Inject Response

|  |
| --- |
| BLUE TEAM X |

|  |  |
| --- | --- |
| To: | White Team |
| From: | Blue Team X CentOS Admin |
| CC: | Board of Directors |
| Date: | 2/11/2018 |
| Re: | Inejct # 06 / Security Assessment |
| Comments: | When it comes to risks with CentOS operating systems, the top risks are the same for most Linux Operating Systems. One of the biggest risks is setting the wrong directory or file permissions in a way that allows important files to be accessed by anyone in the system. The second risk is giving elevated privileges to non-administrative users to make root only changes through miss configuration of proper user permissions. The last risk that can occur is leaving unused ports open on the CentOS machine, like SMTP port 25 is left open even though none of CentOS services use SMTP.  The only application on CentOS is our OScommerce store. There is some risks when you first start using OScommerce. The biggest risk is not deleting the “install” directory which would allow anyone to reinstall our store and we could lose all of our data. The next biggest risk is not using an SSL certificate with HTTPS. If we use just HTTP, we leave passwords and data we send over the network open for packet sniffing, in this case logging in with an admin account would leave our elevated account open for access to anyone. The last biggest risk is injection of php commands through website input fields that can run shell commands of the operating system. A malicious user can gain elevated privileges or break the operating system if one does not jail the HTTP server. |