HARSH

@harshbothra_

Application Security & Penetration Testing 101

BY: HARSH BOTHRA

MODY UNIVERSITY OF SCIENCE AND TECHNOLOGY
LAKSHMANGARH • RAJASTHAN
A Leading Women's University

DETOX

About Me

Cyber Security Analyst @ Detox Technologies

Bugcrowd Top 150 Hackers – All Time & MVP Q1 Q2

Synack Red Teamer

Author – Hacking: Be a Hacker with Ethics
(Recognized by GoI bodies twice)

Author – Mastering Hacking: The Art of Information Gathering & Scanning

International Speaker - @C0c0n, @BugcrowdLevelUp, @RedTeamVillage & others

Security Blogger @ Medium | Learner | Poet

DISCLAIMER!

FOR EDUCATION PURPOSE ONLY!

Please do not practices the methodologies to perform any illegal or malicious action against any organization, body or person in any form. The person will be solely responsible if getting involved into such activities. Please use the knowledge to **Secure the Infrastructure and Make Cyber Space Safe.**

Thank You.

All the visual representation are taken from publicly available image repositories. The copyright belongs to the original author and none of the representations are used for the **commercial purposes.**

Agenda

Cyber Security

Phases & Careers

Application Security – 101

Penetration Testing – 101

Web Applications Threats

Attacks in Action – Demo

Bug Bounties – 101

Further Roadmap

Q/A

Cyber Security Introduction

Protecting Digital Assets

Implementing Defense in Depth

Ensuring Secure Communication

Hardening Infrastructure Security

Implementing Best Practices

Real Time Threat Intelligence and Mitigation

Education & Awareness

Phases in Cyber Security

OFFENSIVE SECURITY

DEFENSIVE SECURITY

Offensive Security

Penetration Testing

Application Security

Bug Bounty

Configuration Review

Red Teaming

Offensive Assessment

Defensive Security

Information Security Audit

Security Operation Center (SOC/NOC)

Log Analysis

Threat Modelling

Threat Hunting

Blue Teaming

Education & Awareness

Careers in Cyber Security

Penetration Tester

Bug Bounty Hunter

Cyber Security Analyst

Cyber Security Consultant

Cloud Security Engineer

DevSecOps

Security Architect

Secure Code Developer

Code Reviewer

Trainer

What

Why

When

How

Application Security - 101

What

Why

When

How

Penetration Testing - 101

Phases in Penetration Testing

01 **Reconnaissance**

02 **Enumeration**

03 **Exploitation**

04 **Post Exploitation & Pivoting**

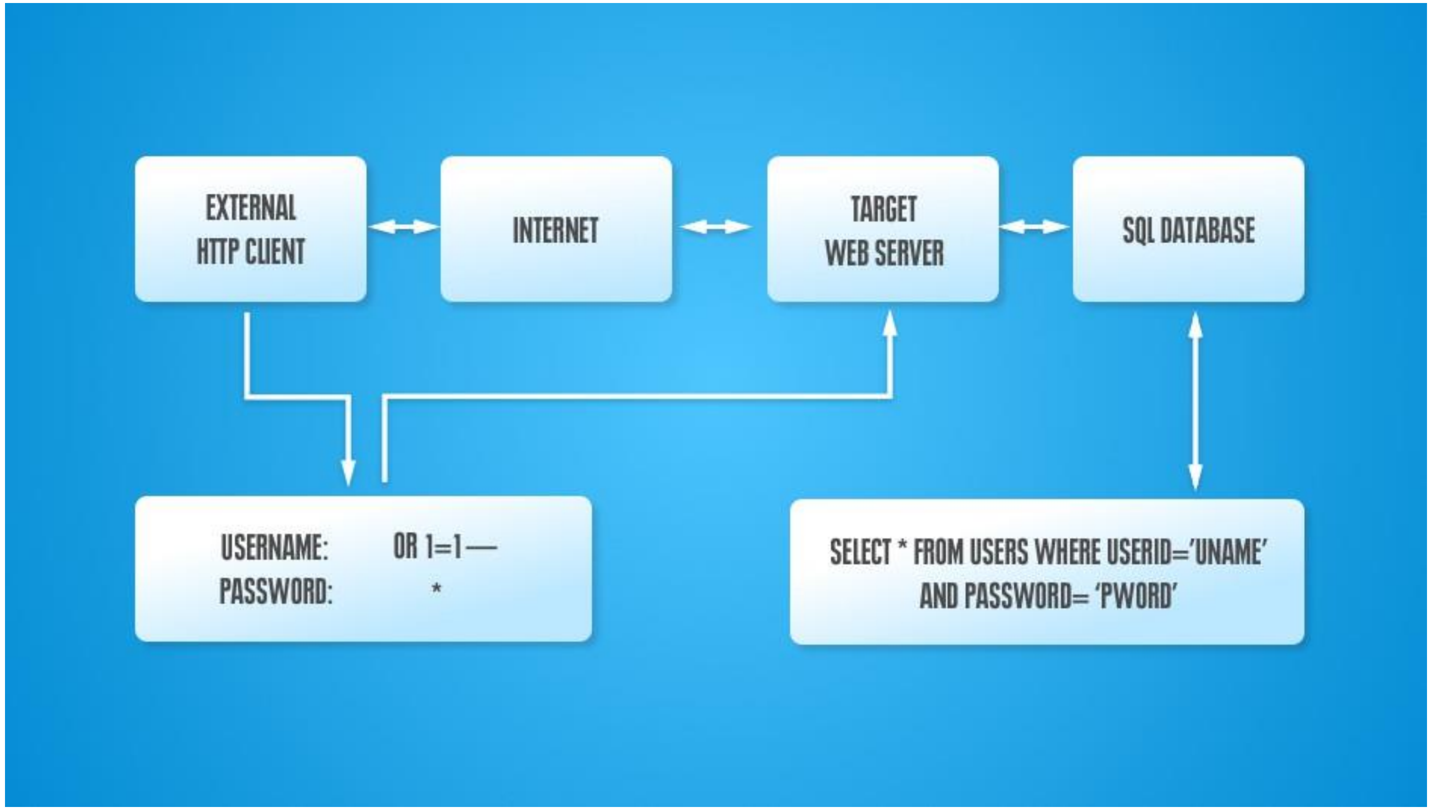
05 **Reporting & Documentation**

Tools Required {For Beginners}

1. Browser Developer Tools
2. **Burp Suite**
3. Browser Extensions like Cookie Editor, Wappalyzer, etc.
4. Nmap
5. Metasploit
6. Osmedeus/Project Bheem
7. Basic Scripting Knowledge
8. Git to Git Clone stuff

Web Application Threats

1. Injection Attacks
2. Known Vulnerable Components
3. Sensitive Data Exposure
4. Security Misconfiguration
5. Broken Access Controls
6. Client-Side Attacks
7. Server-Side Attacks
8. Missing Authorization



EXTERNAL HTTP CLIENT

INTERNET

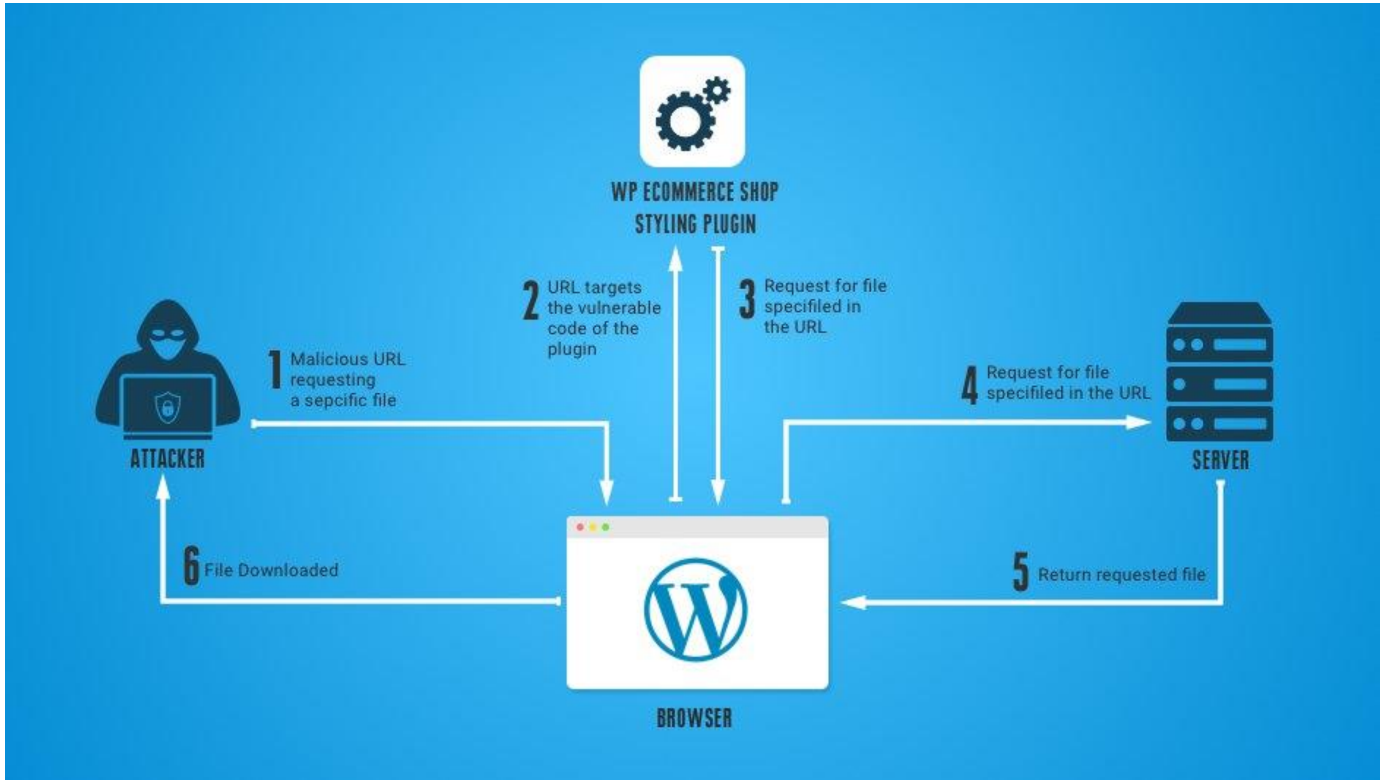
TARGET WEB SERVER

SQL DATABASE

USERNAME: OR 1=1—
PASSWORD: *

SELECT * FROM USERS WHERE USERID='UNAME' AND PASSWORD= 'PWORD'

Injection Attacks


WP ECOMMERCE SHOP STYLING PLUGIN
ATTACKER
1 Malicious URL requesting a sepcific file
2 URL targets the vulnerable code of the plugin
3 Request for file specified in the URL
4 Request for file specified in the URL
SERVER
5 Return requested file
6 File Downloaded
BROWSER

Known Vulnerable Components

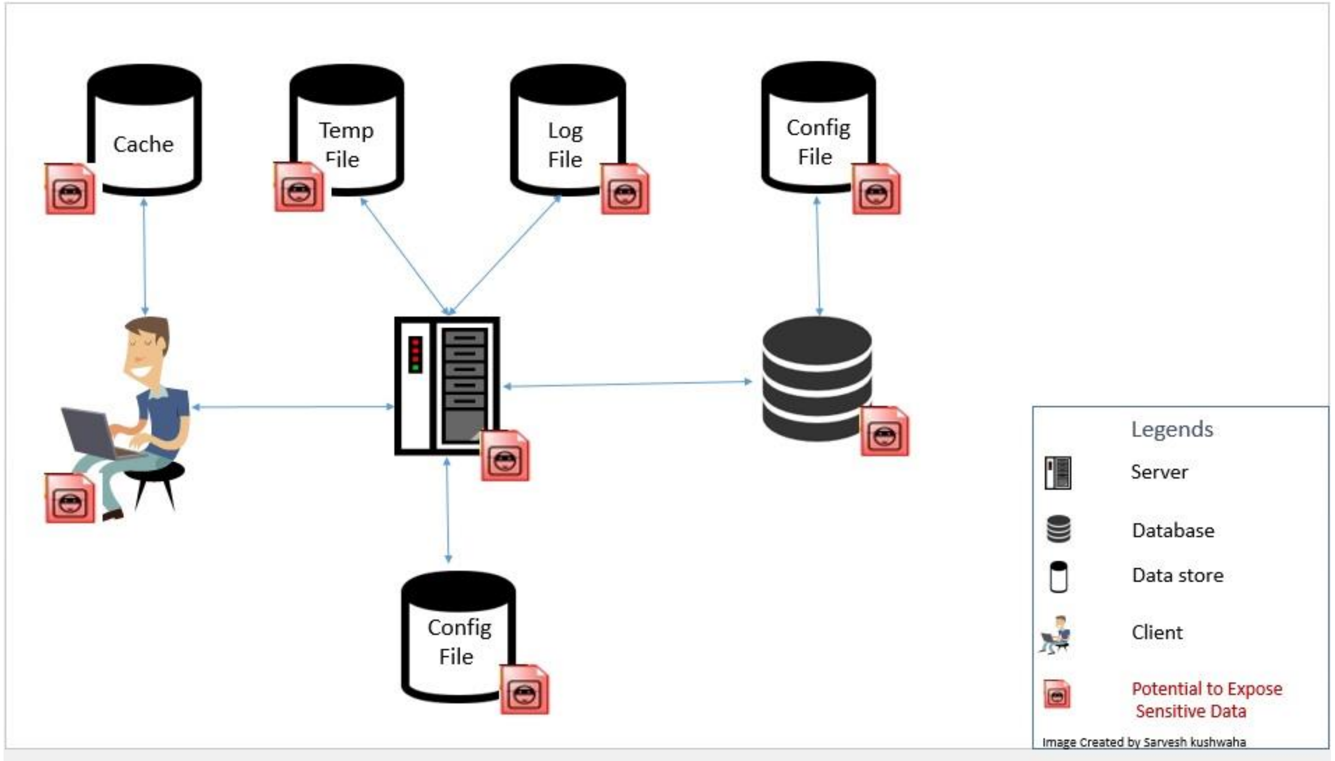
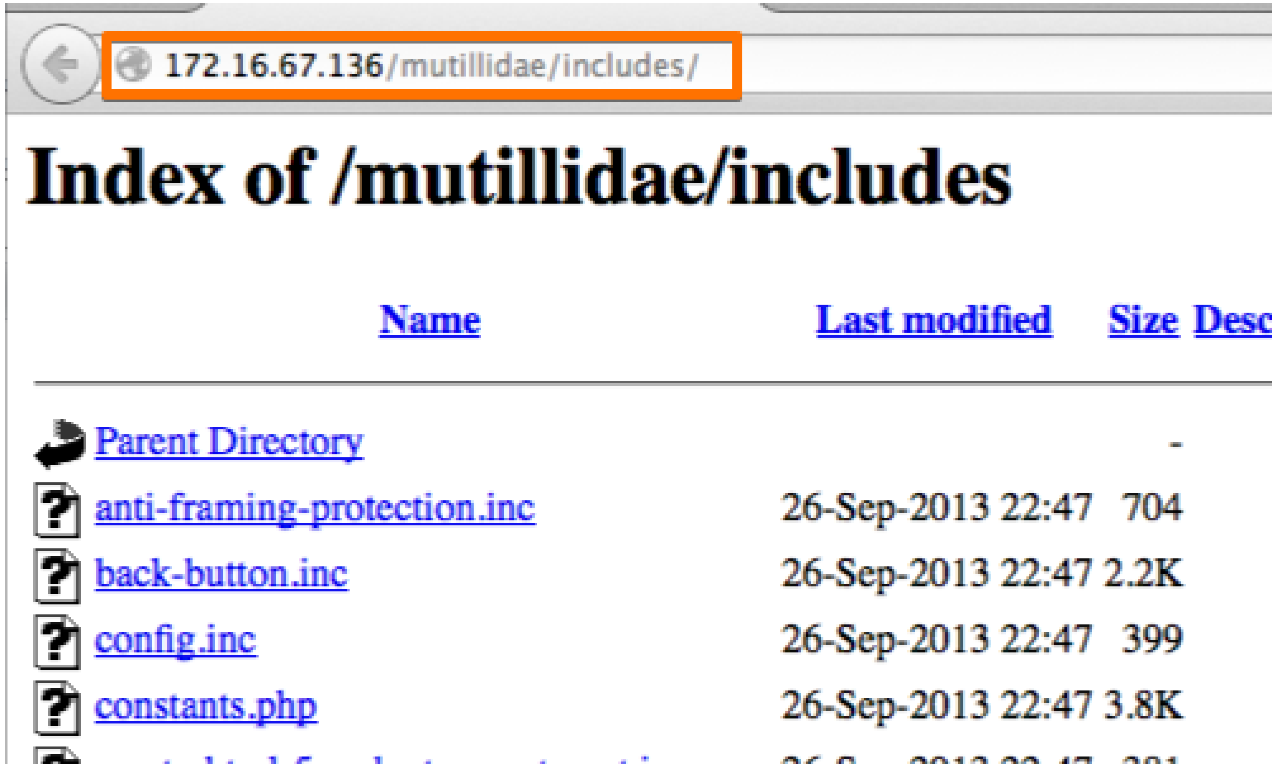


Image Created by Sarvesh kushwaha

Sensitive Data Exposure

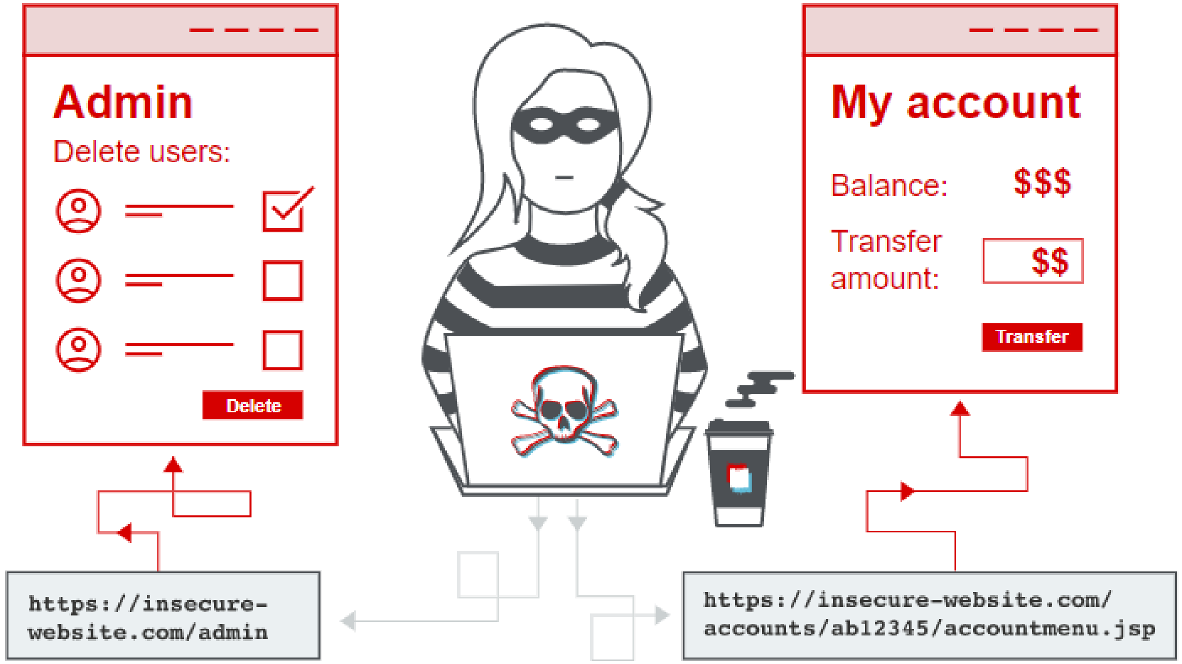


172.16.67.136/mutillidae/includes/

Index of /mutillidae/includes

Name	Last modified	Size	Desc
Parent Directory		-	
anti-framing-protection.inc	26-Sep-2013 22:47	704	
back-button.inc	26-Sep-2013 22:47	2.2K	
config.inc	26-Sep-2013 22:47	399	
constants.php	26-Sep-2013 22:47	3.8K	

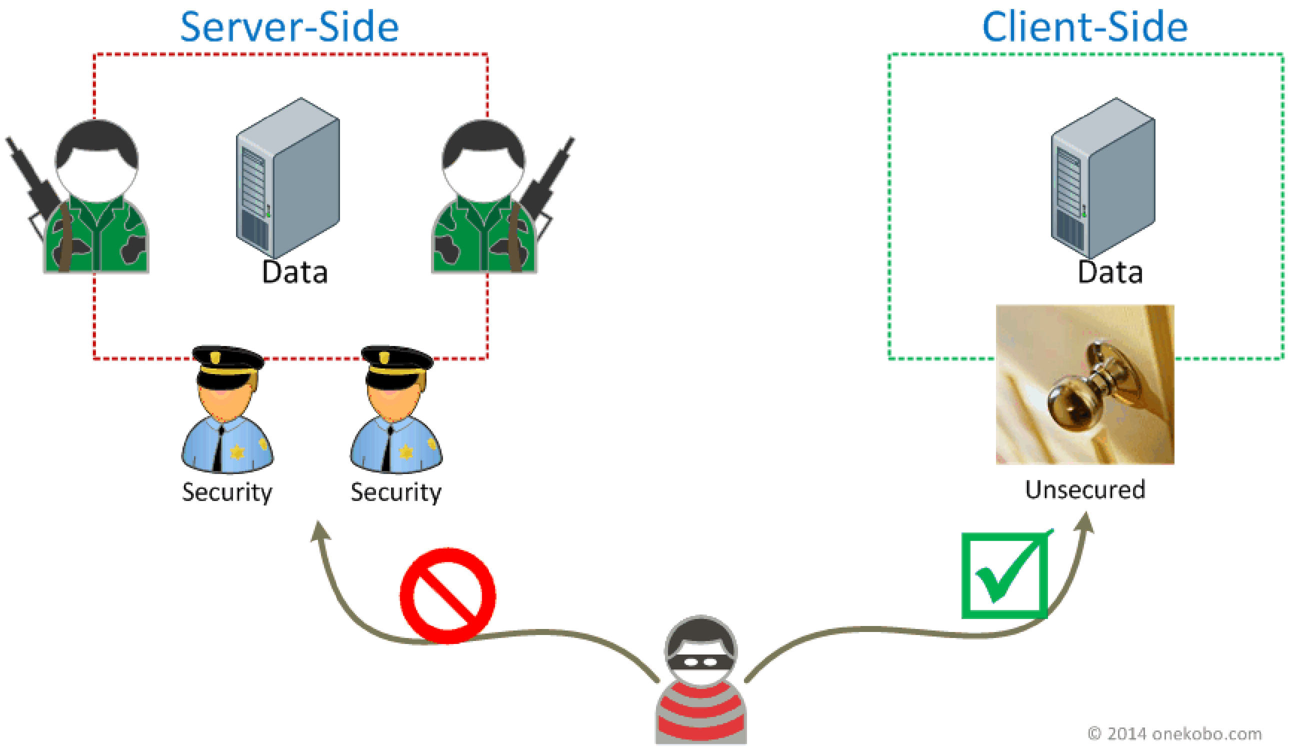
Security Misconfiguration



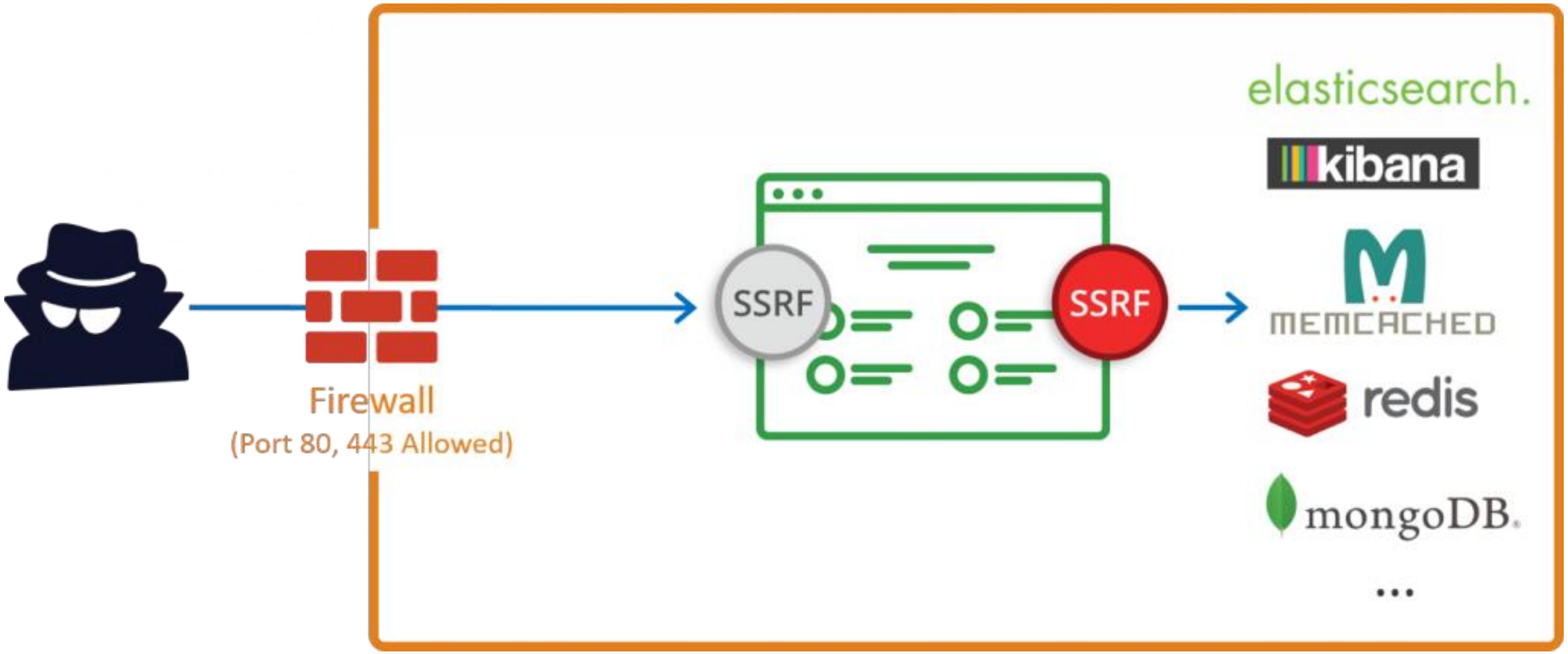
https://insecure-website.com/admin

https://insecure-website.com/accounts/ab12345/accountmenu.jsp

Broken Access Control



Client-Side Attacks



Server-Side Attacks

Missing Authorization

DEMO

Bug Bounties 101

Why Bug Bounties?

1. Recognition & Reputation as an Ethical Hacker
2. Earn $$$$$$$....$$$$
3. Swags
4. Acknowledgement
5. Public Value
6. Fun & Fun
7. AWESOME COMMUNITY
8. COOL CONFERENCES

Where to do Bug Bounties?

- Bugcrowd
- HackerOne
- Intigriti
- Synack
- Cobalt
- YesWeHack
- HackenProof
- Vendor Managed Programs

Bug Bounty Ground Rules

Learn	Learn why something is happening!
Understand	Understand the behavior patterns of the applications and see what is expected vs what is unexpected
Know	Know your strength and weaknesses
Explore out	Explore out of the Box
Create	Create your own methodologies and approaches
Think	Think, Try, Think, Try, Hit!
Do Not Expect	Do Not Expect !! Do Not Stress !! Good Things take time!

My Bug Bounty Methodology

Select target based upon scope – Wide Scope // Large Application

RECON -- Watch my talks on Recon to see how I go about Recon

Do Multiprocessing, While Recon is running, Fire up your Burp Suite and Test for IDORs, Server Side & Client Side Vulns.

Understand the application logics and read the documents to make sure if you find a business logic, that's valid not an expected behavior.

Map your Recon with your Testing – Find more hidden endpoints and new assets where others might not have been going/doing

Report Every Security Issue whether it's a Low or Critical. Sometimes Critical are easy and low are hard to exploit (that's why they are low).

Learn when stuck//something new is booming the market.

Take necessary break, chill out!!

//Hack the world//

Quick Demo

Further Roadmap

Q/A?

Get in Touch at

- Website – https://harshbothra.tech
- Twitter - @harshbothra_
- Instagram - @harshbothra_
- Medium - @hbothra22
- LinkedIn - @harshbothra
- Facebook - @hrshbothra
- Email – hbothra22@gmail.com

Thank You!