🔐 30-Day Beginner's Course in Web Application Penetration Testing (WAPT) & Bug Bounty Hunting Course in English

👉 Start Date: January 28, 2025 | Live on Google Meet

🌟 Free Demo Class: January 27, 2025

🔥 Why This Course Is Your Best Investment

✅ Live, Interactive Classes: Learn directly from a cybersecurity expert, ask questions in real-time, and clarify your doubts every day.

✅ Affordable for Beginners: Original price is $149, but first 20 students enroll for just $99. Don’t miss out!

✅ Beginner-Friendly Approach: No prior hacking knowledge? No problem! Start from scratch and grow to an advanced level.

✅ Certificate of Completion:

✅ Lifetime Access to Recordings: Can’t attend live? Get access to all recordings

right after each class.

✅ Practical Learning: Includes real-world hacking techniques, live demonstrations, and bug bounty skills.

✅ OWASP Top 10 Expertise: Master vulnerabilities like XSS, SQL Injection, IDOR, and much more!

👨‍💻 Who Should Join This Course?

Students: Gain high-demand skills that can earn you money through platforms like HackerOne and Bugcrowd.

Working Professionals: Switch to a cybersecurity career with a minimal investment.

Tech Enthusiasts: Explore ethical hacking and make it a career or a rewarding side hustle.

Freelancers: Add a lucrative skill to your portfolio and start earning fast.

🎁 What’s Included in This Course?

🌟 Live Daily Classes: 1-hour interactive sessions with personalized attention.

📚 Lifetime Access: Class recordings and premium notes are yours to keep forever.

💡 Hands-On Projects: Real-world hacking scenarios to build practical expertise.

🏅 Certificate of completion .

🔧 Tool Mastery: Learn Wireshark, Burp Suite, Nmap, and more like a pro.

🛠️ Comprehensive Support: Get all your questions answered live or through post-class support.

💡 What Will You Learn?

From foundational knowledge to advanced bug bounty skills, this course covers everything:

Networking Basics, Linux Essentials, and Environment Setup.

Tools like Wireshark, Nmap, and Burp Suite for ethical hacking.

Exploiting vulnerabilities like XSS, SQL Injection, and Path Traversal.

Real-world bug reporting and earning on platforms like HackerOne and Bugcrowd.

🌟 Limited Time Offer – First 20 Seats at $99!

🚀 Original Price: $149

💰 Offer for First 20 Students: Enroll for just $99

🎉 Free Demo Class on January 27, 2025

Experience our teaching style, see live demonstrations, and get a glimpse into the tools and techniques used.

🌟 Exclusive Bonus: Enroll after the demo and gain lifetime access to notes and resources at no extra cost!

📩 How to Join?

💬 Type “WAPT” on WhatsApp to +91 9627797555 to secure your spot!

📌 Act Fast! Only 100 seats available, and they’re filling up fast.

📅 Course Schedule

Week 1: Fundamentals & Tools Mastery

💻 Day 1: Networking Basics – TCP/IP, DNS, HTTP vs. HTTPS.

🐧 Day 2: Linux Essentials – Command-line basics for hacking.

🛠️ Day 3: Tool Setup – VirtualBox, Kali Linux, and environment prep.

🌐 Day 4: Wireshark Basics – Analyze network traffic like a pro.

🔎 Day 5: Burp Suite Essentials – Proxy setup and interface.

🗺️ Day 6: Nmap – Master port scanning and target discovery.

📍 Day 7: Reconnaissance – OSINT and passive techniques.

Week 2: Deep Dive into Recon, Scanning, & Enumeration

📂 Day 8: Subdomain Enumeration – Discover hidden assets.

📊 Day 9: Scanning Targets – Uncover vulnerabilities.

⚙️ Day 10: Vulnerability Scanning – Tools and common misconfigurations.

🏆 Day 11: OWASP Top 10 Overview – Learn the basics of web app security.

📝 Day 12: Bug Report Writing – Craft professional reports.

📋 Day 13: Bug Hunting Checklist – Your guide to successful bounties.

🧪 Day 14: Practical – Recon and scanning with Burp Suite.

Week 3: OWASP Top 10 Explored

🚪 Day 15: Broken Access Control – Prevent unauthorized access.

🔒 Day 16: Cryptographic Failures – Understand encryption issues.

💉 Day 17: Injection Attacks – SQL, HTML, and more.

🎨 Day 18: Insecure Design – Secure development principles.

🛠️ Day 19: Security Misconfigurations – Common pitfalls and fixes.

📦 Day 20: Outdated Components – Recognize and remediate risks.

Week 4: Advanced Vulnerabilities & Exploits

🔑 Day 21: Authentication Failures – Session hijacking explained.

✳️ Day 22: XSS – Practical Cross-Site Scripting attacks.

🖥️ Day 23: SSRF – Exploiting server-side vulnerabilities.

🛠️ Day 24: LFI, RFI & Path Traversal – File inclusion attacks.

☠️ Day 25: Subdomain Takeover – Dominating unused domains.

🔗 Day 26: CSRF & IDOR – Exploiting hidden vulnerabilities.

🚀 Day 27: No Rate Limit Exploits – Automation-based attacks.

Week 5: Final Project & Career Boost

🔎 Day 28: Target Building & Testing – Real-world hacking.

💼 Day 29: Submit Bug Reports – Personalized feedback.

🏅 Day 30: Certification & Career Advice – Take the next step.

🌐 Why Wait? Secure Your Spot Today!

💬 Message “WAPT” on WhatsApp to +91 9627797555

🎯 Start your cybersecurity journey NOW. Transform your future in just 30 days!