MITRE Caldera Project Webserver

This webserver is provided by the **MITRE Caldera Project Group** at **The Hague University of Applied Sciences (De Haagse Hogeschool)**.

Purpose of the Webserver

The primary purpose of this webserver is to serve as an entry point into the **Virtualized Operational Technology (OT) Environment**. It provides initial credentials that are supplied directly on the server, simulating a realistic setup often seen in cybersecurity training and testing environments.

Vulnerabilities and Exploitation

Shellshock Vulnerability

The webserver has been intentionally configured to contain a **Shellshock vulnerability**, which can be exploited to achieve **Remote Code Execution (RCE)** within the environment. Once exploited, users can access employee credentials stored on the server.

Gaining Initial Foothold

By utilizing a **reverse shell**, users can establish a foothold in the environment. These credentials can then be used to access the **Human-Machine Interface (HMI)**, providing the opportunity to escalate privileges further within the OT environment.

Logging and Blue Team Activities

All activity from this webserver is logged and sent to **OpenSearch**. These logs are designed to be used for **blue team exercises**, enabling participants to detect, analyze, and respond to simulated attacks in a controlled environment.

This webserver setup is a critical component of the MITRE Caldera Project's training and testing scenarios, offering a safe and practical way to explore the challenges of OT security.