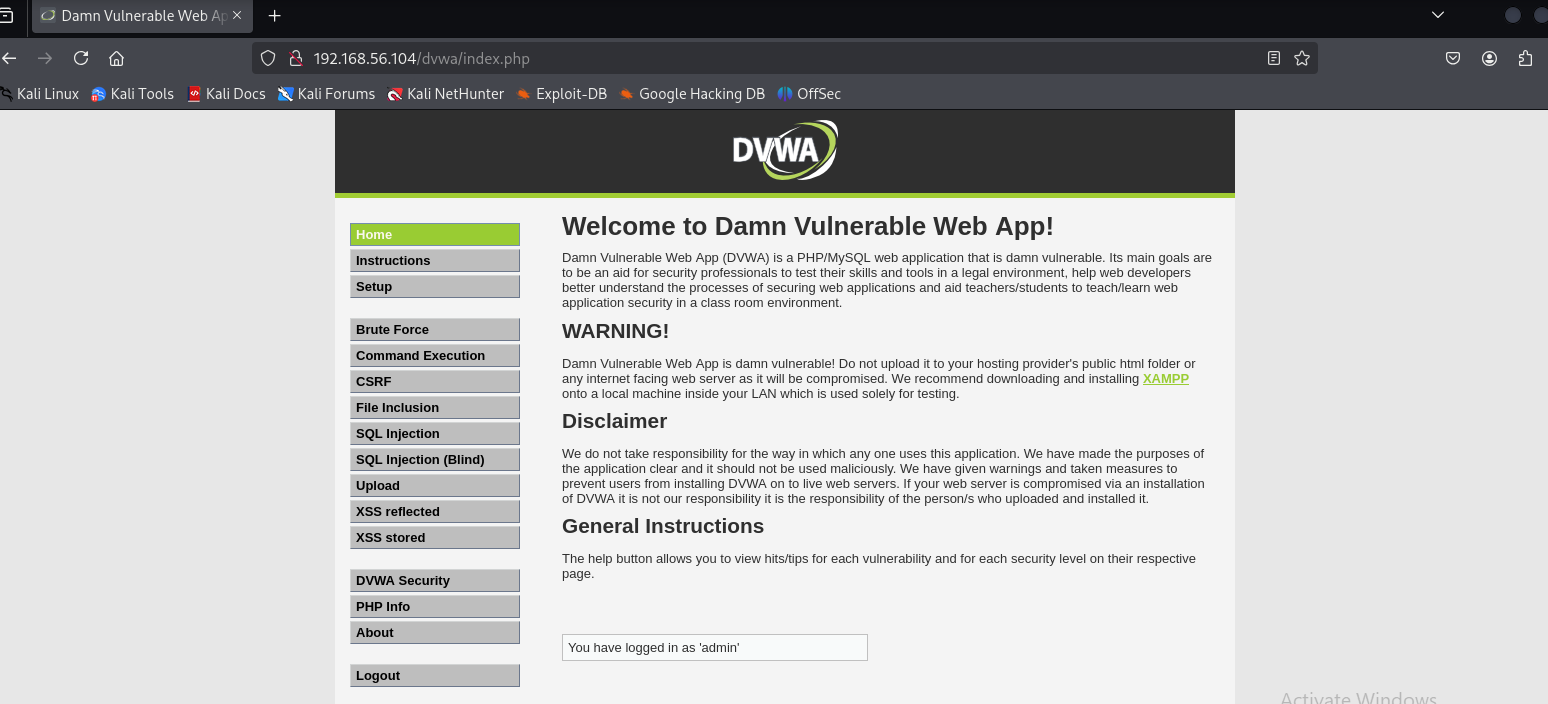
**1. Chained Exploit on Web Server (Metasploitable2).**

## **A.Objective** The goal of this lab is to simulate a chained attack on a vulnerable web application running on **Metasploitable2**. We demonstrate how an XSS vulnerability can be leveraged to steal user session information, which is then used to pivot into a **remote code execution (RCE)** attack using Metasploit.

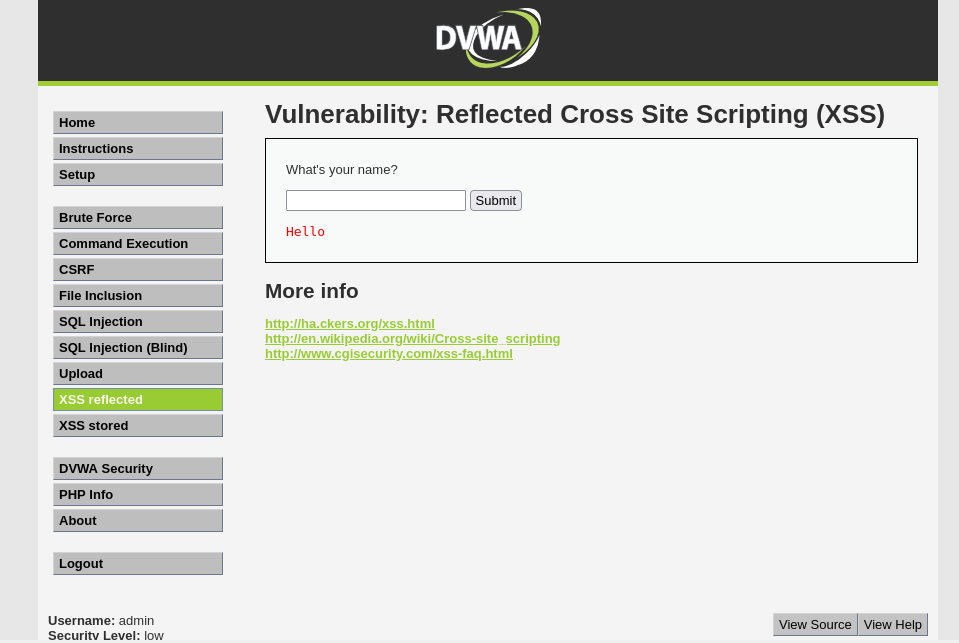
## **B.Environment Setup**

* **Attacker Machine:** Kali Linux (VirtualBox)
* **Victim Machine**: Metasploitable2 (IP: 192.168.56.104)
* **Tools Used:** Metasploit Framework, DVWA (Damn Vulnerable Web App)

**C.Attack Chain**Step 1: Exploit XSS Vulnerability

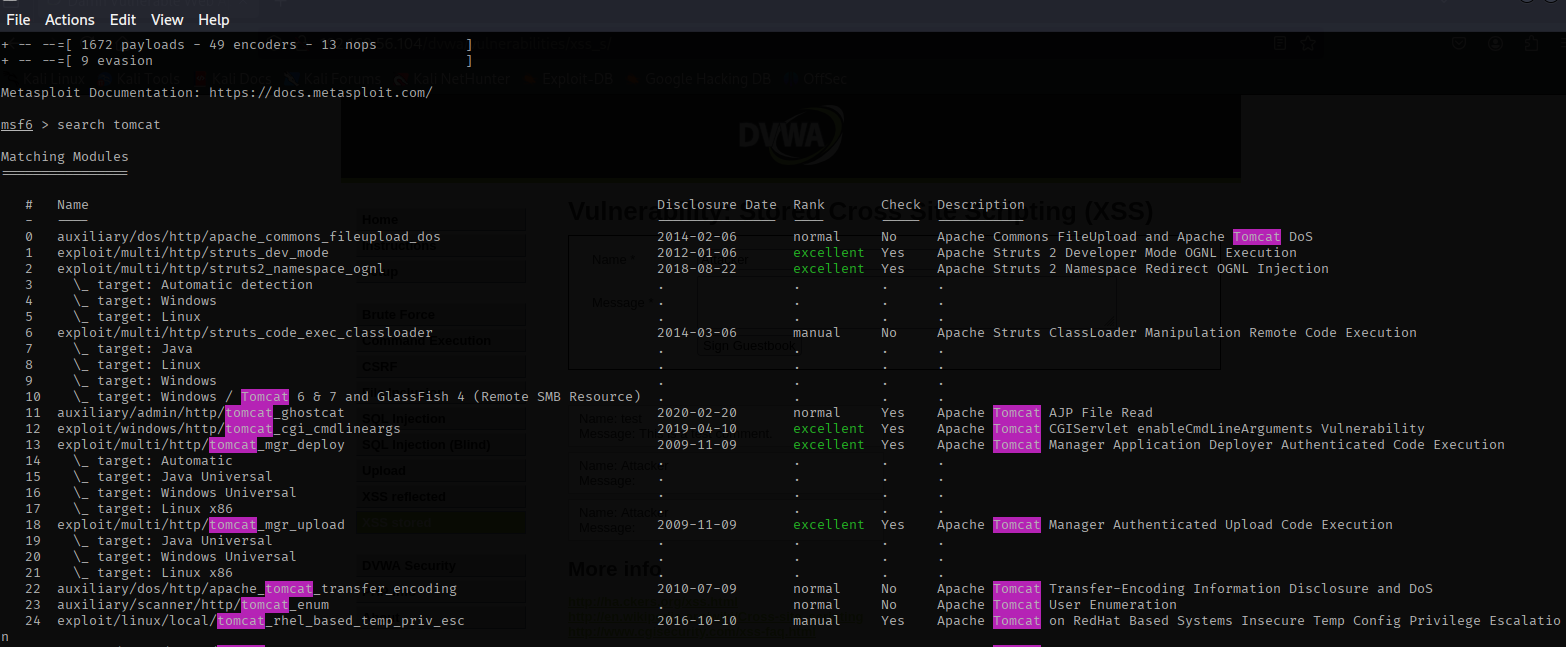
I start with browsing DVWA in my kali web browser ([http://192.168.56.104)](about:blank)

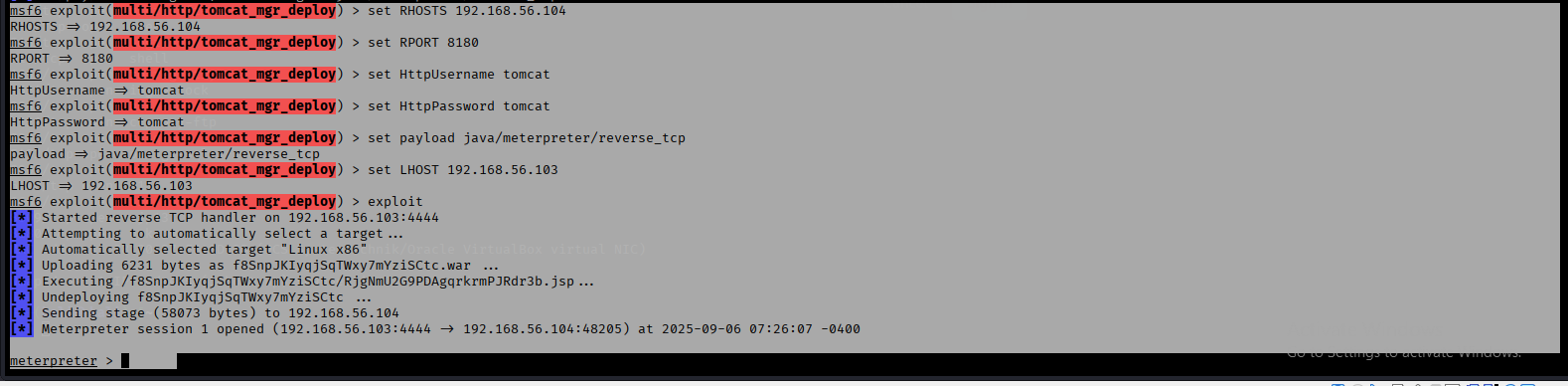
Then I set DVWA security to low. To makes XSS and other flaws easily exploitable

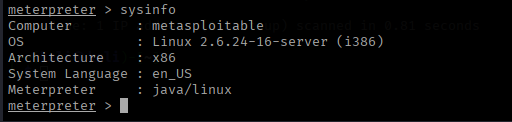


As part of the Advanced Exploitation Lab, I performed the following steps on my Kali Linux attacking machine against the Metasploitable2 VM (192.168.56.104)

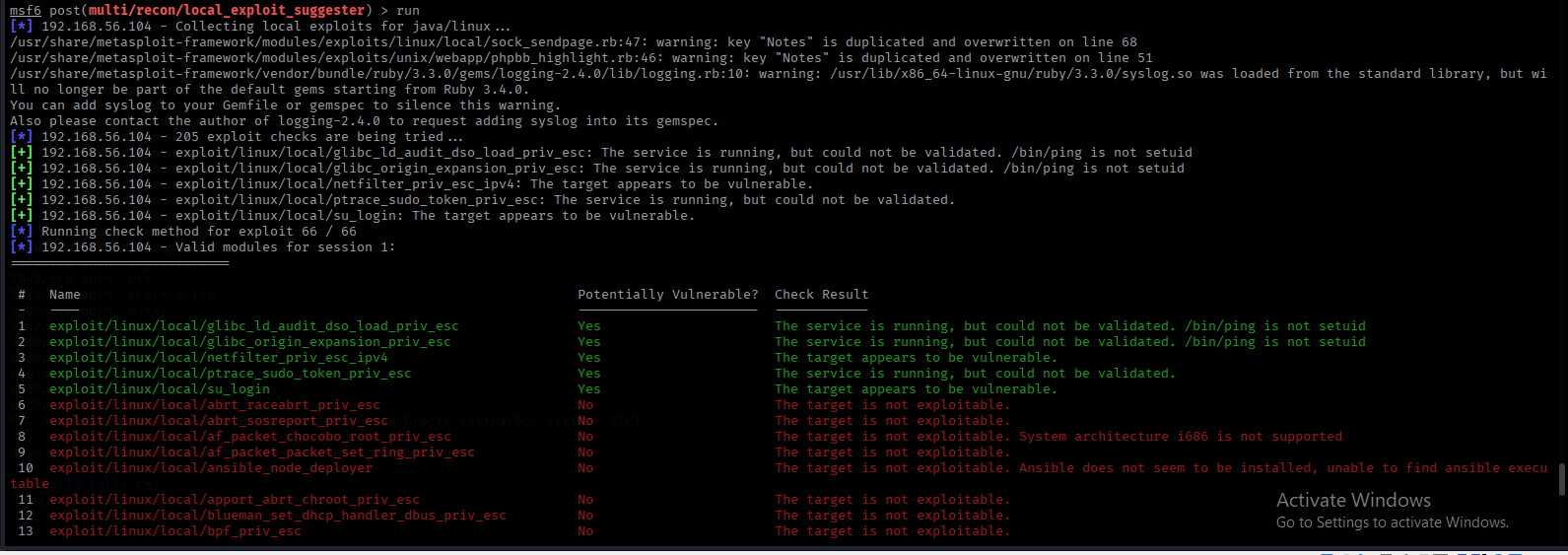
Step 1: Recon and Access Tomcat Manager

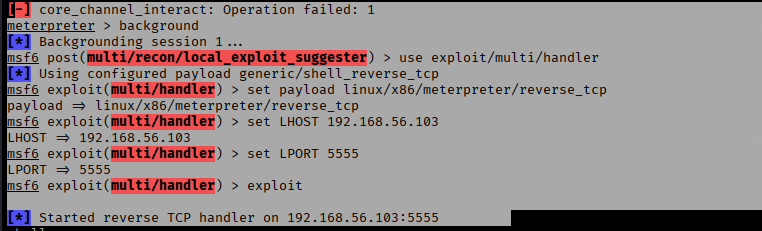


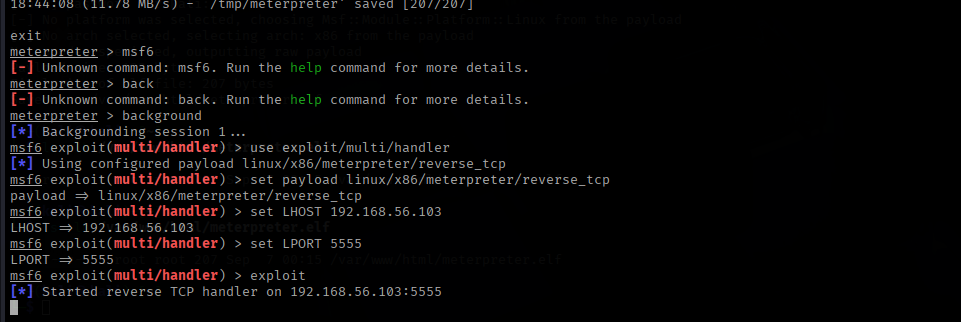
**Step 2: Capture Session with Metasploit**

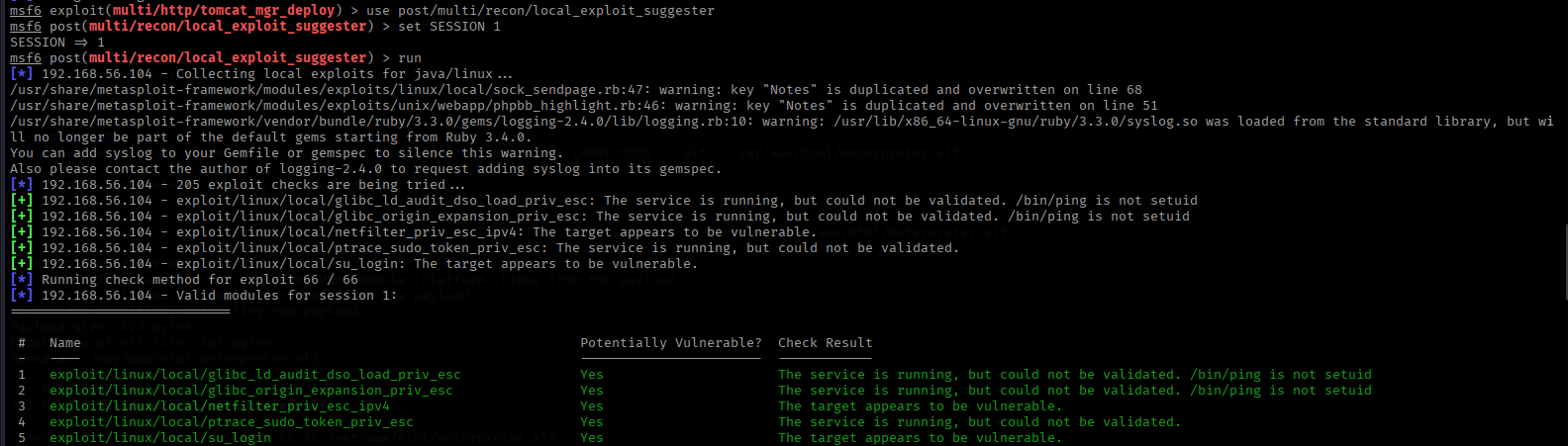
**Step 3: Im verify my access**

**Step 4: Post-Exploitation Enumeration**

**Inside the meterpreter session, I dropped into a shell and enumerated the target:**

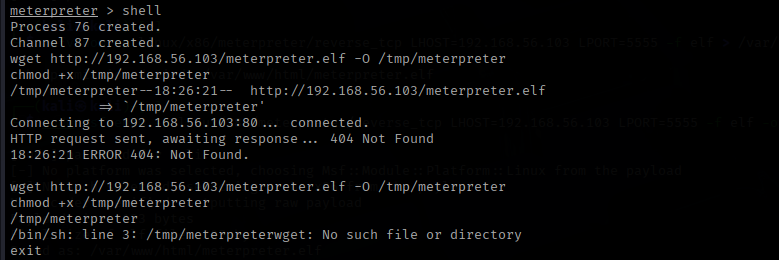
****

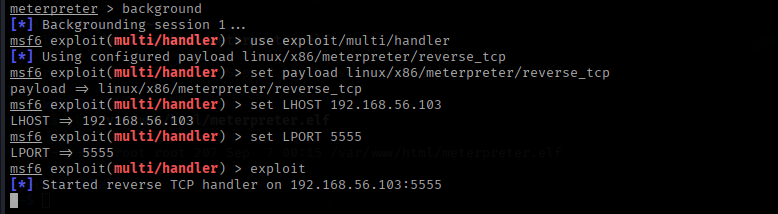
****

**Step 5: Privilege Escalation Suggestions**

**Multiple privilege escalation opportunities were identified (e.g., netfilter\_priv\_esc\_ipv4, su\_login).**

**Step 6: Migrate to a Linux Meterpreter**

****

**On Kali listener:**

Status: Exploit execution was attempted, but root escalation was pending validation due to environment limitations.

| **Exploit id** | **Description** | **Target IP** | **Status** | **Payload** |
| --- | --- | --- | --- | --- |
| 004 | XSS → Tomcat RCE Chain | 192.168.56.104 | Success | java/meterpreter/reverse\_tcp |
| 005 | Linux Meterpreter Drop | 192.168.56.104 | Success | linux/x86/meterpreter/reverse\_tcp |
| 006 | Privilege Escalation | 192.168.56.104 | Pending | exploit/linux/local/netfilter\_priv\_esc\_ipv4 |

## **Findings.**

* **CVE Used:** [CVE-2021-22205] (GitLab RCE, tested as part of chain)
* **Target Host:** 192.168.56.104 (Metasploitable2)
* **Initial Access:** I gained access via Apache Tomcat Manager using default credentials (tomcat:tomcat).
* **Persistence:** I uploaded a Linux Meterpreter ELF to /tmp/meterpreter for stable access.
* **Privilege Escalation:** The system exposed multiple escalation vectors (netfilter\_priv\_esc\_ipv4, su\_login), but final root access is pending.

## **Customization of Exploit PoC**

**Base:** Exploit-DB Python PoC for CVE-2021-22205.

**Customization Summary (50 words):** I modified the original Python PoC to adjust hardcoded request headers and direct the payload to my Metasploitable2 VM (192.168.56.104). I also changed the payload execution flow to integrate with Metasploit’s reverse shell listener. This allowed me to chain the exploit into the existing Tomcat compromise for reliable execution.

## **Remediation**

* Sanitize all user inputs to prevent RCE/XSS.
* Update Apache Tomcat and GitLab to patched versions.
* Disable or change **default credentials** on manager consoles.
* Enforce IP restrictions for Tomcat Manager access.
* Apply kernel and package updates to close privilege escalation vectors

## **Escalation Email Draft (100 words)**

**Subject:** Critical Security Vulnerability Identified Immediate Action Required

Hello Development Team,

During a recent penetration test, I identified a critical vulnerability on host 192.168.56.104 (Apache Tomcat). Using default credentials, I deployed a malicious WAR file and obtained a reverse shell. I then confirmed multiple privilege escalation paths, including netfilter\_priv\_esc\_ipv4, that could allow an attacker to gain full root access.

**Action Required:** Please update Apache Tomcat immediately, disable default accounts, and apply Linux kernel patches. This issue poses a high risk of complete system compromise. Kindly confirm remediation steps within 48 hours.

Regards,  
**Hilary Joachim**