Scan Remediation

Report

Burp Suite Enterprise Edition

Generated by Burp Suite Enterprise Edition | 2022-06-28 4:44 PM

Site name:
secure_home

Status:
Completed

Included URLs:
https://localhost:8081/api/
https://localhost:8081/api/users/login
https://localhost:8081/api/alarmNotifications
https://localhost:8081/api/alarmNotifications/countNotSeend
https://localhost:8081/api/alarmNotifications/notSeen
https://localhost:8081/api/alarmNotifications/setSeen
https://localhost:8081/api/users/deleteUser/9
https://localhost:8081/api/users/getAllUsersButAdmin
https://localhost:8081/api/users/logout
https://localhost:8081/api/users/register
https://localhost:8081/api/users/searchUsers
https://localhost:8081/api/users/unlockUser
https://localhost:8081/api/users/verify-registration/admin
https://localhost:8081/api/devices
https://localhost:8081/api/devices/all
https://localhost:8081/api/devices/createAllReport
https://localhost:8081/api/devices/createReport
https://localhost:8081/api/devices/filterAllMessages
https://localhost:8081/api/devices/filterMessages
https://localhost:8081/api/devices/getAllMessagesFromDevice/Fridge
https://localhost:8081/api/devices/getAllMessagesFromRealEstate/Kuca%201
https://localhost:8081/api/devices/names
https://localhost:8081/api/devices/updateDeviceReadPeriod
https://localhost:8081/api/devices/Fridge
https://localhost:8081/api/logs
https://localhost:8081/api/logs/filterLogs
https://localhost:8081/api/realEstate
https://localhost:8081/api/realEstate/all
https://localhost:8081/api/realEstate/deviceNames/Kuca%201
https://localhost:8081/api/realEstate/findLowestReadPeriod/Kuca%201
https://localhost:8081/api/realEstate/toAssign
https://localhost:8081/api/realEstate/1
https://localhost:8081/api/rules
https://localhost:8081/api/rules/2
https://localhost:8081/api/ownerships
https://localhost:8081/api/ownerships/delete
https://localhost:8081/api/ownerships/fromUser
https://localhost:8081/api/ownerships/Kuca%201

Application logins:
administrator
user

Reference:
#18

Issues by severity

High:	0
Medium:	1
Low:	0
Information:	0
Total issues found:	1

Scan statistics

Total scanned URLs:	38
URLs with errors:	0
Requests made:	6645
Network errors:	0

Issues found on https://localhost:8081

URLs By issue type	Severity	Confidence	More detail
TLS certificate [1]			
/	Medium	Certain	>>

More details for https://localhost:8081

TLS certificate
/

Issue detail:

The following problems were identified with the server's TLS certificate:

- The server's certificate is not valid for the server's hostname.
- The server's certificate is not trusted.

Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

The server presented the following certificate:

Issued to:	SecureHome
Issued by:	UID=2,1.2.840.113549.1.9.1=#161561646d696e5f617366406d61696c64726f702e6363,C=RS,OU=Katedra za informatiku,O=UNS-FTN,CN=Admin
Valid from:	Wed Jun 01 00:00:00 CEST 2022
Valid to:	Thu Jun 01 00:00:00 CEST 2023

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

SSL/TLS Configuration Guide

Vulnerability classifications

CWE-295: Improper Certificate Validation
CWE-326: Inadequate Encryption Strength
CWE-327: Use of a Broken or Risky Cryptographic Algorithm