SECTRIO

CVE-2022-30694

Date: 02/05/2022

Author: K. Narahari

Vulnerability Description:

Siemens ET200SP CPU 1510SP-1 PN device allows Cross-Site Request Forgery (CSRF) on FormLogin page.

Severity:

Category	CVSS 3.0 score
Medium	5.0

Weakness Enumeration:

CWE-ID	CWE-Name
CWE-352	Cross-Site Request Forgery

Detailed Technical Analysis:

1. Identifying the PLC device on the Network

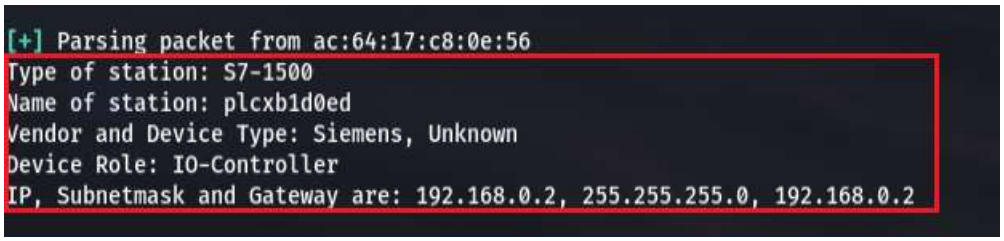

Figure 1 - The Siemens device was running on IP - 192.168.0.2

2. Identifying the Ports and Services Running on the target

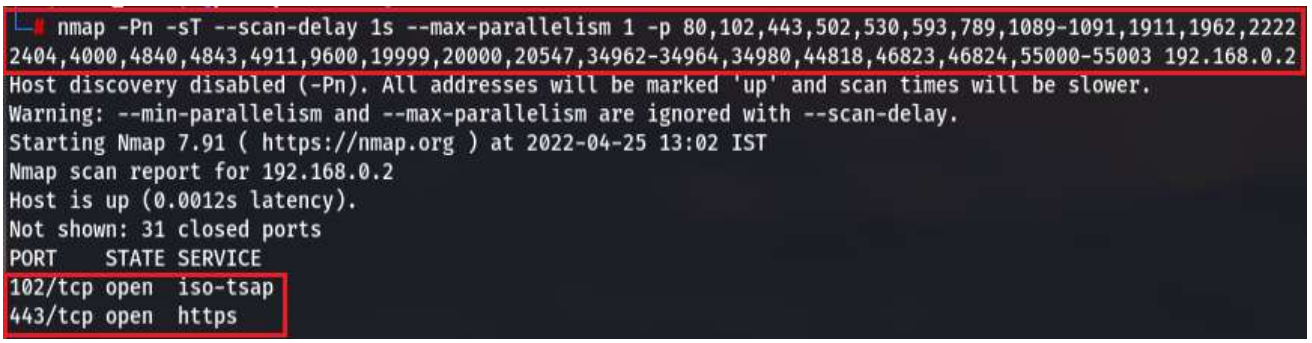

Figure 2 - Ports and Services Discovered

3. Performing device enumeration to know more information about the target

```
102/tcp open  iso-tsap
| s7-info:
|   Module: 6ES7 510-1DJ01-0AB0
|   Basic Hardware: 6ES7 510-1DJ01-0AB0
|   Version: 2.8.3
|   System Name: ET 200SP station_1
|   Module Type: PLC_1
|   Serial Number: S C-MDD844622020
|   Plant Identification:
|_  Copyright: Original Siemens Equipment
```

Figure 3 - Information gathered from device enumeration

4. From the port scan, port 443 https service running so can be accessed from web browser.

Figure 4 - Siemens Web Interface

5. After pressing the enter link on home page, it was redirected to login page.

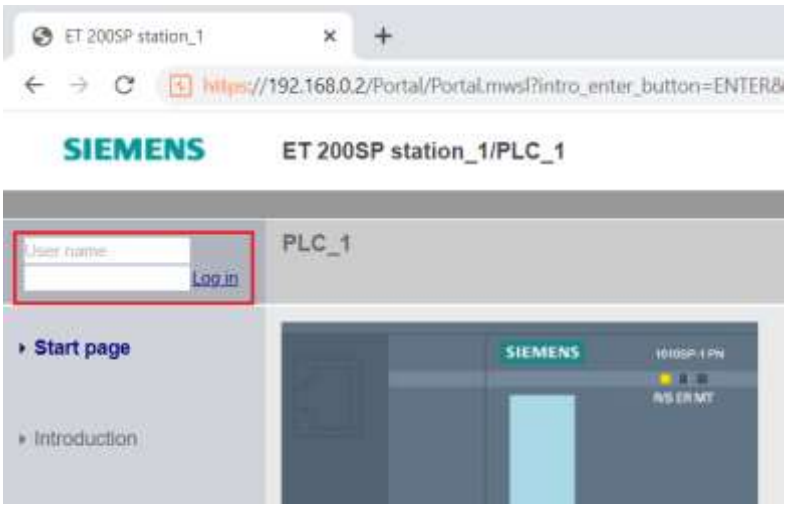

Figure 5 - Login Portal Discovered

6. Enter any credentials and Intercept the HTTP Request.

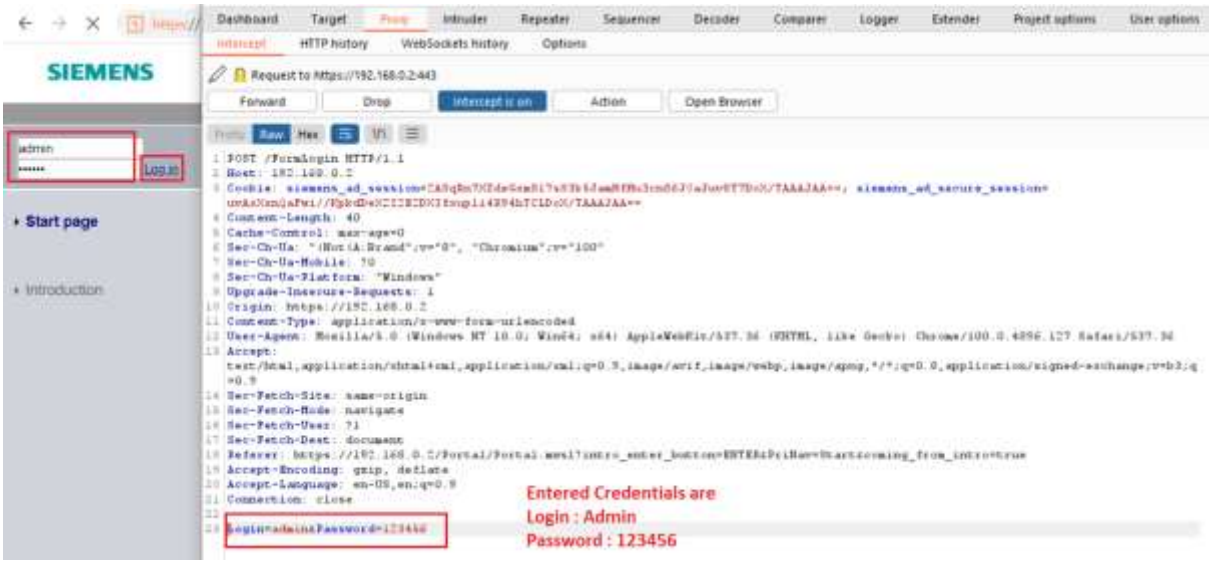

Figure 6 - Login has been intercepted and can observe entered credentials

7. Generate CSRF POC and edit the value of the password parameter

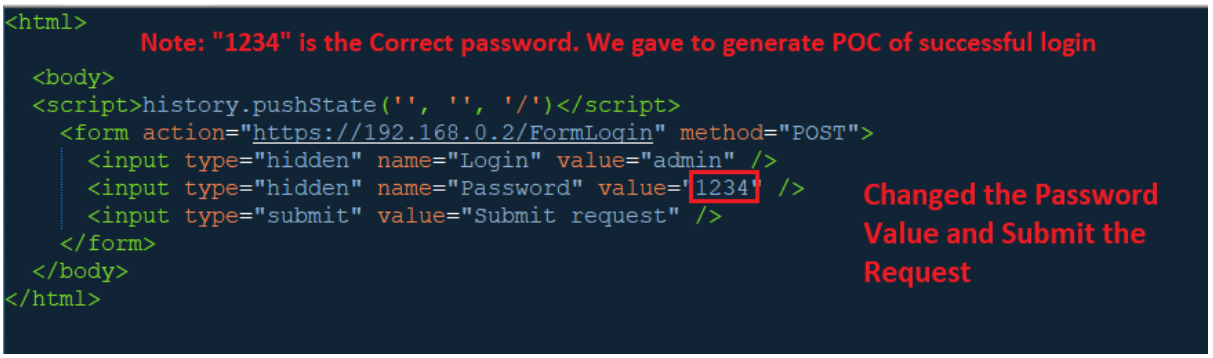

Figure 7 - Generated CSRF POC and changed the value

8. Now submit the CSRF Request

Figure 8 - Submitting CSRF Request

9. Without any error, the http request has been submitted and able to get the webpage.

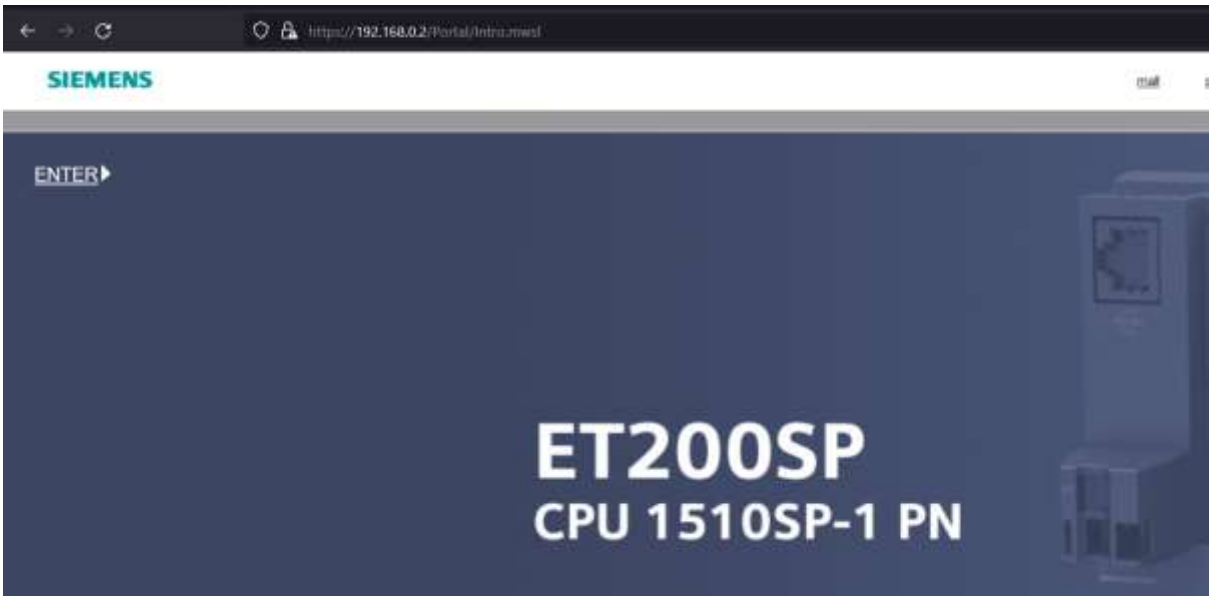

Figure 9 - Webpage has been loaded without error

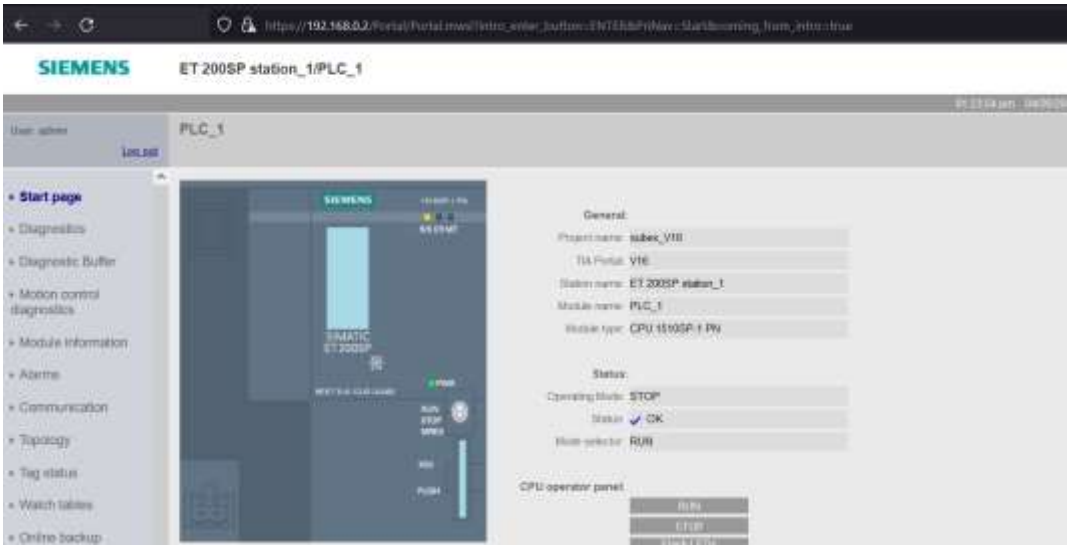

Figure 10 - CSRF attack was Successful

Detection and Mitigation

- Protect OT Network with Sectrio OT Suite
- Implement CSRF Protection
- Login CSRF can be mitigated by creating pre-sessions and including tokens in login form