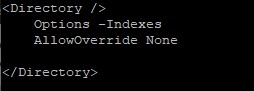
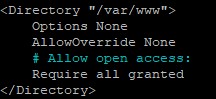
**Aleksandar** Technical writing-

**Andres** Apache server

1. **System settings protection – server will now not allow users to override apache configuration using .htaccess**

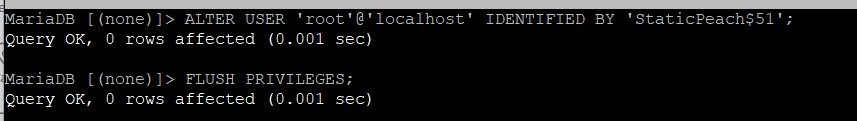


1. **Disabled directory listings**

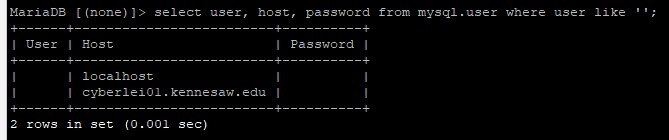


**Brandon** Maria Database

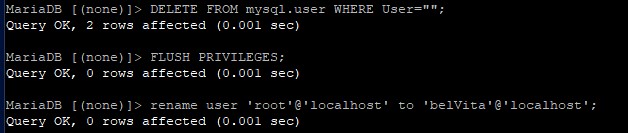
**1. Stronger password on DB-** Changed MariaDB password to StaticPeach$51 and flushed privileges to make new password active.



1. **Removed users without passwords-** Removed all users without passwords.



1. **Deleted blank users and flushed privileges. Also, changed name of root user to ‘belVita’-** Changed name of root user to belVita to make it more difficult for hackers to break into because now they need to find out the username as well.

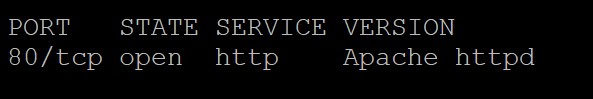
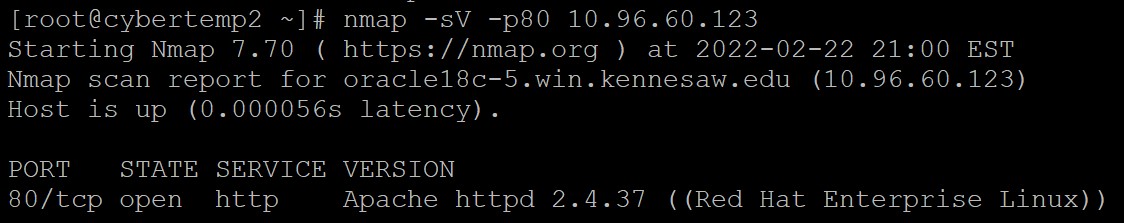


**MariaDB Sites to make into References:** [**https://severalnines.com/database-blog/ten-tips-how-achieve-mysql-and-mariadb-security**](https://severalnines.com/database-blog/ten-tips-how-achieve-mysql-and-mariadb-security) https://mariadb.com/kb/en/mariadb-administration/ [**https://www.oreilly.com/library/view/mysql-reference-manual/0596002653/ch04s02.html**](https://www.oreilly.com/library/view/mysql-reference-manual/0596002653/ch04s02.html)

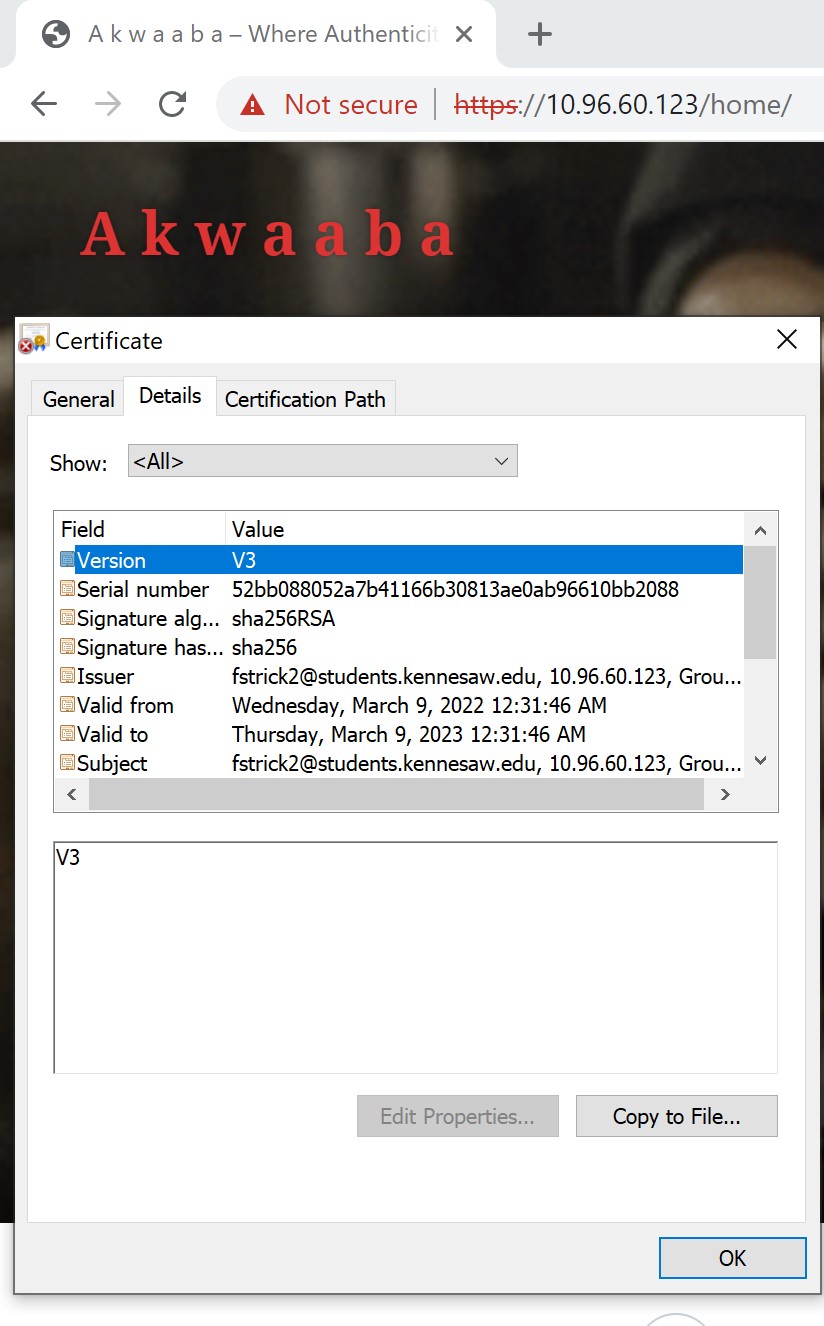
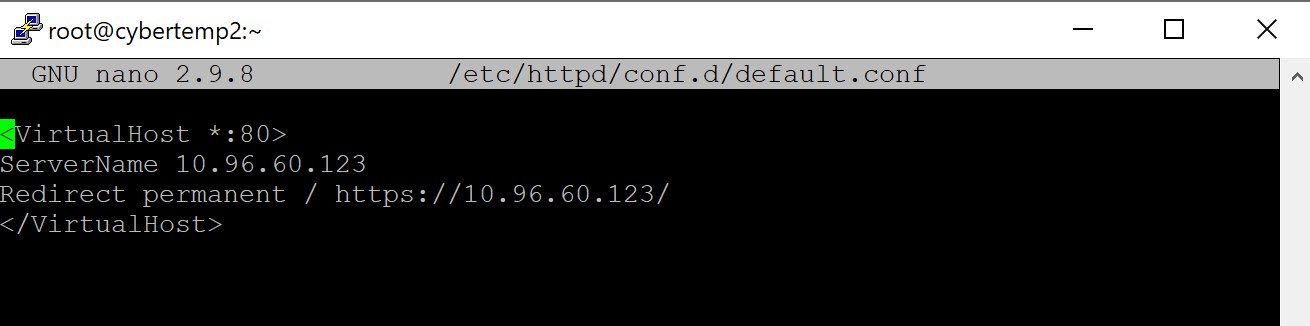
**https://www.digitalocean.com/community/tutorials/how-to-secure-mysql-and-mariadb-databasesin-a-linux-vps**

**Felton** Apache server

1. **Disabled Server Signature-** server now shows less information and prevents banner grabbing attacks. We will be able to remove “Apache” completely from banner once we install WAF (Web Application Firewall).

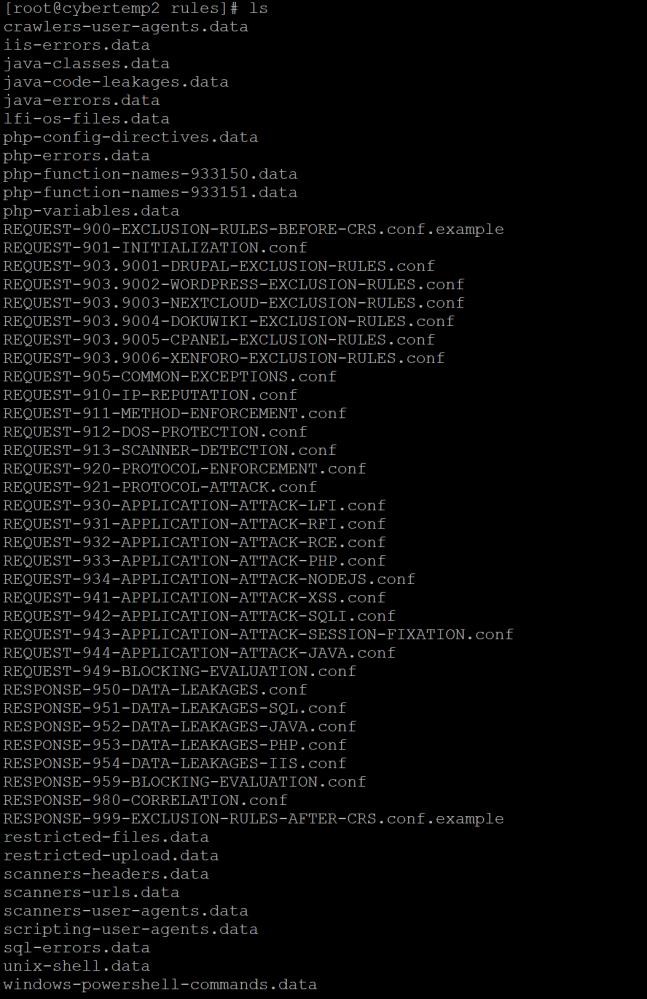


1. **Ensured server-status and server-info directives were not enabled by default.**
2. **Established HTTP/HTTPS redirect with self-signed SSL (Secure Socket Layer) certificate. Because the website is hosted on the local network via VPN, we must use a self-signed certificate. It is completely normal for a self-signed certificate to show as not secure even though SSL is in use.**



**3. Install ModSecurity WAF 2.9.3 with OWASP rule set**

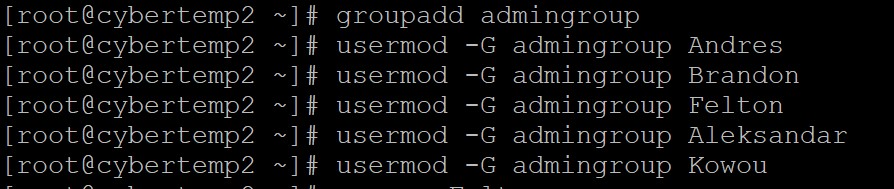




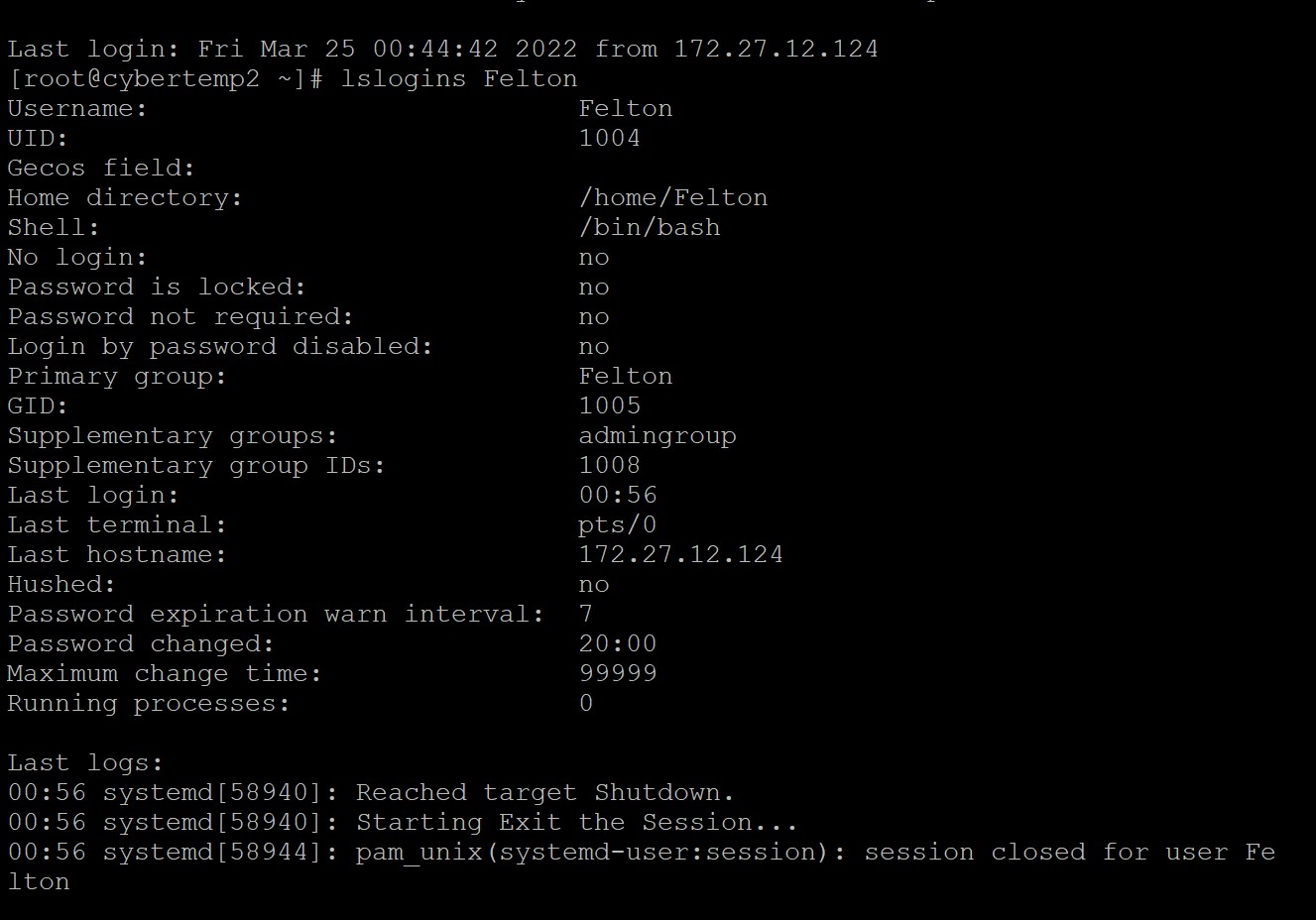
\*List of rules that are configured in ModSecurity WAF to prevent attacks and exploitation.

**Kowou** VM

* 1. **Added individual accounts for each team member and placed users in “admingroup”**



* 1. **Established account logging via root account**



* 1. **Change root password to $up3ru$3r**

