امنیت پایگاه‌داده

مرکز آپا دانشگاه یزد
مهر ۱۳۹۴

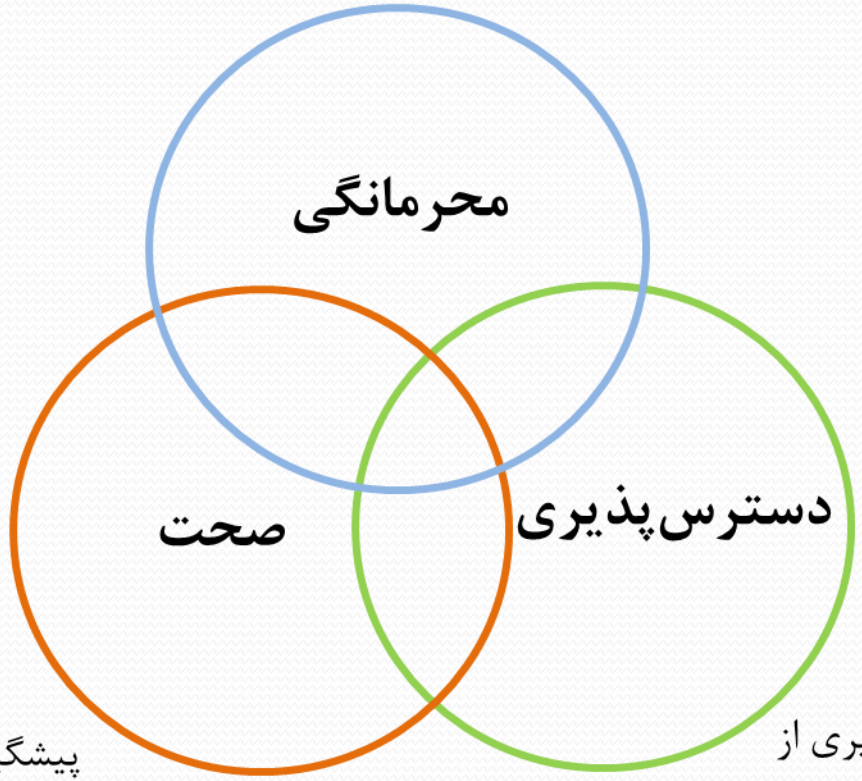
سرخط‌ها

- مقدمه
- تهدیدات امنیتی پایگاه‌داده
- کنترل امنیتی پایگاه‌داده
- جمع‌بندی

مقدمه

امنیت

پیشگیری، تشخیص و جلوگیری از افشای داده

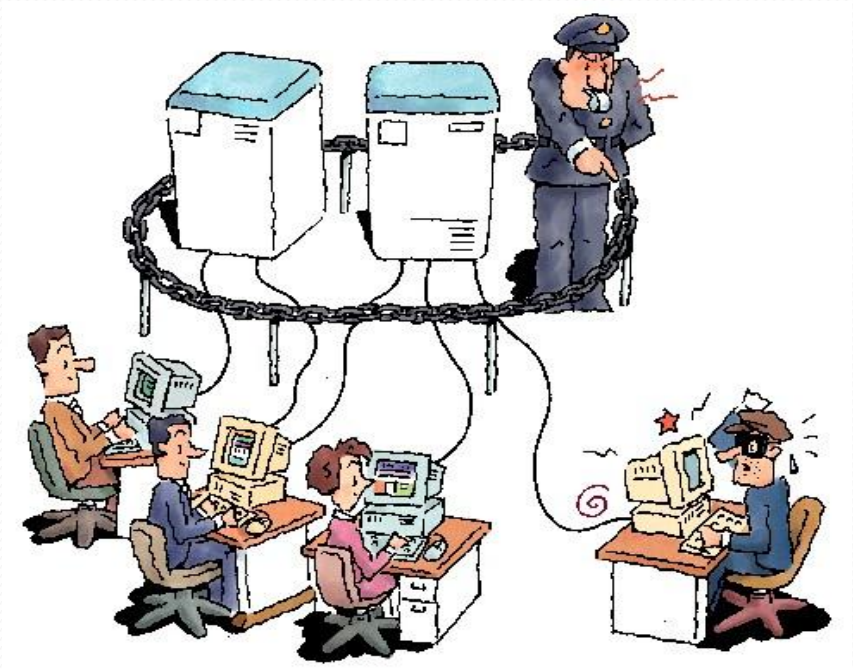


پیشگیری، تشخیص و جلوگیری از
تغییر ناخواسته ی داده

پیشگیری، تشخیص و جلوگیری از
منع دسترسی به سرویس

امنیت پایگاه‌داده

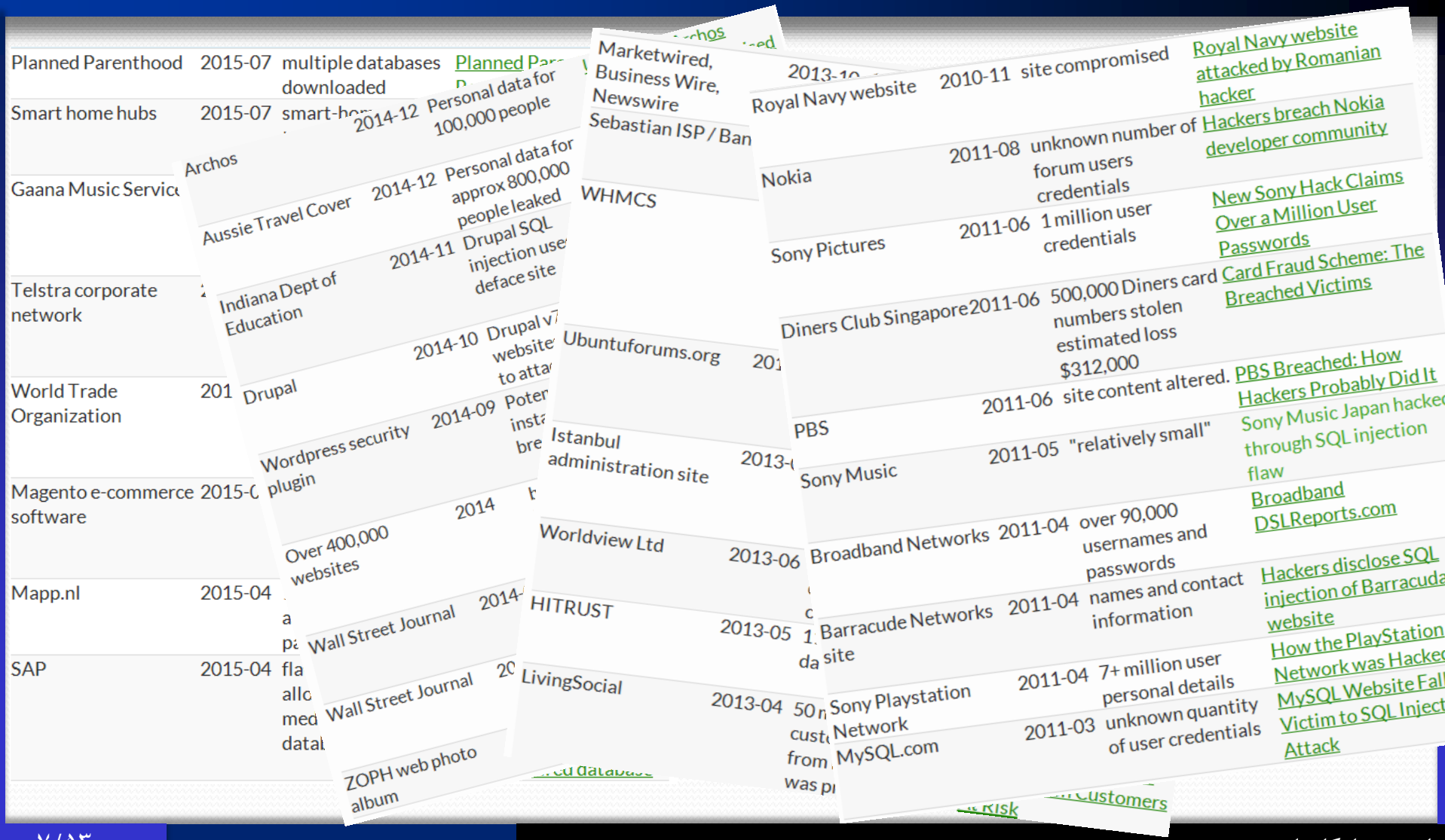
- امنیت پایگاه داده عبارت است از:
  - جلوگیری از افشای غیرمجاز داده
  - جلوگیری از تغییر غیرمجاز داده
  - حفظ اطلاعات و پایداری پایگاه داده



چرا امنیت پایگاه داده مهم است؟

- تمام دارایی یک سازمان داده‌های آن است که معمولا در پایگاه داده ذخیره می‌شوند
- اطلاعات حساب‌های بانکی (اطلاعات کارت اعتباری)
  - اطلاعات شخصی (همچون نام، آدرس، شماره تلفن)
  - آدرس ایمیل
  - نام کاربری و کلمه عبور
- نقض امنیت داده‌های یک سازمان ممکن است پیامدهای جبران‌ناپذیری را برای آن سازمان به بار آورد.

چرا امنیت پایگاه داده مهم است؟



Planned Parenthood	2015-07	multiple databases downloaded	Planned Par...
Smart home hubs	2015-07	smart-ho...	
Gaana Music Servic...			
Telstra corporate network	2		
World Trade Organization	201		
Magento e-commerce software	2015-0		
Mapp.nl	2015-04	a pa...	
SAP	2015-04	fla... allo... med... data...	

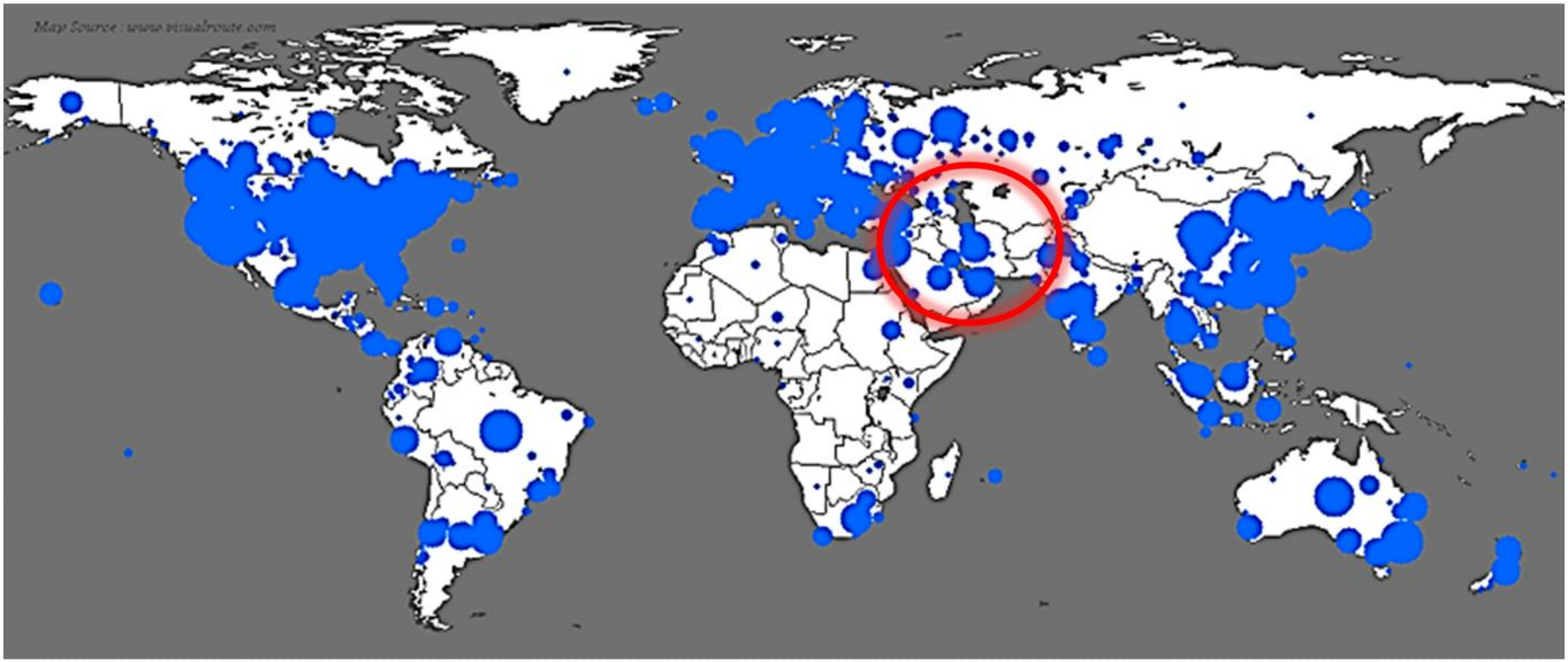
Archos	2014-12	Personal data for 100,000 people	
Aussie Travel Cover	2014-12	Personal data for approx 800,000 people leaked	
Indiana Dept of Education	2014-11	Drupal SQL injection use... deface site	
Drupal	2014-10	Drupal v7 website... to atta...	
Wordpress security plugin	2014-09	Poten... insta... bre...	
Over 400,000 websites	2014	h...	
Wall Street Journal	2014-		
Wall Street Journal	20		
ZOPH web photo album			

Marketwired, Business Wire, Newswire	2013-10	...ched ...ised	
Sebastian ISP / Ban...			
WHMCS			
Ubuntuforums.org	201		
Istanbul administration site	2013-(		
Worldview Ltd	2013-06	c...	
HITRUST	2013-05	1...	
LivingSocial	2013-04	50 m... cust... from ... was pl...	
...ed database			

Royal Navy website	2010-11	site compromised	Royal Navy website attacked by Romanian hacker
Nokia	2011-08	unknown number of forum users credentials	Hackers breach Nokia developer community
Sony Pictures	2011-06	1 million user credentials	New Sony Hack Claims Over a Million User Passwords
Diners Club Singapore	2011-06	500,000 Diners card numbers stolen estimated loss $312,000	Card Fraud Scheme: The Breached Victims
PBS	2011-06	site content altered.	PBS Breached: How Hackers Probably Did It
Sony Music	2011-05	"relatively small"	Sony Music Japan hacked through SQL injection flaw
Broadband Networks	2011-04	over 90,000 usernames and passwords	Broadband DSLReports.com
Barracude Networks	2011-04	names and contact information	Hackers disclose SQL injection of Barracuda website
Sony Playstation Network	2011-04	7+ million user personal details	How the PlayStation Network was Hacked
MySQL.com	2011-03	unknown quantity of user credentials	MySQL Website Fall... Victim to SQL Inject... Attack
...k risk			...Customers

تمامی اتفاقات بد فقط برای دیگران اتفاق می افتد؟

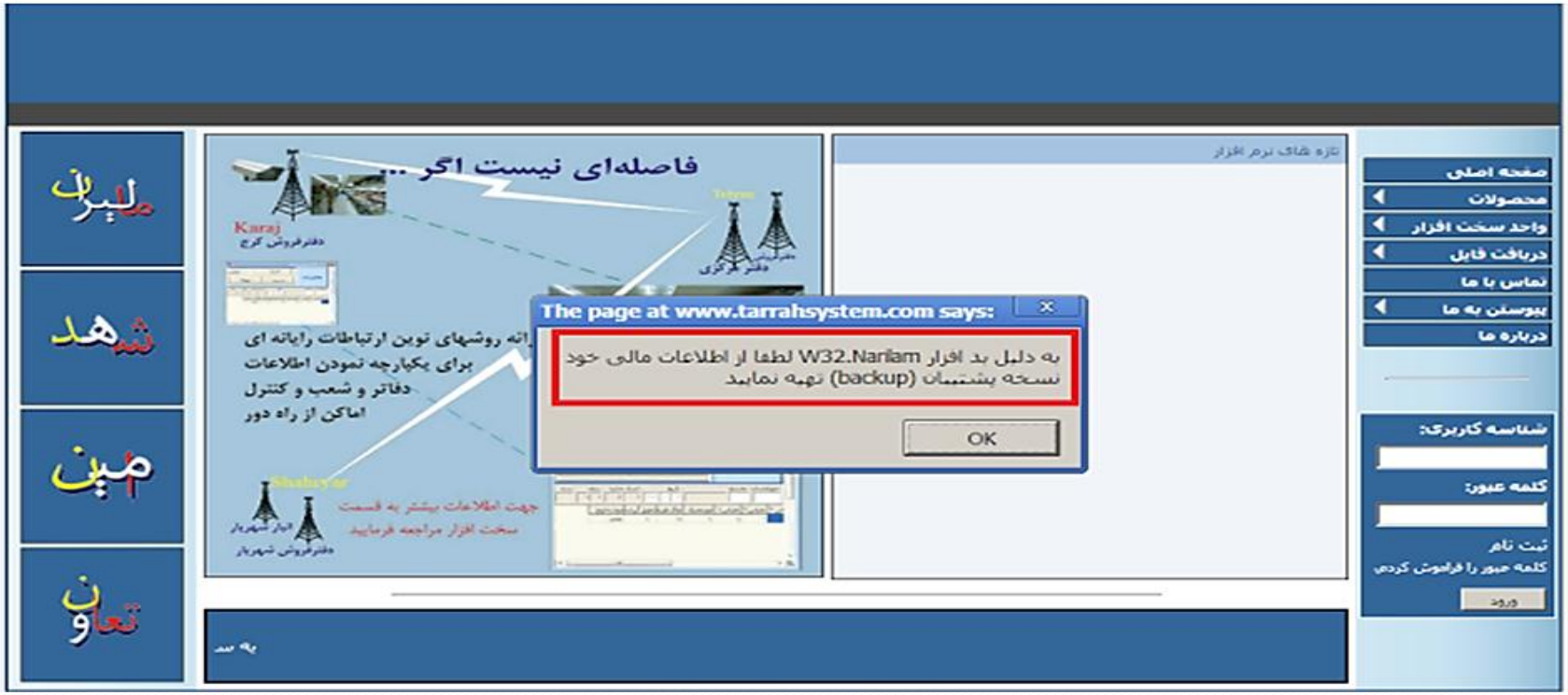
SQL Slammer



تمامی اتفاقات بد فقط برای دیگران اتفاق می افتد؟

Narilam malware target Iran Financial SQL Databases

Monday, November 26, 2012 Mohit Kumar



بنابراین

تهدیدات امنیتی پایگاه‌داده

برخی از تهدیدات امنیتی پایگاه‌داده

- سوءاستفاده از مجوزهای اضافی یا قانونی
- استفاده از آسیب‌پذیری‌های پلت‌فرم، پایگاه‌داده، برنامه‌کاربردی
- افشای اطلاعات پشتیبان
- ناپایداری پایگاه داده
- احراز هویت ضعیف
- حسابرسی ضعیف

تهدید۱– سوءاستفاده از مجوزهای اضافی یا قانونی

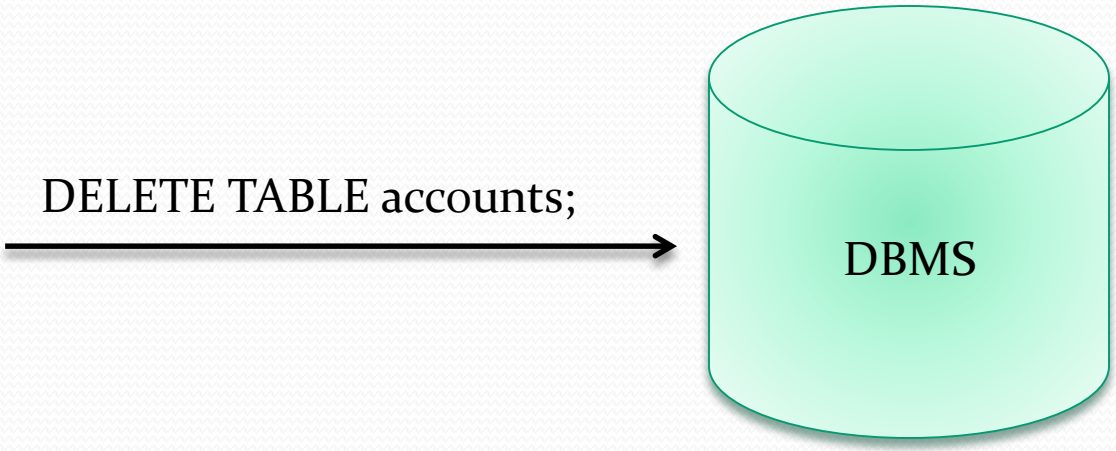
- اعطای مجوزهای دسترسی بیش از حد نیاز به کاربران
  - دسترسی رئیس دانشگاه به نمرات دانشجویان
- اهمیت توجه به تهدیدات داخلی

تهدید۱– سوءاستفاده از مجوزهای اضافی یا قانونی

```
Grant ALL ON accounts TO finantial_admin;
```

finantial_admin

DELETE TABLE accounts;



تهدید۱– سوءاستفاده از مجوزهای اضافی یا قانونی

راه‌حل

- اعطای مجوزهای دسترسی به کاربران در سطح پرس‌وجو

```
GRANT UPDATE ON accounts TO joe;
```

```
REVOKE admins FROM joe;
```

- ردیابی کاربران
- اعمال خط مشی‌های امنیتی
  - نه تنها بر روی داده‌ها بلکه بر نحوه‌ی دسترسی به داده‌ها
    - برنامه‌های کاربردی کارخواه
    - زمان‌های مجاز برای دسترسی به پایگاه‌داده
    - مکان‌های مجاز برای دسترسی به پایگاه‌داده
    - حجم داده‌ها

تهدید۲– سوء استفاده از آسیب‌پذیری‌ها

- استفاده از آسیب‌پذیری پلت‌فرم
  - Blaster worm
    - استفاده از آسیب‌پذیری موجود در سیستم عامل برای از کار انداختن کارگزارها
- استفاده از آسیب‌پذیری پایگاه‌داده
  - SQL slammer
    - استفاده از آسیب‌پذیری سرریز بافر موجود در SQL Server
- استفاده از آسیب‌پذیری برنامه‌کاربردی
  - **آسیب پذیری بخش های غیر مرتبط با پایگاه داده**
  - **تزریق کد**

آسیب پذیری بخش های غیر مرتبط با پایگاه داده

استفاده از آسیب پذیری های موجود در برنامه

بخش آسیب پذیر برنامه به صورت مستقیم با پایگاه داده در ارتباط نیست، ولی با استفاده از آن می توان تهدیدی برای پایگاه داده ایجاد کرد. برای نمونه:

- **آسیب پذیری هایی نظیر سرریز پشته در برنامه**
  - تغییر کد اجرایی ارسالی به پایگاه داده
  - به دست آوردن اطلاعات ارتباط با بانک اطلاعاتی
  - تغییر در داده های ارسالی به پایگاه داده
  - نشر اطلاعات ارسالی و دریافتی از پایگاه داده

- **آسیب پذیری هایی نظیر نشر اطلاعات (Information Disclosure) در برنامه های تحت وب**
  - به دست آوردن اطلاعات ارتباط با بانک اطلاعاتی
  - نشر اطلاعات ارسالی و دریافتی از پایگاه داده

تزریق کد

- یکی از رایج ترین آسیب پذیری های مربوط به بانک اطلاعاتی در برنامه های کاربردی به خصوص برنامه های تحت وب
- تزریق کد مورد نظر مهاجم در کد ارسالی به پایگاه داده
- کد تزریق شده بسته به پایگاه داده مورد نظر متفاوت است
  - **چند نمونه:**
    - SQL Injection
    - NoSQL Injection
    - Xquery Injection
- با توجه به فراگیر بودن پایگاه های داده مبتنی بر SQL، تزریق SQL از رایج ترین آسیب پذیری این دسته می باشند.

تزریق SQL

Login successfully

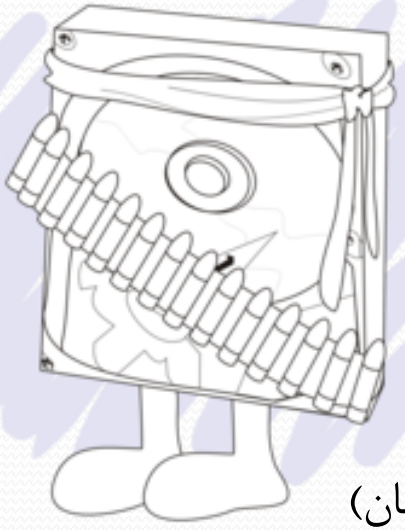
```
SELECT * FROM
users
WHERE
username = 'admin'
AND
password = 'x' OR 'x' = 'x';
```

اهداف کلی حملات تزریق کد

- استخراج، افزودن، حذف یا تغییر داده
- دور زدن احراز هویت
- اجرای از راه دور دستورات
- ارتقاء سطح دسترسی
- استفاده از حملات ترکیبی

تهدید۳– افشای اطلاعات پشتیبان

- **نشر اطلاعات پشتیبان**
  - **سرقت اطلاعات**
    - سرقت فیزیکی اطلاعات پشتیبان
    - نفوذ به شبکه،تجهیزات و محل نگه داری اطلاعات پشتیبان
  - **عوامل انسانی**
    - نشر اطلاعات پشتیبان بر اساس خطای انسانی
    - نشر اطلاعات پشتیبان با استفاده از مهندسی اجتماعی
    - نشر عمدی اطلاعات پشتیبان



- **راه حل:**
  - رمزنگاری فایل‌های پشتیبان
  - استفاده از راهکارهای جلوگیری از نشر اطلاعات (آموزش کارکنان)

تهدید۴– ناپایداری پایگاه داده

- **ناپایداری های بدون ارتباط مستقیم با پایگاه داده**
  - ناپایداری سخت افزار و کمبود منابع
  - ناپاداری مخزن (Storage)
  - ناپایداری شبکه
  - بدافزار
- **ناپایداری های با ارتباط مستقیم با پایگاه داده**
  - عدم توانایی پاسخگویی پایگاه داده به دلیل تعداد بالای تراکنش
  - وجود آسیب پذیری هایی که باعث ناپایداری پایگاه داده می شوند

تهدید۴– ناپایداری پایگاه داده

- **رایج ترین دلایل ناپایداری ناخواسته پایگاه داده در زمان فراهم بودن زیرساخت مناسب:**
  - حملات منع سرویس (DoS/DDoS)
  - آسیب پذیری هایی که باعث منع سرویس می شوند (Dos Vulnerability)

- **راه حل:**
  - پیکربندی صحیح پایگاه داده و انجام تنظیمات امنیتی
  - استفاده از دیواره آتش (Firewall) و سیستم های ضدنفوذ (IPS)
  - بستر سازی مناسب شبکه، مخزن و سخت افزار مربوط به پایگاه داده
  - کنترل کامل در سطوح برنامه کاربردی، شبکه و پایگاه داده

تهدید۴– ناپایداری پایگاه داده

Attackers Using New MS SQL Reflection Techniques

By Bill Brenner February 12, 2015 6:30 AM

The bad guys are using a fairly new technique to tamper with the Microsoft SQL Server Resolution Protocol (MC-SQLR) and launch DDoS attacks.

In an advisory released this morning, Akamai's Prolexic Security Engineering & Response Team (PLXsert) described it as a new type of reflection-based distributed denial of service (DDoS) attack.

PLXsert first spotted attackers using the technique in October. Last month, researcher Kurt Aubuchon studied another such attack and offered an analysis here. PLXsert replicated this attack by creating a script based on Scapy, an open-source packet manipulation tool.

Bank

Bank is flooded with requests and cannot operate effectively.

تهدید۵– احراز هویت ضعیف

- بدست آوردن اطلاعات ورود به سیستم
  - آزمون جامع
  - مهندسی اجتماعی
  - سرقت اطلاعات کاربری

تهدید۵– احراز هویت ضعیف

Login successfully

#1	password
#2	123456
#3	12345678
#4	abc123
#5	123 abc
#6	monkey
#7	letmein
#8	dragon
#9	111111
#10	baseball

تهدید۵– احراز هویت ضعیف

راه حل

- احراز هویت قوی
  - عدم پذیرفتن کلمه عبور ساده
  - ذخیره مقدار درهم شده‌ی کلمه عبور
- تشخیص ورودهای ناموفق متوالی
- ارزیابی خط‌مشی‌های درنظر گرفته شده برای کلمه عبور

تهدید ۶– حسابرسی ضعیف

- حسابرسی
  - آخرین خط دفاعی پایگاه‌داده
  - استفاده برای تشخیص مهاجم و تعمیر سیستم

تهدید ۶– حسابرسی ضعیف

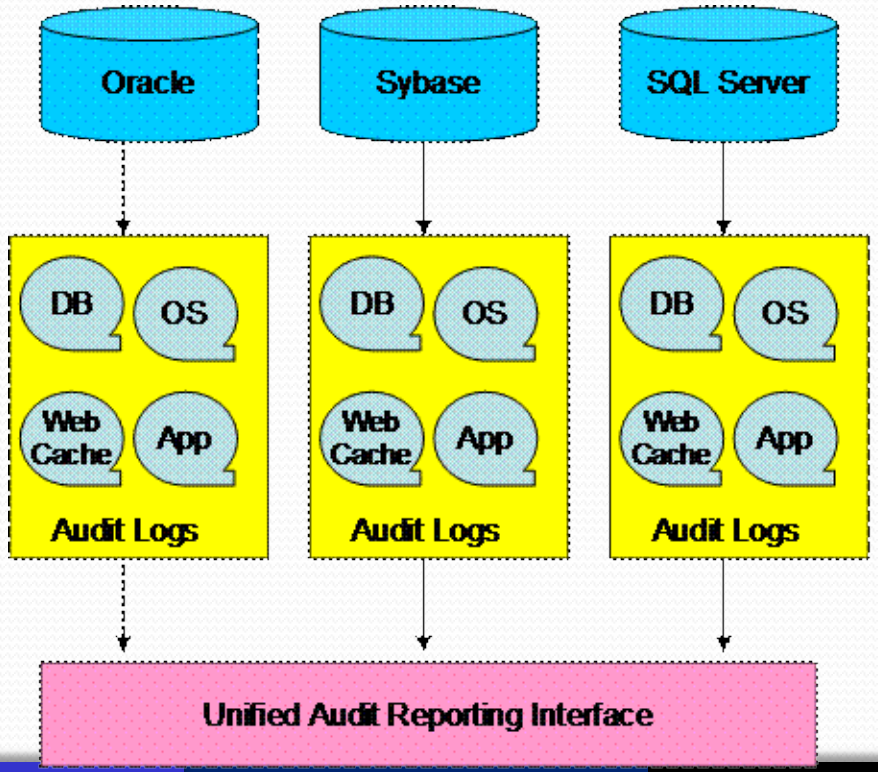
حسابرسی ضعیف در پایگاه‌داده‌ها

- عدم حسابرسی کاربر در صورت اتصال از طریق برنامه‌کاربردی به پایگاه‌داده
- کاهش کارایی کارگزار پایگاه‌داده (مصرف منابع CPU و دیسک)
- امکان غیرفعال شدن حسابرسی توسط مدیران پایگاه‌داده
- عدم ثبت اطلاعات جزئی همچون آدرس IP کاربران
- تفاوت مکانیزم حسابرسی در پایگاه‌داده‌های مختلف و عدم وجود یک مکانیزم جامع

تهدید ۶– حسابرسی ضعیف

راه حل

- استفاده از مکانیزم حسابرسی جامع کارگزار پایگاه‌داده در **سطح شبکه**



کنترل‌های امنیتی پایگاه‌داده

کنترل‌های امنیتی پایگاه‌داده

- **مرحله اول:** مشخص نمودن خط مشی امنیتی سازمان
  - مشخص شدن خط مشی امنیتی سیستم اطلاعاتی
  - مشخص کردن نحوه‌ی کنترل کاربران
- **مرحله دوم:** تعیین کنترل‌های امنیتی مورد نیاز
  - اقدامات امنیتی پیشگیرانه
  - اقدامات امنیتی تشخیص
  - اقدامات امنیتی جرم شناسی

مشخص نمودن خط مشی امنیتی سازمان

مشخص کردن خط‌مشی امنیتی

- مشخص‌کردن اطلاعاتی که نیاز به محافظت دارند
- دسته‌بندی اطلاعات براساس اهمیت آن‌ها

- شناسایی تهدیدات
- ارزیابی ریسک

- تعریف نقش‌های کاربران پایگاه داده
- تعریف حساب‌های کاربرای بر اساس نقش‌ها وکاربران
- تخصیص مجوزهای دسترسی به آنها (با توجه به نیاز آنها)

مشخص کردن خط‌مشی امنیتی

- بازبینی نقش‌ها و مجوزهای دسترسی به طور مداوم برای اطمینان از مناسب بودن آنها با توجه به شرایط فعلی (پس از اعمال هر گونه تغییر در سازمان)

- **تعریف خط مشی برای ثبت فعالیت‌ها**
  - مشخص کردن هدف از ثبت اطلاعات
  - مشخص کردن انواع اطلاعات ثبت شده (اطلاعات سیستم عامل، برنامه کاربردی، پایگاه داده)
  - مشخص کردن نوع دسترسی‌ها و شرایط رخ دادن آن‌ها (زمان، اطلاعات درخواست شده، ورود به سیستم)
  - مشخص کردن جزئیات اطلاعات ثبت شده (زمان، شناسه‌ی کاربر، آدرس IP)
  - مشخص کردن نحوه‌ی نگهداری اطلاعات ثبت شده و کنترل‌دسترسی به آن‌ها

نحوه‌ی کنترل کاربران

- تبیین قوانین امنیتی برای کاربران سیستم
  - منع دسترسی به اطلاعات بدون انجام مجازشماری
  - منع ذخیره‌ی اطلاعات در جایی غیر از رسانه‌های مجاز
  - منع نوشتن شناسه/کلمه عبور در حالی که به صورت آشکار قابل مشاهده باشد
  - عدم تخصیص نقش مدیر پایگاه‌داده و اپراتور سیستم (تفکیک وظایف)
  - الزام کاربران به امضای توافق‌نامه‌های نوشته شده (موافقت با قوانین امنیتی)

نحوه‌ی کنترل کاربران

- تبیین قوانین انضباطی برای متخلفان
- مدیریت پایگاه داده
  - آگاه بودن (دنبال کردن) وقوع حوادث امنیتی که شامل آخرین پایگاه‌داده سازمان هستند و اصلاحاتی که برای آن‌ها ارائه شده‌اند.
  - مجازشماری فعالیت‌های مدیریتی
  - ثبت فعالیت‌های مدیریتی
  - چرخش دوره‌ای مدیران سیستم (اختیاری)
- آموزش کارکنان و همکاران

کنترل‌های امنیتی

- کنترل‌های امنیتی پایگاه‌داده در قبال دسترسی غیرمجاز

کنترل‌های امنیتی – اقدامات پیشگیرانه

پیکربندی اولیه

- نصب آخرین وصله‌های امنیتی ارائه شده
- انتخاب و نصب حداقل ویژگی‌های مورد نیاز و حذف ویژگی‌های اضافی
- محدود کردن دسترسی پایگاه داده

احراز هویت

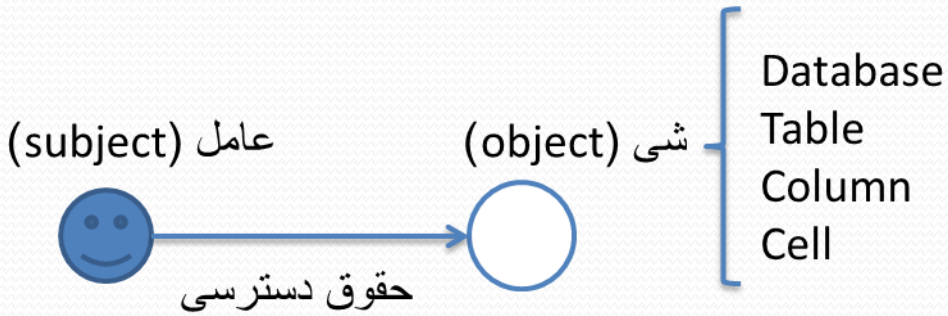
- مدیریت حساب‌های کاربری
  - ایجاد حساب‌های مورد نیاز
  - حذف حساب‌های اضافه
  - مسدود کردن ورودهای ناموفق
- مدیریت کلمه عبور
  - پیچیدگی کلمه عبور
  - تغییر دوره‌ای کلمه عبور
  - تعیین تاریخ انقضا برای کلمه عبور

رمزنگاری

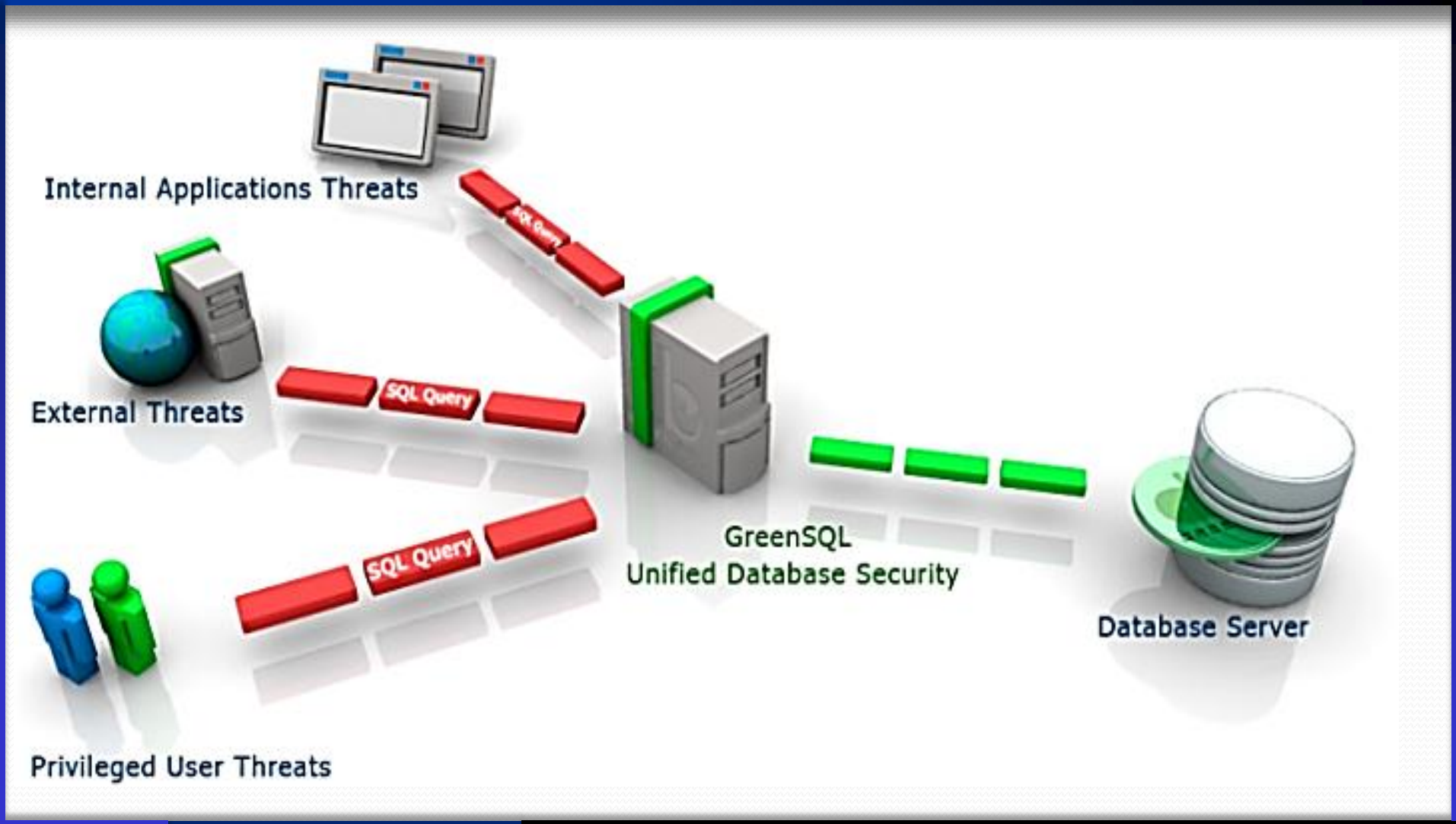
- رمزنگاری داده‌های در حال انتقال بین کارگزار و کارخواه
  - SSL/TLS
- رمزنگاری داده‌های ذخیره شده در پایگاه‌داده
  - فایل‌های داده
  - فایل‌های ثبت
  - فایل‌های پشتیبان
- مدیریت کلیدهای رمزنگاری

کنترل دسترسی

- اطمینان از مجاز بودن دسترسی به داده
- مولفه‌های کنترل دسترسی
  - خط‌مشی دسترسی: مشخص کننده‌ی دسترسی‌های مجاز به سیستم
  - مکانیزم کنترل دسترسی: پیاده‌سازی و اعمال خط‌مشی دسترسی
    - کنترل دسترسی اختیاری
    - کنترل دسترسی اجباری
    - کنترل دسترسی نقش مبنا



سایر اقدامات امنیتی

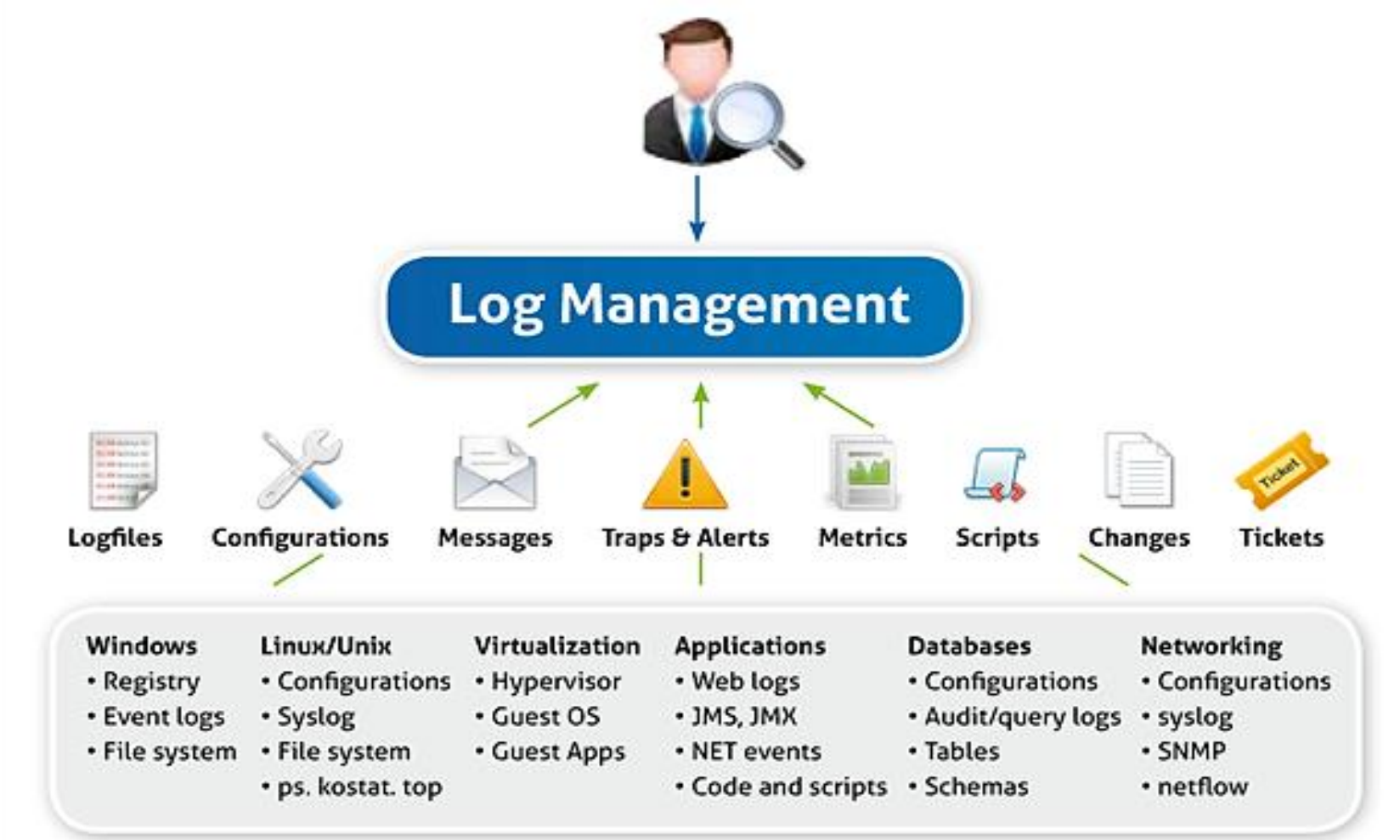


کنترل‌های امنیتی – اقدامات تشخیص و جرم‌شناسی

اقدامات تشخیص و جرم‌شناسی

- تهیه‌ی گزارش‌های مناسب برای تشخیص مشکل و تحلیل جرم
- مدیریت اطلاعات ثبت شده (Logs)
- محافظت از اطلاعات ثبت شده
- تشخیص تلاش برای دسترسی غیرمجاز
- تحلیل اطلاعات ثبت شده برای مشخص شدن نقص امنیتی

مدیریت اطلاعات ثبت شده (Logs)



محافظت از اطلاعات ثبت شده

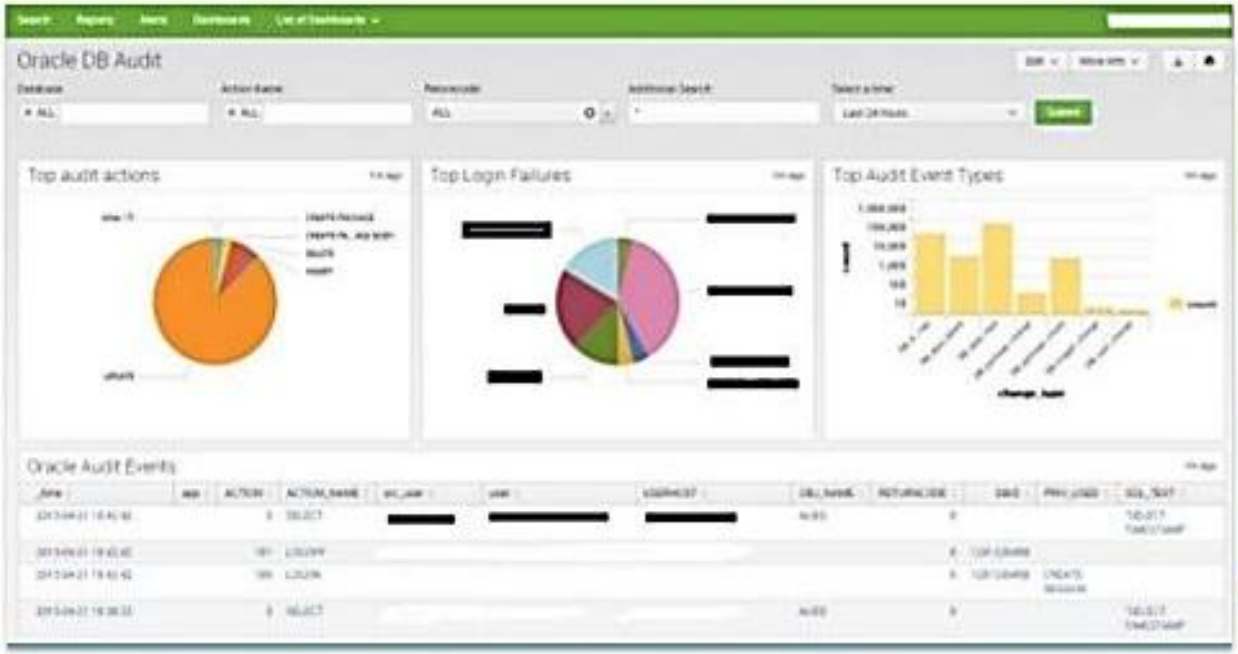
- ذخیره‌سازی اطلاعات ثبت شده در مکان های ذخیره سازی ایمن
- جلوگیری از تغییر اطلاعات ثبت شده
- رمزنگاری اطلاعات ثبت شده

تشخیص تلاش برای دسترسی غیرمجاز

- بررسی زمان دسترسی
- بررسی دسترسی از ترمینال‌های غیرمجاز (با توجه به آدرس IP)
- بررسی دسترسی به حساب‌های مدیریتی
- بررسی الگوی دسترسی کاربران
- تشخیص حملات حدس زدن نام کاربری / کلمه عبور
- نظارت بر دستورات اجرا شده
- نظارت بر اشیاءی ایجاد شده یا تغییر یافته
- خاتمه دادن به دسترسی غیرمجاز

تحلیل اطلاعات ثبت شده برای مشخص شدن نقص امنیتی

- استفاده از ابزارهای تحلیل اطلاعات ثبت شده (در صورت وجود)
- تحلیل دوره‌ای اطلاعات ثبت شده



Dashboard to analyze audit logs from multiple Oracle database servers

جمع‌بندی

تحلیل اطلاعات ثبت شده برای مشخص شدن نقص امنیتی آیا

- اهمیت نیاز به محافظت از پایگاه‌داده
- تهدیدات امنیتی پایگاه‌داده
- نیاز به انجام اقدامات امنیتی در حوزه‌ها و سطوح مختلف

با تشکر از توجه شما ...

مرکز آپا دانشگاه یزد
http://cert.yazd.ac.ir

مرکز آپا شریف
https://cert.sharif.edu