Threat Modeling Report

Created on 2/28/2022 1:09:21 PM

Threat Model Name: Login Authorization - from a web application using an external authorization provider

Owner: Noel Varghese

Reviewer: -

Contributors: -

Description: Several vulnerabilities exist in this architecture model - such as Cross Site Scripting , Cross Protocol vulnerability and attacks like Denial of Service, though the connection is secured (using HTTPS) Significant steps to identify and justify the vulnerabilities have been applied.

Assumptions:

External Dependencies: None

Threat Model Summary:

Not Started	0
Not Applicable	1
Needs Investigation	3
Mitigation Implemented	0
Total	4
Total Migrated	0

Diagram: Diagram 1

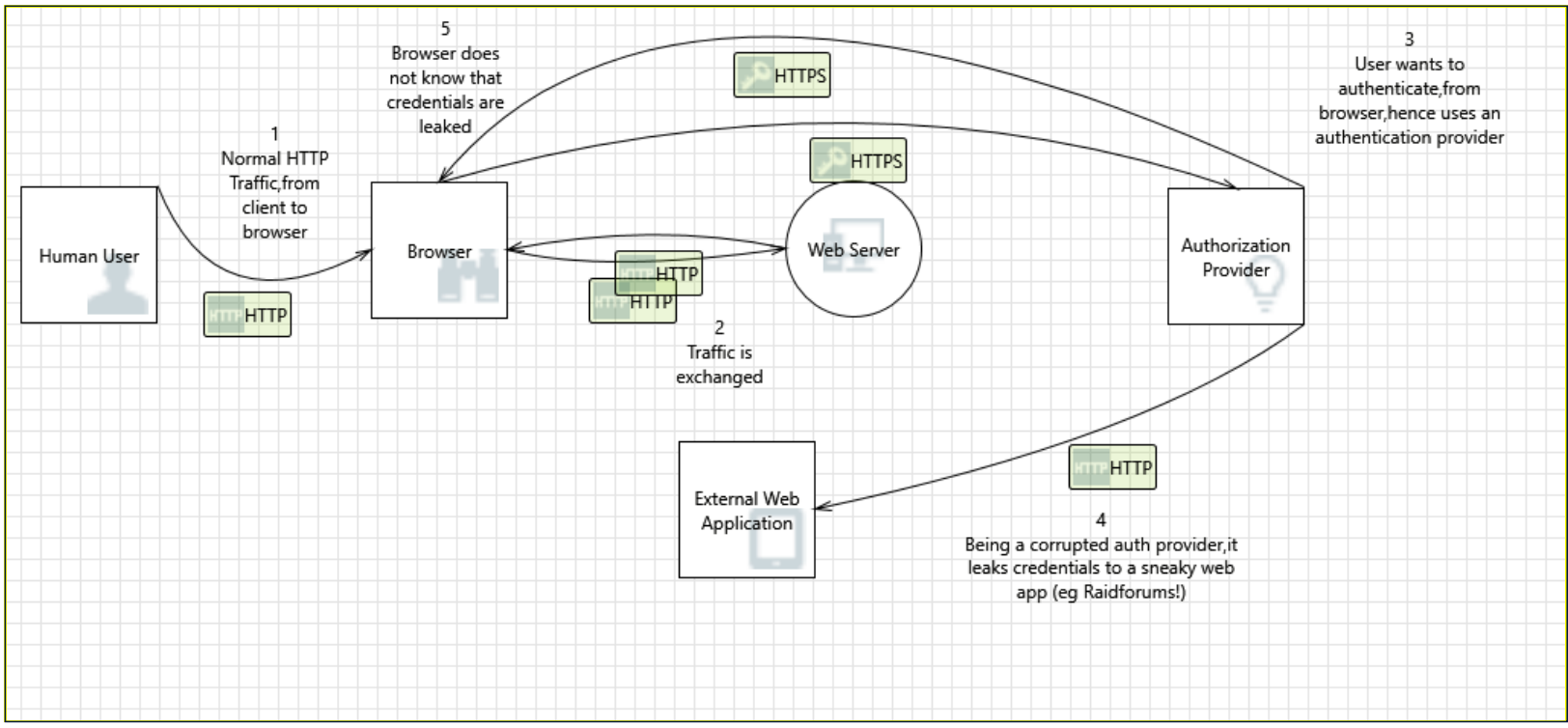
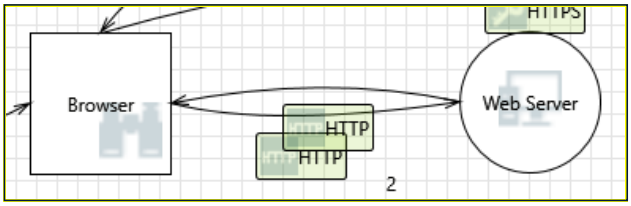


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	1
Needs Investigation	3

Mitigation Implemented	0
Total	4
Total Migrated	0

Interaction: HTTP



1. Cross Site Scripting [State: Needs Investigation] [Priority: High]

Category: Information Disclosure
Description: The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: XSS attack is a possibility,if browser does'nt sanitize the input properly

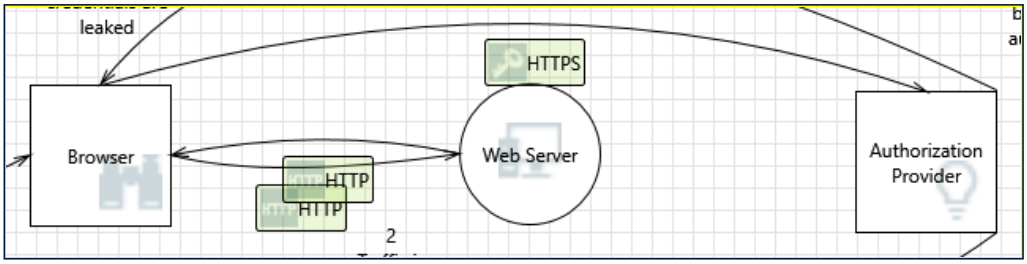
2. Spoofing the Browser External Entity [State: Needs Investigation] [Priority: High]

Category: Spoofing
Description: Browser may be spoofed by an attacker and this may lead to unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the external entity.
Justification: Spoofing of browser requests

3. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Information Disclosure
Description: Web Server may be able to impersonate the context of Browser in order to gain additional privilege.
Justification: A user would not want to attack his own web server that is hosted on his VM

Interaction: HTTPS



4. Weakness in SSO Authorization [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.
Justification: Weak SSO solutions are not acceptable in today's tech advancement,as identity of users are made vulnerable to the CIA triad