

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.

The image displays two screenshots related to a security audit of Zero Bank.

The top screenshot shows the Zero Bank login page. The URL is `zero.webappsecurity.com/login.html`. The page has a header "Zero Bank" and a main heading "Log in to ZeroBank". The login form includes fields for "Login" (containing "admin") and "Password" (masked with "*****"). There is a "Keep me signed in" checkbox and a "Sign in" button. A link for "Forgot your password ?" is also present. At the bottom, there are links for "Download WebsInspect", "Terms of Use", "Contact Micro Focus", and "Privacy Statement". A footer note states: "The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of demonstrating the functionality and effectiveness of Micro Focus Fortify's WebsInspect products in detecting and reporting Web application".

The bottom screenshot shows the Netsparker 5.8.1.28119 interface. The main window displays a vulnerability report titled "Password Transmitted over HTTP" with a status of "CONFIRMED" and a severity of "HIGH". The report details the following:

- URL:** `http://zero.webappsecurity.com/login.html`
- Input Name:** `user_password`
- Form target action:** `http://zero.webappsecurity.com/signin.html`

Vulnerability Details: Netsparker detected that password data is being transmitted over HTTP.

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

Actions to Take: See the remedy for solution. Move all of your critical forms and pages to HTTPS and do not

CLASSIFICATION:

Standard	Score
PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	319
CAPEC	65
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE:

Category	Score
Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

The interface also shows a sidebar with a site map, a search bar, and a "Netsparker Assistant" panel on the right with a warning about "DOM Simulation Timeout Exceeded". The bottom status bar indicates "Crawl and Attack phase started" and "Crawling & Attacking (2/3) 6%".

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.