SECURITY ASSESSMENT

Vulnerability Assessment Report

Submitted to: Development Team
Security Analyst: Shrividya Ranjani Kaliyur NarayanaPrasad

Date of Testing: 2/21/2021
Date of Report Delivery: 2/22/2021

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

The engagement was requested by the Development team. The goal of this engagement is to understand what security risks the web-application is posing to the organization and what security measures can be taken to increase the security posture and reduce the risk to the organization.
The engagement is to be completed by the Security Analyst of the organization.
This engagement needs to be repeated on a regular basis, more so whenever a new functionality is developed and released to the web application.

Scope

The scope of this engagement is to conduct a vulnerability assessment on the web application. Vulnerability assessment is one way of securing the organization's assets. Being aware of the vulnerabilities through regular vulnerability assessments, helps mitigate them.

Executive Risk Analysis

After the vulnerability/risk analysis is completed, the overall severity level of all the risks together is found to be Medium-High. Most of the vulnerabilities found on the website are of medium severity level. But XSS was one vulnerability that was found to be of high severity. Since most of the attackers use attacks such as XSS, CSRF, SQL and Command injection commonly to exploit web applications, it is one of the most important issue that is to be resolved. Together, the severity level can be considered as Medium-High.

The vulnerabilities found during the assessment are: Cross site scripting and Untrusted SSL certificate.

Cross site scripting is a vulnerability that allows the attacker to gain access to the application and full control over the functionality and data of the application. The attacker can make the user do things according to his wishes.

Untrusted SSL certificate can lead to Man-in-the-Middle attacks. The attacker can impersonate the website and defraud the users and collect all the data. This also leads to confidential data leaks and damage to the organization's name.

Executive Recommendation

The main and most important vulnerability that must be remediated first is the Cross-Site scripting vulnerability, which has the severity level - high. An attacker can use this vulnerability to hack the website, steal data such as session tokens or control user's computers. This vulnerability must be fixed immediately and once it is fixed; another vulnerability scan must be conducted to make sure that the risk has been eliminated.

Significant Vulnerability Summary

High Risk Vulnerabilities

- Cross Site Vulnerability (XSS)

Medium Risk Vulnerabilities

- SSL Certificate cannot be trusted.
- SMB Signing not required.

Low Risk Vulnerabilities

- None

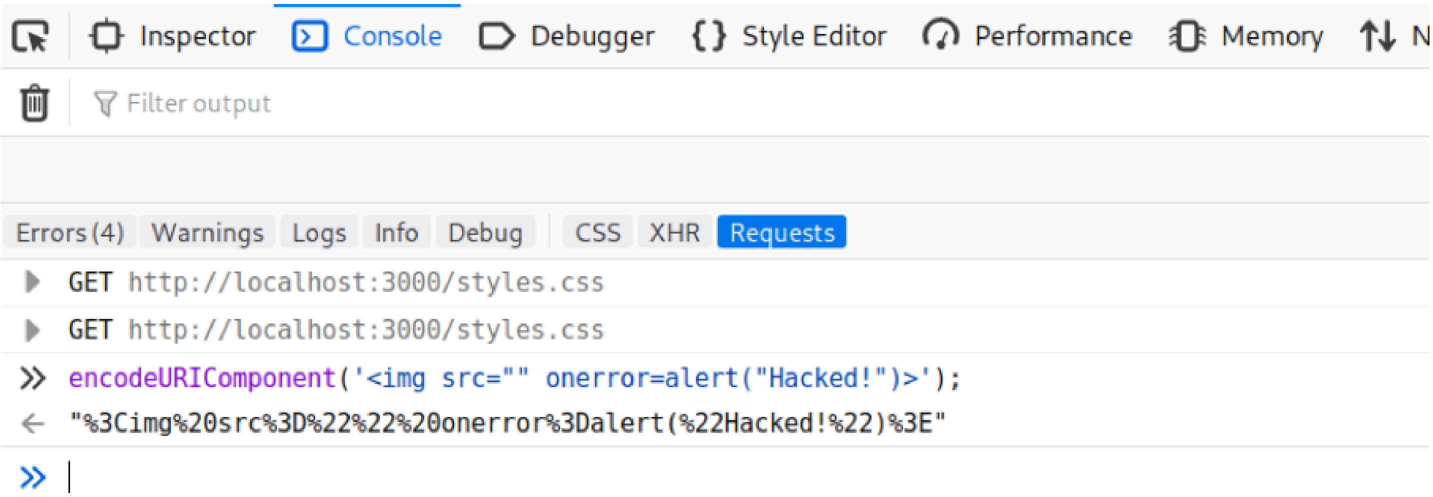
Significant Vulnerability Detail

Cross-Site Scripting

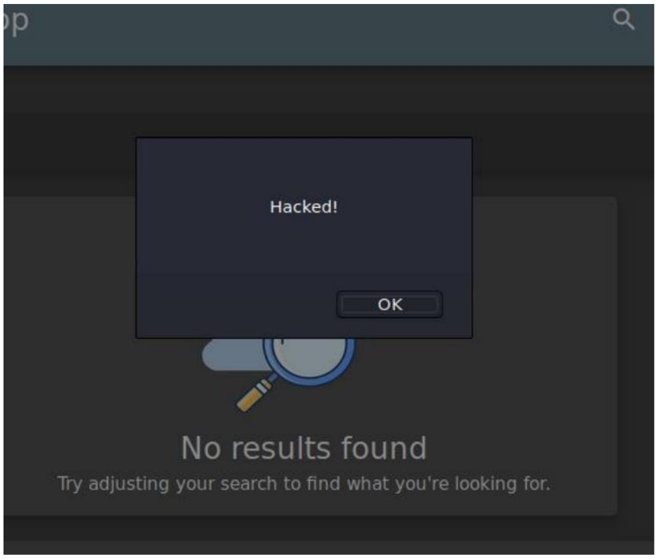
This is a web security vulnerability that allows an attacker to gain access to all the interactions that users have with a vulnerable application. An attack can masquerade a victim to carry out any actions that the user can perform and access all the user data. If the user has privileged access to the application, the attacker may gain full control over all the application's functionality and data.

RISK LEVEL HIGH

- Cross-Site Scripting has a severity level High.
- A sample XSS attack was performed on the URL which would give display a pop-up alert stating "Hacked! ". When the attack was conducted, the result was that the vulnerability was exploited. A customized arbitrary command was created which would then be added to the URL. When the URL is executed, as a result an alert with the message "Hacked!" would be displayed.



```
GET http://localhost:3000/styles.css
GET http://localhost:3000/styles.css
>> encodeURIComponent('<img src="" onerror=alert("Hacked!")>');
← "%3Cimg%20src%3D%22%22%20onerror%3Dalert(%22Hacked!%22)%3E"
>>
```



- The probability of an XSS attack is very high, as many of the attackers use attacks like XSS, CSRF and SQL injection to exploit the web applications.
- XSS has a huge impact on all the people involved with the web-application. This includes all the users, departments, and the business itself. XSS can lead to leak of sensitive data, stolen credentials, hijacking, access to client computers, access to a staff members' computers etc. If one of the insiders is compromised all the confidential data is compromised and the cost of resolving everything is very high.

- The remediation steps are - never trust user input, have proper sanitization and validation of user input on both client side and server side, remove or encode all the special HTML characters, use appropriate response headers, have Content Security Policy ready to reduce the severity of an XSS vulnerability.

Untrusted SSL Certificate

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

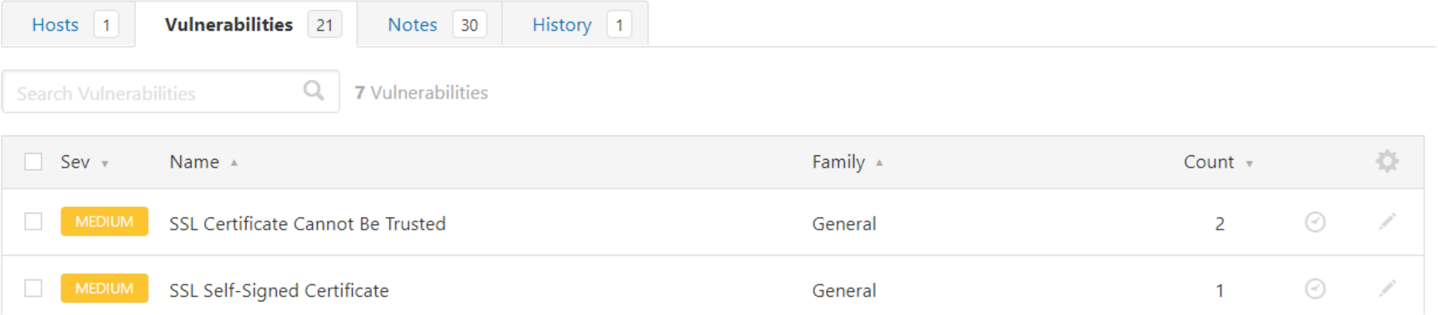
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either did not match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

MEDIUM

- The risk level of this vulnerability is Medium.
- The vulnerability was identified and verified using the Nessus Vulnerability scanner.



7 Vulnerabilities

□	Sev	Name	Family	Count
□	MEDIUM	SSL Certificate Cannot Be Trusted	General	2
□	MEDIUM	SSL Self-Signed Certificate	General	1

- The probability of this vulnerability being exploited is medium.
- Since the certificate cannot be trusted, the browsers will show the website as “Not Secure” which will lead to losses. This in turn will cause damage to the organization. An attacker can impersonate the website and collect all the data or cheat the users and at the end the company is held responsible.
- A possible remediation of this issue is to purchase or generate a proper SSL certificate for this service.

Methodology

The main goal of this assessment is to find the vulnerabilities of the Web-Application. To conduct a vulnerability assessment, we need a set of tools. A tool to scan for vulnerabilities and a tool to validate the vulnerabilities.

The tools used to conduct this assessment are:

1. Nessus Vulnerability Scanner

2. Kali Linux Virtual Machine

Nessus Vulnerability Scanner was used to scan for vulnerabilities, Kali Linux virtual machine was used to conduct exploits and validate the vulnerabilities.

After a complete scan of the web-application the following vulnerabilities were found on the web-application. The vulnerabilities are:

1. Cross-Site Scripting

2. Untrusted SSL certificate

3. SMB signing not required.

Steps to validate that the web-application is vulnerable to Cross-site scripting:

1. Creating a sample arbitrary command that can be added to the URL.

2. When the URL is executed the website will display an alert saying “Hacked!” if it is vulnerable to the exploit and nothing will happen if there is no alert displayed. But it does not mean that the website is not vulnerable to the exploit. Further exploitation techniques must be conducted to confirm whether the website is vulnerable or not.

After the exploit was conducted the result confirms that the website is vulnerable to cross-site scripting.

Validating Untrusted SSL Certificate:

1. A vulnerability scan was conducted, and the output was that the web-application is vulnerable to untrusted SSL certificate.

2. Using the browser to find out if the website is insecure and untrusted SSL certificate is being used.

The output confirmed that the website is vulnerable to untrusted SSL certificate.

Validating SMB signing is not required:

1. A scan was conducted on the website and the output confirmed that the website is vulnerable to this vulnerability.

Assessment Toolset Selection

The tools used for the vulnerability assessment and validation are:

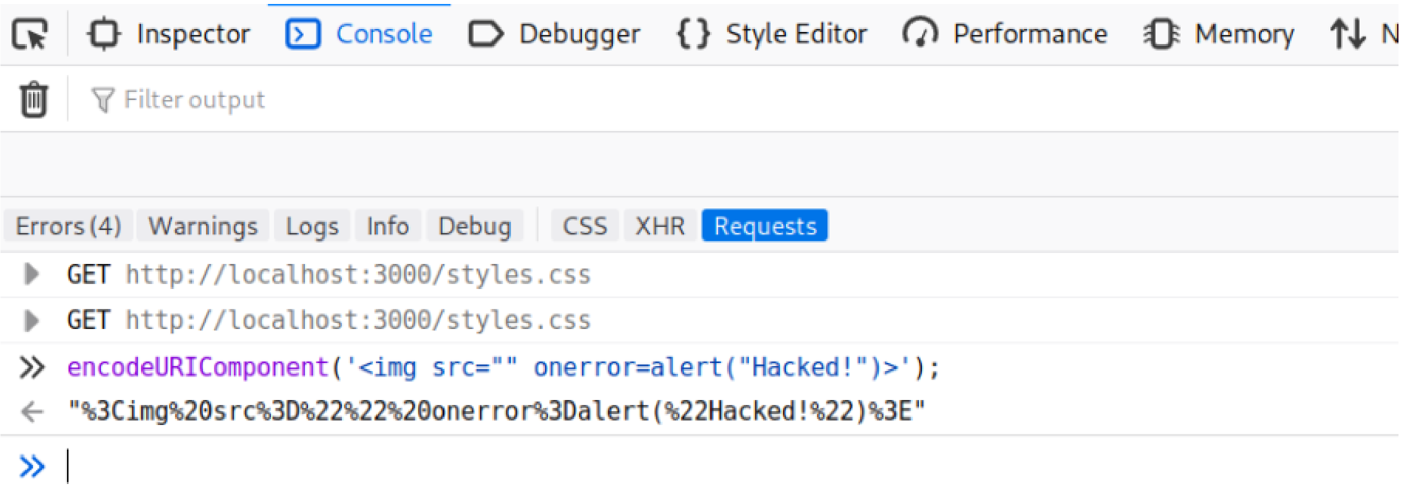
1. Nessus Vulnerability Scanner

2. Kali Linux Virtual Machine

Assessment Methodology Detail

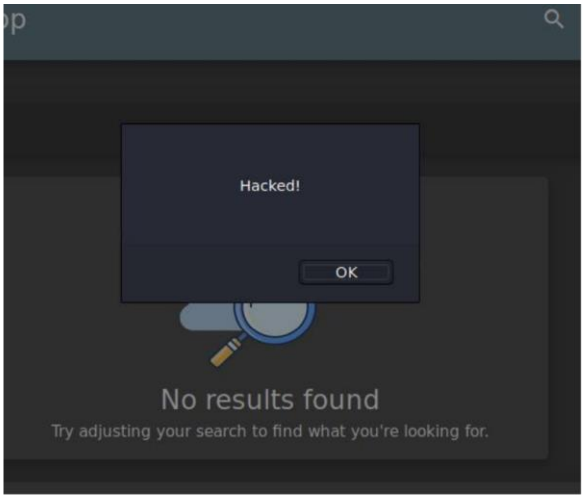
1. Cross-Site Scripting:

Creation and execution of an arbitrary command to validate that the website is vulnerable to the vulnerability.



```
GET http://localhost:3000/styles.css
GET http://localhost:3000/styles.css
>> encodeURIComponent('<img src="" onerror=alert("Hacked!")>');
<- "%3Cimg%20src%3D%22%22%20onerror%3Dalert(%22Hacked!%22)%3E"
>>
```

Output:

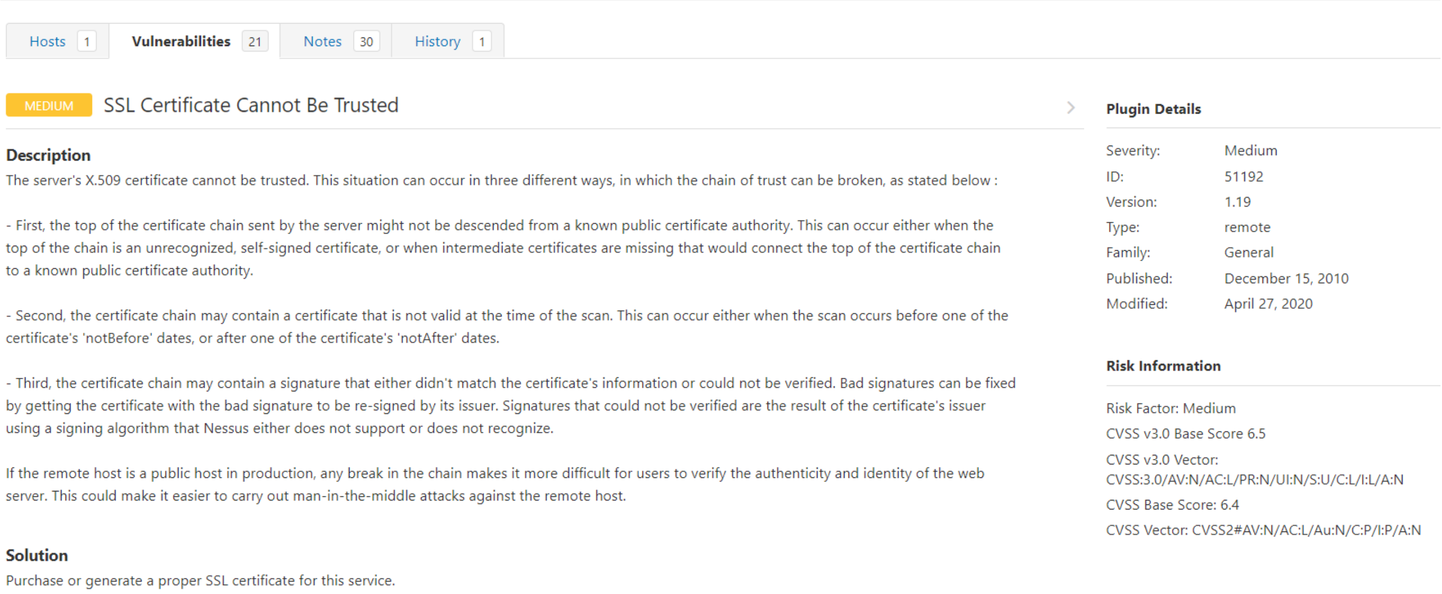


No results found

Try adjusting your search to find what you're looking for.

2. Untrusted SSL certificate:

The vulnerability scanning report and the validation of the vulnerability:



MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

Plugin Details

Severity:	Medium
ID:	51192
Version:	1.19
Type:	remote
Family:	General
Published:	December 15, 2010
Modified:	April 27, 2020

Risk Information

Risk Factor: Medium

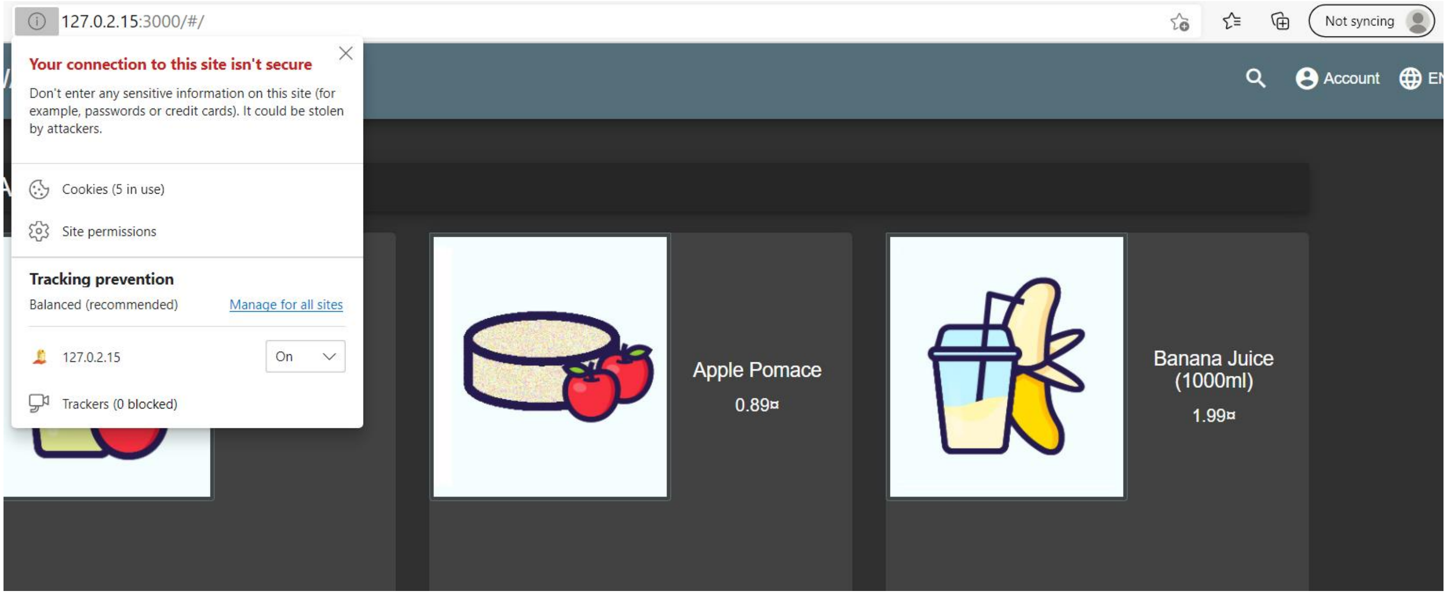
CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Output:



Your connection to this site isn't secure

Don't enter any sensitive information on this site (for example, passwords or credit cards). It could be stolen by attackers.

Cookies (5 in use)

Site permissions

Tracking prevention

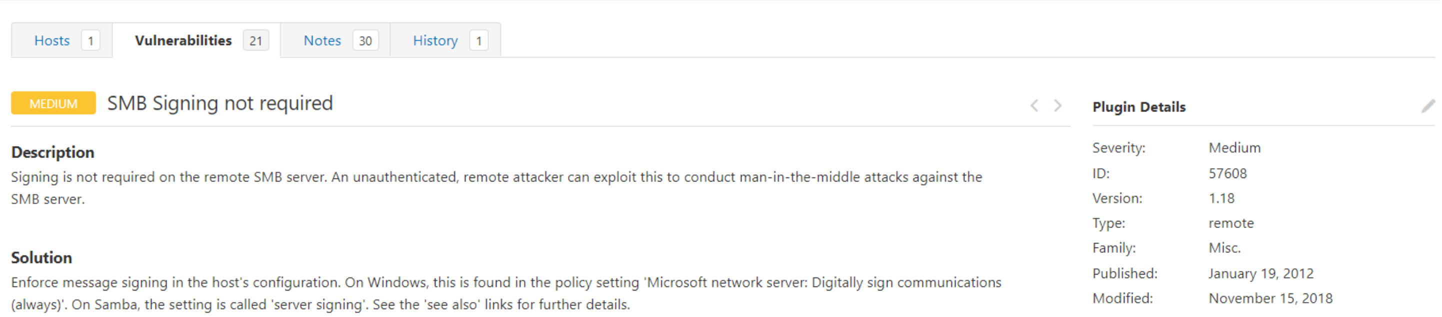
Balanced (recommended) Manage for all sites

127.0.2.15 On

Trackers (0 blocked)

3. Signed SMB is not required:

The scan report confirms that the web-application is vulnerable to the vulnerability.



MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.18
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	November 15, 2018

This concluded the vulnerability assessment methodology portion of this report.