Web Application Bug Hunting
Project Synopsis Presentation
Date: 15/02/2023

Major Project (ICI651)
Degree : BCA CTIS

Project Guide:
Mr. Praful Saxena
Senior Faculty (i-Nurture TMU)

Abdul Ahad (TCA2056002)
Kafeel Ahmad (TCA2056013)
Rishi (TCA2056018)

FACULTY OF ENGINEERING & COMPUTING SCIENCES
TEERTHANKER MAHAVEER UNIVERSITY, MORADABAD

Student Name	Role
Abdul Ahad	Bug Hunter
Kafeel Ahmad	Bug Hunter
Rishi	Reporting

Content

1. Project Brief
2. What is VAPT?
3. Methodology
4. Technologies/ Tools to be used
5. Context Diagram (Overall Project)
6. Flow Chart
7. Data Flow Diagram (DFD)
8. Advantages
9. References

- Web application penetration testing, also known as web app pen testing, is the process of identifying vulnerabilities in a web application by attempting to exploit its weaknesses. This is typically done by using various tools and techniques to simulate attacks that a malicious hacker might use, with the goal of identifying and remedying any security flaws before they can be exploited by real attackers. The ultimate aim is to improve the security posture of the web application and protect against potential security breaches.

- Basically, WAPT (Web Applications and Penetration Testing) is the process of finding web app based vulnerability on the Websites.

- In this project, we will find vulnerabilities and exploit them and we also give remediation of those vulnerabilities.

- Combination of manual and automated tests to identify vulnerabilities, security flaws and/or threats in a web applications, Networks, Systems, Mobile Apps.
- Categorized into three types:
  - White box: Tester has complete access and in-depth knowledge of the system. Access to source code is usually given.
  - Black box: Tester is given little to no information about the system. Just the URL of the application is usually given.
  - Grey box: Combination of white box and black box penetration testing. Limited information and access is given to the tester.
- Most important thing to keep in mind: you need permission to perform a security test!
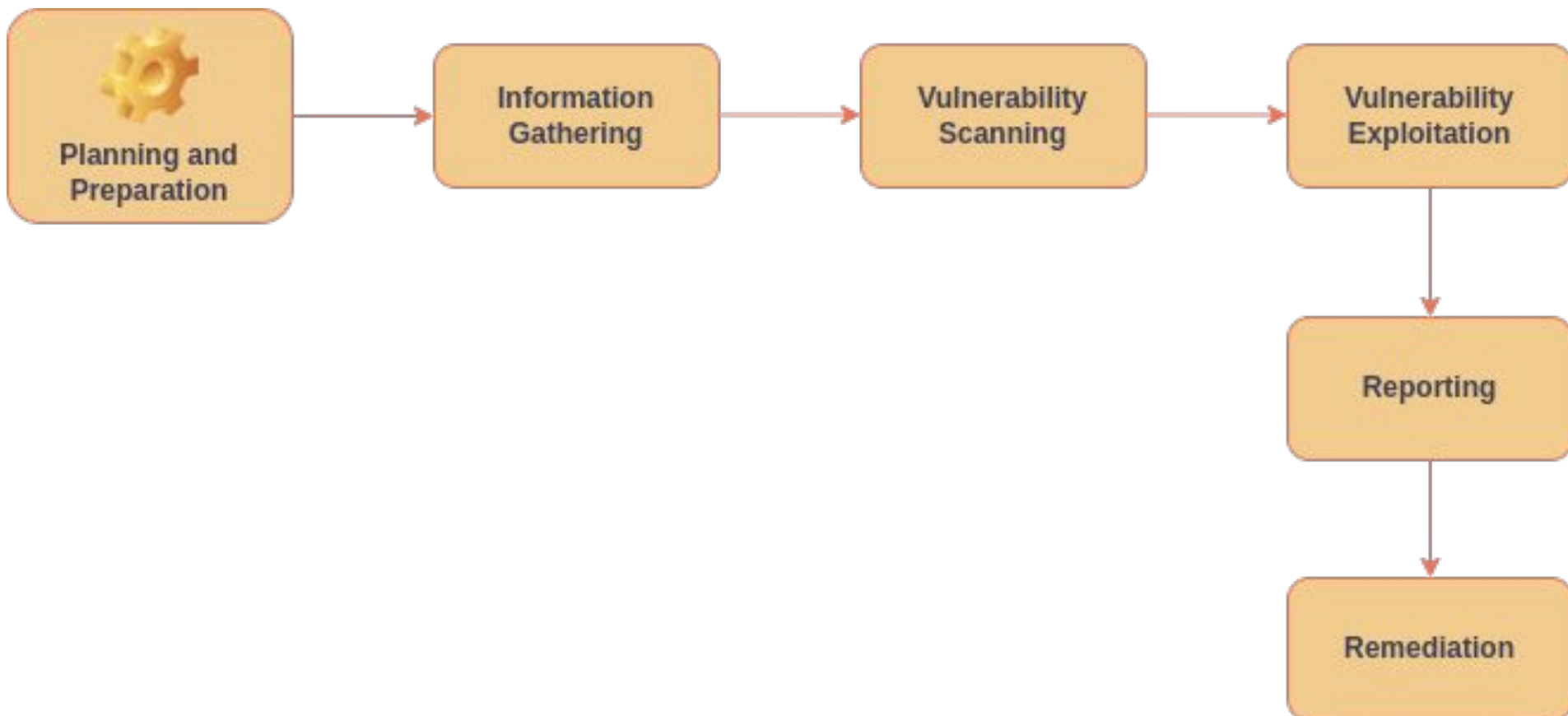
Web Application Security Testing Methodology

Information Gathering → Planning Analysis → Vulnerability Detection → Penetration Testing → Reporting

- OWASP Zap

- Burp-Suite Community Edition

- Nikto

```
+----------------+              +------------------+
|                |              |                  |
|    Web App     |              |     Pen Tester   |
|                |              |                  |
+----------------+              +------------------+
        |                               |
        |      1. Request Pen Test       |
        +------------------------------->|
        |                               |
        |      2. Grant Access           |
        |<------------------------------+
        |                               |
        |      3. Provide Test Scope      |
        +------------------------------->|
        |                               |
        |      4. Conduct Testing         |
        |<------------------------------+
        |                               |
        |      5. Report Findings          |
        +------------------------------->|
        |                               |
        |      6. Remediate               |
        |<------------------------------+
        |                               |
        |      7. Verify Remediation       |
        +------------------------------->|
        |                               |
        |      8. Final Report            |
        |<------------------------------+
```
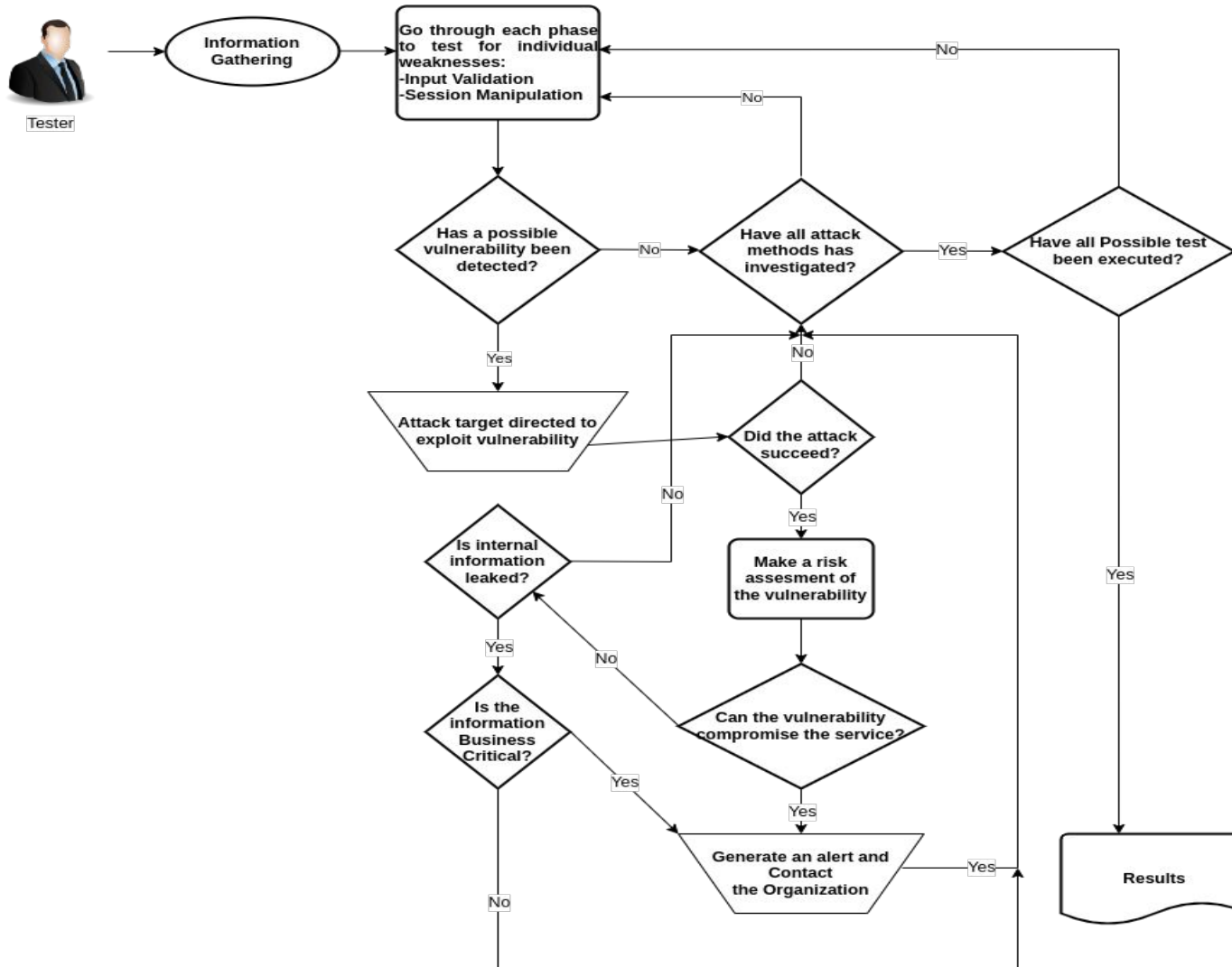
Guidelines: This slide is optional

1. Identify Security Vulnerabilities
2. Improve Security Posture
3. Meet Compliance Requirements
4. Save Money and Reputation
5. Enhance User Trust
6. Continuous Improvement

References, if any

- https://www.ecsbiztech.com/web-vulnerability-assessment-penetration-testing-vapt/#:~:text=Web%20Application%20VAPT%20is%20essentially,in%20web%20applications%20and%20APIs.
- https://xiarch.com/services/web-application-penetration-testing/
- https://ieeexplore.ieee.org/abstract/document/8463920
- https://link.springer.com/article/10.1007/s11416-014-0231-x
- https://ieeexplore.ieee.org/abstract/document/5593250

THANKS