**Portfolio Project: Exploiting Debug Mode in Werkzeug Console**

**Project Title:** Breaking In Through Debug Mode – Werkzeug Console Misconfiguration

**Category:** Web Application Security | OWASP Top 10 (A05:2021 – Security Misconfiguration)

**Objective**

To demonstrate how an exposed **Werkzeug debug console** in a Python-based web application can lead to **Remote Code Execution (RCE)** and full application compromise. The challenge simulated a real-world vulnerability that contributed to the 2015 Patreon breach.

**Environment**

* **Target Application:** Flask-based web app hosted on a vulnerable machine
* **Exposed Werkzeug Console:** Accessible via /console endpoint
* **Platform:** TryHackMe (vulnerable virtual machine)

**Tools & Commands Used**

* Built-in **Werkzeug interactive console**
* Python standard library (os, open)
* Shell commands executed via Python: ls -l, cat app.py

**Steps Performed**

* **Step 1:** Discovered an active debug console at /console, indicating a major misconfiguration.
* **Step 2:** Executed remote OS commands from the Python shell using:

python

import os; print(os.popen("ls -l").read())

This revealed several files, including todo.db and app.py.

* **Step 3:** Read the entire application source using:

python

print(open("app.py").read())

* **Step 4:** Located and extracted the secret variable inside the Python file:

secret\_flag = "THM{Just\_a\_tiny\_misconfiguration}"

**Lessons Learned**

* Even small misconfigurations, like leaving debug mode on, can lead to **critical vulnerabilities**.
* Tools like Werkzeug are powerful for development but dangerous if left exposed in production.
* This challenge reflects a real-world vulnerability that affected **Patreon in 2015**, where an exposed Werkzeug console was reportedly part of the compromise path.

**Outcome**

* Successfully exploited a security misconfiguration to gain **remote shell access** via Python code execution.
* Read sensitive application data including source code and secret values.
* Demonstrated a full path from misconfiguration to critical data disclosure, aligning with OWASP A05:2021.