

## Lab 6.6.4 Network Vulnerability Scanning with OpenVAS

*From TestOut CompTIA Security+ Course*

In this lab I will be scanning a network's machines for vulnerabilities using a custom configuration of OpenVAS.

### **The scenario for this lab is as follows:**

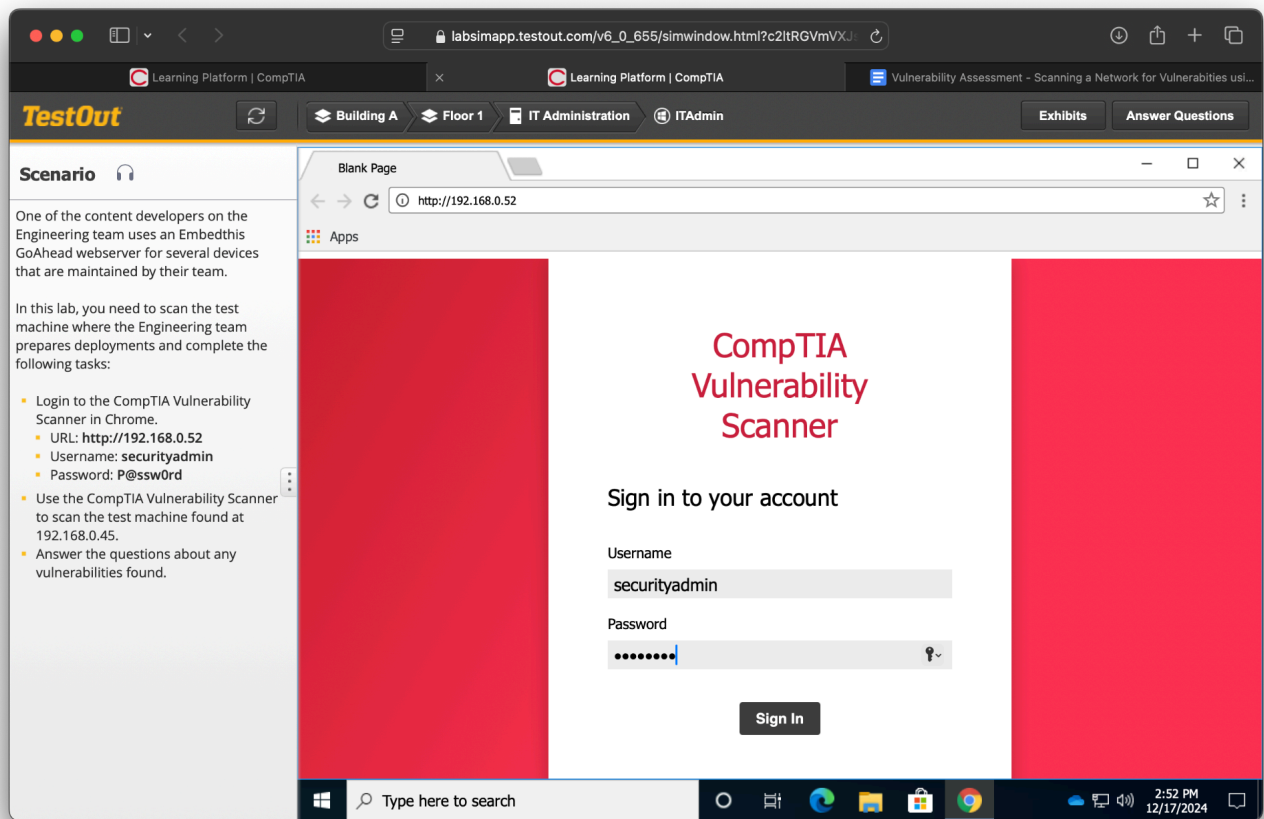
“One of the content developers on the Engineering team uses an Embedthis GoAhead webserver for several devices that are maintained by their team.

In this lab, you need to scan the test machine where the Engineering team prepares deployments and complete the following tasks:

- **Login to the CompTIA Vulnerability Scanner in Chrome.**
  - **URL:** `http://192.168.0.52`
  - **Username:** `securityadmin`
  - **Password:** `P@ssw0rd`
- **Use the CompTIA Vulnerability Scanner to scan the test machine found at 192.168.0.45.**
- **Answer the questions about any vulnerabilities found.”**

First, I will go ahead and log in to the Vulnerability Scanner which is located at **192.168.0.52** and log in with the credentials provided.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sat December 14th 2024



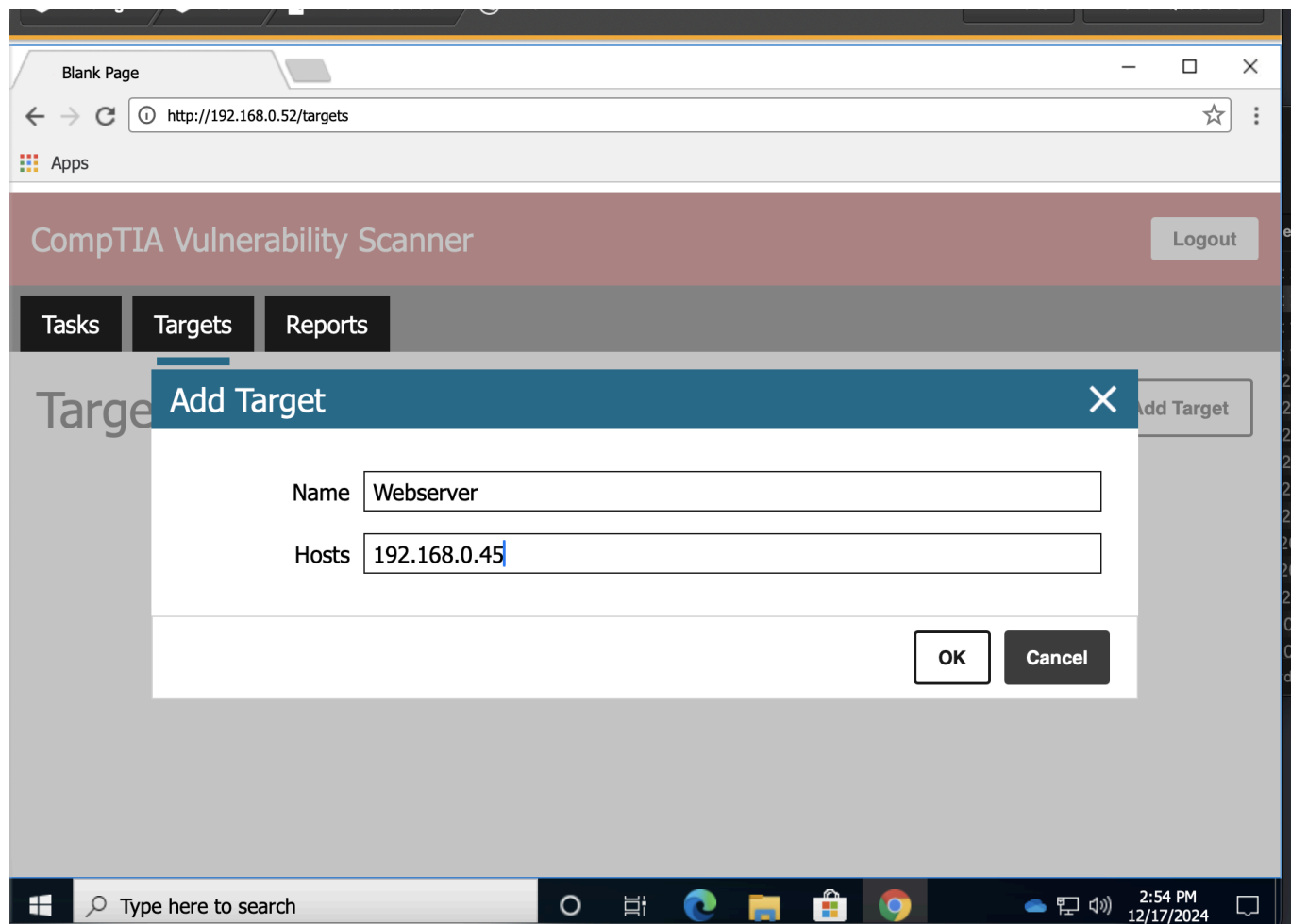
Once logged in I need to scan the webserver that's being used by the engineers in this hypothetical lab. We need to find out if their EmbedThis GoAhead Webserver has any potential vulnerabilities for attackers to exploit.

I will navigate on the top menu bar to **Target** and enter the IP address of the webserver which is **192.168.0.45**

Robert Carpenter

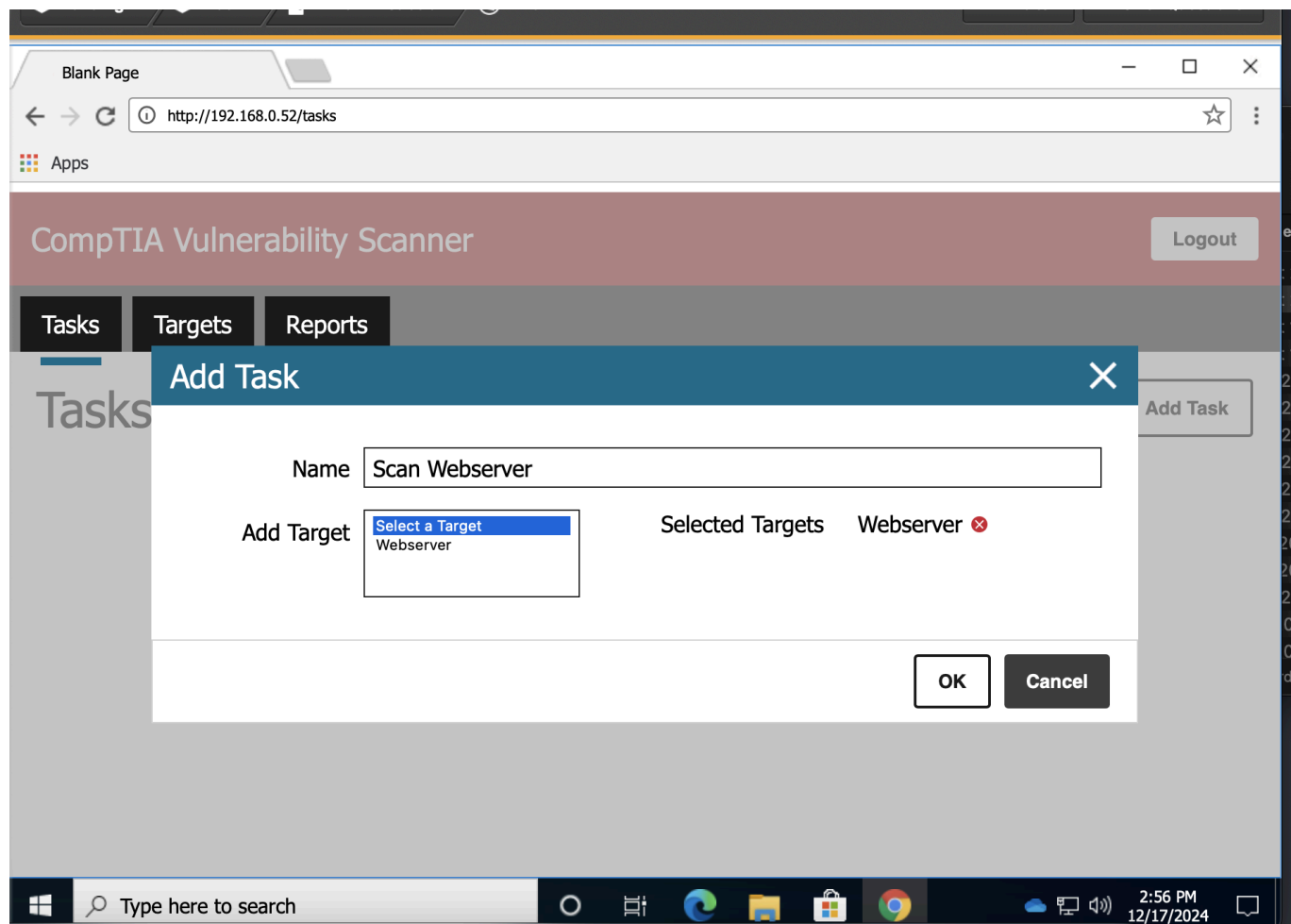
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)

Sat December 14th 2024



Now that I have a target I will head to the **Tasks** page at the top menu bar and assign a Task for the scanner to scan the Webserver I added in the **Target** page.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sat December 14th 2024

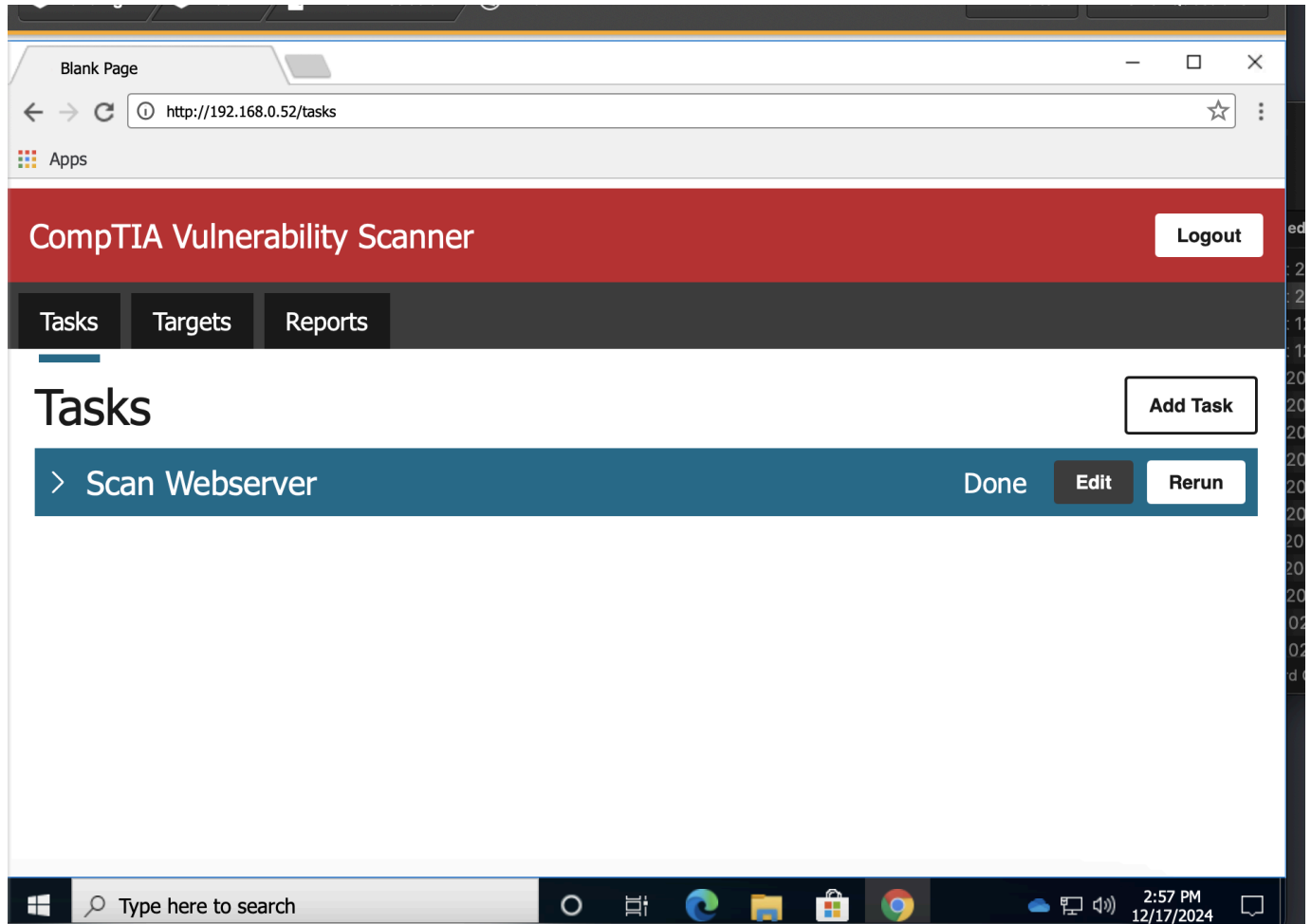


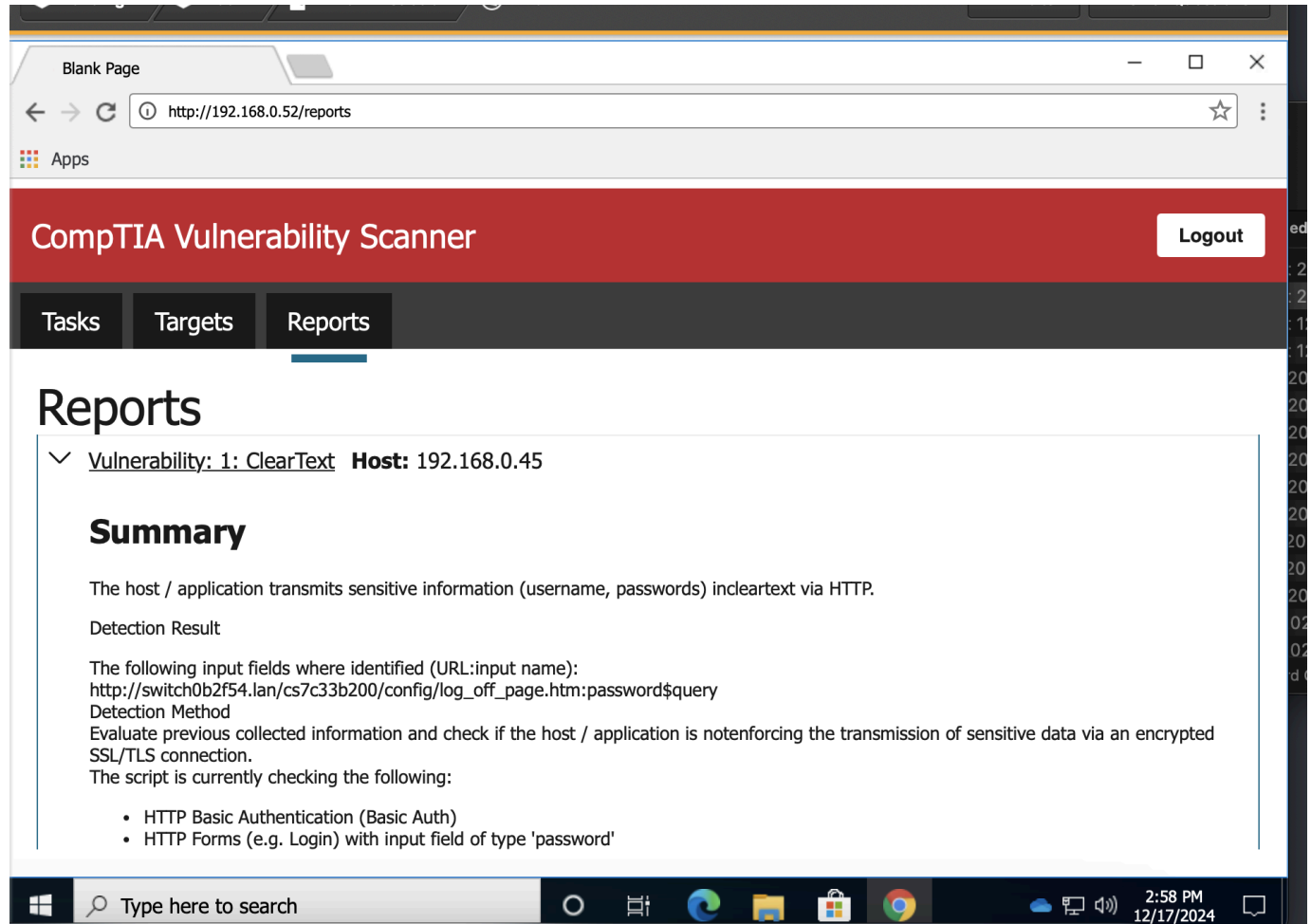
After that , I will click the **RUN** button and once it's done I will head to the Reports tab to see what it's found.

Robert Carpenter

[github.com/robertmcarpenter](https://github.com/robertmcarpenter)

Sat December 14th 2024

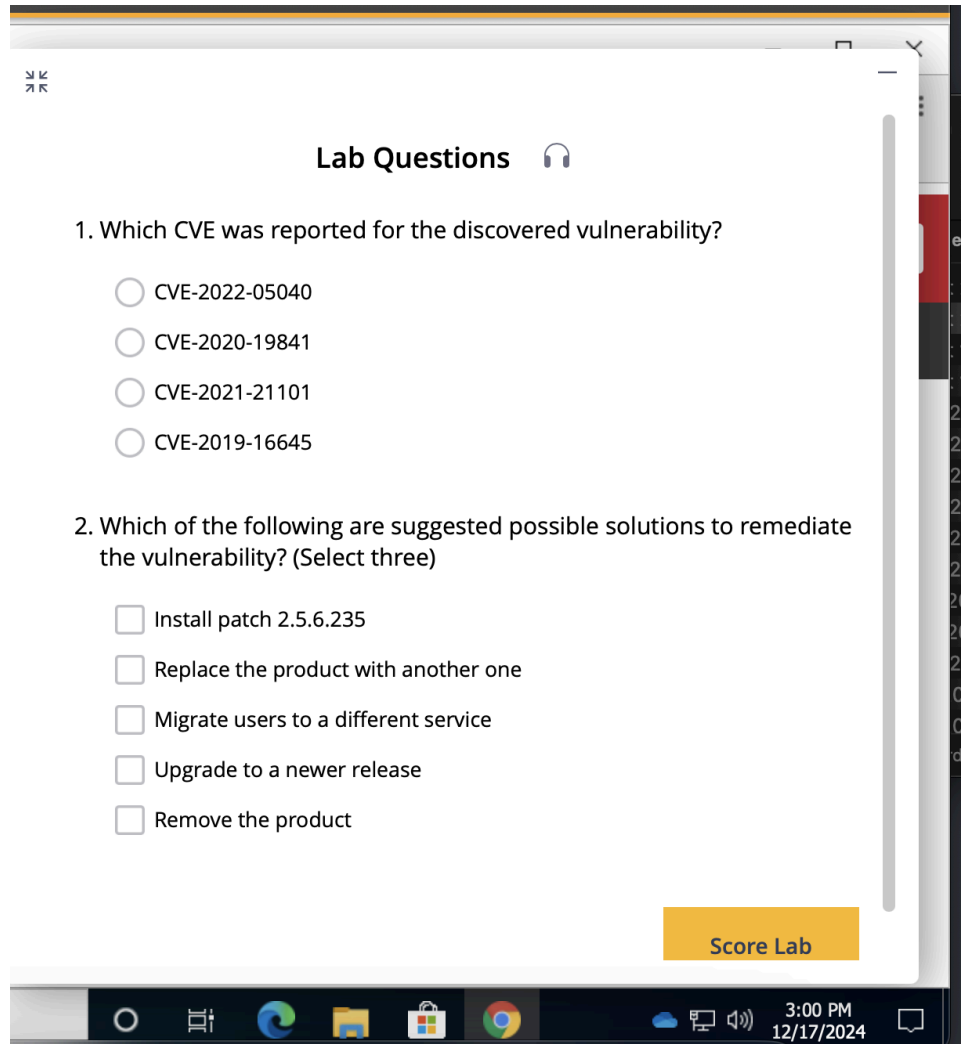




As we can see the scanner found that the credentials being submitted to the webserver are done with cleartext. This is really bad because an attacker that penetrates the network can simply open a Wireshark session and listen in on traffic , sniffing any HTTP packets. Since HTTP is not secure everything is visible in the packet.

A good solution would be for the engineers to configure the server to use HTTPS instead.

Now that I've finished all of the lab's instructions I will go ahead and answer the questions and conclude the lab.



The screenshot shows a web-based interface titled "Lab Questions" with a headphones icon. It contains two questions. Question 1 asks for the CVE reported for a discovered vulnerability, with four radio button options: CVE-2022-05040, CVE-2020-19841, CVE-2021-21101, and CVE-2019-16645. Question 2 asks for suggested possible solutions to remediate the vulnerability, with five checkbox options: Install patch 2.5.6.235, Replace the product with another one, Migrate users to a different service, Upgrade to a newer release, and Remove the product. A yellow "Score Lab" button is located at the bottom right of the question area. The interface is displayed within a browser window, with a Windows taskbar visible at the bottom showing the time as 3:00 PM on 12/17/2024.

**Lab Questions** 🎧

1. Which CVE was reported for the discovered vulnerability?

- ☐ CVE-2022-05040
- ☐ CVE-2020-19841
- ☐ CVE-2021-21101
- ☐ CVE-2019-16645

2. Which of the following are suggested possible solutions to remediate the vulnerability? (Select three)

- ☐ Install patch 2.5.6.235
- ☐ Replace the product with another one
- ☐ Migrate users to a different service
- ☐ Upgrade to a newer release
- ☐ Remove the product

**Score Lab**

The CVE reported by the lab is:

**CVE-2019-16645**

**Summary:**

An issue was discovered in Embedthis GoAhead 2.5.0. Certain pages (such as goform/login and config/log\_off\_page.htm) create links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker. This could potentially be used in a phishing attack.

**Links:**

<https://nvd.nist.gov/vuln/detail/CVE-2019-16645>

Since this CVE is version specific we can simply patch the GoAhead version to a newer one to solve the issue.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sat December 14th 2024

The screenshot shows a web browser window with the TestOut Learning Platform interface. A 'Lab Report' modal is open, displaying the following information:

- Lab Report**
- Time Spent: 14:11
- Score: 3/3 (100%)
- TASK SUMMARY
- Required Actions & Questions
- ✓ Scan the host at IP address 192.168.0.45.
- ✓ Q1: Which CVE was reported for the discovered vulnerability?  
Your answer: CVE-2019-16645  
Correct answer: CVE-2019-16645
- ✓ Q2: Which of the following are possible solutions to remediate the vulnerability?

The background interface includes a 'Scenario' section with instructions, a 'References' section, and a 'Score Lab' button. The browser address bar shows the URL: [labsimapp.testout.com/v6\\_0\\_655/simwindow.html?c2ltRGVmVXJl](http://labsimapp.testout.com/v6_0_655/simwindow.html?c2ltRGVmVXJl).