



# SQL INJECTION

Laryssa Nkoumondo & Beni Broohm



# DATABASES AND SQL

Early 1960s :

- Enterprises start using computers widely for business purposes
- They need to access and manage information
- Charles Bachman introduces the first DBMS
- IBM follows with their own

# DATABASES AND SQL

Late 1960s :

- Introduction of CODASYL, a standard for data retrieval
- Too complicated and lack of consistency in data storage
- Edgar Codd introduces a new way of storing data in 1970
- IBM later follows with a language for data querying : SQL

# DATABASES AND SQL

Nowadays :

- Informations on websites are stored in databases
- The information is retrieved using SQL
- Backend software allows to run SQL queries
- Results are presented at the frontend level

# DEFINITION SQL INJECTION

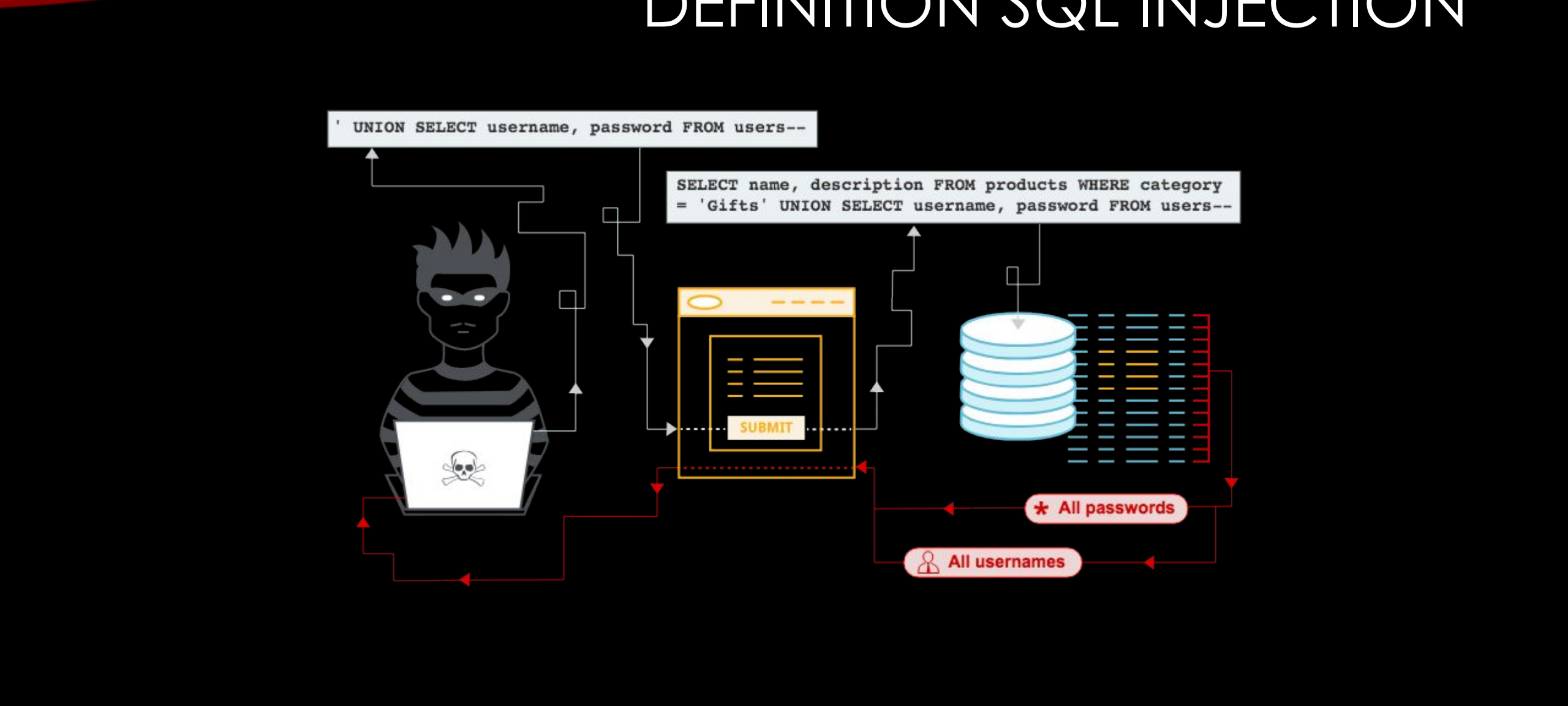
What is a SQL Injection?

- A method that allows an attacker to run SQL queries
- The attacker can retrieve information
- The attacker might take complete control (in serious cases)
- Based on a flaw in the design of the backend software



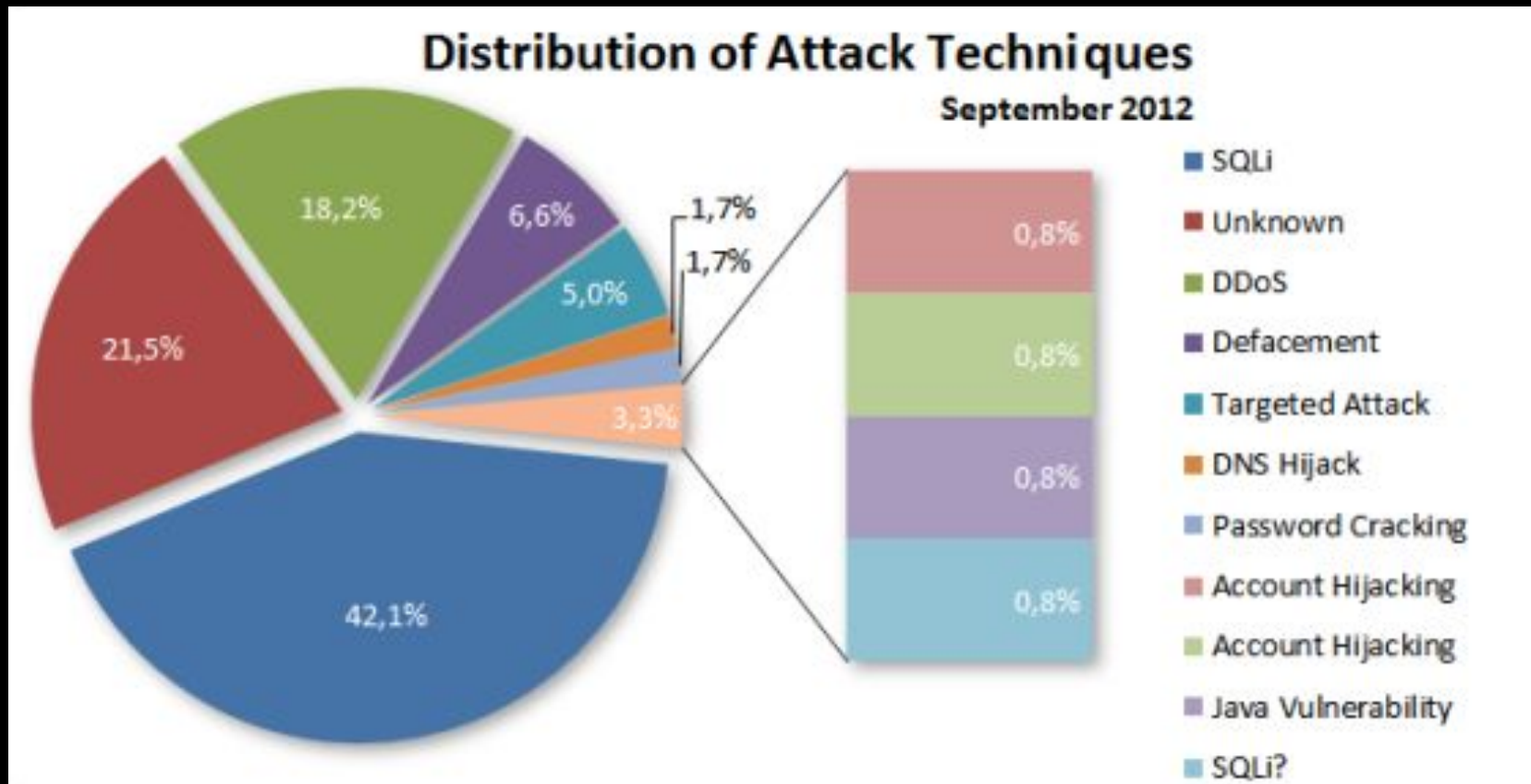


# DEFINITION SOL INJECTION



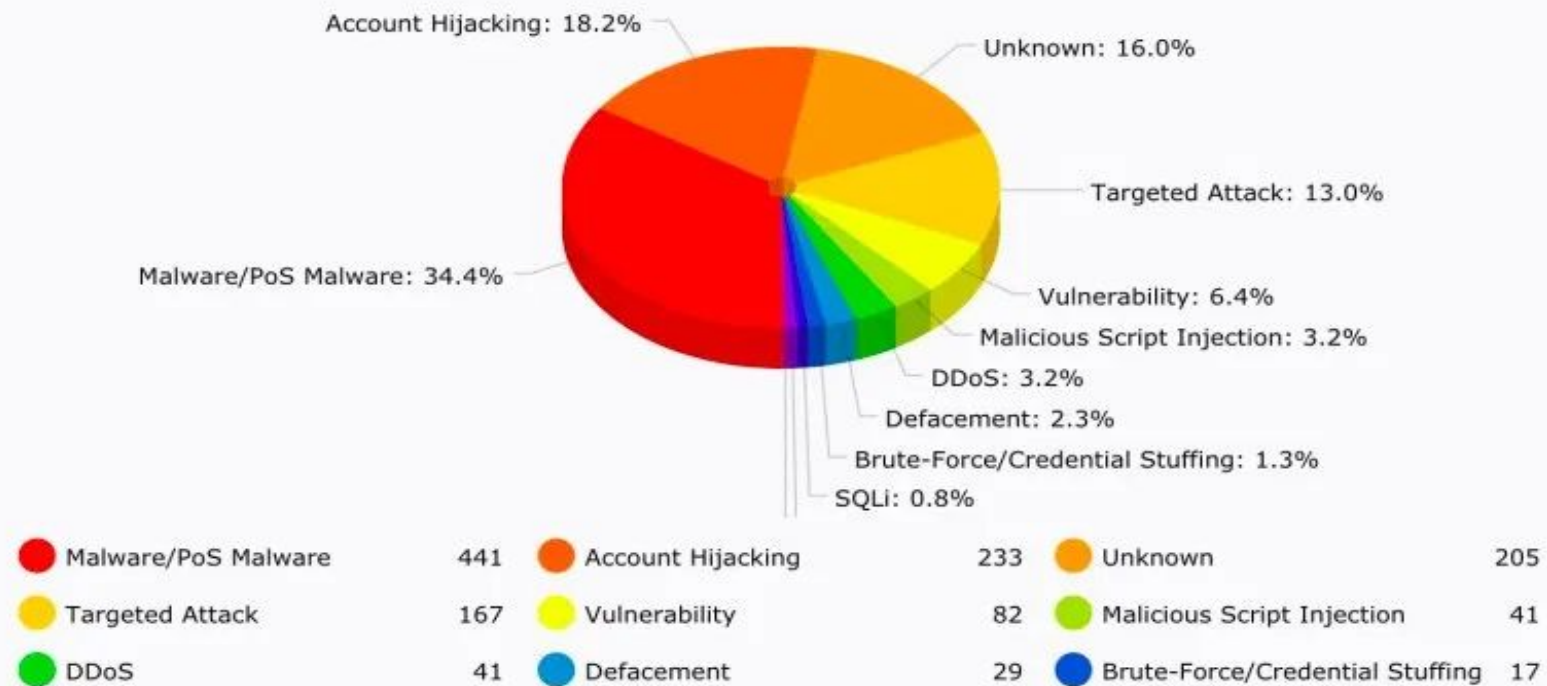


# SQL INJECTION ATTACKS



# SQL INJECTION ATTACKS

Attack Distribution (Top 10 2018)





# SQL INJECTION ATTACKS

Famous SQL injection case : SONY

- In April 2011 Sony's SOE system was the target of an SQL attack.
- The attackers hacked into approximately 24.6 millions accounts
- Information revealed : names, addresses, dates of birth, gender, phone numbers, user IDs, passwords and credit card numbers.

# SQL INJECTION ATTACKS

Famous SQL injection case : World Trade Organization

- In May 2015, Anonymous hacked the World Trade Organization (*ecampus.wto.org*) using *SQL Injection*
- *About 53000 users (including 2100 officials) data were stolen*
- Informations such as first and last names, phone numbers, login credentials...

# SQL INJECTION TECHNIQUES

SQL Injection techniques :

- Blind based method
- Error based method
- Union based method




DATA RETRIEVAL

- Stacked queries method



COMPLETE CONTROL

The image features a solid black background. At the top, there is a decorative border consisting of several overlapping, wavy, translucent bands of color. From left to right, these bands transition through a spectrum: yellow, orange, red, and finally into shades of green and cyan on the far right. The text "DEMO TIME" is centered horizontally in the middle of the black area.

DEMO TIME

# CONSEQUENCES OF SQL INJECTION

What are the threats of such an attack?

SQL injection attacks directly threaten :

- **Integrity**
- **Availability**
- **Confidentiality**



# CONSEQUENCES OF SQL INJECTION

Security threat:

- Access to data → confidentiality
- Data deletion → availability
- Data modification → integrity
- The disclosure of data → confidentiality
- Paralysis of the IT infrastructure by a DoS → availability



# CONSEQUENCES OF SQL INJECTION

Criminal offence: Swiss law



- Détérioration de données proprement dite (144bis ch. 1 CP)
- Soustraction de données (143 CP)
- Soustraction de données personnelles (179novies CP)
- L'accès indu à un système informatique proprement dit (143bis al. 1 CP)
- La mise à disposition d'informations d'accès indu (143bis al. 2 CP)

# PREVENTION AGAINST SQL ATTACKS

Prevention against SQL attacks :

- Disable multiple query run at backend level
- Use parameters when getting input from users
- Queries can be manually tested at the application's entry points.
- Use vulnerability detectors



# REFERENCES

- <https://www.france24.com/fr/20110503-sony-admet-milliers-joueurs-ligne-playstation-SEO-carte-coordonnees-bancaire-piratage-vol>
- <https://portswigger.net/web-security/sql-injection>
- <https://pentest-tools.com/website-vulnerability-scanning/sql-injection-scanner-online>
- <https://geekflare.com/find-sql-injection/>
- <http://securityaffairs.co/wordpress/36528/hacking/anonymous-breached-wto-db.html>
- <https://fossbytes.com/world-trade-organization-hacked-by-anonymous/>
- <https://pdfs.semanticscholar.org/c6cb/08ba2a25339c171de117037ce8aff848b1e0.pdf>
- <https://medium.com/@hninja049/example-of-a-error-based-sql-injection-dce72530271c>
- <https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html>