is cheaper and more effective than fixing security breaches later.

Example: The **Equifax data breach (2017)** exposed **147M customer records** due to an **unpatched software vulnerability** in a web application.

INTRODUCTION TO OWASP

What is OWASP?

- The **Open Worldwide Application Security Project (OWASP)** is a nonprofit focused on improving **software security**.
- Provides **open-source tools, frameworks, and security best practices**.
- Maintains the **OWASP Top 10** – a list of **the most critical web application security risks**.

Why does this matter? Many compliance standards, like **PCI-DSS and NIST**, reference OWASP guidelines.

HOW IS OWASP TOP 10 UPDATED?

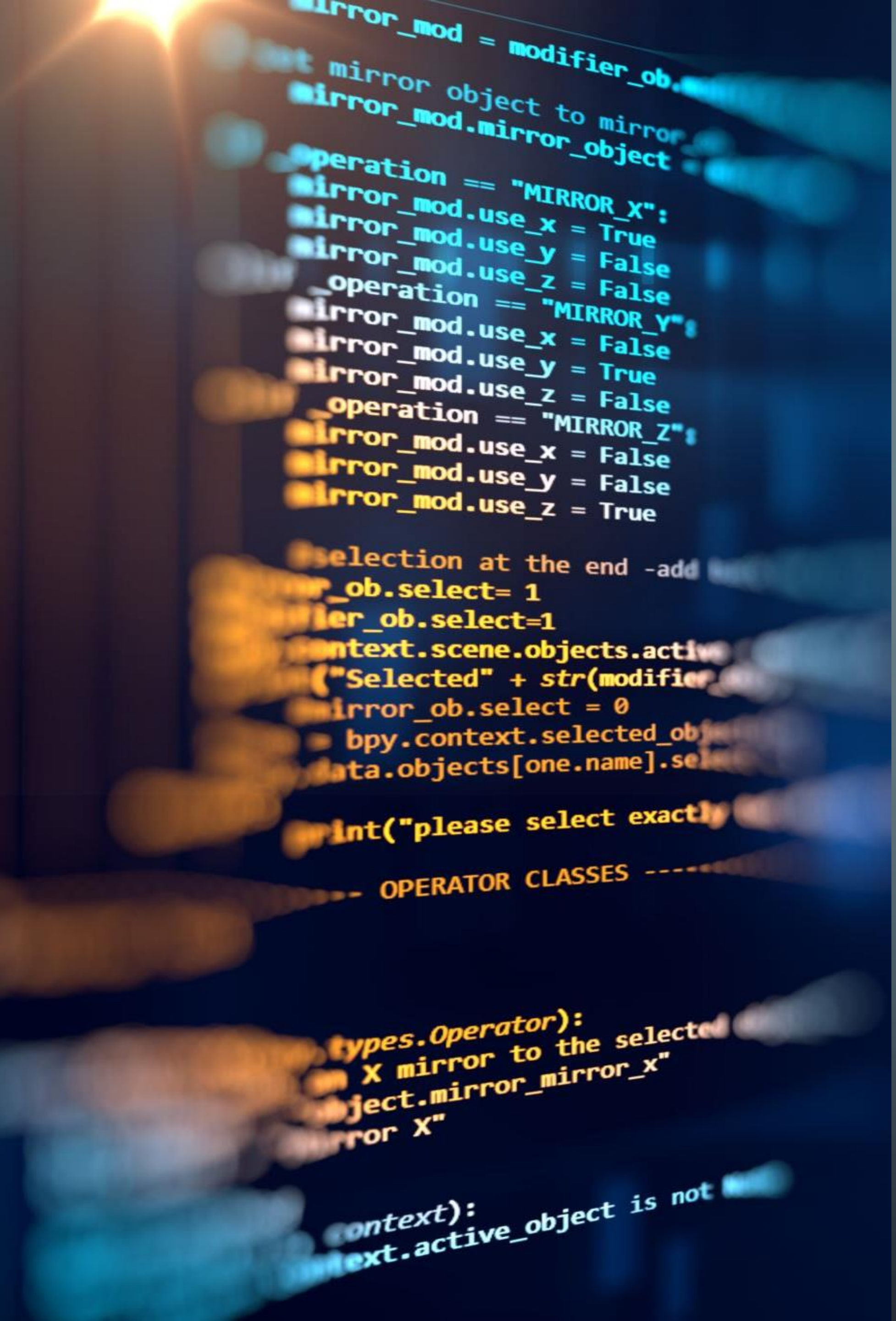
OWASP Top 10 is updated every 3-4 years based on:

Global data collection from security research.

Threat intelligence reports & vulnerability trends.

Ranking based on exploitability & impact.

Latest update: The **2021 OWASP Top 10** introduced **new categories like Insecure Design and SSRF**.



```
irror_mod = modifier_ob.
mirror object to mirror
irror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
 operation == "MIRROR_Y"
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z"
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
ier_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifie
irror_ob.select = 0
 bpy.context.selected_obj
ata.objects[one.name].se

int("please select exactl

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

ontext):
ext.active_object is not
```

OWASP TOP 10 THREATS (2021)

Most critical web application vulnerabilities:

1. Broken Access Control
2. Cryptographic Failures
3. Injection Attacks
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable & Outdated Components
7. Identification & Authentication Failures
8. Software & Data Integrity Failures
9. Security Logging & Monitoring Failures
10. Server-Side Request Forgery (SSRF)

BROKEN ACCESS CONTROL

Definition: Attackers bypass permissions to access restricted data or functionalities.

Example: A normal user modifies a URL to access an admin-only page.

Mitigation: Enforce **role-based access control (RBAC)** and strict **session management**.

CRYPTOGRAPHIC FAILURES

Definition: Weak encryption or missing encryption leads to data breaches.

Example: Websites storing passwords in plaintext instead of hashing them.

Mitigation: Use **AES-256, TLS 1.3, and bcrypt for passwords**.

INJECTION ATTACKS (SQL, COMMAND, LDAP, NOSQL INJECTION)

Definition: Attackers inject malicious code into user inputs, exploiting weak database or command handling.

Example: OR 1=1 -- in a login field bypasses authentication.

Mitigation: Use prepared statements and sanitize all inputs.

INSECURE DESIGN

Definition: Applications designed **without security in mind**, allowing for easy exploitation.

Example: An e-commerce site allowing **unlimited failed login attempts** without a lockout policy.

Mitigation: Conduct **threat modelling** and secure application design reviews.

SECURITY MISCONFIGURATION

Definition: Applications left with **default settings, exposed files, or unnecessary features** enabled.

Example: A server left with an **open directory listing**, exposing sensitive files.

Mitigation: Regular **configuration audits** and **principle** of **least privilege** implementation.

VULNERABLE & OUTDATED COMPONENTS

Definition: Using outdated or vulnerable software libraries and frameworks.

Example: The **Log4j vulnerability (2021)** allowed attackers to execute remote code.

Mitigation: Implement **automated dependency tracking** and apply patches regularly.

IDENTIFICATION & AUTHENTICATION FAILURES

Definition: Weak authentication mechanisms allow unauthorized access.

Example: Allowing **brute force attacks** without account lockout mechanisms.

Mitigation: Enforce **Multi-Factor Authentication (MFA)** and strong password policies.

SOFTWARE & DATA INTEGRITY FAILURES

Definition: Unverified software updates and insecure serialization leading to code execution attacks.

Example: A malicious actor **injects code into a software update**, compromising all users.

Mitigation: Use **signed updates and integrity checks** for all external components.

SECURITY LOGGING & MONITORING FAILURES

Definition: Lack of effective logging allows attacks to go undetected.

Example: A hacker attempts 1000 failed logins, but no alerts are triggered.

Mitigation: Implement **real-time security monitoring** and **log correlation** for early detection.

SERVER-SIDE REQUEST FORGERY (SSRF)

Definition: Attackers **trick a web server into making unauthorized internal requests**.

Example: A cloud-based web app retrieves external files but **allows unrestricted internal access**, letting an attacker extract data.

Mitigation: Restrict **remote network calls** and validate URLs before processing requests.

WHAT IS INCIDENT RESPONSE?

Incident response (IR) is a structured approach organizations use to **identify, manage, and recover from cybersecurity incidents**. A well-defined **Incident Response Plan (IRP)** helps minimize damage, reduce recovery time, and prevent future attacks.

Why is Incident Response Important?

- **Reduces downtime & financial losses** from cyberattacks.
- **Minimizes data breaches** by containing threats quickly.
- **Ensures compliance** with industry security regulations (e.g., GDPR, NIST).

THE 6 PHASES OF INCIDENT RESPONSE

The **Incident Response Plan (IRP)** includes:

1. **Preparation** – Establish security policies & train employees.
2. **Detection & Analysis** – Identify security breaches.
3. **Containment** - Limit the damage.
4. **Eradication** – Remove threats.
5. **Recovery** – Restore systems to normal.
6. **Post-Incident Analysis** – Learn from the attack & improve security.

PREPARATION

Goal: Ensure the organization is **ready to handle incidents** effectively.

- Establish **security policies & protocols**.
- Train employees on **cybersecurity best practices** (phishing awareness, social engineering).
- Set up **logging & monitoring tools** to detect threats early.
- Define **incident severity levels** (low, medium, high, critical).
- Conduct **Tabletop Exercises (TTX)** – Simulated cyberattack drills.

DETECTION & ANALYSIS

Goal: Identify the attack, assess its scope, and determine the impact.

- Use **Intrusion Detection/Prevention Systems (IDS/IPS)** to spot unusual activity.
- Analyze **firewall logs, system alerts, and network traffic** for anomalies.
- Identify **Indicators of Compromise (IoCs)** (e.g., unusual login attempts, data exfiltration).
- Categorize the attack: **Malware, Phishing, Ransomware, DDoS, Insider Threat, etc.**

Example: A **DDoS attack floods a company's website**, causing slowdowns—security logs reveal thousands of fake requests from a single region.

CONTAINMENT

Goal: Isolate & limit the impact of the attack.

- **Short-term containment:** Disconnect affected systems from the network.
- **Long-term containment:** Apply security patches, strengthen authentication.
- **Quarantine infected files** to prevent malware from spreading.
- Implement **temporary firewall rules** to block further attacks.

Example: A **ransomware attack** encrypts company files—security teams **immediately disconnect infected systems** to stop the spread.

ERADICATION

Goal: Remove the threat completely from the environment.

- **Delete malware files**, malicious accounts, and backdoors.
- Apply **security patches & software updates** to fix vulnerabilities.
- Strengthen **endpoint security** to prevent reinfection.
- Use **threat intelligence reports** to understand the attacker's tactics.

Example: After removing a **trojan virus**, security teams discover it entered via an **unpatched software vulnerability**—they immediately apply the missing patch.

RECOVERY

Goal: Restore affected systems & resume normal operations securely.

- Restore data from **clean backups** (ensure backups weren’t compromised).
- Monitor for **signs of reinfection** before reconnecting systems.
- Conduct **post-incident vulnerability assessments**.
- Strengthen **network defenses** (firewalls, MFA, encryption).

Example: After a **data breach**, an organization resets **all employee passwords** and enforces **Multi-Factor Authentication (MFA)** for added security.

POST-INCIDENT REVIEW

Goal: Analyze the attack, improve defenses, and prevent recurrence.

- Conduct a **post-mortem analysis** – What happened? What went wrong?
- Update the **Incident Response Plan (IRP)** based on findings.
- Implement **security awareness training** for employees.

CASE STUDY – UBER DATA BREACH (2022)

What Happened?

- Hacker used **social engineering** to access Uber's internal systems.
- **MFA Bypass Attack** tricked employees into granting access.

Incident Response Actions:

- Uber **revoked compromised credentials** and locked down access.
- Implemented **stricter MFA policies** and enhanced security awareness.

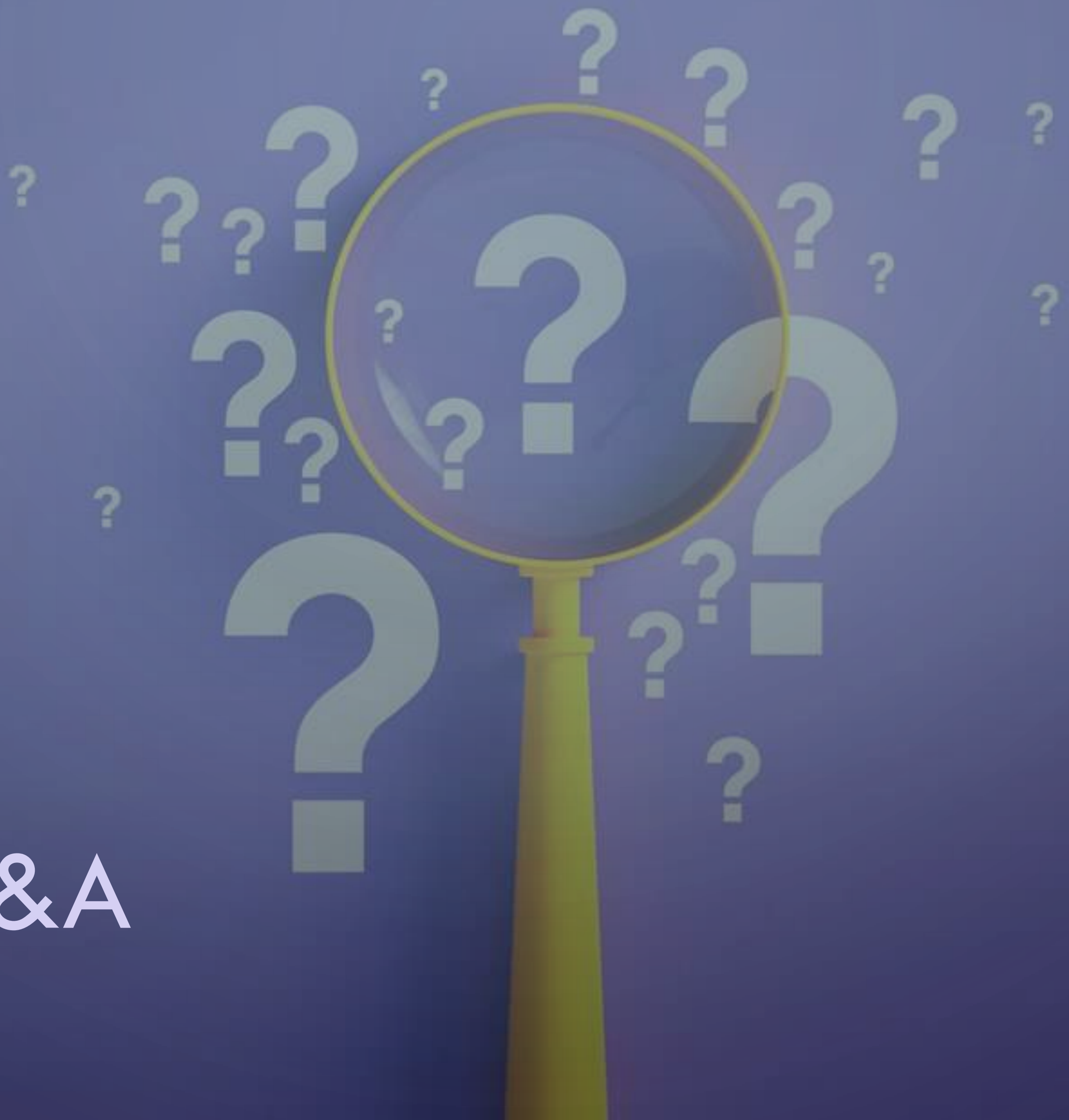
Conclusion: Employee awareness is critical – even advanced security can fail to social engineering.

KEY TAKEAWAYS

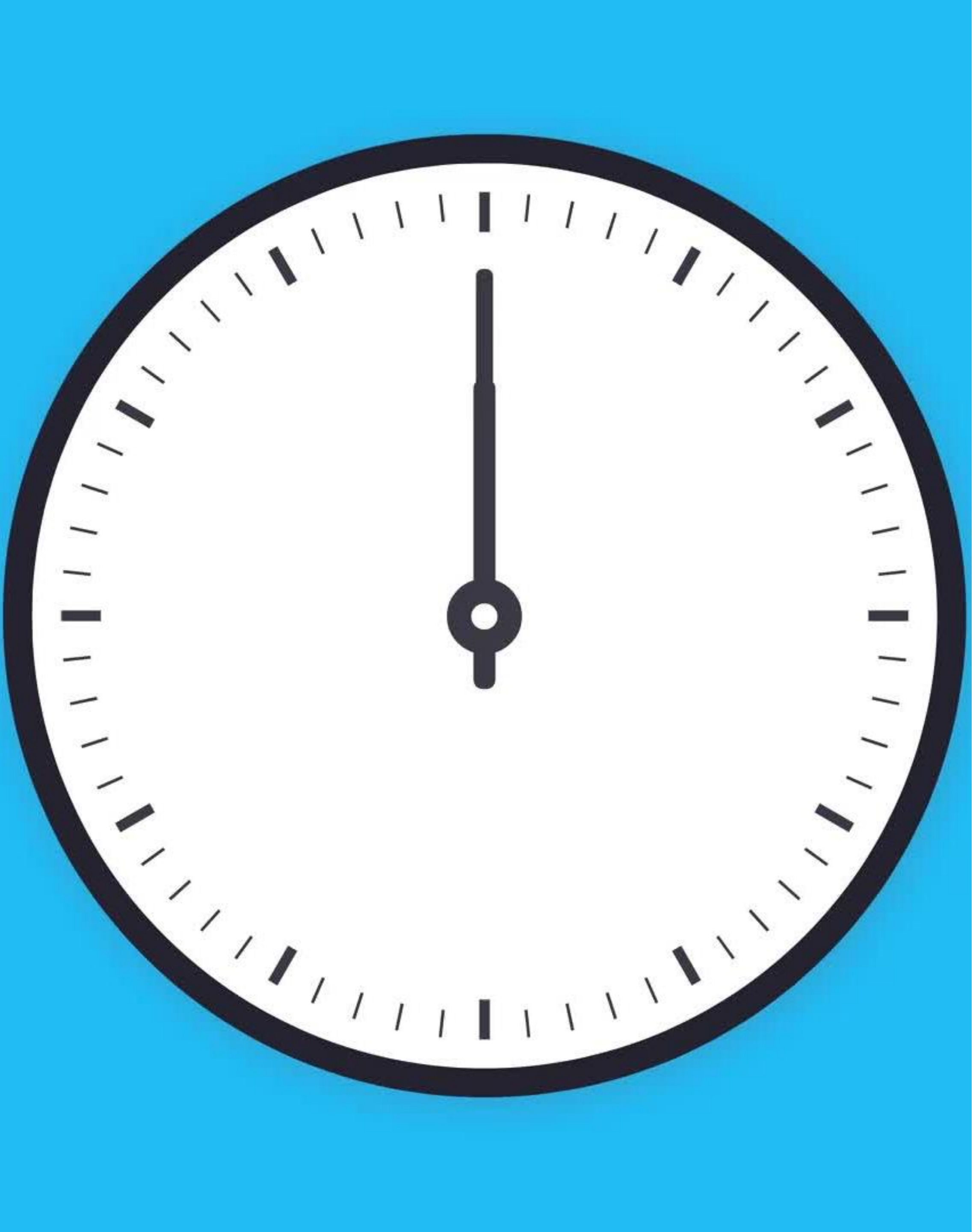
- **OWASP Top 10** is **critical** – Web applications are prime attack targets.
- **Incident Response** must be structured – A well-defined process minimizes damage.
- Cyber Threat Intelligence helps organizations stay ahead of attacks.
- **Threat Hunting is an advanced cybersecurity skill** used in real-world SOCs.

NEXT WEEK PREVIEW

- Introduction to **Penetration Testing**
- Exploring Ethical Hacking Concepts.
- **Cyber Laws & Ethics** – Understanding legal aspects of hacking.
- **Final Exam Overview** – What to expect & key topics to review.



Q&A



Quiz Time!

- Time Limit – 15 Minutes. Quiz begins at 7:45 pm and will close at 8:00 pm.
- Questions: MCQs, True or False and Short Answers.
- Some questions require multiple choices, only choosing all the correct ones will get points.