Pre-Voltron Security Specifications

Document Name :	Pre-Voltron Security Specifications
Version :	1.0
Version Date :	3/06/2022
Modified By :	Marc MARTINEZ
Creation Date :	3/06/2022
Created by :	Marc MARTINEZ
Approved by :	Marc MARTINEZ
Confidentiality Level :	INTERNAL

Modification History

	Date	Author	Commentary
1.0	5/06/2022	Marc MARTINEZ	Creation of the document
1.0	9/06/2022	Alan Garbo	Presentation document & link

Introduction

This document will present the preparations we made for the pre voltron phase and the solutions we thought off to ensure the correct security of this project and of the functionnalities that will be produced.

Content

Security in Documentation

To ensure the security of all documentation produced for this project we have chosen to use a Notion. This Notion allow us to write detailed documentation that can only be seen by people added to the notion.

This way we can also store important or critical informations in notes in this service.

Furthermore we also implemented a confidentiality level to all documentation so that people know what to share and what not to share, as well as a formal modification history (the software also allow us to have a modification history as a functionnality to go back on changes and prevent information loss). The correct way to write the documentation is explained in a specific document in the General Information tab (see Document Drafting Policy).

All communication is done through Discord and Microsoft Teams, only added people can see the communication content.

Members of the SEC group are in charge of the Discord and the Notion.

Security in Servers

We will secure the servers connexions by putting fail2bans jails on the ssh connexion and others exposed ports.

We will also implement iptables scripts to close unused ports.

Depending on the technologies used by the others specialities we can implement specific securities, like a req_limiter on nginx.

Some monitoring software can be used to monitor connexions and users permissions, like the easy and usefull webmin (that we can protect using fail2ban).

We could also change default ports to deter simple scrapping bots.

Finaly we should put in place a rigid password policy to prevent an easy bruteforcing of our connexions, or social engineering of the password.

Security in Development

We need to be active with the dev specialities to be sure that they are not creating functionnalities with obvious securities holes in them.

We should also make sure that they have some notions of quality coding, to prevent easy mistakes that would create vulnerabilities.

Security in CI/CD

We should insure that importants informations do not get send in clear on the CI/CD process. As well as in the versionnings tools used for code quality.

For example if Ansible is used by the devs, we can make sure that Ansible Vault is used to prevent passwords and ENV variables to be shown in clear in the code.

Security in Audits

On the audit part we will scan ports and try to find vulnerabilities in the application using various tools.

For example we can use hydra and john the ripper to try and brute force our way into the applications.

Thoses tools are easily available on the linux distribution Kali Linux, but they can be installed on others distribution if needed.

Document presentation

Here is the link of our security presentation : https://docs.google.com/presentation/d/1hSzWHI6-ncZ9oS2AOReQZHK-sdwuF8672BonQ-ZPG_I/edit?usp=sharing