Scan Remediation

Report

Generated by Burp Suite Enterprise Edition | 2022-06-28 4:43 PM

Site name:
admin_app

Status:
Completed

Included URLs:
https://localhost:8080
https://localhost:8080/api/users/login
https://localhost:8080/api/users/unlockUser
https://localhost:8080/api/certificates/getAliases
https://localhost:8080/api/certificates
https://localhost:8080/api/certificates/getCertificat
e/asdf
https://localhost:8080/api/certificates/revoke
https://localhost:8080/api/certificates/validate
https://localhost:8080/api/csrs
https://localhost:8080/api/csrs/verified
https://localhost:8080/api/csrs/verify-csr
https://localhost:8080/api/csrs/2

Application logins:
administrator

Reference:
#21

Issues by severity

High:	0
Medium:	1
Low:	0
Information:	1
Total issues found:	2

Scan statistics

Total scanned URLs:	13
URLs with errors:	0
Requests made:	3728
Network errors:	0

Issues found on https://localhost:8080

URLs By issue type	Severity	Confidence	More detail
TLS certificate [1] /	Medium	Certain	>>
Email addresses disclosed [1] /api/csrs	Info	Certain	>>

More details for https://localhost:8080

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:	AdminApp
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 15 00:00:00 CEST 2022
Valid to:	Thu Jun 15 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

Email addresses disclosed
/api/csrs

Issue detail:

The following email addresses were disclosed in the response:

- csr1@maildrop.cc
- csr2@maildrop.cc
- csr3@maildrop.cc
- csr4@maildrop.cc
- csr5@maildrop.cc
- csr6@maildrop.cc

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

Web Security Academy: Information disclosure

Vulnerability classifications

CWE-200: Information Exposure
CAPEC-37: Retrieve Embedded Sensitive Data

Request:

```
GET /api/csrs HTTP/1.1
Host: localhost:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
ike Gecko) Chrome/103.0.5060.53 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response:

```
HTTP/1.1 200
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cache-control: no-store
Pragma: no-cache
X-Frame-Options: DENY
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Type: application/json
Date: Tue, 28 Jun 2022 14:38:31 GMT
Connection: close
Content-Length: 1432
```


```
[{"id":1,"email":"csr1@maildrop.cc","commonName":"csr1name","organizationUnit":"cs
r1organizationunit","organization":"csr1organization","city":"csr1city","state":"c
sr1state","country":"c1","securityCode":"23i5yg23b5i23vA","verified":true},{"id":
2,"email":"csr2@maildrop.cc","commonName":"csr2name","organizationUnit":"csr2organ
izationunit","organization":"csr2organization","city":"csr2city","state":"csr2stat
e","country":"c2","securityCode":"Aii5yg24b5i23yf","verified":true},{"id":3,"emai
l":"csr3@maildrop.cc","commonName":"csr3name","organizationUnit":"csr3organization
unit","organization":"csr3organization","city":"csr3city","state":"csr3state","cou
ntry":"c3","securityCode":"4uo5yg23b5i23vC","verified":true},{"id":4,"email":"csr4
@maildrop.cc","commonName":"csr4name","organizationUnit":"csr4organizationunit","o
rganization":"csr4organization","city":"csr4city","state":"csr4state","country":"c
4","securityCode":"13i5yg23b5i73vA","verified":false},{"id":5,"email":"csr5@maildr
op.cc","commonName":"csr5name","organizationUnit":"csr5organizationunit","organiza
tion":"csr5organization","city":"csr5city","state":"csr5state","country":"c5","sec
urityCode":"BBi5yg23b5i28vA","verified":false},{"id":6,"email":"csr6@maildrop.cc
","commonName":"csr6name","organizationUnit":"csr6organizationunit","organizatio
n":"csr6organization","city":"csr6city","state":"csr6state","country":"c6","securi
tyCode":"hri5yu27b8928vy","verified":fa
```


Snip