Inject Response

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

|  |  |
| --- | --- |
| To: | White Team |
| From: | Blue Team X Debian Admin |
| CC: |  |
| Date: | 2/11/2018 |
| Re: | Inject # 1 |
| Comments: | The three biggest vulnerabilities to Debian are as follows; Bad configurations, which allow for compromises and unauthorized uses to gain access to the operating system. Incorrect user permissions and passwords, this is a vulnerability that creates an opportunity for an unauthorized user to run damaging commands on the machine which can seriously impact security. Finally, complacency and user error are a big security concerns in any operating system and can compound any security problems a machine already has.  The three biggest risks to Squirrelmail are as follows; Bad Apache configurations that provide an opportunity for exploits to be run. Apache, and a component PHP, by default are rather insecure. Squirrelmail is also vulnerable to bad SSL certificates, this is primarily a configuration issue that can be solved with best practices to the configuration files. Finally bad or short passwords are a risk to the users on squirrelmail. |