18th January 2023

**COMMIX TESTBED LABS**

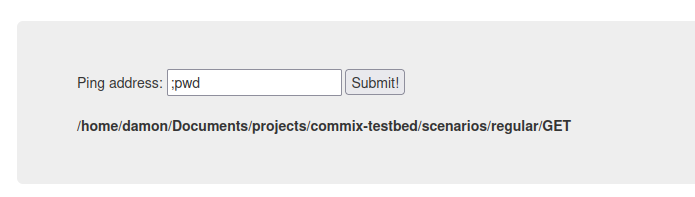
**Classic GET request**

**Summary of Results**

The URL <http://localhost:8000/scenarios/regular/GET/classic.php?addr=INJECT_HERE> was targeted using commix. Testing the connection showed that the GET parameter ‘addr’ might be injectable via classic command injection technique. A pseudo shell was opened allowing execution of OS commands, which confirmed the vulnerability.

**Attack Narrative**

A test command ‘pwd’ was submitted in the ‘ping address’ section of the testbed.



This returned the GET request URL to the vulnerable application running on localhost.



The URL is submitted to commix to check for OS command injection vulnerability, which prompted a pseudo shell so the application.

