Password Transmitted over HTTP in webappsecurity.com

Disclosed : 18 August 2021

Reported to : internshipstudio.com

Reported at : 18 August 2021

Asset : zero.webappsecurity.com

URL : http://zero.webappsecurity.com/login.html

Weakness : Password Transmitted over HTTP

Severity : Critical

Participants : PRATHMESH BHARTI

Summary:

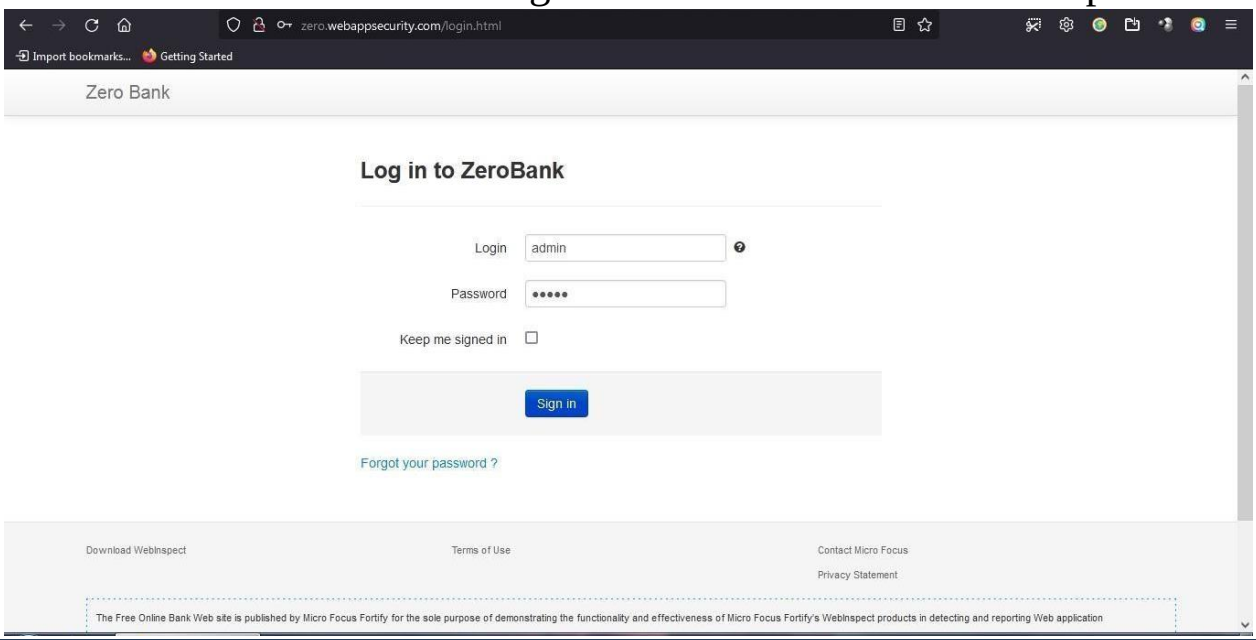
The URL http://zero.webappsecurity.com/login.html has a critical vulnerability namely Password Transmitted over HTTP in form target 'signin.html'. Due to this, user's passwords are transmitted over HTTP. The transmission protocol used to transfer passwords is not secure.

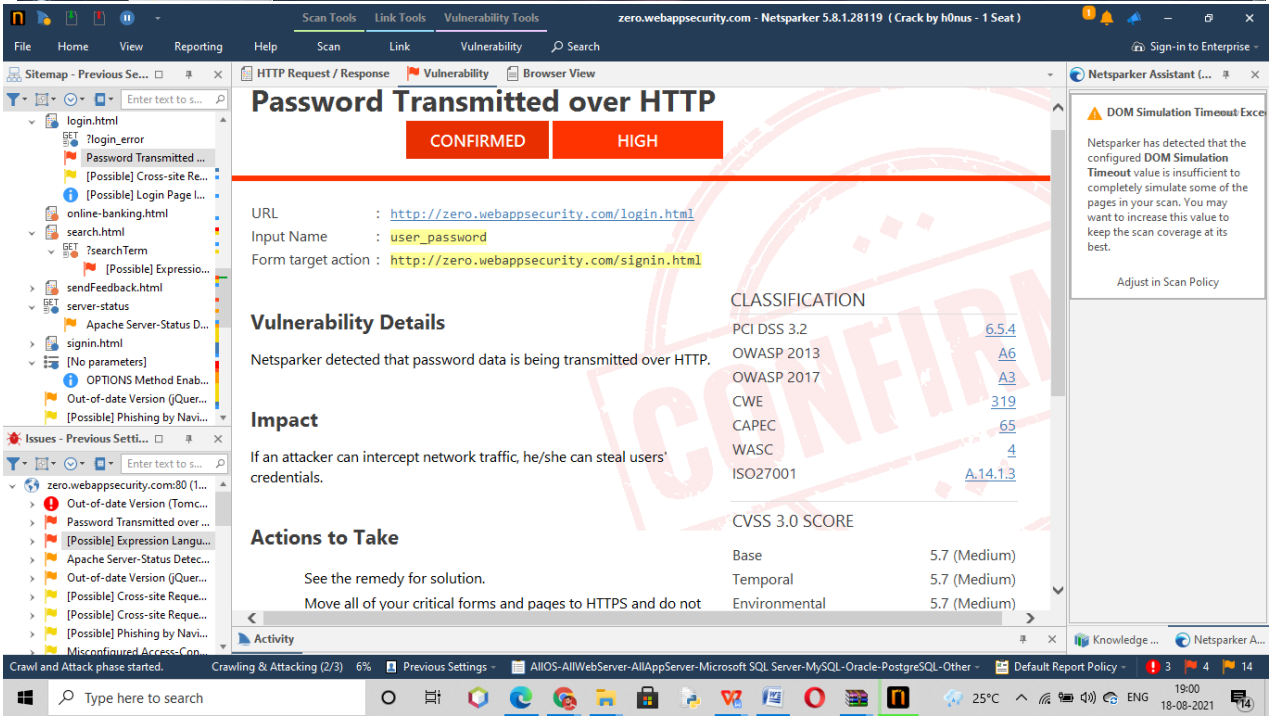
Steps to Reproduce:

- Enter URL http://zero.webappsecurity.com/login.html
- Enter your username and password
- Click 'Sign in'
- After user clicks 'Sign in', attacker can detect password transferred.

Supporting Material/References:

Screenshots and video recording has been submitted with this report.





Impact:

An attacker can use this vulnerability to steal user's username and passwords, and further sensitive information.

If an attacker can intercept network traffic, he/she can steal users' credentials.

Actions suggested to be taken:

- Move all forms and data transferred through HTTPS.
- User's login credentials should be stored using HTTPS.