Module 3 Lab: Vulnerability Scanning Worksheet

## Student Feedback 1

* Under the Hosts tab what ports are reported as open on the target? (3pts)
  + none
* Under the Vulnerabilities tab how many vulnerabilities are listed? (3pts)
  + 2
* What are the severity (Sev) levels of the vulnerabilities? (3pts)
  + info

## Student Feedback 2

* How many vulnerabilities are discovered? (3pts)
  + 32
* What is the vulnerability with the highest CVSS score and what is the score? (3pts)
  + 6.1 jQUERY 1.2 < 3.5.0 MUTIPLE XSS
* Select the title of the highest CVSS score vulnerability, what is the solution to this vulnerability? (3pts)
  + 1 jQUERY 1.2 < 3.5.0 MUTIPLE XSS

Solution is to upgrade JQuery version 3.5.0 or later.

* Click the Hosts Tab on your report and provide a screenshot of your complete browser window. (2pts) A screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generated

A screenshot of a computer

Description automatically generated

## Student Feedback 3

* What is the STIG Severity of the JQuery 1.2 < 3.5.0 Multiple XSS vulnerability? (4pts)
  + ll
* What is the complete CVSS v3.0 Base Score? (4pts)
  + 6.1
  + A screenshot of a computer

    Description automatically generated

## Student Feedback 4

* Compare the results of the credentialed and uncredentialed scan. How did the number of vulnerabilities change (less/more/about the same)? How did the number of severity classes change (less/more/about the same)? What was the reason for this change? (6pts, 2 each answer)
* **Credentialed Scan**:
  + Critical: 10
  + High: 51
  + Medium: 33
  + Low: 4
  + Info: 69
* **Uncredentialed Scan**:
  + Critical: 0
  + High: 0
  + Medium: 7
  + Low: 1
  + Info: 36

**Change**:

* There were **significantly more vulnerabilities** detected in the credentialed scan compared to the uncredentialed scan. The credentialed scan identified **10 critical and 51 high** vulnerabilities, which were completely missing in the uncredentialed scan. Additionally, the number of medium, low, and informational vulnerabilities was higher in the credentialed scan.

**Comparison of the Number of Severity Classes:**

* **Credentialed Scan**:
  + Detected vulnerabilities across **all five severity classes**: Critical, High, Medium, Low, and Info.
* **Uncredentialed Scan**:
  + Detected vulnerabilities in **only three severity classes**: Medium, Low, and Info.

**Change**:

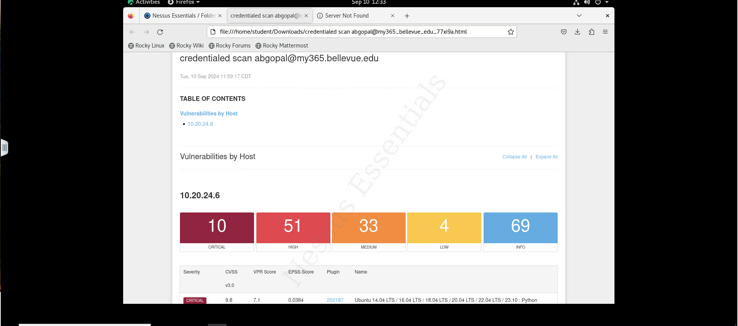
* The **number of severity classes increased** in the credentialed scan. Critical and High vulnerabilities, which were absent in the uncredentialed scan, were detected only in the credentialed scan, resulting in broader vulnerability coverage.

### **Reason for the Change**:

The **key reason for the difference** is the **access level**.

* In the **credentialed scan**, the scanner had access to privileged information such as system configuration files, detailed software versions, internal services, and other sensitive system-level data. This allowed it to identify deeper vulnerabilities, particularly those that would affect internal operations (Critical and High severities).
* The **uncredentialed scan**, on the other hand, had limited access, relying mostly on publicly exposed services and resources. This type of scan is more effective for surface-level vulnerabilities but misses deeper security issues that require administrative or privileged access.
* In the report:
  + How many critical vulnerabilities are there? (4pts)
    - 10
  + How many vulnerabilities have a CVSS v3.0 score of 8.6? (4pts)
    - three
* According to Plugin ID 182769 (check the plugin column on the report), what is the CVSS number attached Vim vulnerability (4pts)
  + 9.8 vim vulnerabilities (USN-6420-1)
* Click the Hosts Tab on your report and provide a screenshot of your complete browser window. (4pts)

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated