Tutorial: How to hack OPC UA

INTRODUCTION

OPC UA is a long-standing and widely used communication protocol for industrial automation. It enables unified data exchange, telemetry collection, and control of Operational Technology (OT) systems of various vendors. Engineers can use it, for instance, to monitor and operate all machinery in a factory from a single interface.

Today, critical sectors ranging from Aerospace & Defense to Energy & Mining use OPC UA. Given its wide use and key role in critical sectors, security issues in OPC UA systems may affect human lives and the welfare of entire nations.

This report covers the process of identifying those security issues and evaluating their impact so they can be fixed.

GOAL

The goal of this report is to walk you through the practical process of discovering OPC UA systems, scanning them for vulnerabilities, analyzing the results, and finally exploiting them.

TABLE OF CONTENTS

1. TARGET DISCOVERY

The goal of this step is to discover OPC UA servers. The three methods for discovery are port scanning, Multicast DNS (mDNS), and querying Discovery Servers.

Port scanning can be used to find OPC UA servers on the public internet and private networks. The servers listen on TCP port 4840 by default, but it is common to use non-standard ports. They may communicate using either binary protocol or HTTP. Only a fraction of servers use the HTTP protocol, thus we focus only on the binary.

mDNS only works within Local Area Networks (LANs). Not all servers are configured to reply to mDNS queries, and thus relying only on mDNS for discovery may result in missed targets.

OPC UA servers may be registered on special Discovery Servers that can be queried without authentication. The Discovery Servers are private to each environment; thus, you need to find them first. They can be discovered using the first two methods.

It is recommended to use both port scanning and mDNS if applicable. Even better if you could supplement your findings with a list of OPC UA servers provided by network operators. Discovery through discovery servers is redundant as it is automated by our vulnerability scanner of choice.

1.1. PORT SCANNING

The OPC UA binary protocol is currently unknown to port scanners. Therefore, it is hard to know if you have found all servers on the target network. We recommend scanning at least TCP ports 4840 and 53530 and assume all open ports are OPC UA servers.

1. Install nmap
2. Scan ports TCP ports 4840 and 53530 on the target network
   nmap -T4 -n -Pn -p 4840,53530 --open -oG - <TARGET NETWORK>

```
valtteri@t490:~$ sudo nmap -T4 -n -Pn -p 4840,53530 --open -oG - 172.16.1.1/24
# Nmap 7.80 scan initiated Sun Dec 31 13:51:49 2023 as: nmap -T4 -n -Pn -p 4840,53530 --open -oG - 172.16.1.1/24
Host: 172.16.1.8 ()     Status: Up
Host: 172.16.1.8 ()     Ports: 53530/open/tcp/////      Ignored State: filtered (1)
Host: 172.16.1.12 ()    Status: Up
Host: 172.16.1.12 ()    Ports: 53530/open/tcp/////      Ignored State: filtered (1)
Host: 172.16.1.13 ()    Status: Up
Host: 172.16.1.13 ()    Ports: 53530/open/tcp/////      Ignored State: filtered (1)
# Nmap done at Sun Dec 31 13:51:52 2023 -- 256 IP addresses (256 hosts up) scanned in 2.59 seconds
```

Figure 1 Discovering 3 possible OPC UA servers using port scanning.

1.2. mDNS

1. Install UaExpert
2. Launch UaExpert
3. Select Add Server
4. Select the arrow left to ServersOnNetwork
5. Wait for loading to stop
6. If servers are found, they are displayed under the ServersOnNetwork
7. Select a server, select Advanced, Record Endpoint Url
8. Repeat for all found servers

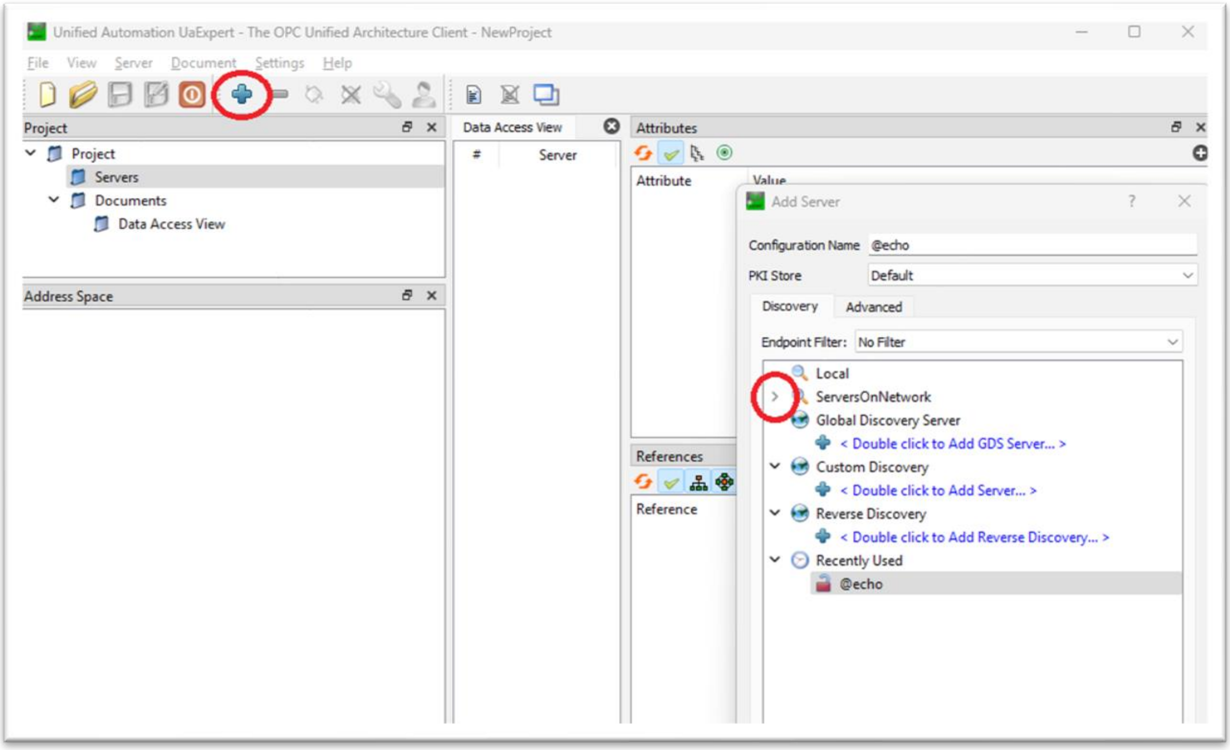

Figure 2 mDNS discovery using UaExpert.

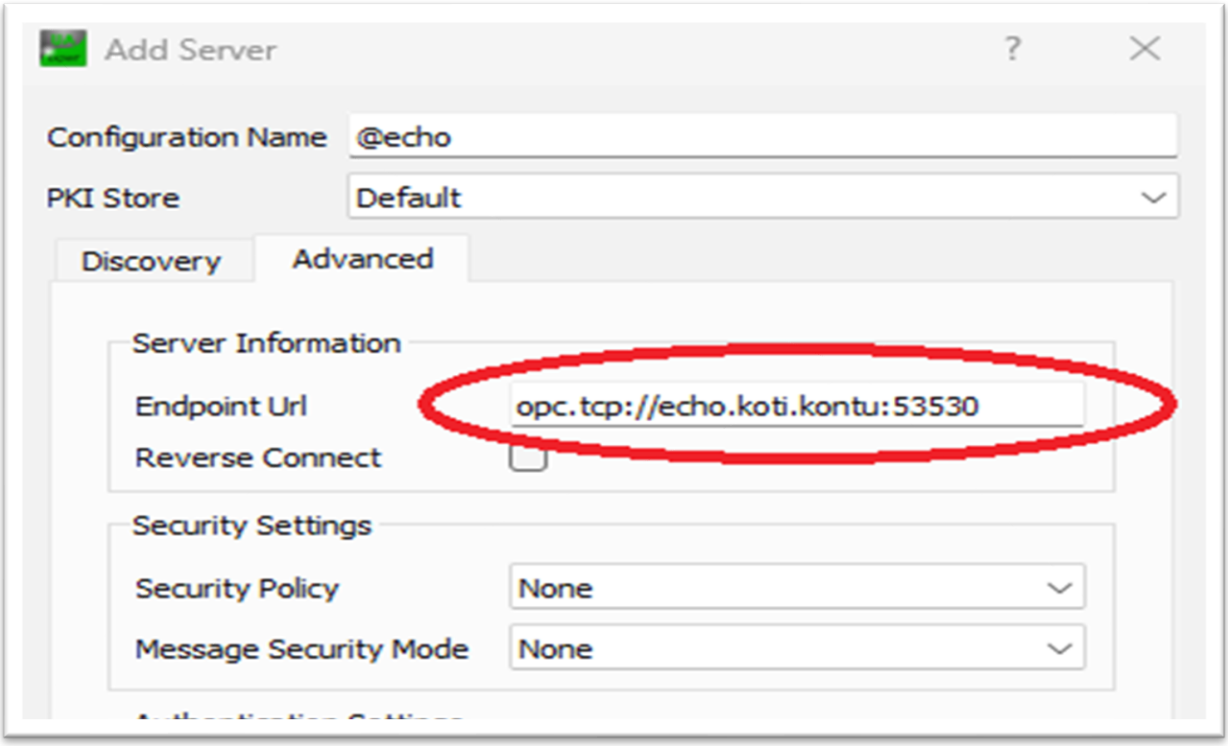

Figure 3 Endpoint Url of a server discovered by UaExpert.

1.3. QUERYING DISCOVERY SERVERS

This is not required as it is automated by our vulnerability scanner of choice.

1.4. FORMATTING TARGETS

By the end of target discovery, you need to have a list of OPC URLs. You should format the targets into OPC UA URLs as follows:

opc.tcp://<hostname or IP address>:<port>

For example, port 53530 on 172.16.1.8 becomes opc.tcp://172.16.1.8:53530

Collect the URIs in a text file for easy handling.

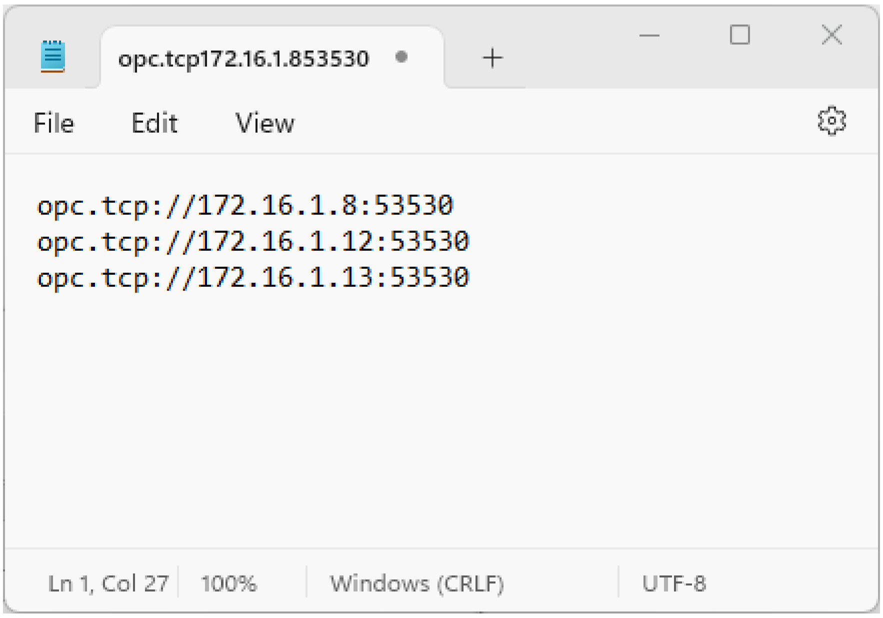

Figure 4 Text file with 3 OPC UA URLs ready for vulnerability scanning.

2. REVEALING VULNERABILITIES

The goal of this step is to check the discovered OPC UA servers for security issues. We do this by running a vulnerability scan against them using OpalOPC.

All vulnerabilities discovered should be reported to the system owners regardless of severity.

2.1. SCANNING FOR VULNERABILITIES

1. Install OpalOPC
2. Launch OpalOPC
3. Add targets from your list of OPC UA URLs
4. Optionally configure settings
    a. Default settings are already very effective
5. Select Scan
6. Wait for the scan to finish

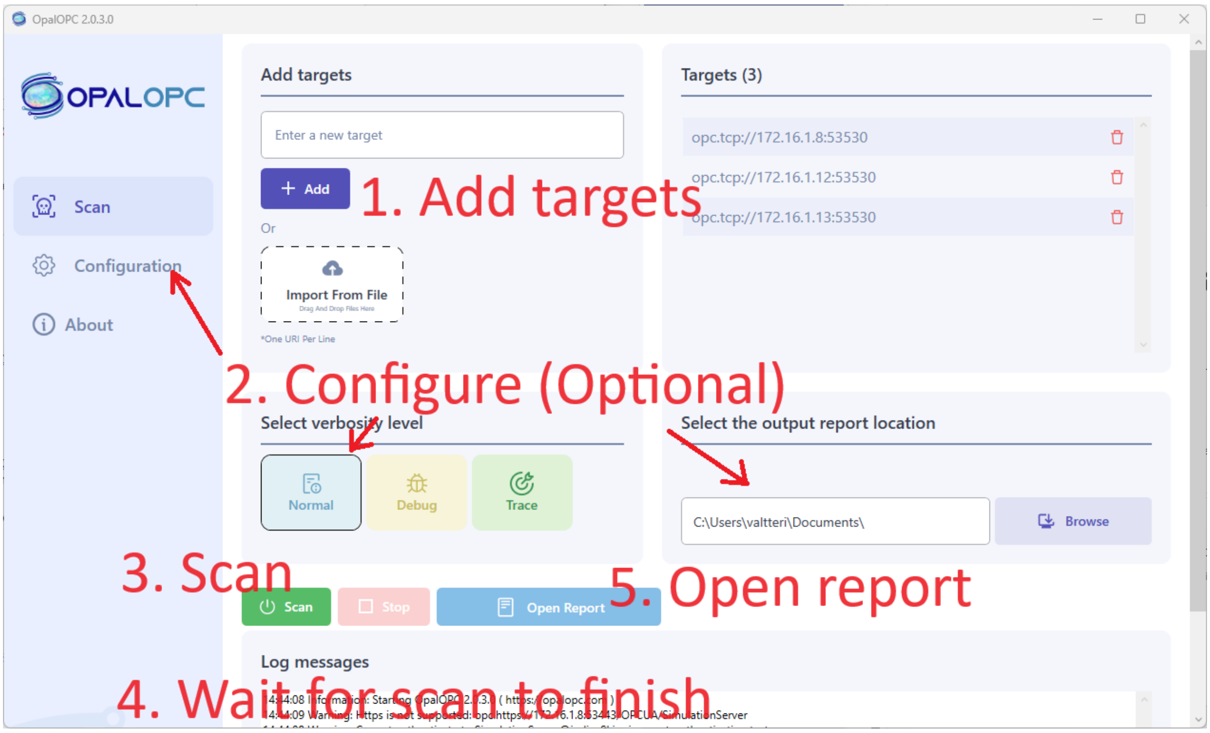

Figure 5 Vulnerability scan using OpalOPC GUI.

2.2. ANALYSING RESULTS

1. Select Open Report
2. View the table of security issues for the first target
    a. The Application name and Product URI may help you figure out what kind of device the target is.
    b. Look especially for issues that allow authentication with the server (Severity >= 7.0). These are the most dangerous ones.
    c. Issues with lower severity may also allow exploitation!
3. Repeat for the rest of the targets

Results Summary (3 Applications Found)

Severity levels	Info	Low	Medium	High	Critical
	0	[0,1-3,9]	[4,0-6,9]	[7,0-8,9]	[9,0-10,0]

0

Application name	SimulationServer@echo
Application type	Server
Application URI	urn:echo:OPCUA:SimulationServer
Product URI	urn:prosysopc.com:OPCUA:SimulationServer
Errors	1

Discovery URL	Issue type	Plugin Id	Severity
opc.tcp://echo:53530/OPCUA/SimulationServer	Anonymous authentication enabled	10001	High (7,3)
	Message Security Mode None	10006	Medium (6,5)
	Security Policy None	10009	Medium (5,4)
	Self-signed client application certificates trusted	10010	Medium (5,4)
	Auditing disabled	10002	Medium (5)
	Deprecated Security Policy Basic128Rsa15	10007	Medium (4,8)
	Deprecated Security Policy Basic256	10008	Medium (4,8)
	RBAC not supported	10004	Info (0)
opc.https://echo:53443/OPCUA/SimulationServer	• Https is not supported: opc.https://172.16.1.8:53443/OPCUA/SimulationServer		

Figure 6 Table of security issues in opc.tcp://172.16.1.8:53530 with the most severe issue highlighted.

3. EXPLOITING VULNERABILITIES

In this step, the goal is to exploit vulnerabilities found in target servers. This is mainly for the reader's information, to underline the severity of the issues. Having a list of vulnerabilities is enough to fix them, but some clients want to see proof of the concept demonstrating the exploitation.

We cover only the exploitation of issues that allow authentication with the targets. If such vulnerabilities are found, we can configure the OPC UA client accordingly, and take a closer look at the target. Depending on the privileges of the user we can access, and the type of the target device, we may be able to read confidential information and even control the device.

Warning: Poking around without knowing what you are doing may cause serious health hazards to people and monetary losses to your client. Do not do this on production systems without written sign-off from the client.

3.1. BYPASSING AUTHENTICATION

1. Install UaExpert
2. Launch UaExpert
3. Select Add Server

4. Select Advanced
5. In Endpoint Url, paste the Discovery Url of the target
6. Configure Security settings according to the issue
7. Configure Authentication settings according to the issue
8. Configure a session name, such as pentest
9. Select OK
10. Right-click the server in Project view, and select Connect
11. If the connection is successful, you will now see the target server's address space
12. The address space may include confidential information that you can read

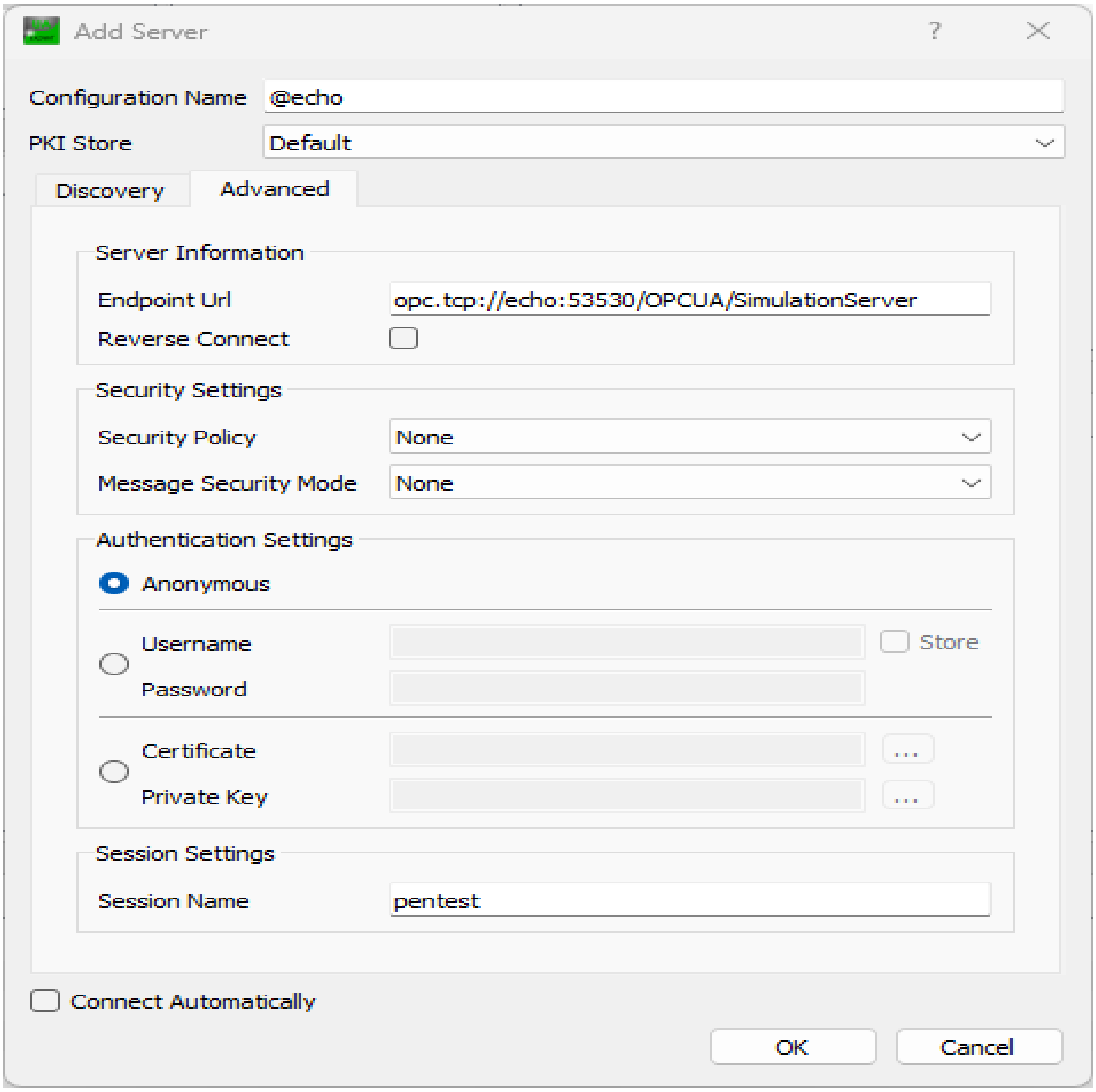

Figure 7 UaExpert configuration for target server that allows anonymous authentication.

3.2. VIEWING SERVER INFORMATION

1. Look for node “ServerStatus” in the address space
2. Drag and drop it to the Data Access View
3. Double-click the Value
4. A new window is presented with detailed information about the server

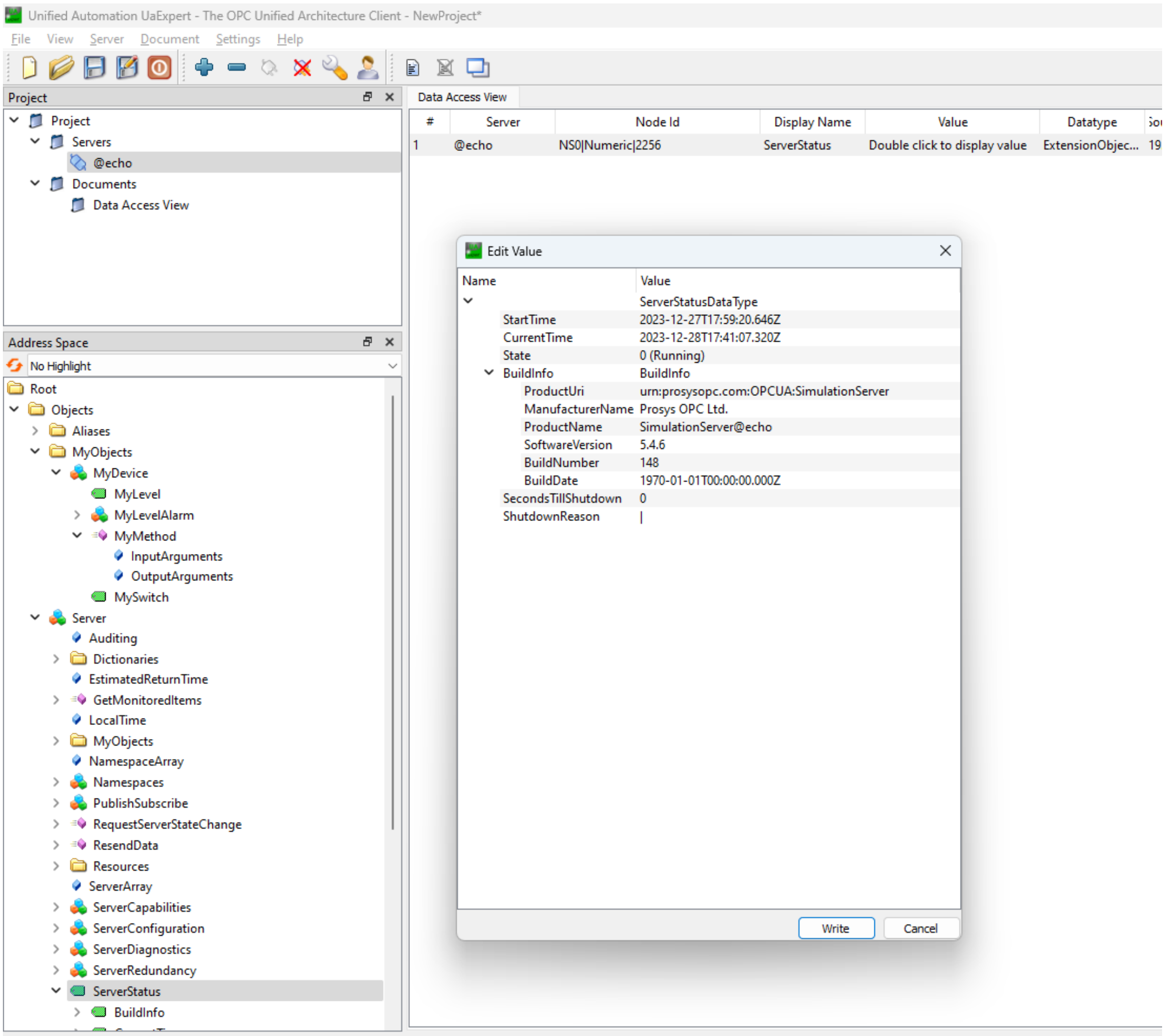

Figure 8 Viewing target server information.

3.3. CONTROLLING THE DEVICE

If you have write permission to nodes in address space that correspond to device controls, you can control it. The controls differ between devices; thus you may need to consult the manual after identifying the device. The device may have named its controls descriptively in an object; thus, it is worth checking if all else fails.

Controlling via changing values

1. Drag and drop the control nodes to the Data Access View
2. Double-click the value you want to edit
3. Edit the value and click Write

Controlling via calling methods

1. Right-click the method you want to call and select Call...
2. Set input arguments
3. Select Call
4. View the result and output

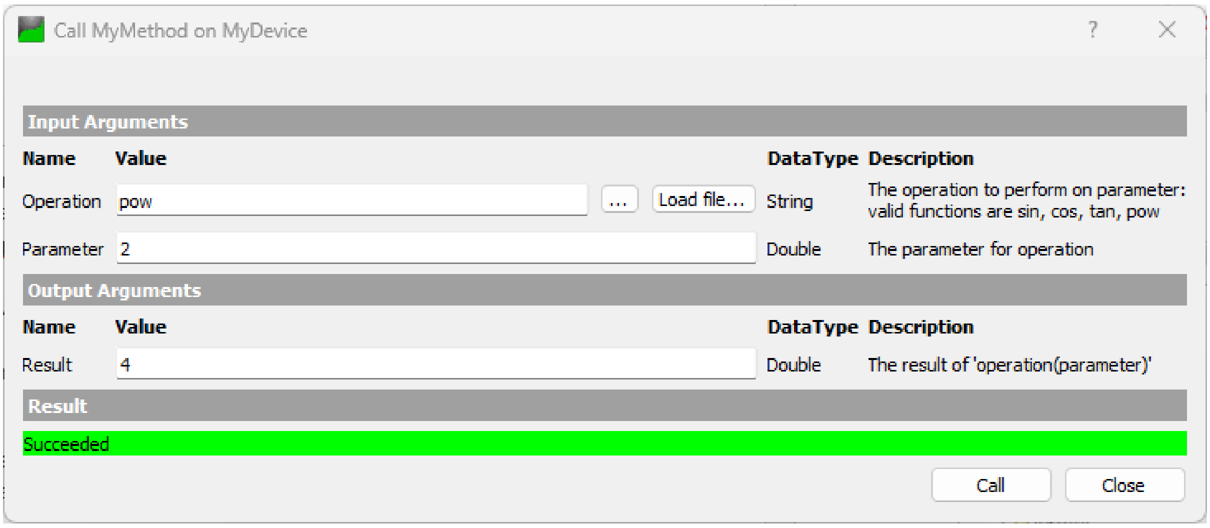

Figure 9 Calling sample method on the target.

4. CONCLUSION

Security issues in OPC UA systems may affect human lives and the well-being of whole nations. This report helped you identify the issues so they can be fixed. You were walked through target discovery, vulnerability scanning, result analysis, and finally exploitation of the vulnerabilities.

THANK YOU!

ADDRESS

Vuorenpeikontie
Helsinki, 00820

CONTACT

Phone: + 358 45 783 730 40
Email: info@molemmat.fi