**INCIDENT REPORT: 18512**

**Date: 02/10/24**

**Executive summary: Linux Server information is being sold on the darkweb even after using input sanitation to stop .php files from being loaded and executed.**

**Results**

**Application details:**

**After looking over the server logs there were some suspicious command prompt commands that are giving out IP address, network, passwords, password hashes as well as commands to configure these networks.**

* cat/etc/network/interfaces
* cat/etc/sysconfig/network
* cat/etc/resolv.conf

The above commands help the intruder gain network information such as IP address, what networks they work on as well as the hostname of the user and the username of the client.

* cat/etc/passwd
* cat/etc/shadow

The above commands cat/etc/passwd and etc/shadow give the individual password information such as the hashes used to encrypt the password.

**Conclusion:**

Even with using sanitation procedures and making sure that the client is not leaving an action trail behind with the above commands even with an unnoticeable breach with the commands to gain ip information is all that was needed. Once the IP address was obtained and the file configurations of the passwords and hashes any sanitation procedures are no longer secure as the person attacking the server has all the information they need to load and execute malware.