parallel
oracle expert team

SQL Injection: Napadi i odbrane

Autori:
Zoran Pavlović, Security Manager
Maja Veselica, Security Consultant

ORACLE Certified Expert

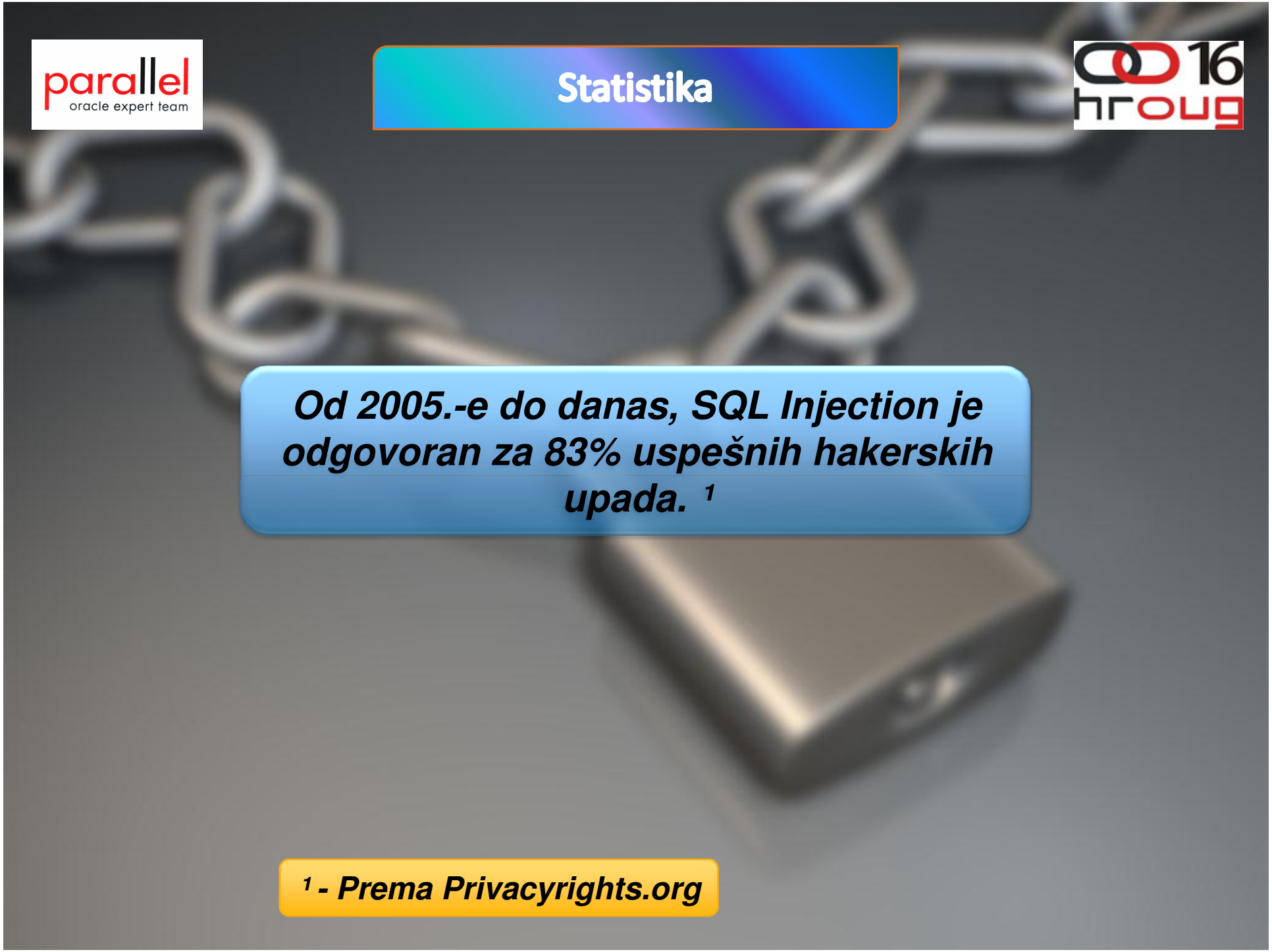
ORACLE Certified Specialist

parallel
oracle expert team

Agenda

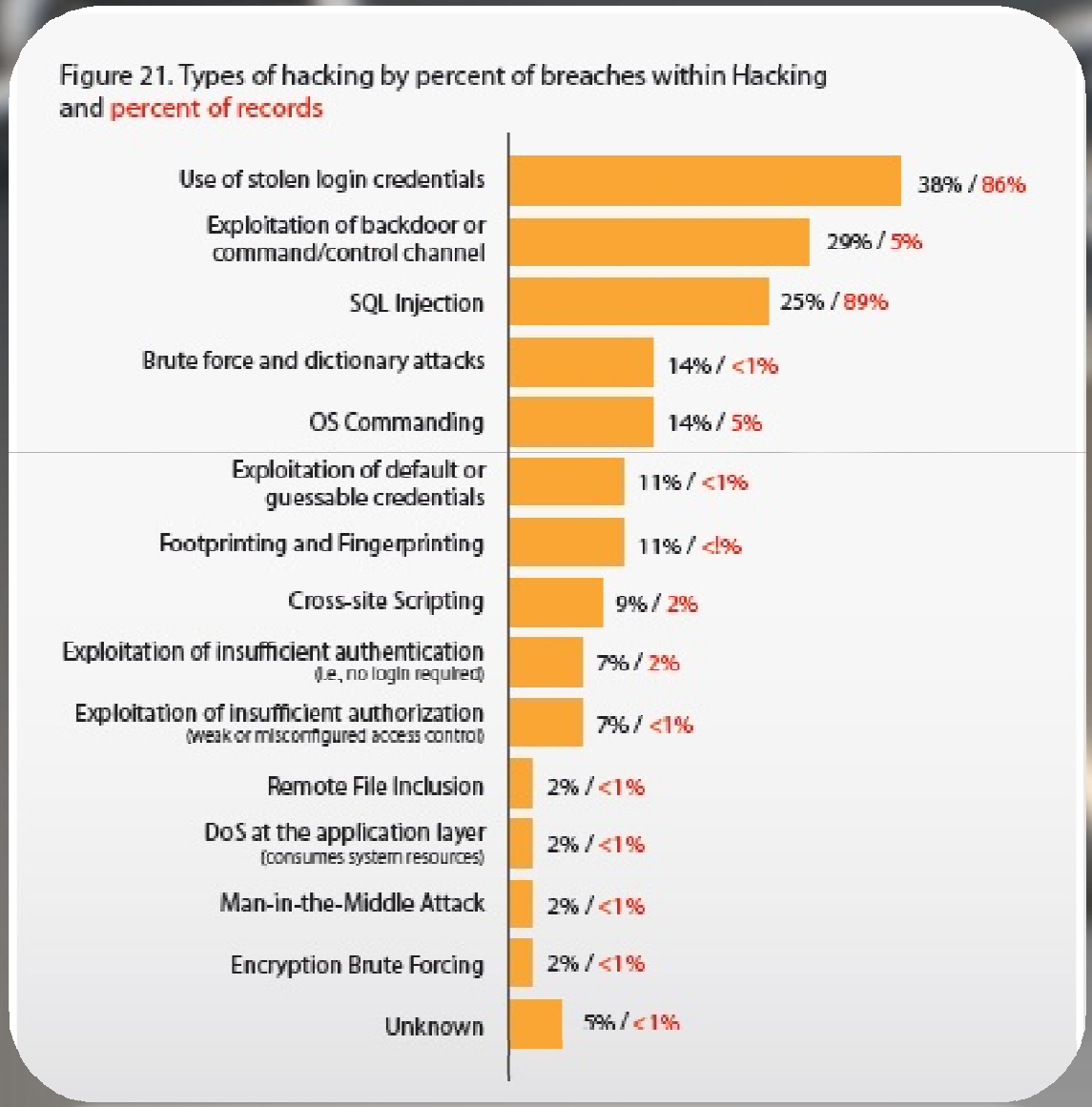
16 hroug

1. Statistika
2. Šta je SQL Injection?
3. Opasnosti
4. Normalno korišćenje
5. Neovlašćen pristup
6. Krađa podataka
7. Neovlašćena izmena podataka
8. Blind SQL Injection
9. Ranjivosti
10. Odbrane
11. Database firewall
12. Database firewall - Karakteristike
13. Parsiranje unosa


parallel
oracle expert team
Statistika
16
hroug
Od 2005.-e do danas, SQL Injection je odgovoran za 83% uspešnih hakerskih upada. [1]
[1] - Prema Privacyrights.org

parallel
oracle expert team

Statistika



Verizon-ova statistika za 2010-u godinu

parallel
oracle expert team

Šta je SQL Injection?

16 hroug

SQL Injection je tehnika kojom se zloupotrebljava neparsirani unos podataka kako bi se kroz web aplikaciju prosledile SQL komande bazi na izvršenje.

parallel
oracle expert team

Opasnosti

16 hroug

- Neovlašćen pristup
- Izmena podataka
- Krađa podataka
- Brisanje podataka
- Zadavanje komandi operativnom sistemu
- Instalacija malicioznih softvera na mrežu

parallel
oracle expert team

Normalno korišćenje

Username

admin

Password

Login

select * from users where
username = ‘&username’
and password = ‘&password’

select * from users where
username = ‘admin’
and password=‘adminisst12’

parallel
oracle expert team

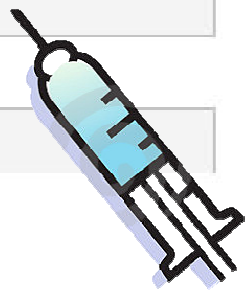
Neovlašćen pristup

Username

admin' or 1=1 --

Password

Login



select * from users where
username = ‘&username’
and password = ‘&password’

select * from users where
username=‘admin’ or 1=1 --
and password=‘fhsdjfsdfjd’

parallel
oracle expert team

Krađa podataka

Username

admin' union select * from credit_cards--

Password

Login

select * from users where
username = ‘&username’
and password = ‘&password’

select * from users where
username=‘admin’ union
select * from credit_cards --
and password=‘fhsdjfsdfjd’

parallel
oracle expert team

Neovlašćena izmena podataka

Username

admin' update users set mail='pr@st.co' where id=1 --

Password

••••••••••••••

Login

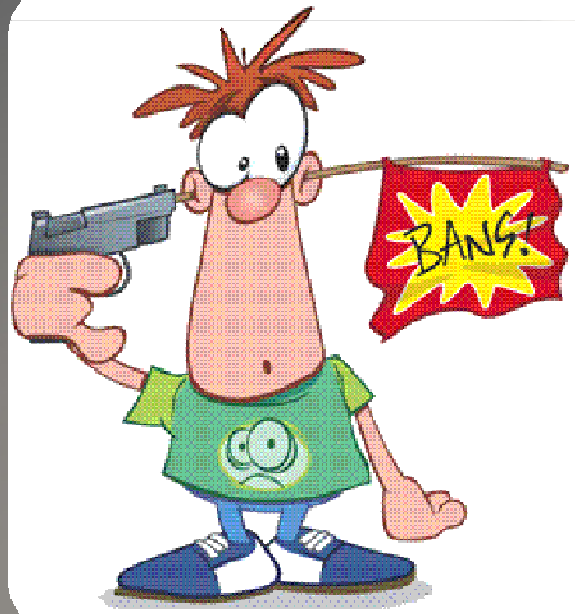
select * from users where
username = '&username'
and password = '&password'

select * from users where
username='admin'; update
users set mail='pr@st.co'
where id=1 --
and password='fhsdjfsdfjd'

parallel
oracle expert team

Blind SQL Injection

Napad u kojem je web aplikacija ranjiva na SQL Injection, ali umesto korisnih poruka o grešci, napadač dobija generičku stranu



Page not Found

Sorry but the page you are looking for cannot be found.

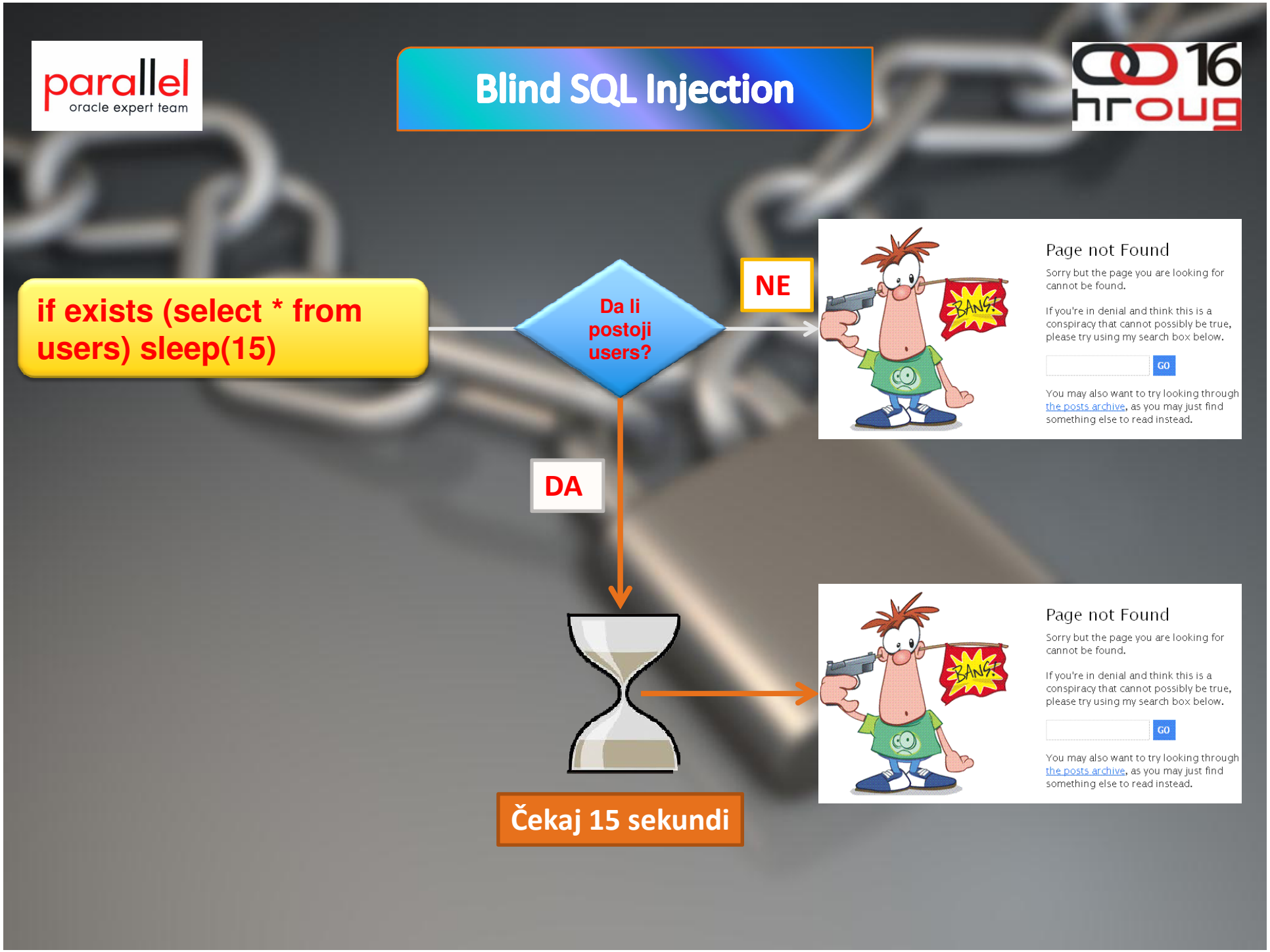
If you're in denial and think this is a conspiracy that cannot possibly be true, please try using my search box below.

GO

You may also want to try looking through the posts archive, as you may just find something else to read instead.

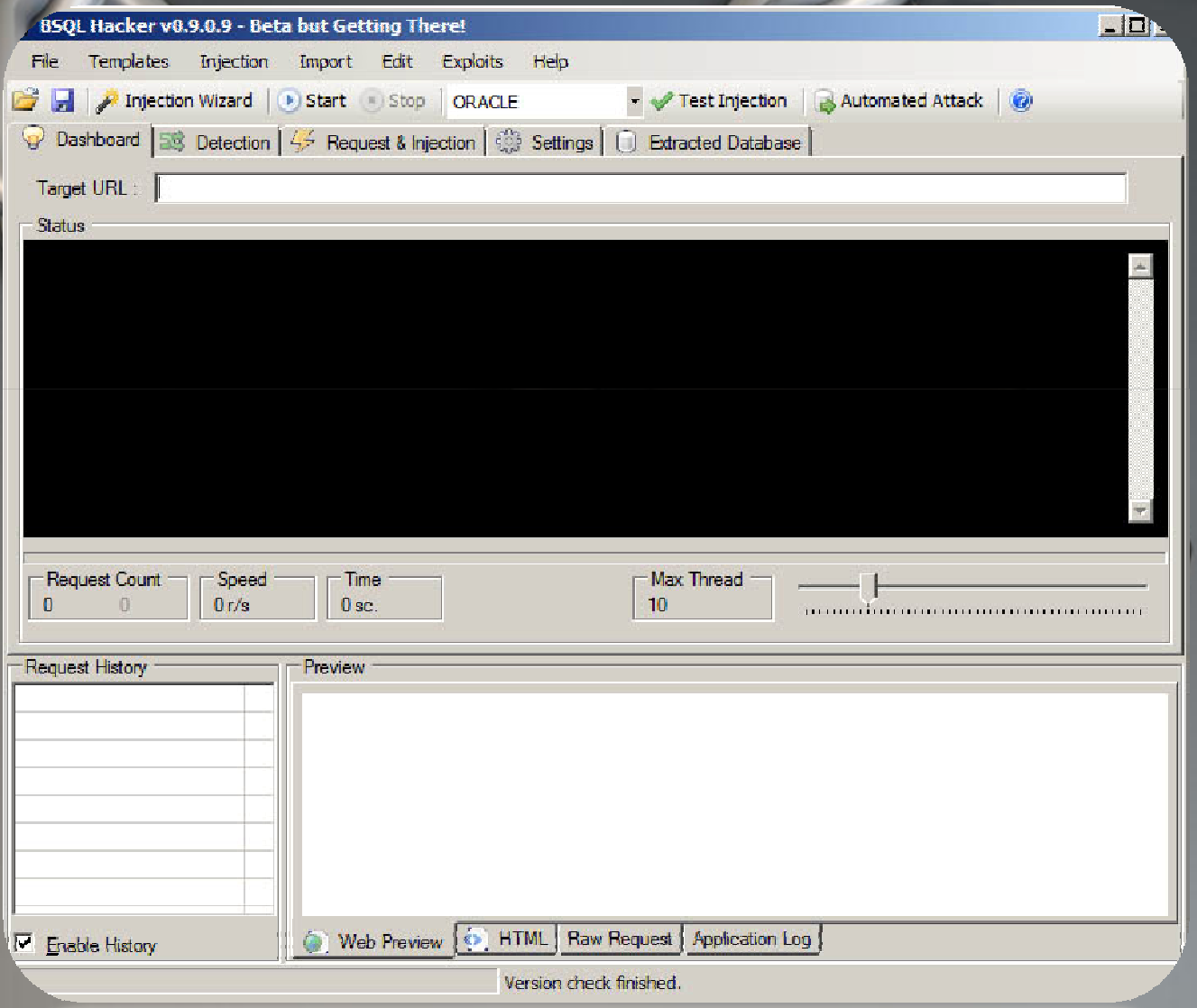
parallel
oracle expert team

Blind SQL Injection



parallel
oracle expert team

BSQL Hacker



parallel
oracle expert team

Ranjivosti

16 hroug

- Neparsiran unos podataka
- Aplikativnom user-u su date prevelike privilegije u bazi
- Poruke o greškama odaju previše podataka
- Baza potpuno veruje aplikaciji

parallel
oracle expert team

Odbrane - Smernice

Obavezno parsirati i prečistiti unos od strane korisnika

Kreirati generičku stranu za greške u aplikaciji

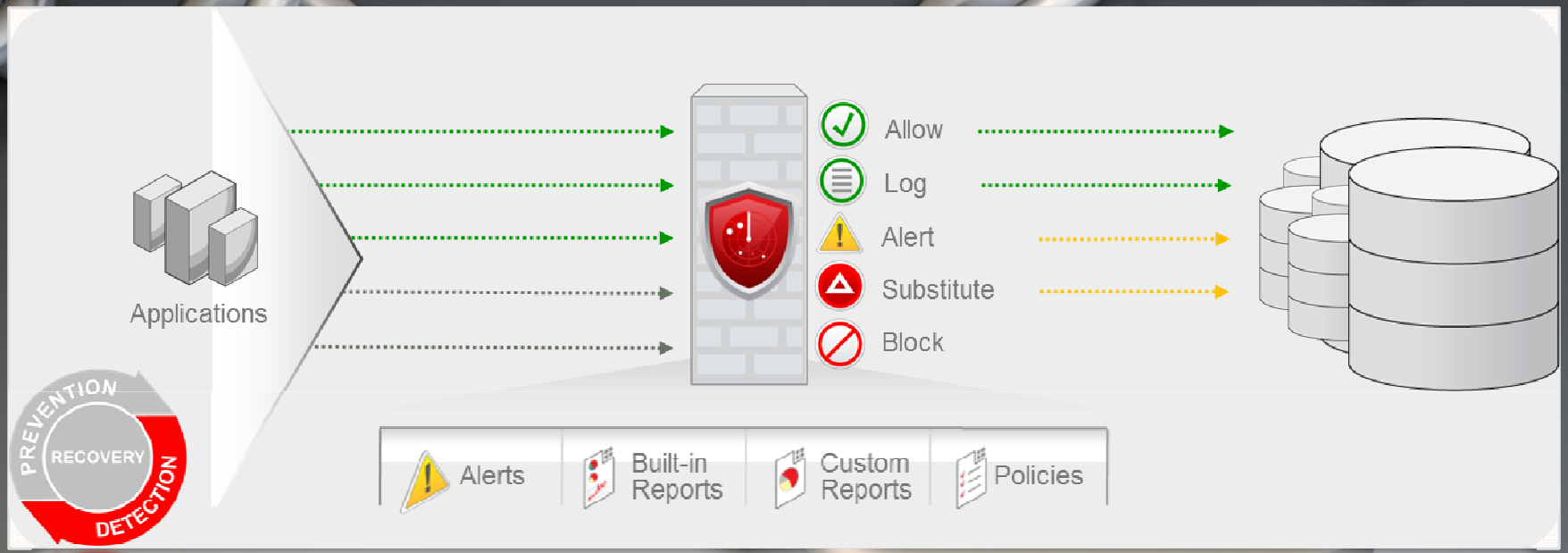
Aplikativnom korisniku dati najmanji skup privilegija.

Koristiti Database Firewall za praćenje aktivnosti baze i blokiranje SQL naredbi

Testirati aplikaciju na SQL Injection

parallel
oracle expert team

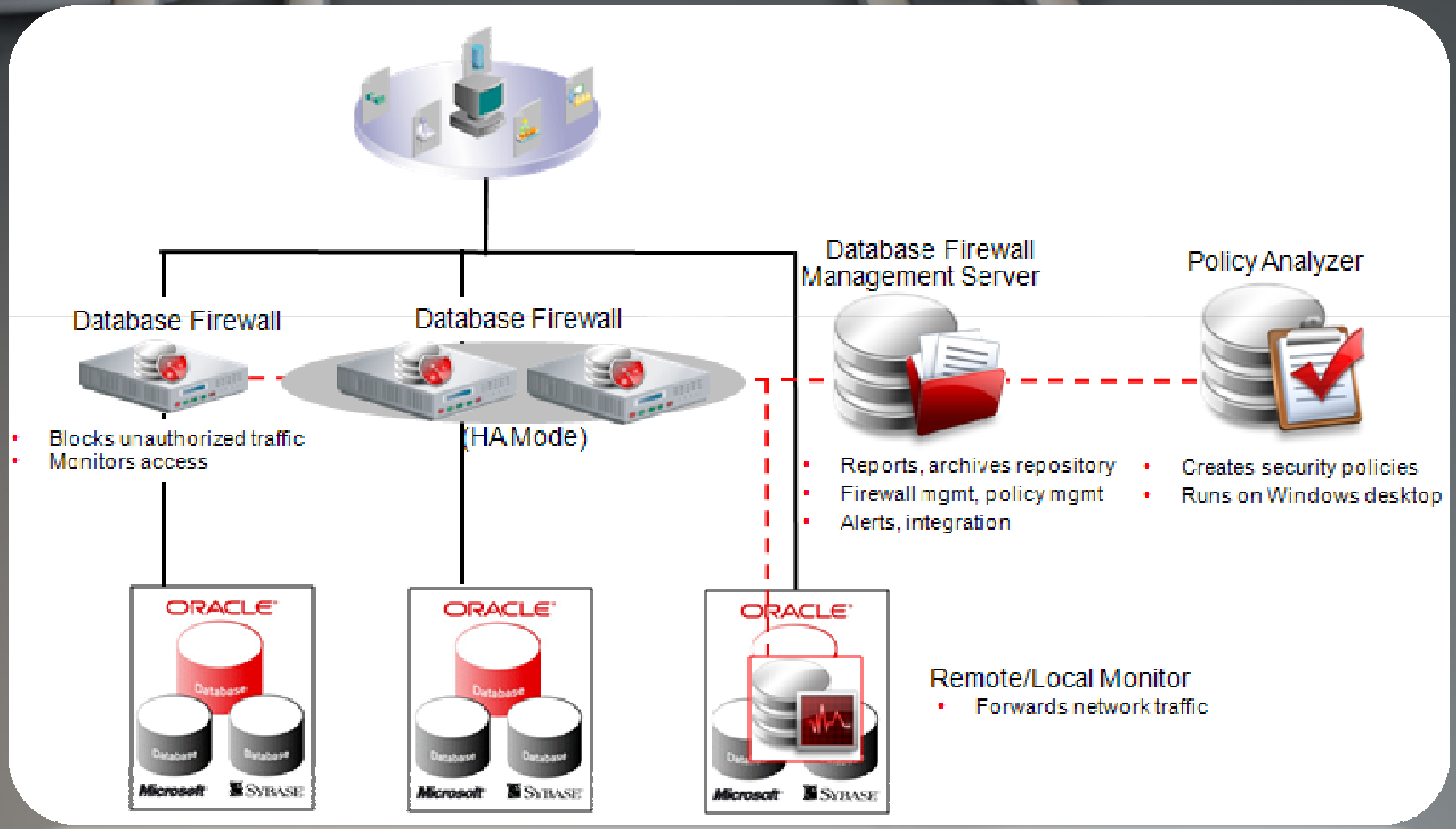
Database firewall



Proverava svaku SQL naredbu i na osnovu politike može da: dozvoli; loguje; uzbuni; supstituiše; blokira naredbu

parallel
oracle expert team

Arhitektura database firewall-a



parallel
oracle expert team

Database firewall management server

16
hroug

ORACLE

Dashboard | Appliances | Monitoring | Reporting | Archiving | System | Logout

Oracle Database Firewall Management Server Administration Console

Welcome. You are logged in as *zoki* | Version: 5.0 | 02:52:36

Threat Status: Alert

Known Blocked:	12
Unseen Blocked:	0
Known Warned:	261
Unseen Warned:	0

Throughput Status: OK

Statement Rate:	0
Total Statements: (In Last Hour)	284

Quick Start

Monitor databases System settings

Top Ten Threats (Last Week)

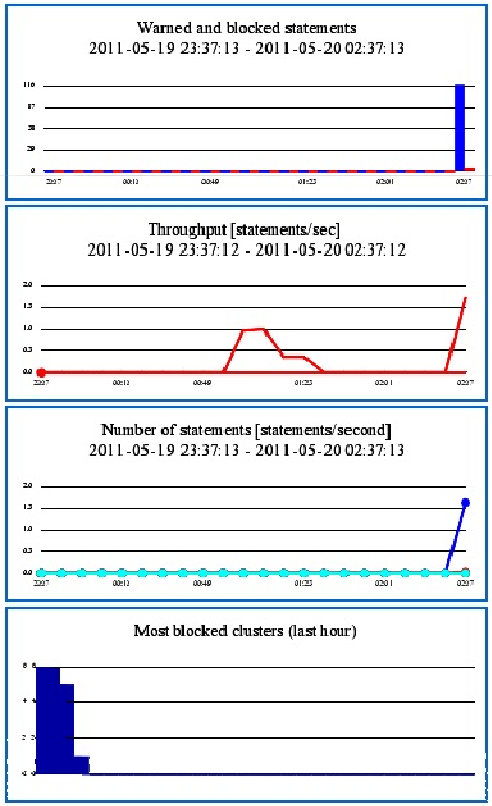
Count	Status	Statement	Seen	Log Level	Source	Destination
5		select salary from...	yes	always	192.168.46.32	192.168.46.10
4		select * from v$ve...	yes	always	192.168.46.32	192.168.46.10
2		select * from v$ve...	yes	always	192.168.46.32	192.168.46.20
1		select * from empl...	yes	always	192.168.46.32	192.168.46.10
12		select parameter,v...	yes	always	192.168.46.32	192.168.46.10
6		select parameter,v...	yes	always	192.168.46.32	192.168.46.20
4		alter session set ...	yes	always	192.168.46.32	192.168.46.10
2		alter session set ...	yes	always	192.168.46.32	192.168.46.20
1		SELECT '###### ty...	yes	always	192.168.46.32	192.168.46.10
45		select 0 from Dba_...	yes	always	192.168.46.32	192.168.46.10

Enforcement Points

Name	Appliance	IP Address
enf_point	DBFirewall	192.168.46.7

Traffic Snapshot at 2011-05-20 02:52

Filter (no filter active)



parallel
oracle expert team

Database firewall policy analyzer

Id	Action	Logging	Threat	Statement	Count	IpAddresses	Tables	Columns	Users	StatementType	Client Progra
12074488	Pass	Always	Minor	select 0 from dba_tab_columns where 0=0	2	192.168.46.32	DBA_TAB_COLUM		HR, SH	Data Manipulation Read Only	SQL Developer
28544362	Pass	Always	Minor	select 0 from dba_objects where 0=0	3	192.168.46.32	DBA_OBJECTS		HR, SH	Data Manipulation Read Only	SQL Developer
161522608	Pass	Always	Major	select * from v$version where banner like '##	4	192.168.46.32	V$VERSION	*, BANNER	HR, OE, SH	Data Manipulation Read Only	SQL Developer
192357953	Pass	Always	Minor	select 0 from dba_triggers where 0=0	2	192.168.46.32	DBA_TRIGGERS		SH	Data Manipulation Read Only	SQL Developer
203175021	Warn	Always	Moderate	select * from (select o.object_name, o.obje	2	192.168.46.32	RECYCLEBIN, SYS	*, OBJECT_ID, OE	HR, SH	Data Manipulation Read Only	SQL Developer
245408782	Warn	Always	Moderate	select '######' type, username owner, use	1	192.168.46.32	ALL_OBJECTS, AL	COLUMN_ID, COL	HR	Data Manipulation Read Only	SQL Developer
310115106	Warn	Always	Moderate	select /*oracledictionaryqueries.all_timestamp	2	192.168.46.32	RECYCLEBIN, SYS	RECYCLEBIN.PUR	HR, SH	Data Manipulation Read Only	SQL Developer
370316298	Warn	Always	Moderate	select partition_name from sys.all_tab_pa	1	192.168.46.32	SYS.ALL_TAB_PAR	PARTITION_NAME	SH	Data Manipulation Read Only	SQL Developer
379470739	Warn	Always	Moderate	select table_owner, table_name from all_sync	2	192.168.46.32	ALL_SYNONYMS,	OBJECT_NAME, O	HR, SH	Data Manipulation Read Only	SQL Developer
471940417	Warn	Always	Minor	select '######' type, username owner, use	2	192.168.46.32	ALL_OBJECTS, AL	OBJECT_NAME, O	HR, OE	Data Manipulation Read Only	SQL Developer
476443515	Warn	Always	Minor	select 0 from dba_tab_privs where 0=0	3	192.168.46.32	DBA_TAB_PRIVS		HR, SH	Data Manipulation Read Only	SQL Developer
596985961	Pass	Always	Minor	select 0 from dba_synonyms where 0=0	2	192.168.46.32	DBA_SYNONYMS		SH	Data Manipulation Read Only	SQL Developer
721721395	Block	Always	Major	select salary from employees	1	192.168.46.32	EMPLOYEES	SALARY	HR	Data Manipulation Read Only	SQL Developer
775265104	Block	Always	Major	select * from employees	1	192.168.46.32	EMPLOYEES	*	HR	Data Manipulation Read Only	SQL Developer
781921795	Pass	Always	Minor	select 0 from sys.obj$ where 0=0	4	192.168.46.32	SYS.OBJ$		HR, OE, SH	Data Manipulation Read Only	SQL Developer
813890625	Pass	Always	Minor	select sys_context('#######','#######:	4	192.168.46.32	DUAL		HR, OE, SH	Data Manipulation Read Only	SQL Developer
814486371	Warn	Always	Moderate	select /*oracledictionaryqueries.all_table_ora	2	192.168.46.32	ALL_MVIEWS, ALL	ALL_MVIEWS.MVI	HR, SH	Data Manipulation Read Only	SQL Developer
838360186	Pass	Always	Minor	alter session set time_zone = '#########	4	192.168.46.32			HR, OE, SH	Data Definition	SQL Developer
847618782	Pass	Always	Minor	select 0 from dba_queue_tables where 0=0	3	192.168.46.32	DBA_QUEUE_TABI		HR, SH	Data Manipulation Read Only	SQL Developer
864971147	Pass	Always	Minor	select 0 from dba_directories where 0=0	2	192.168.46.32	DBA_DIRECTORIE		SH	Data Manipulation Read Only	SQL Developer
889700803	Pass	Always	Minor	select count(0) from all_objects where object_	4	192.168.46.32	ALL_OBJECTS	OBJECT_NAME	HR, OE, SH	Data Manipulation Read Only	SQL Developer
992225707	Pass	Always	Minor	select 0 from sys.external_tab$ where 0=0	3	192.168.46.32	SYS.EXTERNAL_TA		HR, SH	Data Manipulation Read Only	SQL Developer
994124125	Pass	Always	Minor	select dbtimezone from dual	4	192.168.46.32	DUAL		HR, OE, SH	Data Manipulation Read Only	SQL Developer
1046761591	Pass	Always	Minor	select 0 from sys.dba_recyclebin where 0=0	3	192.168.46.32	SYS.DBA_RECYCL		HR, SH	Data Manipulation Read Only	SQL Developer
1361014943	Pass	Always	Minor	select 0 from dba_snapshot_logs where 0=0	2	192.168.46.32	DBA_SNAPSHOT_L		SH	Data Manipulation Read Only	SQL Developer
1373844356	Pass	Always	Minor	select 0 from dba_plsql_object_settings where	2	192.168.46.32	DBA_PLSQL_OBJE		SH	Data Manipulation Read Only	SQL Developer
1498987224	Pass	Always	Minor	select 0 from dba_views where 0=0	2	192.168.46.32	DBA_VIEWS		SH	Data Manipulation Read Only	SQL Developer
1648119752	Pass	Always	Minor	select 0 from dba_indexes where 0=0	2	192.168.46.32	DBA_INDEXES		SH	Data Manipulation Read Only	SQL Developer
1850358902	Pass	Always	Moderate	select * from sales	1	192.168.46.32	SALES	*	SH	Data Manipulation Read Only	SQL Developer
1886932416	Warn	Always	Moderate	alter session set plsql_optimize_level=0	4	192.168.46.32			HR, OE, SH	Data Definition	SQL Developer
2129816678	Warn	Always	Moderate	select * from promotions	1	192.168.46.32	PROMOTIONS	*	OE	Data Manipulation Read Only	SQL Developer
2382142404	Pass	Always	Minor	select 0 from dba_editions where 0=0	3	192.168.46.32	DBA_EDITIONS		HR, SH	Data Manipulation Read Only	SQL Developer
2486962943	Warn	Always	Moderate	select count(*) from sales	1	192.168.46.32	SALES	*	SH	Data Manipulation Read Only	SQL Developer
2539045733	Pass	Always	Minor	select 0 from dba_queues where 0=0	3	192.168.46.32	DBA_QUEUES		HR, SH	Data Manipulation Read Only	SQL Developer
2905949966	Pass	Always	Minor	select /*oracledatabaseimpl.all_roles_query*/	4	192.168.46.32	SESSION_ROLES	ROLE	HR, OE, SH	Data Manipulation Read Only	SQL Developer

parallel
oracle expert team

Karakteristike Database Firewall-a

16 hroug

Ugrađeni „out of the box“ izveštaji za sve veće standarde kao što su: PCI, SOX, itd.

Koristi white list-e i black list-e koje kao parametre mogu koristiti doba dana, dan u nedelji, mrežu, aplikaciju

Moguće je postaviti da su za određenu aplikaciju dozvoljene samo unapred poznate SQL naredbe

parallel
oracle expert team

Odbrane - Smernice

Obavezno parsirati i prečistiti unos od strane korisnika

Kreirati generičku stranu za greške u aplikaciji

Aplikativnom korisniku dati najmanji skup privilegija.

Koristiti Database Firewall za praćenje aktivnosti baze i blokiranje SQL naredbi

Testirati aplikaciju na SQL Injection

parallel
oracle expert team

Parsiranje unosa – Pogrešno!

16 hroug

Nikada ne koristiti korisnički unos direktno u sql naredbi, niti vršiti konkatenaciju (dodavanje) neparsiranih stringova!

```
String ime =
request.getParameter(“ime");
PreparedStatement pstmt =
conn.prepareStatement("insert into
EMP (EIME) values ('" + ime + "')");
pstmt.execute();
pstmt.close();
```

parallel
oracle expert team

Parsiranje unosa – Ispravno!

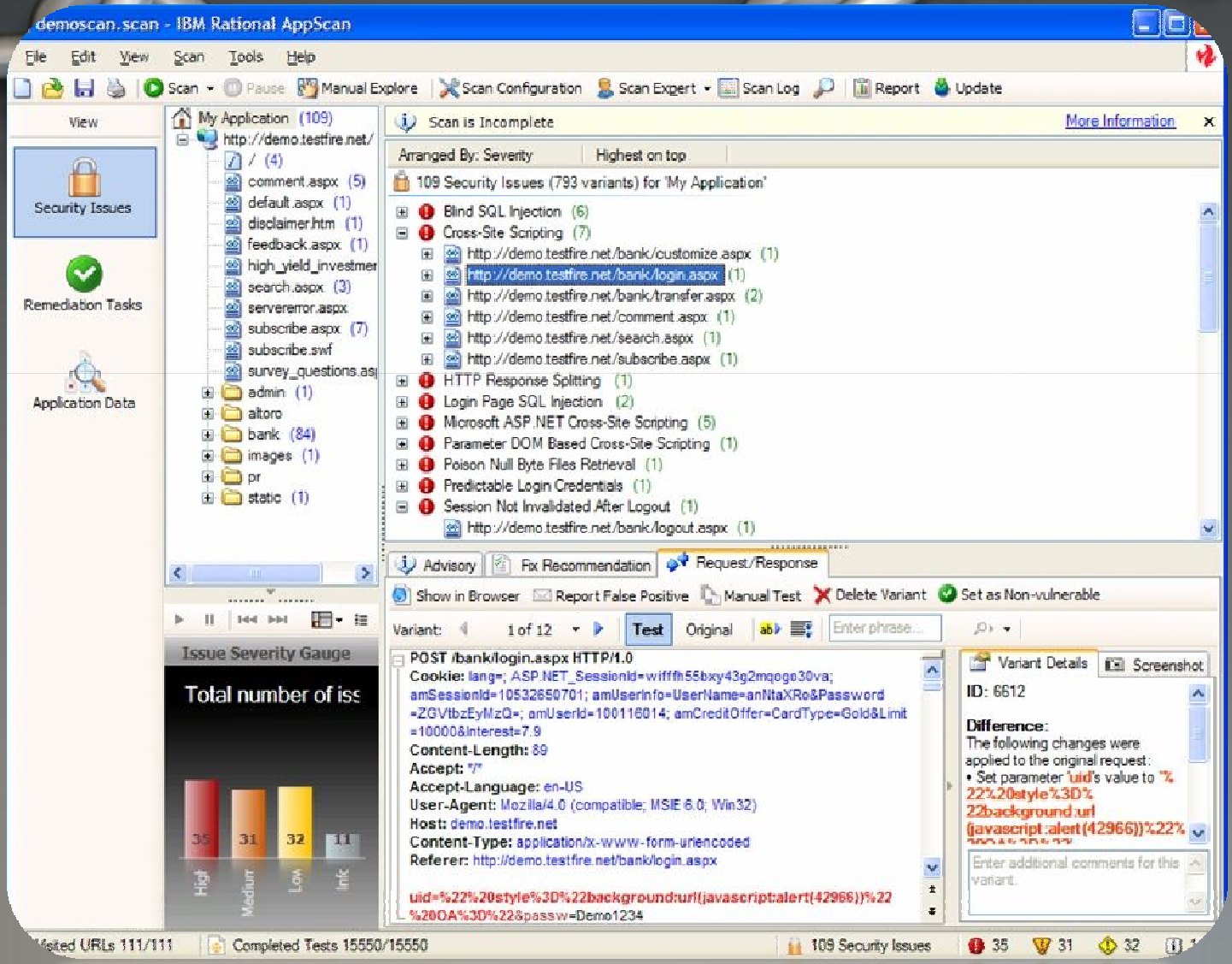
16 hroug

U Javi koristiti prepared statement sa bind promenljivom

```
PreparedStatement pstmt =
conn.prepareStatement ("insert into
EMP (EIME) values (?)");
String ime =
request.getParameter(“ime");
pstmt.setString (1, ime);
pstmt.execute();
Pstmt.close();
```

parallel
oracle expert team

IBM - AppScan



parallel
oracle expert team

Zaključak

SQL Injection predstavlja napad koji je jednostavan za učenje, a može naneti veoma veliku štetu. Iz spomenutih razloga, potrebno je posvetiti posebnu pažnju odbrani od ovog napada.

16 hroug

parallel
oracle expert team

Prilog

16 hroug

Obezbeđen je disk, kao prilog prezentaciji, na kojem se nalazi 20-to minutni film o konfiguraciji i upotrebi Oracle Database Firewall-a, instalacije softvera za SQL Injection kao i Oracle SQL Injection Cheat Sheet.

Kontakt

Autori:

Zoran Pavlović, *Security Manager*
zoran.pavlovic@parallel.rs

Maja Veselica, *Security Consultant*
maja.veselica@parallel.rs

Parallel d.o.o:

e-mail: info@parallel.rs

adresa: Pariske komune 24, Novi Beograd

telefon: +381 11 260 74 84

parallel
oracle expert team

16
hroug

Hvala na pažnji!


parallel
oracle expert team
16
hroug
?