
THE ART OF HACKING
ORGANIZED BY: ENCIPHERS | POWERED BY: HACKERS

The Art Of HACKING

ORGANIZED by ENCIPHERS

September 29th, 2018

WEB HACKING
BASIC LEVEL

The Art Of Hacking

A series of training focused on teaching practical penetration testing on Web and Mobile applications. These sessions are going to be hands on, classroom based, lab focused. Training sessions will be divided into Basic and Advance level.

Organized by ENCIPHERS

At ENCIPHERS, we love to share the knowledge of ethical hacking, penetration testing and information security via the workshops and trainings. ENCIPHERS organize numerous class room, online and conference trainings throughout the year.

ENCIPHERS also have dedicated portal for online trainings where students can get free and paid course subscriptions. Go ahead and checkout the portal: https://training.enciphers.com

Who we are ?

ENCIPHERS

Demystifying Security

What we do?

- An information security firm, focused on making the internet safe, one vulnerability at a time.
- Penetration Testing & Vulnerability Assessments:
  - Web Applications
  - Mobile Applications
  - Network/Infrastructure
- Training Provider:
  - Online Training: https://training.enciphers.com
  - Workshops
  - Conference Trainings
- Responsible Disclosure Consultancy

Penetration Testing

Penetration testing is the practice of testing a computer system, network, Web or Mobile application etc. to find security vulnerabilities that a person with malicious intent could exploit.

Vulnerability Assessments

Vulnerability assessment is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, application or communications infrastructure.

Responsible Disclosure Consultancy

Responsible Disclosure or Bug Bounty, are programs offered by organizations seeking security expertise for their network, application or product. Security researchers help the organizations by finding vulnerabilities and in return, the researcher's get rewards or recognition.

Let’s start the **training**

the more you **ASK,** the more you **LEARN**

Quick check

Are you all set?

Agenda

Web Application Hacking (Basic Level)

- Module 1: Basics of everything
- Module 2 – Recon
- Module 3 – Finding the “easy money bugs”
- Module 4 – Finding high paying bugs
- Module 5 – How not to suck at bug bounties

Basics of everything - |

HTTP | SSL | Methods

- How does web apps work?
- HTTP Request | Response | Methods
- Sessions | AJAX | API
- Encryption | Encoding | Hashing
- HTTP | HTTPS | SSL

Basics of everything - ||

User Input | DNS | Burp

- Vulnerability scanning | Penetration Testing | Bragging
- Let’s trace a packet till the destination and back
- What are domains? Subdomains? Why subdomain hijacking?
- What is user input with regards to web app security?
- Why a proxy? Why Burp Suite? What all burp suite can do?

Basics of everything

Burp Suite basics and set up

- Run the burp suite in virtual machine
- Set up a network proxy to capture the traffic in burp
- Open “www.bbc.com” in browser. Can you see the traffic in burp?
- Now open, “www.facebook.com”. Can you see the traffic in burp? Why?

Basics of everything

Importing SSL and setting up apps

- Import the SSL certificate in browser
- Now open, “www.facebook.com”. Can you see the traffic in burp? Well, you should.
- Quick walkthrough of burp suite pro
- Best and most used features
- Case scenario for some burp usages (Access related testing with repeater and brute forcing with Intruder)

End of Module 1

Any questions?

Recon

What | Why | How

- What is reconnaissance?
- Nmap: *nmap -sS -A -PN -p- --script=http-title testsite.com* | What are we looking for?
- Enumerating subdomains:
  - https://github.com/TheRook/subbrute
  - site:testsite.com -www
  - Many more tools for finding subdomains. But remember, you are looking for subdomains, not subdomain hijacking.
- Shodan | Github

Recon

Easy to find vulnerabilities

- Do you see “jenkins” in your subdomain scan result?
- Sub domain hijacking: Yes, you can get money by telling someone that they forgot to renew a domain or update DNS record.
- Nmap scan: any interesting port/service?
- Wordpress issues: wp-json, wpscan, brute force+username enum

Some more low severity, easy to find issues

- Clickjacking: how to find? What can we do with it?
- Anti automation missing
- Unintentional data leakage in API response
- Password reset related issues
  - Token expiration, reuse, creation, validation
- Cookie secure, HTTPOnly
- Login brute forcing
- Security headers
- CORS misconfiguration

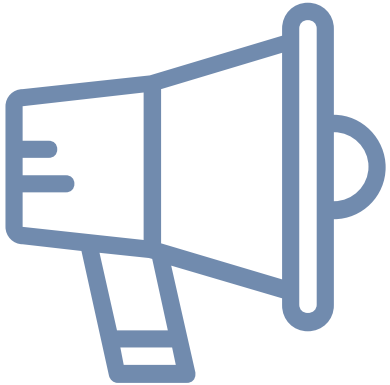
Reporting the right way

Never report a weakness, report an exploit

- CORS misconfiguration: Create a simple POC (CORS_POC)
- Login Bruteforce? Show the impact with user enumeration and weak password policy
- Cookie not HTTPOnly? Show a video with XSS exploitation
- Unintentional data leakage? Show how you can automate this and capture a huge amount of data, not just one.
- Most important: Be humble, Be respectful, Be cool. Trust is the key here. And yeah, DO NOT BEG

End of Module 2

Any questions?



Now some announcements

Web Application Hacking

(Advance Level)

Unique Features

Why to attend the advanced level training?

Classroom Training

Focused on finding server level issues

The VPS

Use the custom VPS to hunt for bugs

Find Bugs

Start bug bounties

Ask the Experts

Two Q&A sessions

What's your ROI?

How much did you earn?

How to Enroll? Fee etc

Limited Seats | First to enroll will get confirmation

Discounted Fee (Only till 1st Oct, 5PM IST):

- 10,000 INR per person inclusive of all taxes
- Includes:
    - Web Application hacking advance level training (1 Day)
    - 1 month access to bug hunter's VPS
    - Access to two online Q&A session
    - Access to a seperate channel for asking doubts, taking help

Fee without discount: 12,000 INR (inclusive of taxes)

How to enroll for advanced level training?

1. Complete the payment 2. Fill the google form 3. Get confirmation email

Step 1. Complete the payment.

- UPI: **enciphers@icici**
- IMPS/NEFT:
  - Bank Name (India): ICICI Bank Ltd
  - ACC. No: 628205025182
  - Account Name: ENCIPHERS
  - IFSC: ICIC0006282

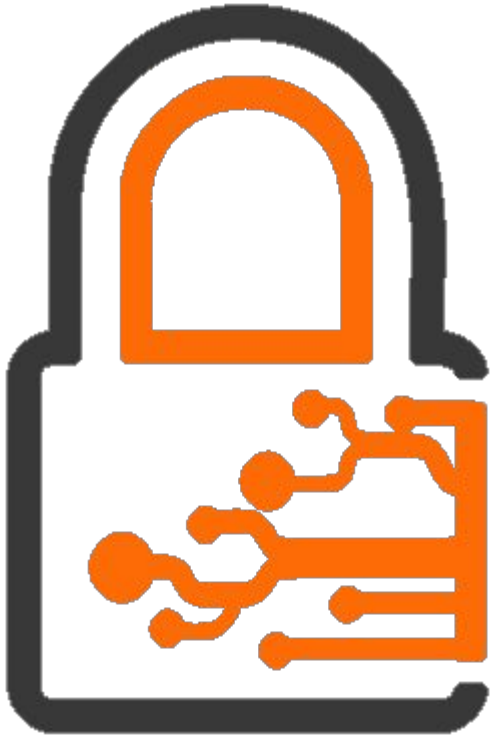
Step 2. Save the payment transaction number

Step 3. Submit the google form:

Enrollment Form: https://tinyurl.com/y9cmlzoy

Let’s have lunch

See you after 60 minutes



Finding the “easy money bugs”

XSS | CSRF | Access Control |

- Cross Site Scripting:
  - Understanding the issue.
  - How to do you test? *“><img src=x onerror=alert(‘1’)>* ?
  - What are the places to test XSS?
  - Instead, input “>XXXX<’aaaa and check the response
  - Inject X approach (https://forum.bugcrowd.com/t/tutorial-injectx-to-find-xss/790)
  - API responses: Check the content-type
  - Burp Extension: Reflector
  - Blind XSS testing
- If not XSS, maybe HTML injection
- Some interesting XSS cases studies (audience, anyone?)

Finding the “easy money bugs”

XSS | CSRF | Access Control |

- Cross Site Request Forgery:
  - What is it? How to test? How to fix?
  - Are REST APIs secure against it?
  - X-forwarded with?
  - Where all does it matter to fix CSRF?
  - 5 Step CSRF testing (https://whitton.io/)
    - The way I normally check for these is as follows:
    - Perform the request without modifying the parameters, so we can see what the expected result is
    - Remove the CSRF token completely (in this case, the `fb_dtsg` parameter)
    - Modify one of the characters in the token (but keep the length the same)
    - Remove the value of the token (but leave the parameter in place)
    - Convert to a GET request

Finding the “easy money bugs”

XSS | CSRF | Access Control |

- Access control issues:
  - What are they? How to test? Where they commonly occur?
  - Any finding from crowd?
  - REST API access control
  - PUT | POST | DELETE | GET on API endpoints
- Improper Session Management:
  - Session on multiple devices
  - Session validation on password change
  - Session timeout
  - API auth and refresh token

End of Module 3

Any questions?

Finding high paying bugs

IDOR | Password Reset Issues | MFA Bypass |

- Insecure Direct Object References:
    - What are they?
    - How to test?
    - REST API structure ?
    - Some interesting case studies
    - Using Burp Extensions to find IDORs
    - Example of IDORs. What if the identifier is too long to guess?
    - Approach to find IDORs
    - User to Admin IDORs.

Finding high paying bugs

IDOR | Password Reset Issues | MFA Bypass |

- Password Reset issues:
  - How are the tokens generated? Guessable?
  - Are token + User mapped and validated?
  - Reusable tokens?
  - Expiry of tokens?
  - Token expiry cases.
  - When are these issues “high paying”?
- MFA Bypass and session management issues
  - OTP (One time password)
  - Brute forcing? Reuse of OTP?
  - Anti automation on the OTP generation

End of Module 4

Any questions?

How not to suck at bug bounties

Reporting | Duplicates | Resources |

- Reporting is the key to success
- Ways to improve reporting:
  - Always mention an exploit scenario
  - Always create a POC
  - Report exploit, not weakness
- Do you really think your report is going to help the client become more secure? Or is it just for the t-shirt?
- Do not be an asshole while reporting.

How not to suck at bug bounties

Reporting | Duplicates | Resources |

- Reporting is the key to success
- Ways to improve reporting:
  - Always mention an exploit scenario
  - Always create a POC
  - Report exploit, not weakness
- Do you really think your report is going to help the client become more secure? Or is it just for the t-shirt?
- Do not be an asshole while reporting. Don’t do beg-bounties.

How not to suck at bug bounties

Reporting | Duplicates | Resources |

- Avoiding duplicates:
  - The best way is to have a unique approach
  - What do you hunt for? XSS? CSRF? Weakness?
  - Where are you looking for bugs?
  - Explore more, recon more
  - Focus on high impact bugs
- Choosing the target/program:
  - Don’t like the payout? Leave the program.
  - Don’t like the transparency? Leave the program.
  - Don’t like the attitude? Leave the program.

How not to suck at bug bounties

Reporting | Duplicates | Resources |

- Available Platforms for Bug Bounty:
  - BugCrowd
  - Hackerone
  - Synack
  - Inigriti | Bugbounty.jp | Bountyfactory | Yogosha

- Resources:
  - Read blogs | Follow members on twitter
  - Web Application Hackers Handbook | OWASP Testing Guide
  - Play CTF | HackTheBox
  - Refer to handout given in this training

End of Module 5

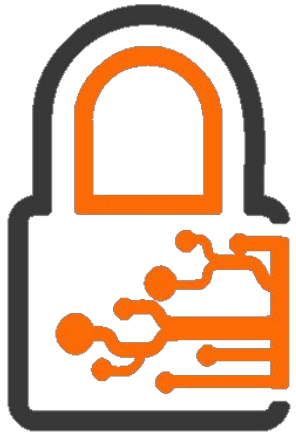
Any questions?

Some Other Information

- The agenda of Web Application Hacking Advanced level training will soon be disclosed on the slack channel.
- The venue of advanced level will be somewhere in Delhi NCR (not a company's office).
- Presentation, virtual machine, and other content from this training will be made available for everyone soon. Keep checking the slack channel for details/link.
- Follow us on twitter, for quick updates and notifications about trainings: https://twitter.com/enciphers_

ENCIPHERS

Demystifying Security



Penetration Testing
Vulnerability Assessments
Responsible Disclosure Consultancy
Corporate Trainings
Online trainings

www.enciphers.com

+91-945-082-8700

hello@enciphers.com

See You at ....

Credits for this template

Shapes & Icons

Vectorial Shapes in this Template were created by **Free Google Slides Templates** and downloaded from **pexels.com** and **unsplash.com**.

Icons in this Template are part of Google® Material Icons and **1001freedownloads.com**.

Backgrounds

The backgrounds were created by **Free Google Slides Templates**.

Images

Photos in this template were downloaded from **pixabay.com**. Attribution is located in each slide notes and the Credits slide.

Fonts

The fonts used in this template are taken from **Google** fonts. (Muli)
You can download the fonts from the following url: https://www.google.com/fonts/

Color Palette

The Template provides a theme with four basic colors:

#4e6e9aff	#4e6e9acc
#5477a7cc	#eeeeeeff

Trademarks

Microsoft® and PowerPoint® are trademarks or registered trademarks of Microsoft Corporation.

Google Drive® is a registered trademark of Google Inc.