PUNE VIDYARTHI GRIHA'S COLLEGE OF ENGINEERING & S. S. DHAMANKAR INSTITUTE OF MANAGEMENT, NASHIK

DEPARTMENT OF COMPUTER ENGINEERING

INTERNSHIP BASED SEMINAR

ON

ETHICAL HACKING

BY

HRITIK RAKESH SHIRSATH

GUIDE

PROF. I M SHAIKH

FRIDAY, 29 APRIL 2022

INTERNSHIP
ON
“ETHICAL HACKING”

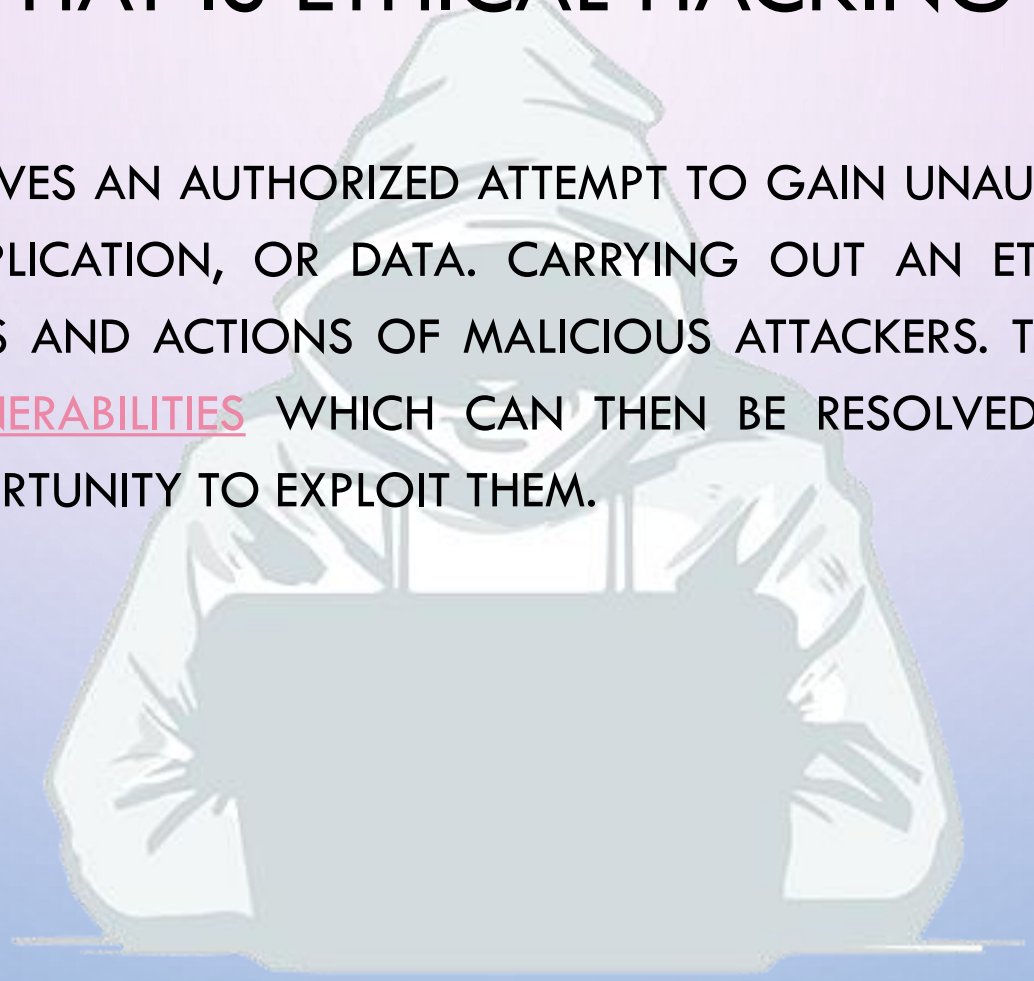
DURATION
8 WEEK INTERNSHIP
ON
“ETHICAL HACKING”

CONTENT

- BASICS OF INFORMATION SECURITY AND COMPUTER NETWORKING
- INFORMATION GATHERING AND BASICS OF WEB DEVELOPMENT
- INTRODUCTION TO WEB VAPT, OWASP AND SQL INJECTIONS
- ADVANCED WEB APPLICATION ATTACKS
- CLIENT SIDE ATTACKS
- IDENTIFYING SECURITY MISCONFIGURATIONS AND EXPLOITING OUTDATED WEB APPLICATIONS
- AUTOMATING VAPT AND SECURE CODE DEVELOPMENT
- DOCUMENTING AND REPORTING VULNERABILITIES

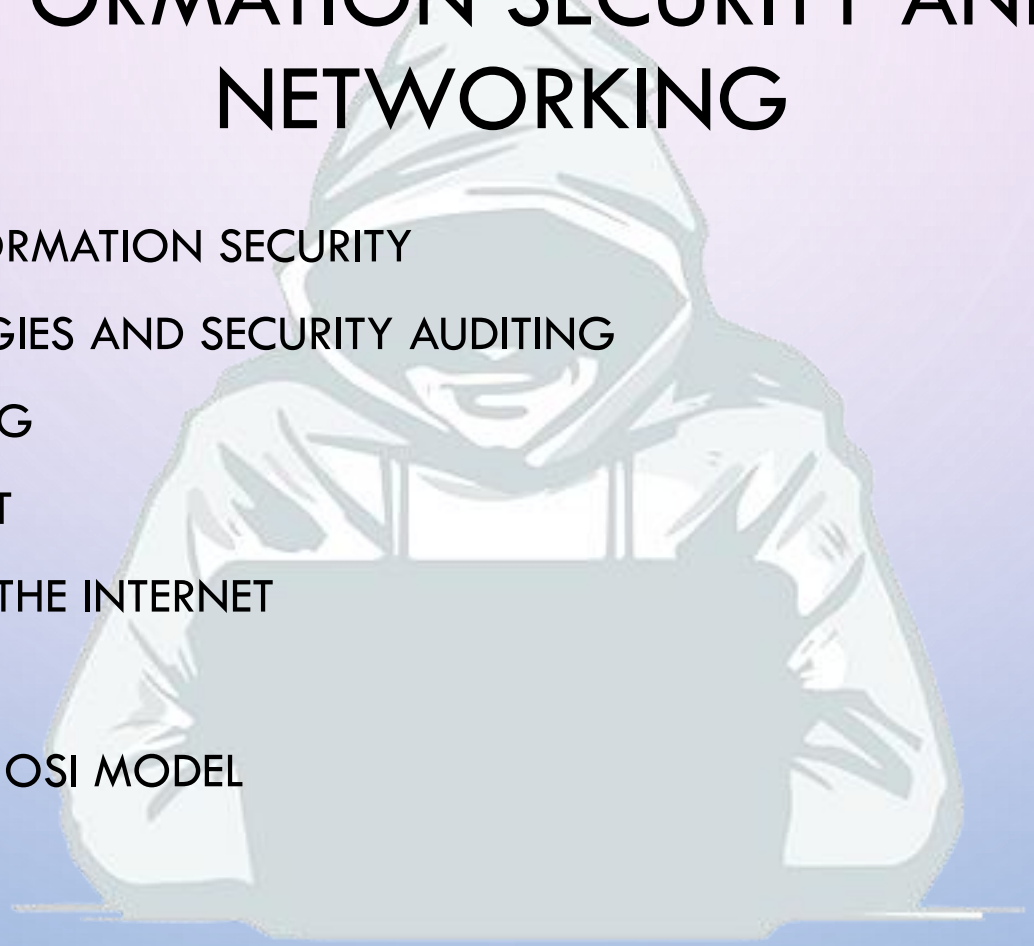
WHAT IS ETHICAL HACKING ?

ETHICAL HACKING INVOLVES AN AUTHORIZED ATTEMPT TO GAIN UNAUTHORIZED ACCESS TO A COMPUTER SYSTEM, APPLICATION, OR DATA. CARRYING OUT AN ETHICAL HACK INVOLVES DUPLICATING STRATEGIES AND ACTIONS OF MALICIOUS ATTACKERS. THIS PRACTICE HELPS TO IDENTIFY SECURITY VULNERABILITIES WHICH CAN THEN BE RESOLVED BEFORE A MALICIOUS ATTACKER HAS THE OPPORTUNITY TO EXPLOIT THEM.



WEEK 1

BASICS OF INFORMATION SECURITY AND COMPUTER NETWORKING



- INTRODUCTION TO INFORMATION SECURITY
- HACKING METHODOLOGIES AND SECURITY AUDITING
- COMPUTER NETWORKING
- IP ADDRESSING AND NAT
- THE GOOGLE MAPS OF THE INTERNET
- PORTS AND SERVICES
- PROTOCOLS, TCPIP AND OSI MODEL
- PROXY AND VPN

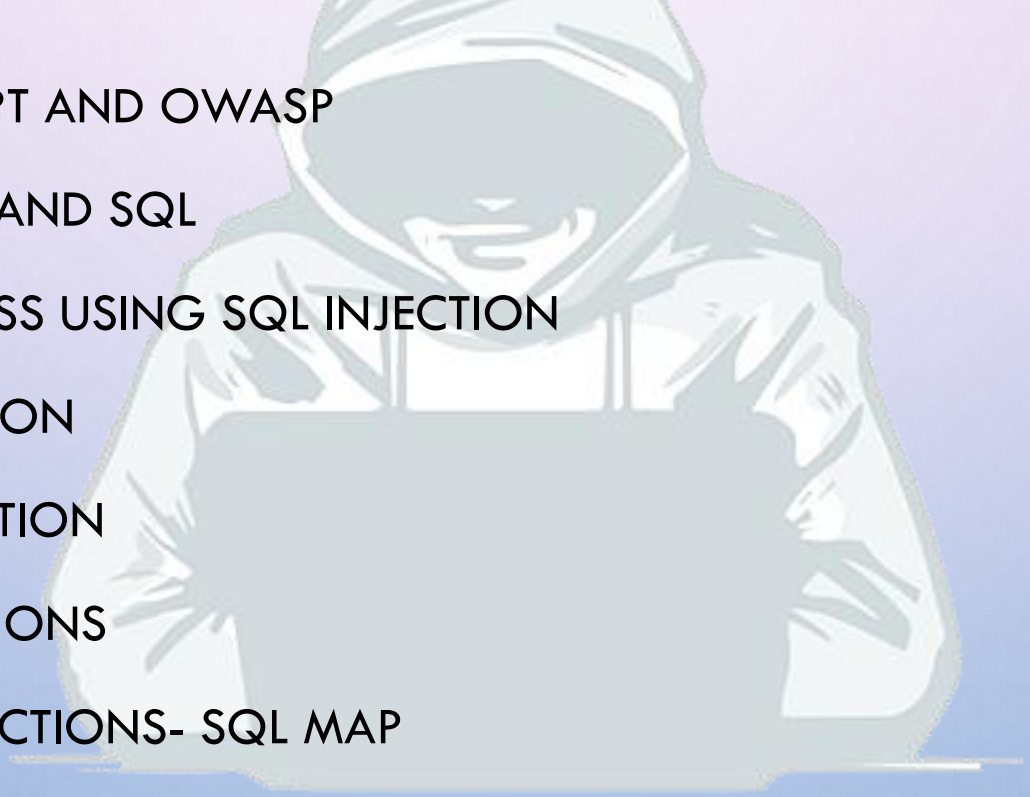
WEEK 2

INFORMATION GATHERING AND BASICS OF WEB DEVELOPMENT

- DIGITAL FOOTPRINTS AND INFORMATION GATHERING
- ADVANCED INFORMATION GATHERING ABOUT PEOPLE AND WEBSITES
- GOOGLE DORKING- HACKING USING GOOGLE
- INTRODUCTION TO WEB ARCHITECTURE AND UNDERSTANDING COMMON SECURITY MISCONCEPTIONS
- HTML BASICS
- HTML AND INTRODUCTION TO JAVASCRIPT
- INTRODUCTION TO PHP AND SETTING UP XAMPP
- PUTTING BRAINS INTO BEAUTY- WORKING WITH PHP
- HANDLING USER INPUT AND BUILDING BASIC APPLICATIONS USING PHP

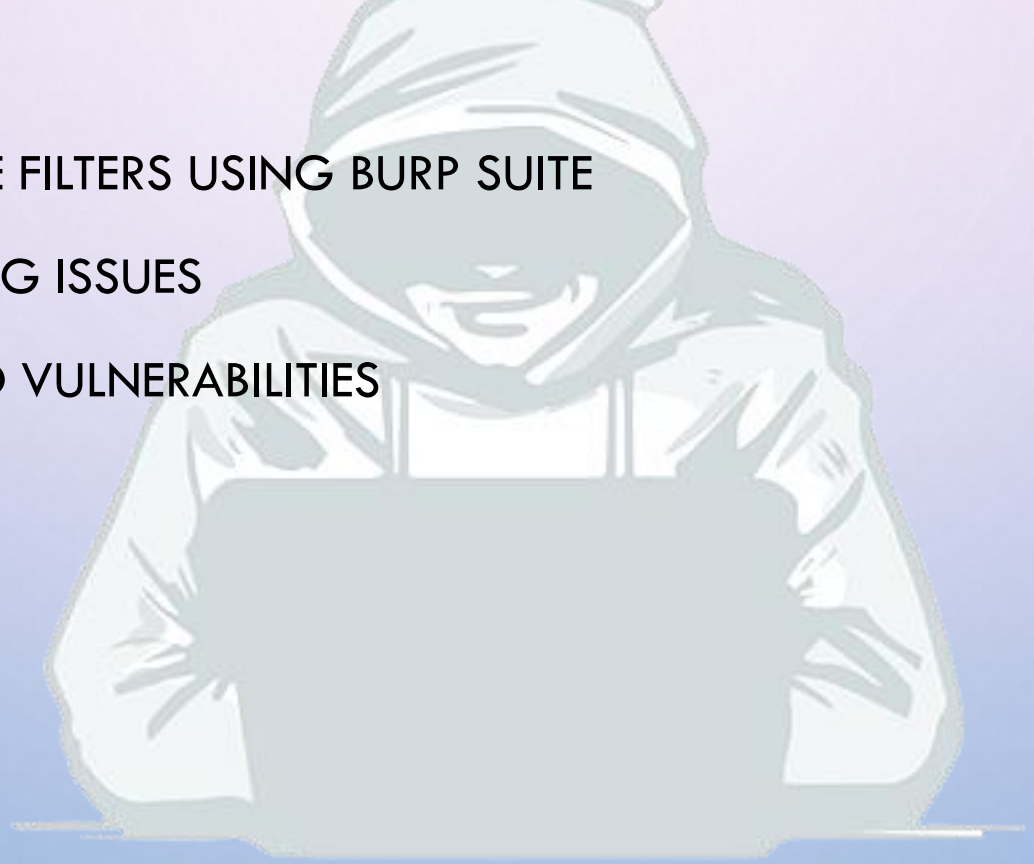
WEEK 3

INTRODUCTION TO WEB VAPT, OWASP AND SQL INJECTIONS



- INTRODUCTION TO VAPT AND OWASP
- BASICS OF DATABASES AND SQL
- AUTHENTICATION BYPASS USING SQL INJECTION
- GET BASED SQL INJECTION
- POST BASED SQL INJECTION
- ADVANCED SQL INJECTIONS
- AUTOMATING SQL INJECTIONS- SQL MAP

WEEK 4
ADVANCED WEB APPLICATION ATTACKS



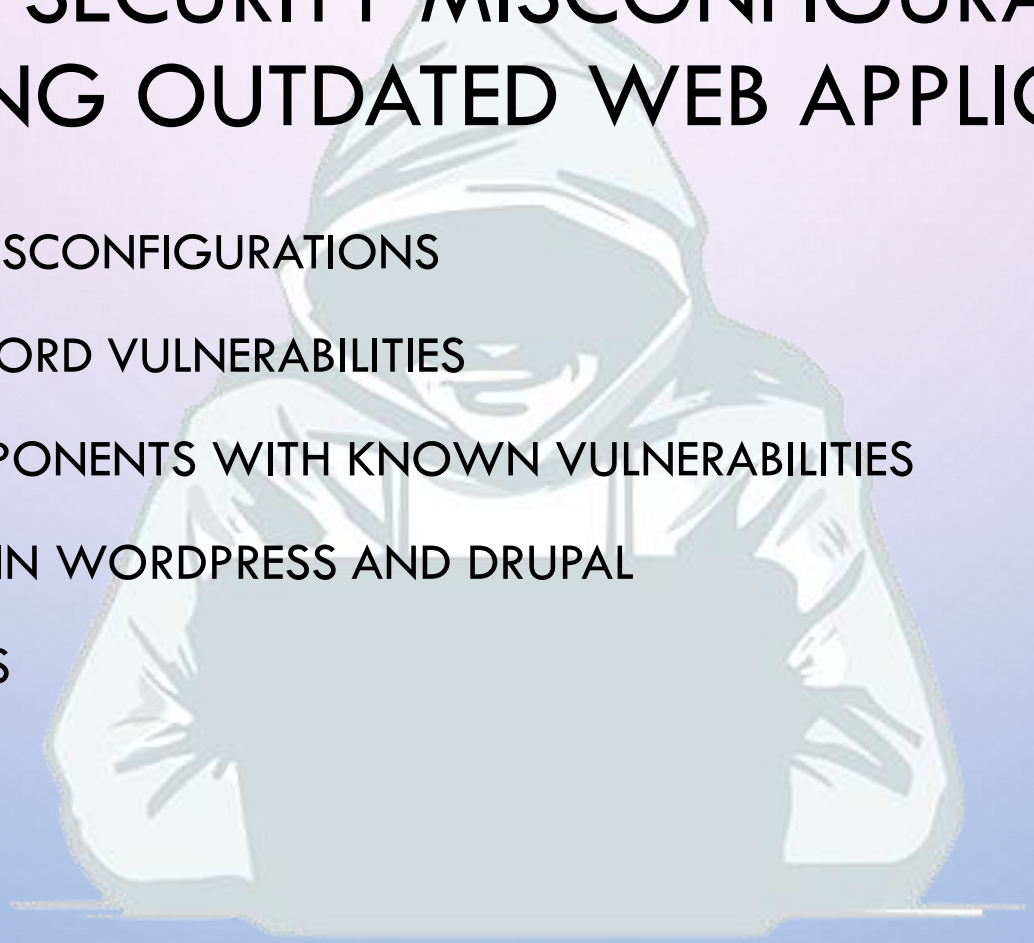
- BYPASSING CLIENT SIDE FILTERS USING BURP SUITE
- IDOR AND RATE-LIMITING ISSUES
- ARBITRARY FILE UPLOAD VULNERABILITIES

WEEK 5
CLIENT SIDE ATTACKS

- UNDERSTANDING IMPORTANT RESPONSE HEADERS, DOM, AND EVENT LISTENERS
- FUNDAMENTALS OF CROSS SITE SCRIPTING (XSS)
- UNDERSTANDING FORCED BROWSING AND SESSION-COOKIE FLAWS
- CROSS SITE REQUEST FORGERY (CSRF) AND OPEN REDIRECTIONS
- DICTIONARY BASED BRUTE FORCE ATTACKS
- LOGICAL BRUTE FORCE ATTACKS
- PERSONALLY IDENTIFIABLE INFORMATION (PII) LEAKAGE AND SENSITIVE INFORMATION DISCLOSURE

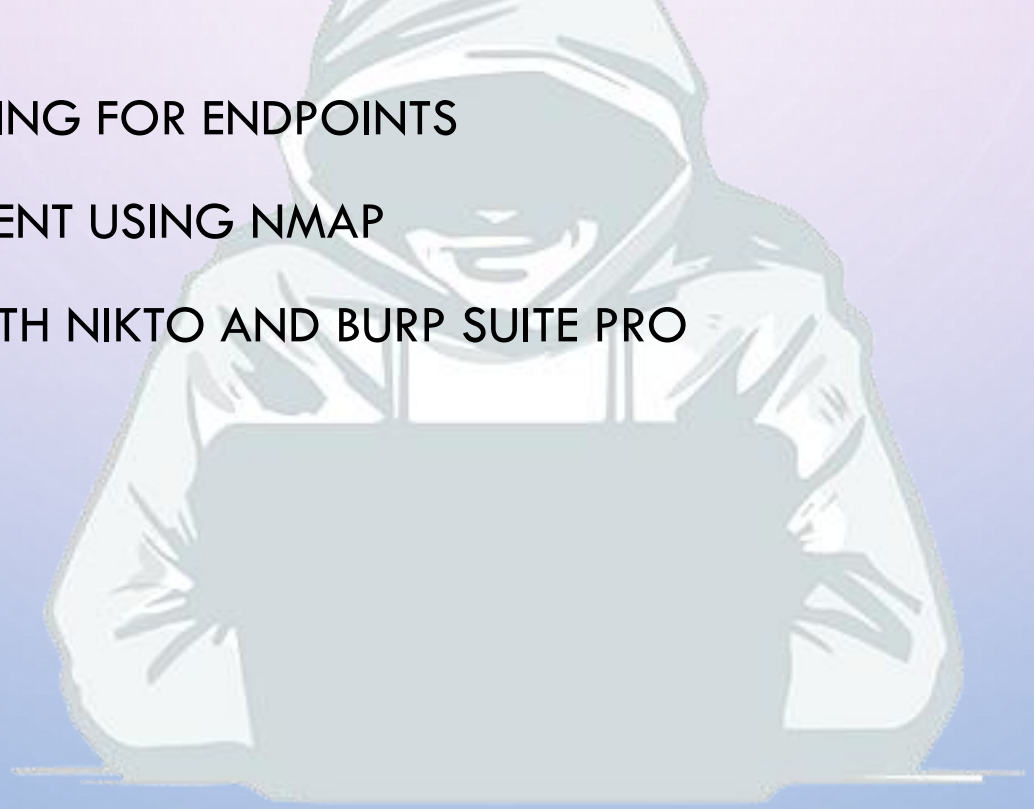
WEEK 6

IDENTIFYING SECURITY MISCONFIGURATIONS AND EXPLOITING OUTDATED WEB APPLICATIONS



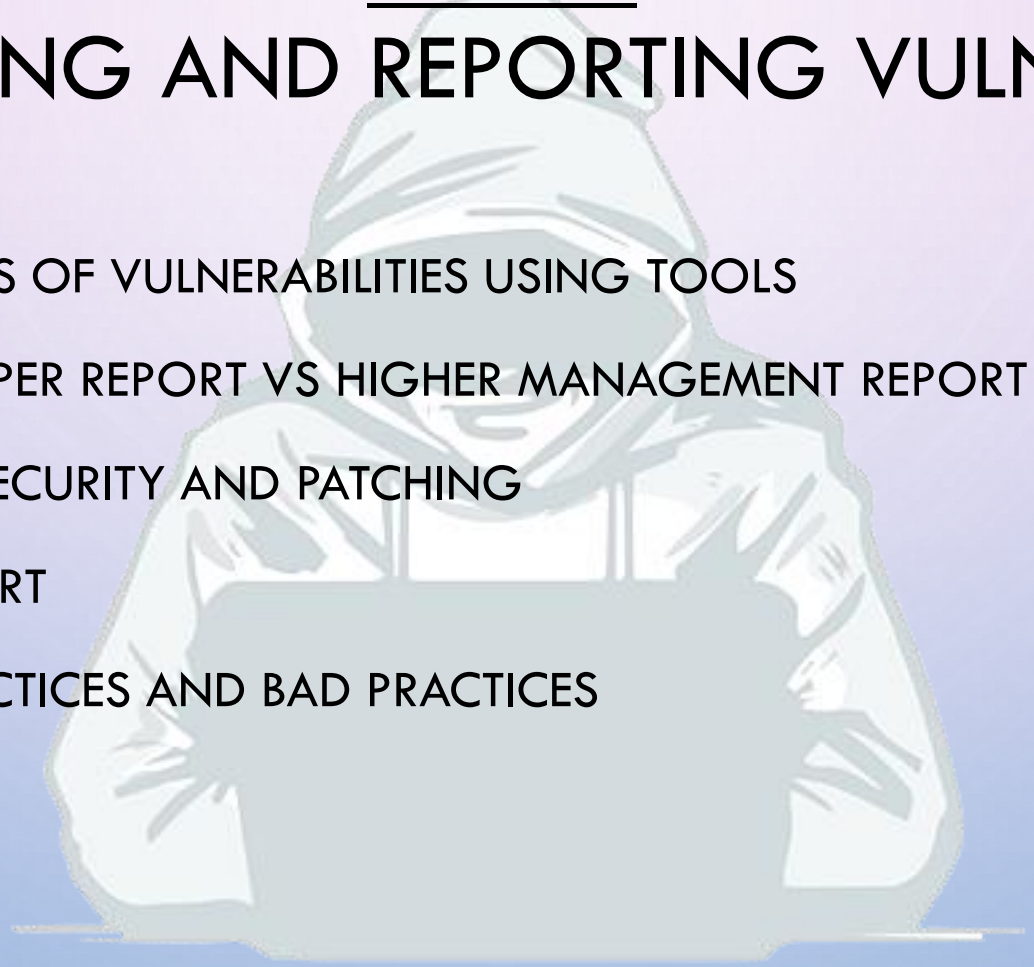
- COMMON SECURITY MISCONFIGURATIONS
- DEFAULT WEAK PASSWORD VULNERABILITIES
- FINGERPRINTING COMPONENTS WITH KNOWN VULNERABILITIES
- SCANNING FOR BUGS IN WORDPRESS AND DRUPAL
- USING PUBLIC EXPLOITS

WEEK 7
AUTOMATING VAPT AND SECURE CODE DEVELOPMENT



- INFORMATION GATHERING FOR ENDPOINTS
- APPLICATION ASSESSMENT USING NMAP
- AUTOMATING VAPT WITH NIKTO AND BURP SUITE PRO

WEEK 8
DOCUMENTING AND REPORTING VULNERABILITIES



- DOCUMENTING STAGES OF VULNERABILITIES USING TOOLS
- VAPT REPORTS DEVELOPER REPORT VS HIGHER MANAGEMENT REPORT
- CONCEPTS OF CODE SECURITY AND PATCHING
- PARTS OF A VAPT REPORT
- COMMON GOOD PRACTICES AND BAD PRACTICES

THANK YOU