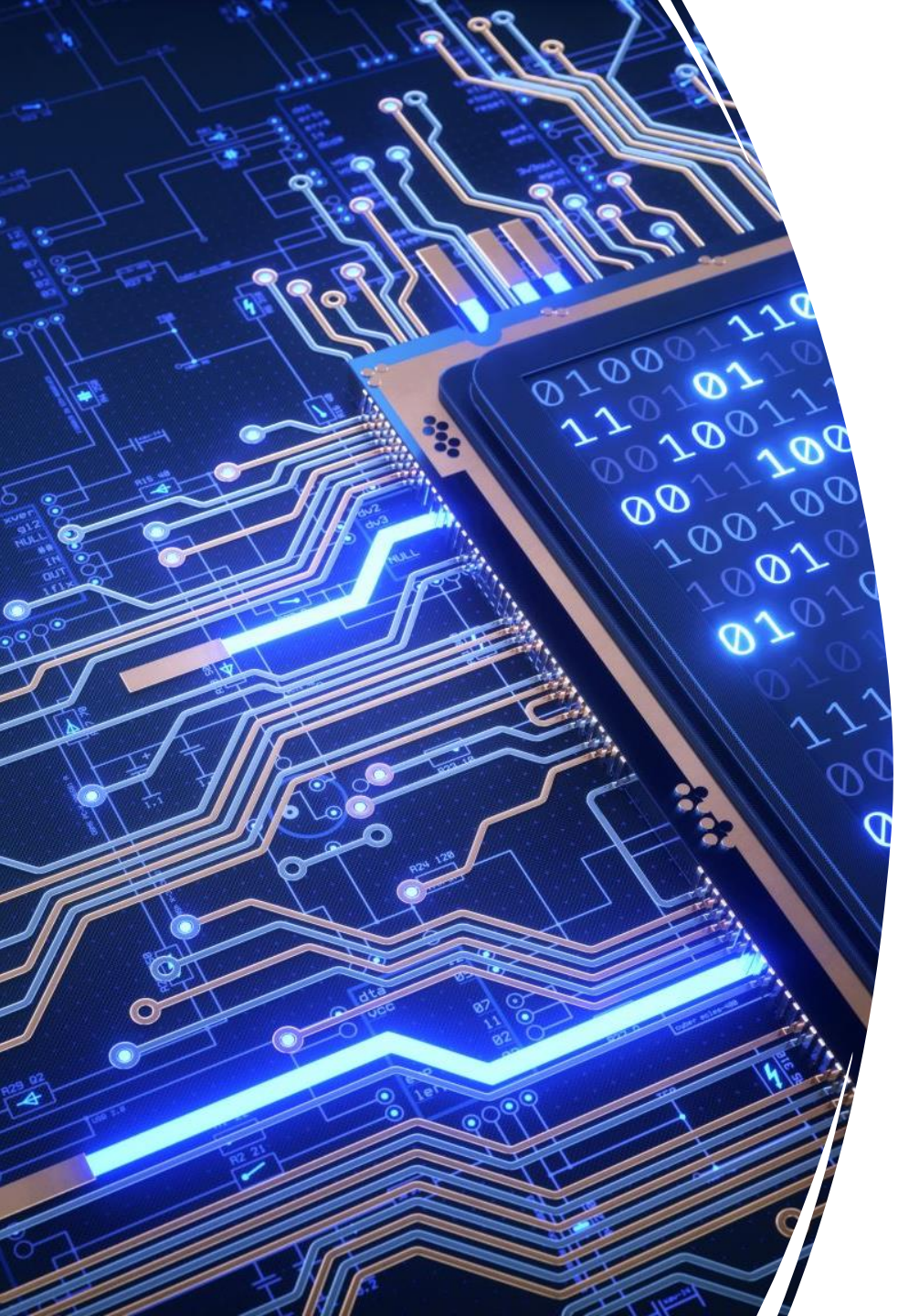


Let’s Get a Better Understanding of SQL Injection

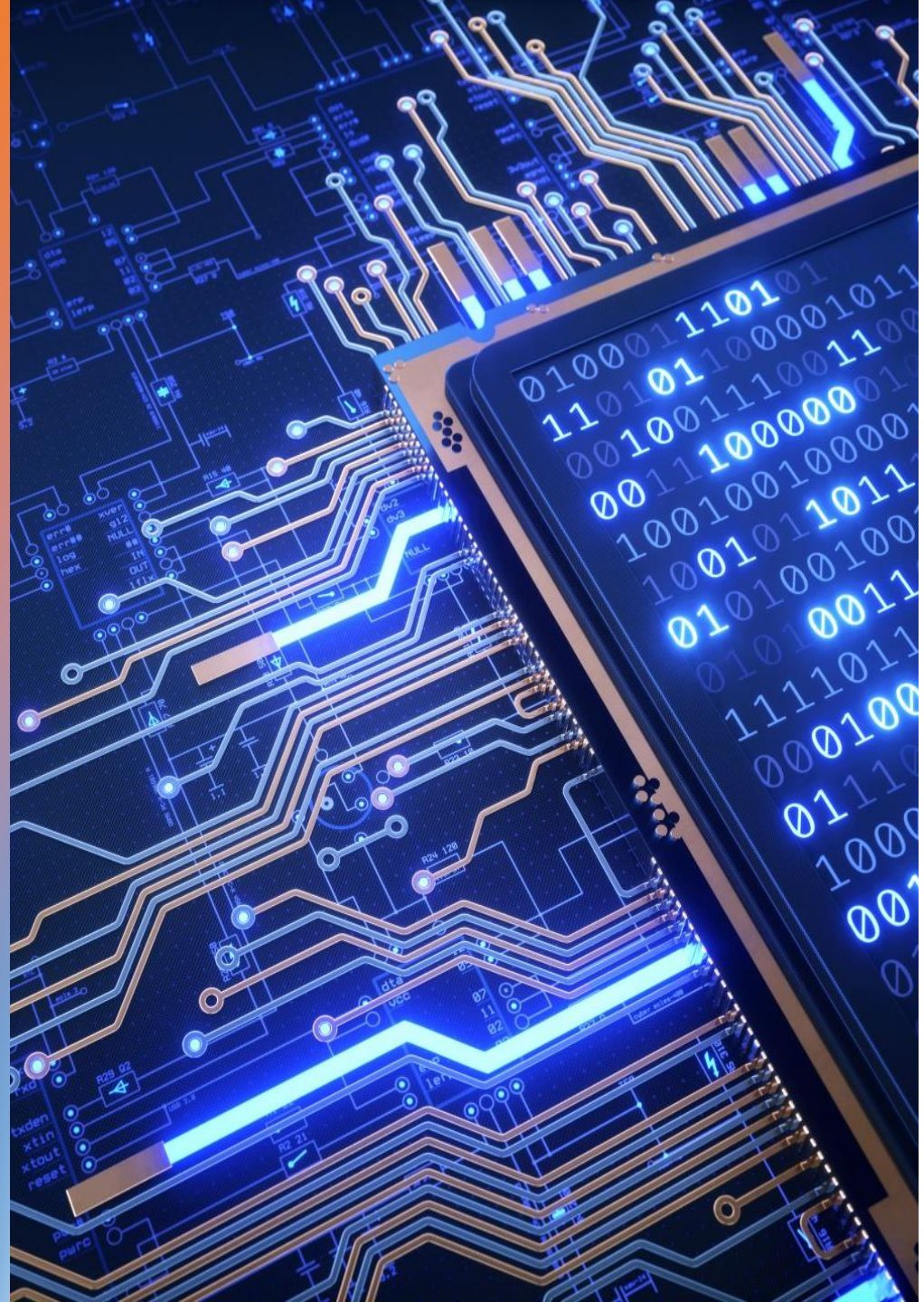
Stephen Aldrich
Senior Information Security Specialist | St. Charles Health System

What is SQL Injection?

The insertion of an unintended SQL query submitted with an expected user supplied value into a web application. The query is then executed on the database with the intended query.

Select name, description FROM products WHERE category = ‘Gifts’

Select name, description FROM products WHERE category = ‘Gifts’ UNION SELECT username,password FROM users-- //’

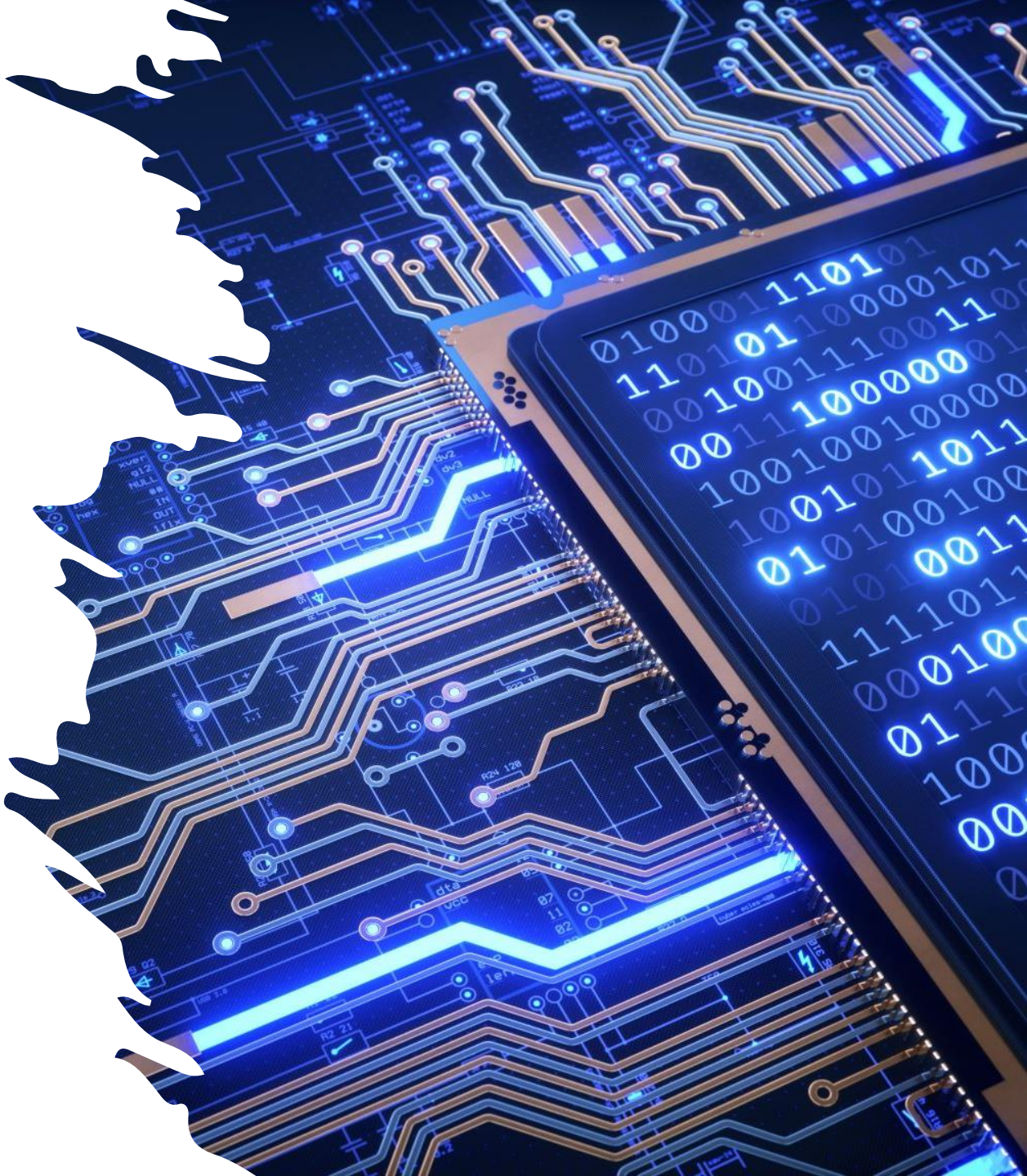


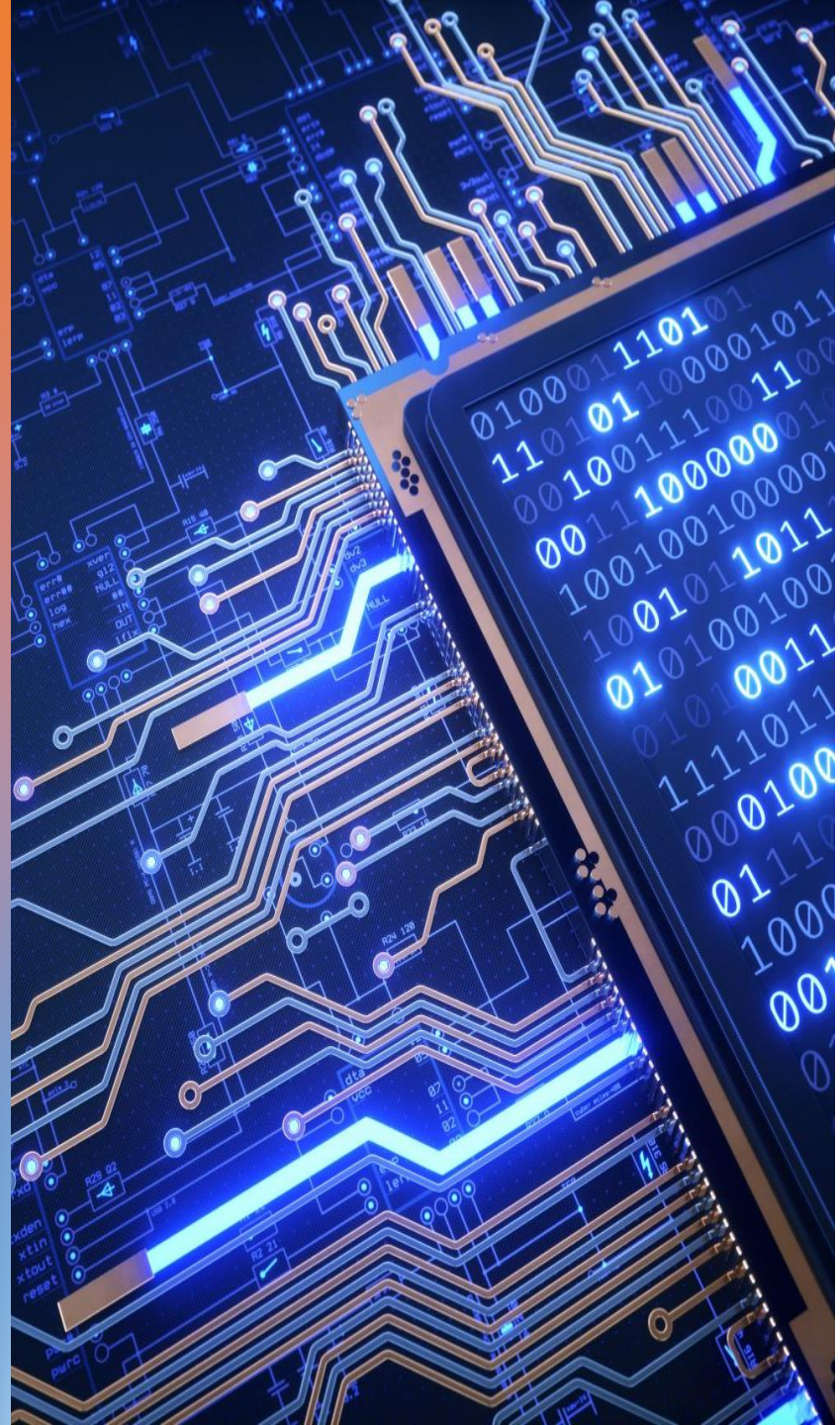
Consequences of SQL Injection

- Exposure of confidential data.
- Corruption of data integrity.
- Lose of data availability.
- Remote code execution on the application server.
- Authentication bypass.

SQL Injection Prevention

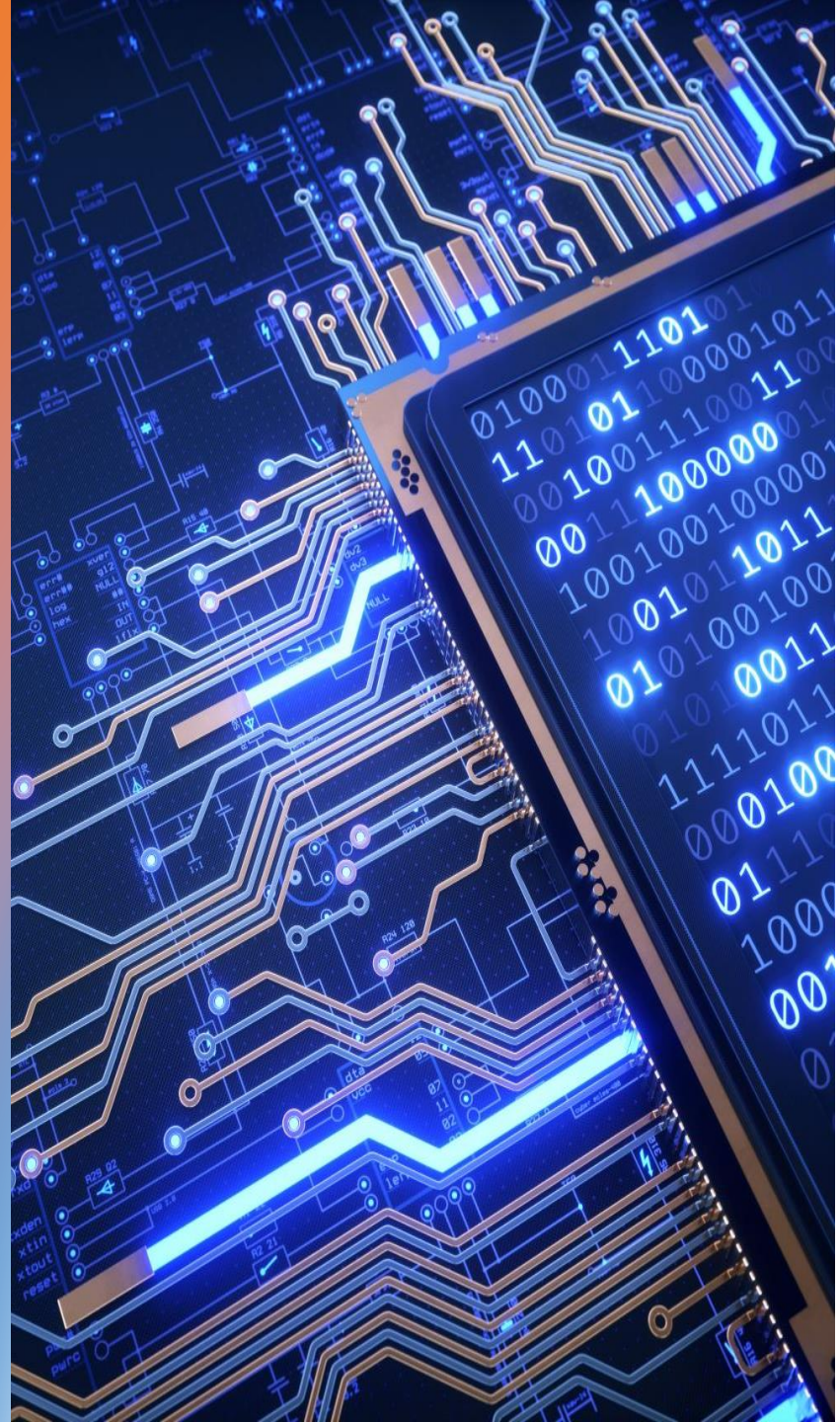
- Prepared statements with variable binding
- Stored procedures
- Input validation and data sanitation
- Turn off error messages
- Don’t allow extended URLs
- Least privilege
- Monitoring





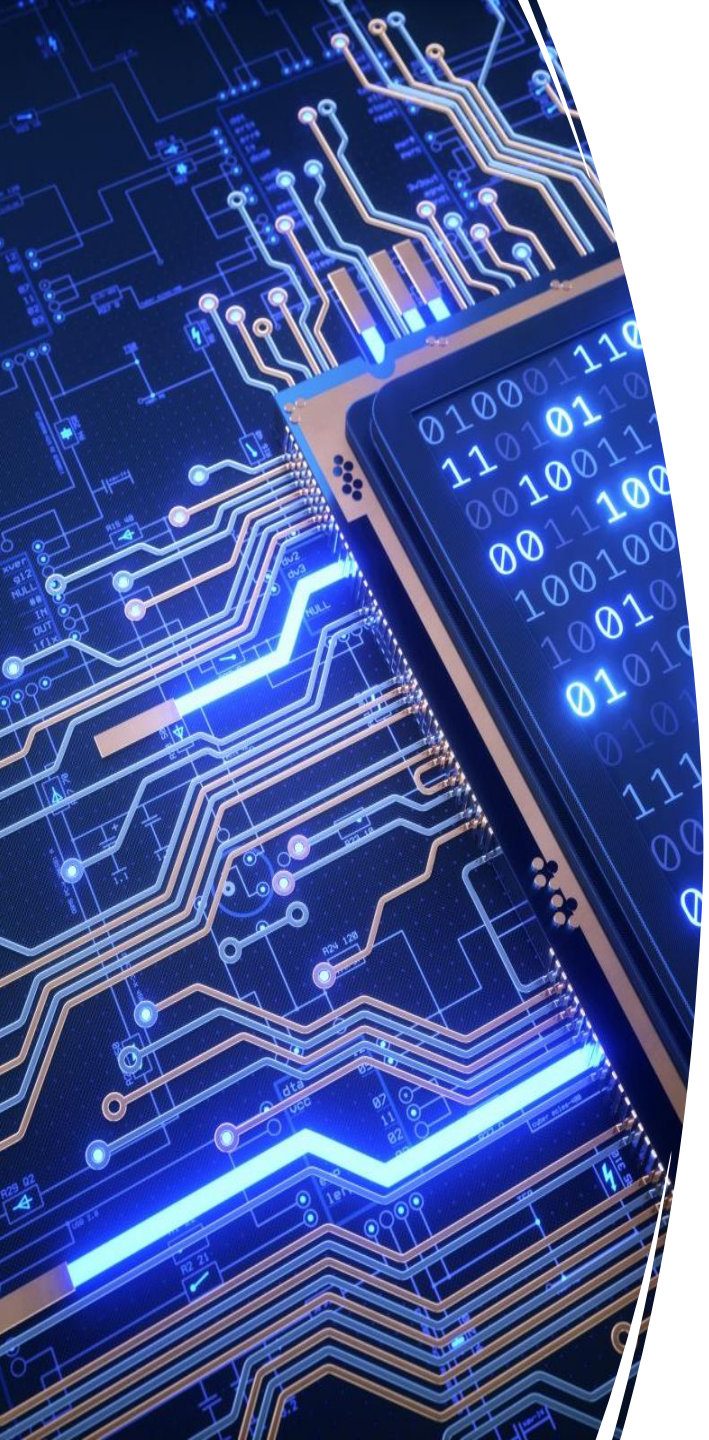
SQL Terminology

- MySQL, Microsoft SQL, Oracle
- Statement operators
  - SELECT
  - UPDATE
  - INSERT
  - DROP/DELETE
- Comments -> -- //
- WHERE Clause
- UNION
- Boolean Operators -> 1=1, 1=2, OR, AND
- Time -> SELECT CASE WHEN (1=1) THEN pg_sleep(10) ELSE pg_sleep(0) END



Testing for SQL Injection

- Find an input field on a website.
- Visualize what the SQL query looks.
- Fuzz the inputs with various characters, such as ‘, “, ;,(,),<,>,*,%,--.
- Look for errors or varying response behavior.
- Automated tools -> sqlmap, ZAP (Zed Attack Proxy), Burp Suite.
- Cheat sheets
  - SQL Injection | pentestmonkey
  - SQL injection cheat sheet | Web Security Academy (portswigger.net)



Disclaimer

- For demonstration/educational purposes only.
- Only use on systems you own or have permission to test/attack.
- DO NOT attempt at work or on the Internet.

Demos

- PortSwigger Academy
  - Web Security Academy: Free Online Training from PortSwigger
- DVWA
  - GitHub - digininja/DVWA: Damn Vulnerable Web Application (DVWA)

Topics

- Authentication Bypass
- UNION based SQL injection
- Blind SQL injection

Demo 1 - Authentication Bypass

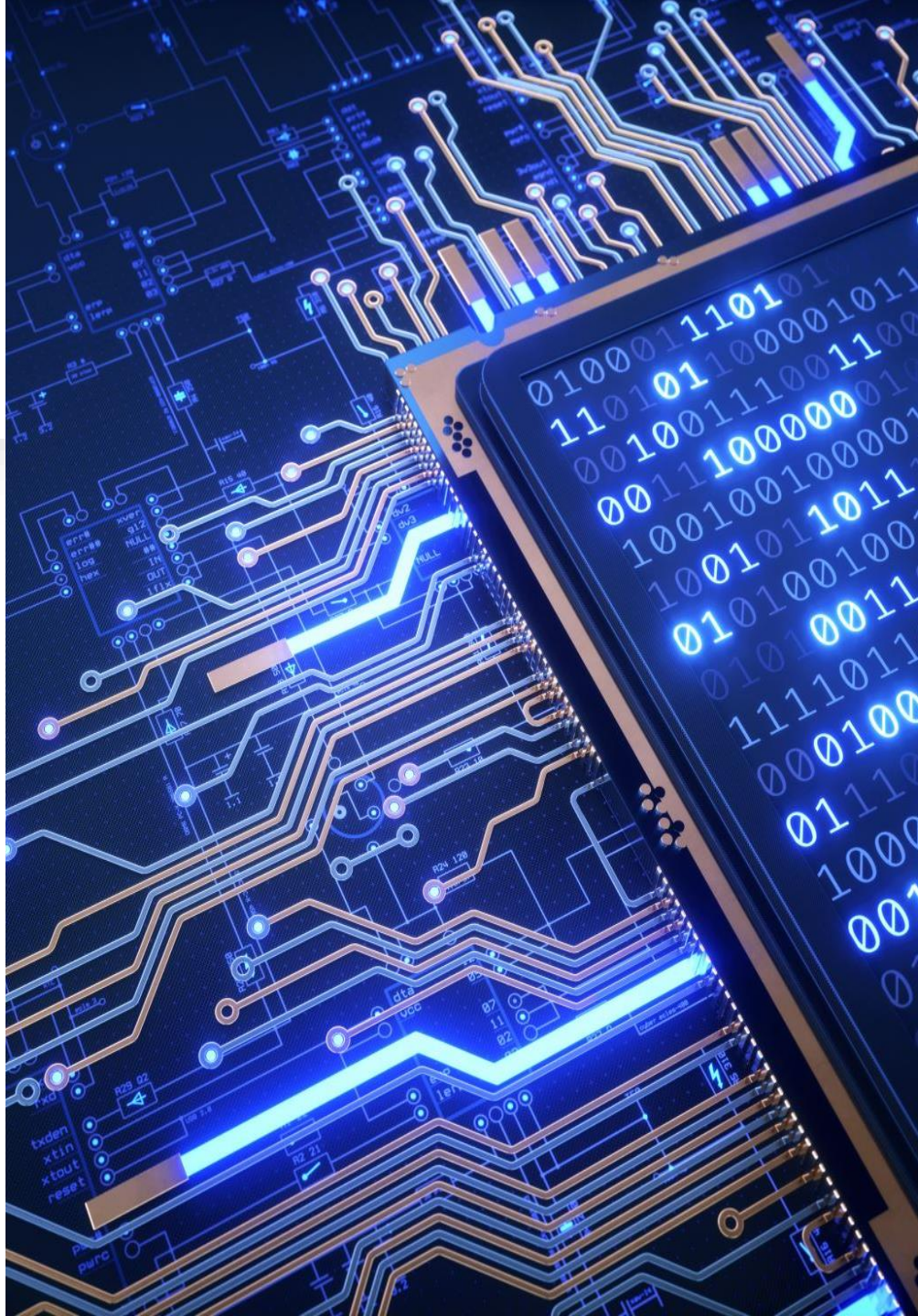
Allows an attacker to bypass authentication on a website.

Demo 2 – UNION-based SQL Injection

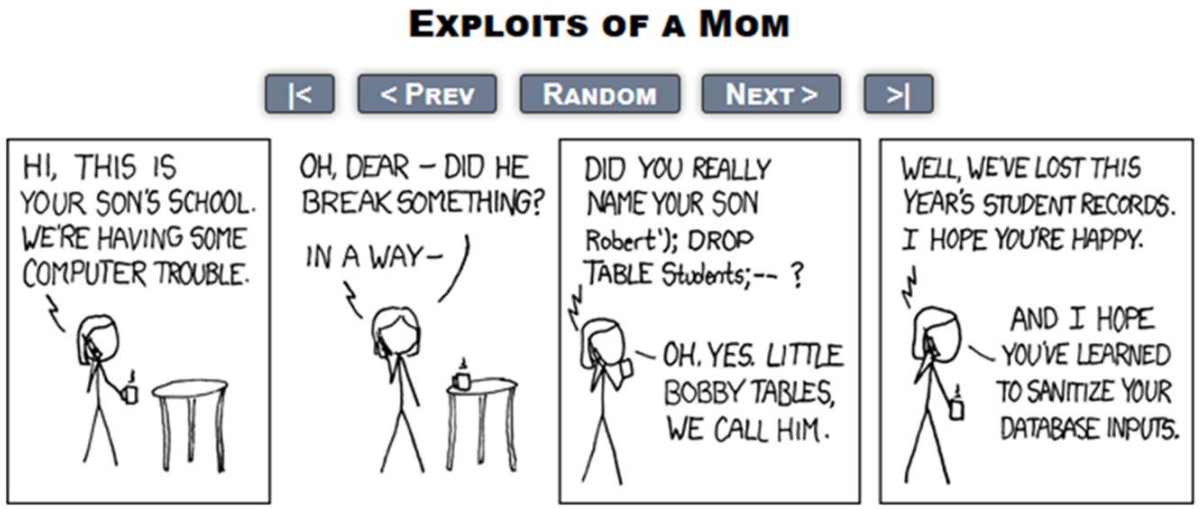
- Enables execution of an extra SELECT statement allowing for the retrieval of unintended data from a database.
- Requires two things.
  - Query must return the same number of columns.
  - Data types in columns must match.
- Determine number of columns.
  - UNION SELECT NULL-- //
  - ORDER BY 1-- //
- Determine data type of columns.
  - UNION SELECT ‘a’,NULL,NULL-- //

Demo 3 – Blind SQL Injection

- Uses Boolean logic or time-based queries to make true or false requests to the database.
- Information is inferred based on the response.
- Tedious and time consuming.
- Good case for using automated tools.

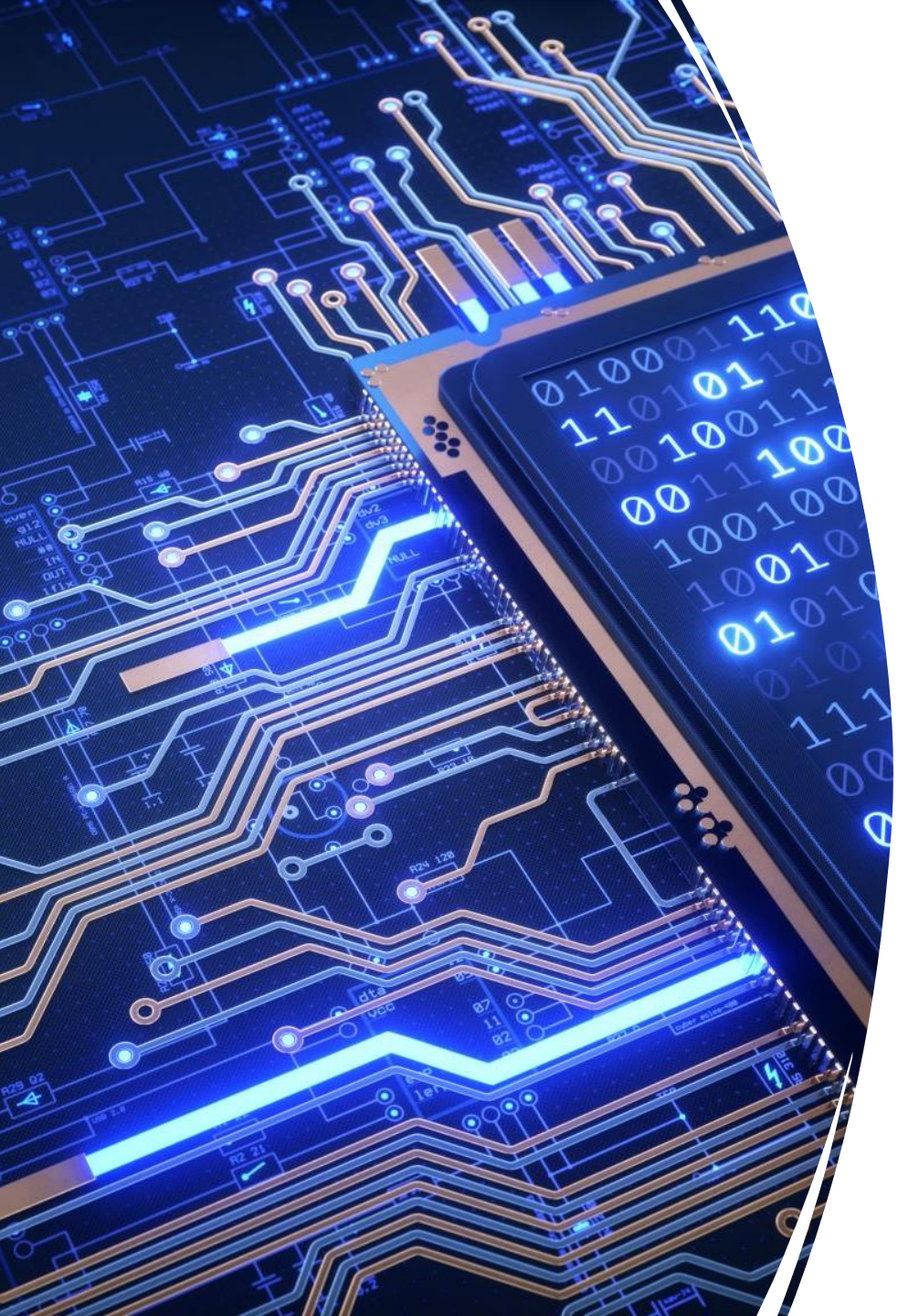


Questions?



https://xkcd.com/327

Email contact: cinderbeast@hotmail.com



Resources

- SQL Injection | OWASP Foundation
- What is SQL Injection? Tutorial & Examples | Web Security Academy (portswigger.net)
- SQL Injection - SQL Server | Microsoft Learn
- SQL Tutorial (w3schools.com)
- sqlmap: automatic SQL injection and database takeover tool
- ZAP (zaproxy.org)
- Download Burp Suite Community Edition - PortSwigger