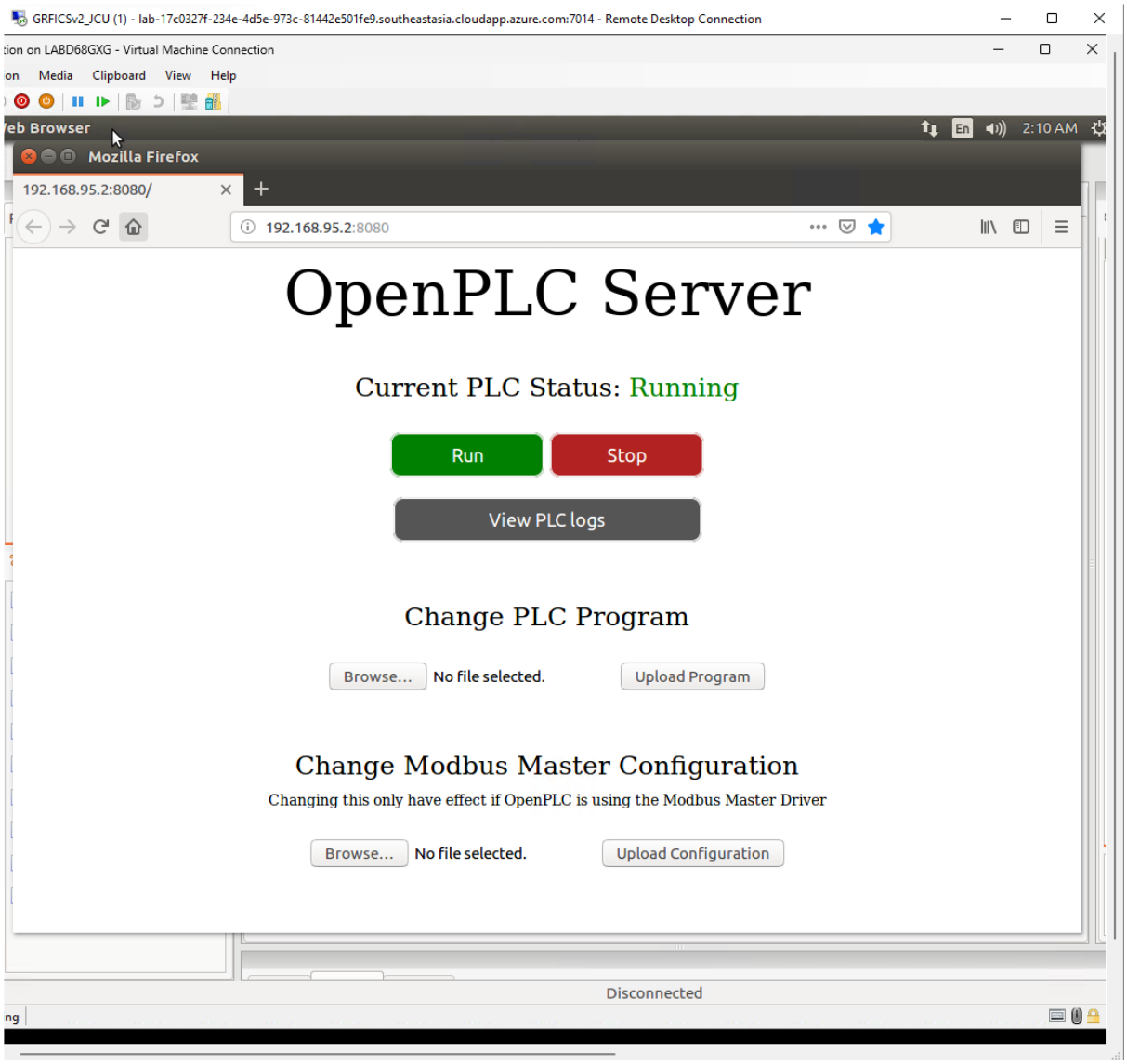
It looks like a ladder, with vertical power rails and horizontal rungs that represent different control operations. Each rung contains contacts and coils that work like electrical switches—normally open contacts allow current flow when activated, while normally closed contacts block current until activated. Coils control devices like motors or lights based on input conditions

In our plc logic inside hyper V, there are several stages that sets the valve position for running plc

And at the very bottom, that has run bits, where coil 40 was injected into from last practical

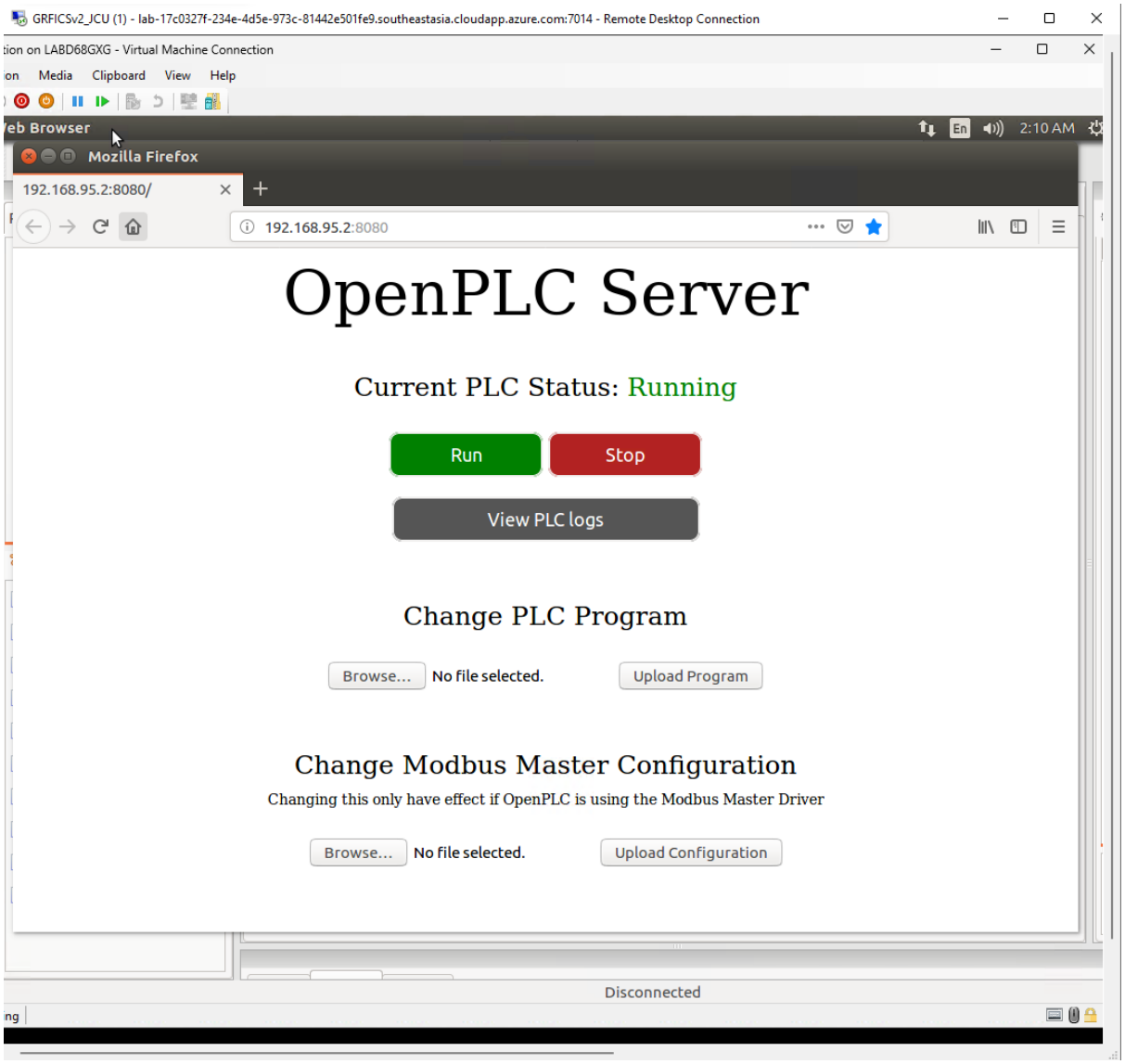
The malicious version of plc has larger press spc than chemical version of plc, if malicious version of plc is applied, the plc would explode due to larger press than usual

The malicious version of plc has larger press spc than chemical version of plc, if malicious version of plc is applied, the plc would explode due to larger press than usual



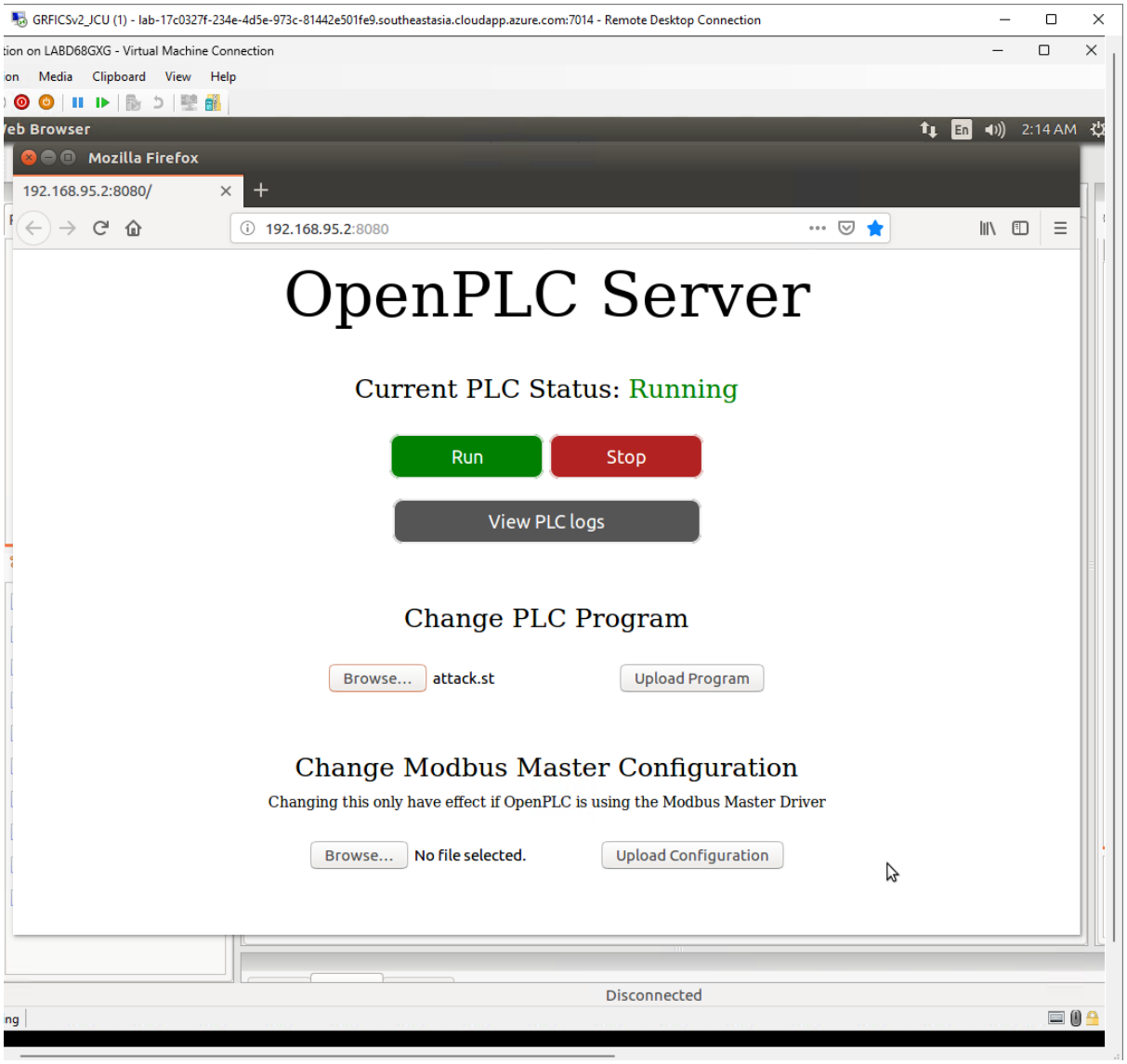
After saving the malicious plc as attack.st

I opened firefox on workstation and this plc page poped up

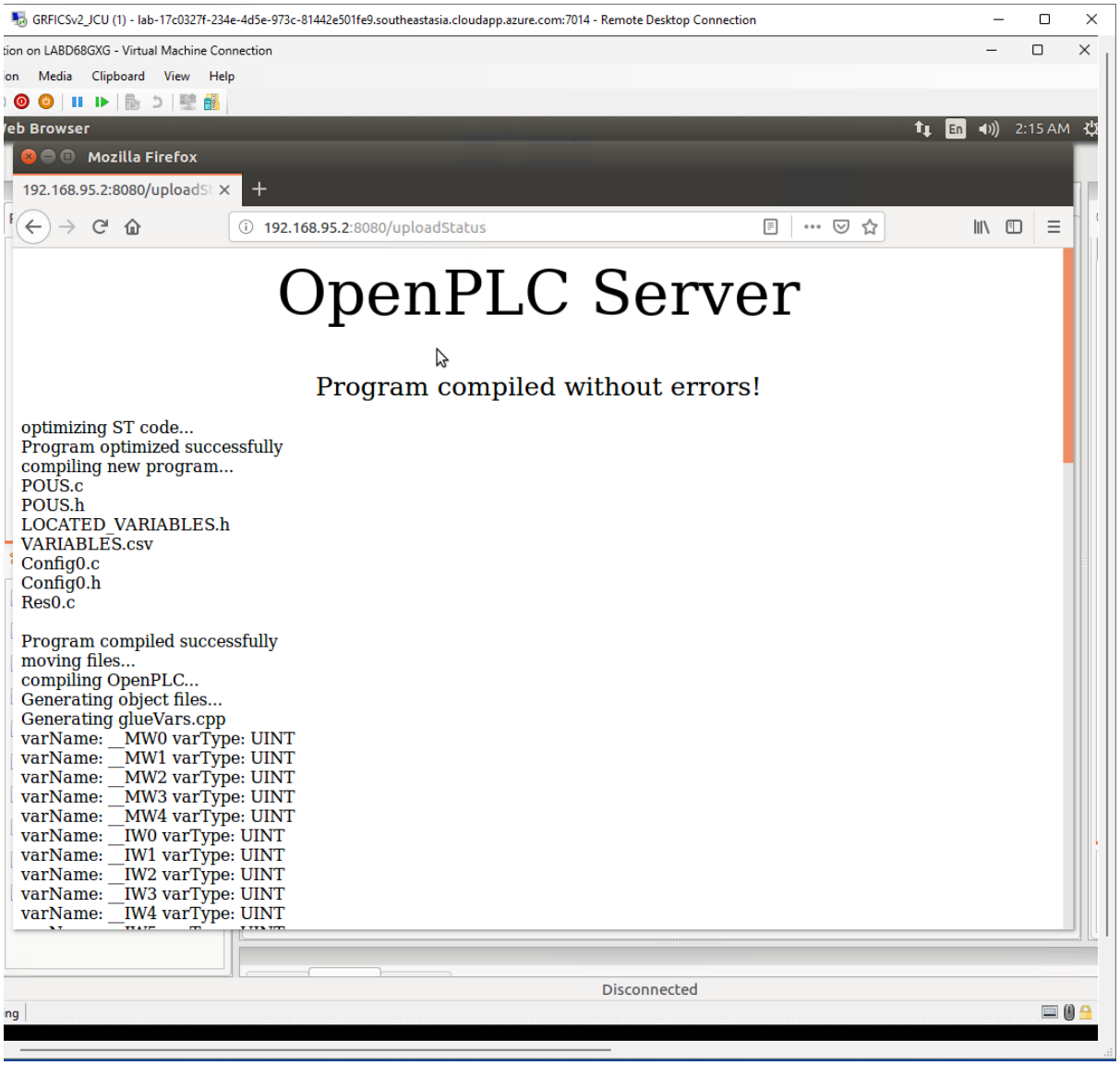


After saving the malicious plc as attack.st

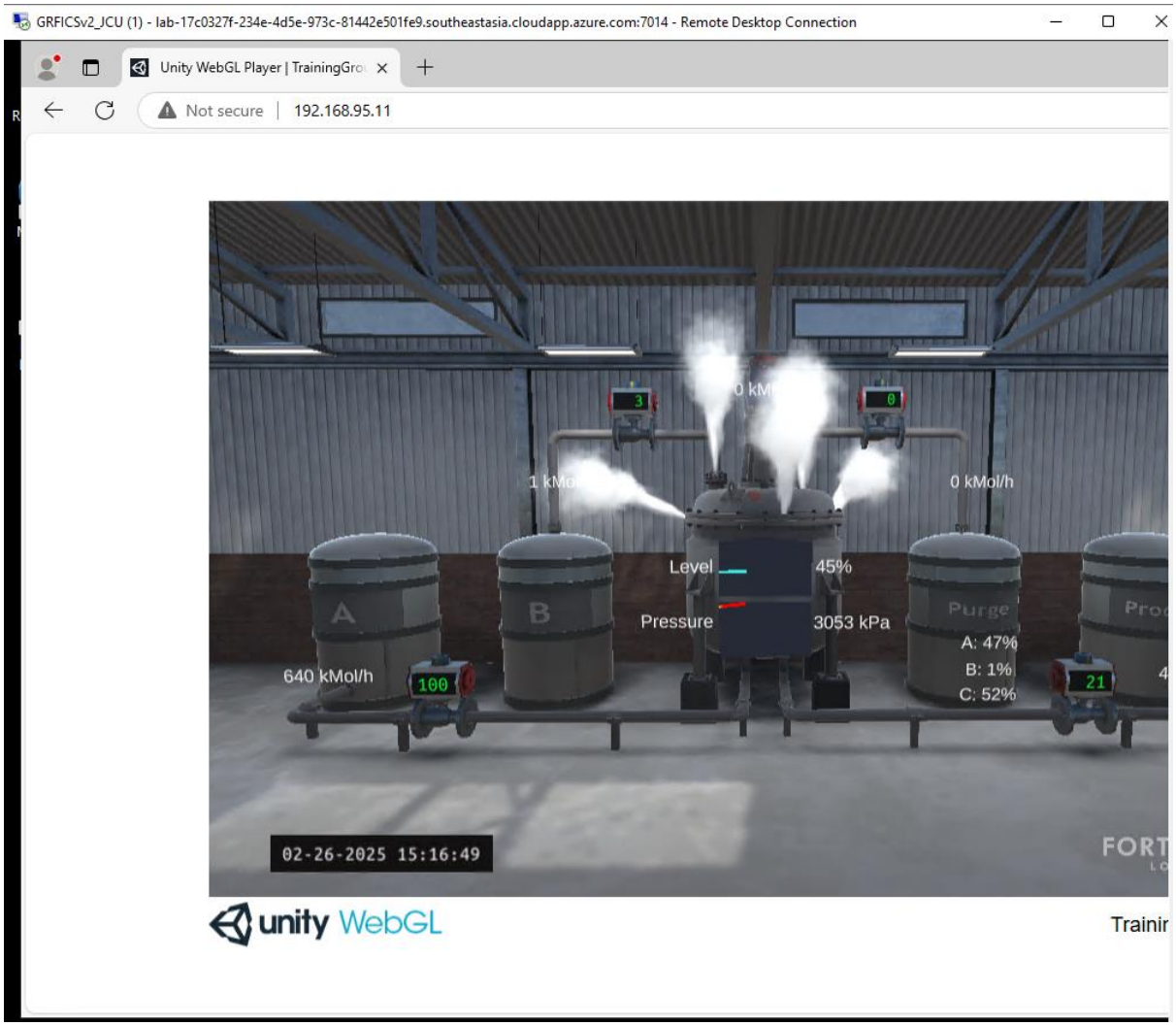
I opened firefox on workstation and this plc page poped up



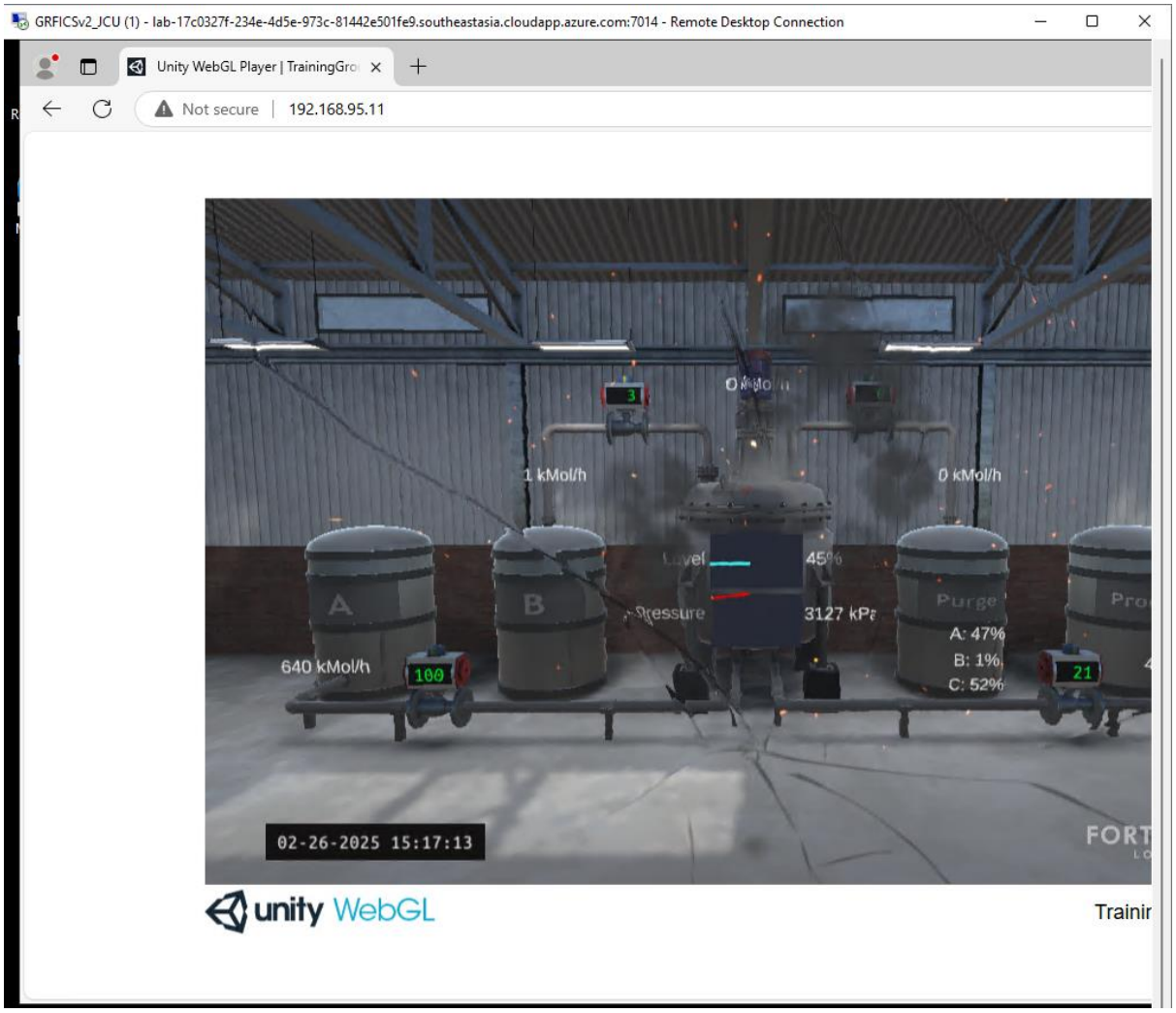
Uploaded malicious plc as plc program



compilation successful



pressure begins to be higher



and eventually explodes

Challenges in exploiting this type of attacks are

Accessing the plc network

Granting access in authentication and security controls

Uploading the malicious program successfully

Avoiding detection system until attack is succeed

Possible weaknesses in the system are

Weak authentication method that might allow attackers to easily bypass the security system resulting in installing the malicious attack

Weak detection and monitoring system

If detection is not functioning properly the malicious act will have zero chance of being caught before and after the exploitation

Insecure plc operation

Because after the attack, instantly our plant chemical was exploded indicating it did not have a proper security system that by simply changing the file folder of ladder logic the whole plant chemical was destroyed

Explanation of ladder logic and exploitation

Ladder logic is a programming method used in Programmable Logic Controllers (PLCs), designed like an electrical circuit. It has contacts and coils that control devices such as motors and valves. In this scenario, the PLC inside VM follows multiple steps to set valve positions and control system operations. At the bottom of the logic, coil 40 was injected in a previous attack, making it possible to manipulate the PLC's behaviour

The attack involved uploading a malicious PLC program through a workstation's web browser. This modified the PLC's logic to increase pressure beyond safe levels. Once compiled and executed, the system's pressure kept rising until it exploded, showing that the PLC lacked safety restrictions to prevent dangerous changes

Several challenges exist when exploiting a PLC, The attacker must gain access to the PLC network, bypass authentication, and successfully upload the malicious program. They must also avoid detection systems, which might log or block unauthorized modifications

The weaknesses that made this attack possible include weak authentication methods, poor monitoring, and insecure PLC operations. Without proper security, attackers can remotely change critical settings, leading to serious consequences. Similar attacks, like Stuxnet and Triton malware, have targeted industrial systems, proving the need for stronger security in critical infrastructure

References

https://ladderlogicworld.com/ladder-logic-basics/#google_vignette