CRS

AMRITA VISHWA VIDYAPEETHAM

SQL-INJECTION VULNERABILITY DETECTION

PRESENTED BY

P Chinni Krishna Kowsik

H Uday Reddy

CRS

Introduction

1. SQL stands for Structured Query Language.

2. SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database.

3. Cheat codes

- admin' OR '1'='1
- admin or 1=1#
- admin'--

https://demo.testfire.net/login.jsp

CRS

Objectives

- Identify and mitigate SQL injection vulnerabilities in web applications.
- Protect sensitive data from unauthorized access, modification, or deletion.
- Prevent attackers from gaining unauthorized control of web applications.
- Reduce the risk of data breaches and other security incidents.

CRS

Problem Identification

problem # 1

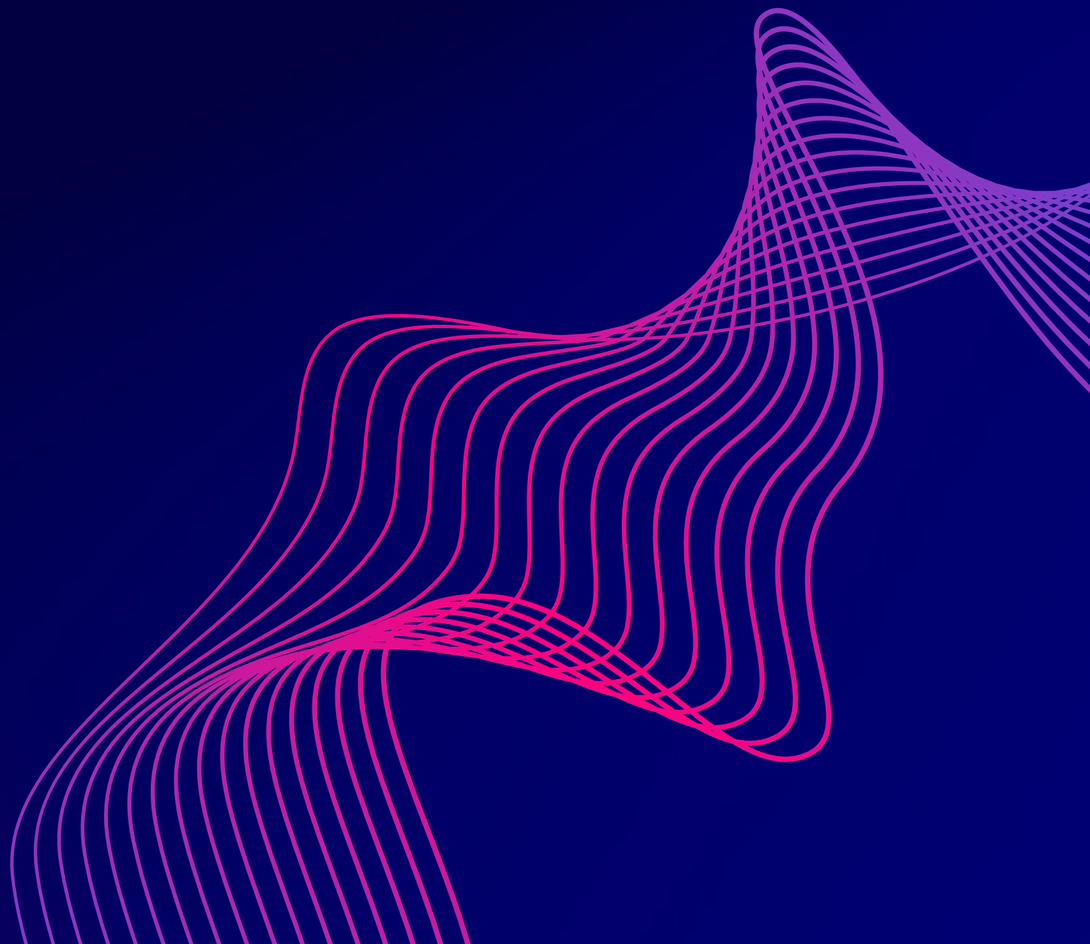
Inadequate Input Validation

problem # 2

Generate false positives and mutated payloads

problem # 3

Use of dynamic SQL



Tools 

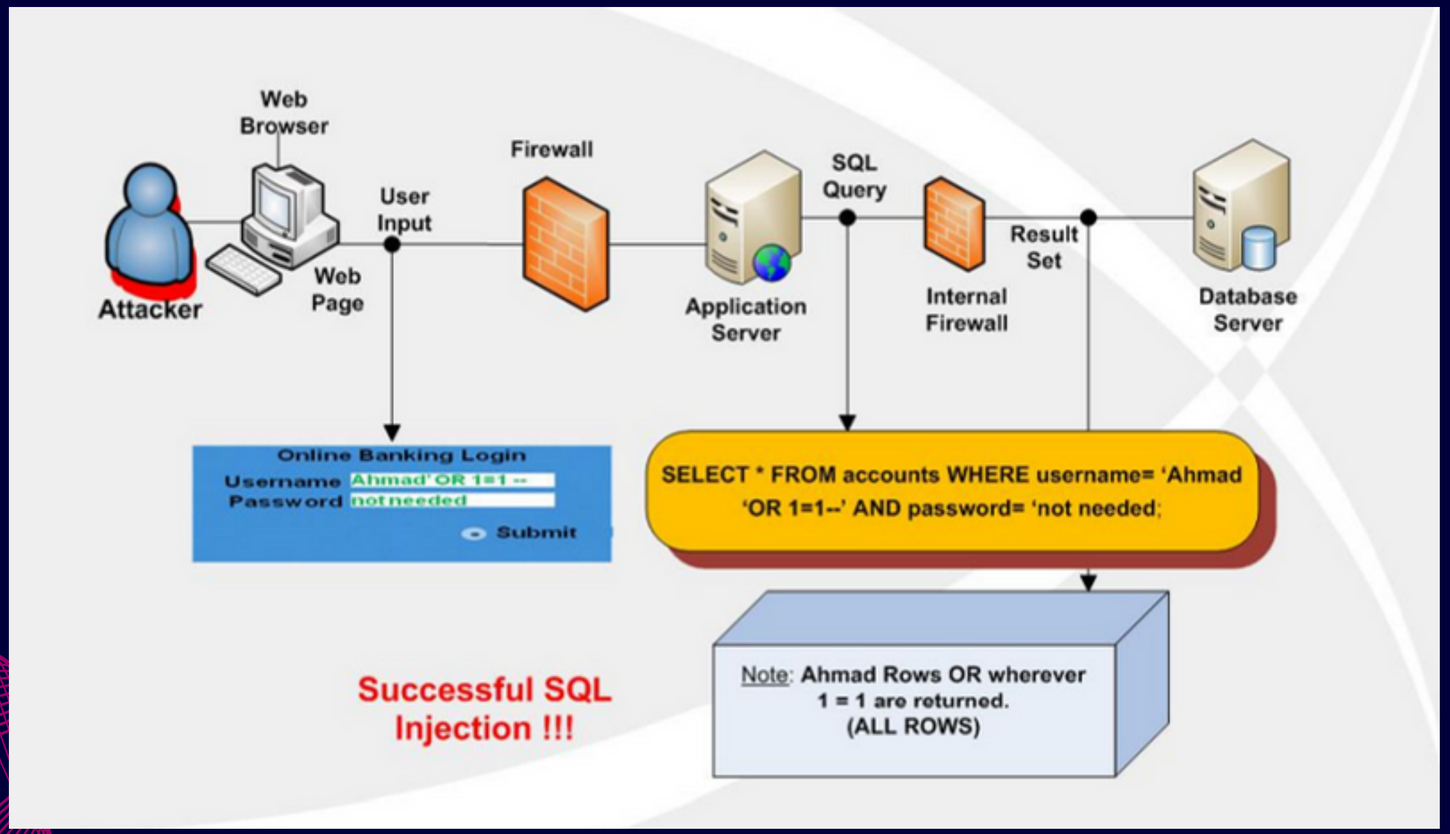
- sqlmap
- nikto
- AppScan

Algorithms 

- fuzz technique
- model checking
- Pattern matching

CRS

Block Diagram :



CRS

Project Statements

- SQL injection attacks are a serious security vulnerability that can allow attackers to gain unauthorized access to sensitive data.
- Static analysis tools are not always effective at detecting SQL injection vulnerabilities, especially those that are protected by white or black lists.
- There is a need for a more effective way to detect SQL injection vulnerabilities, especially in web applications with complex input validation logic.

CRS

Preventing SQL injection

1. Parameterized Queries (Prepared Statements)

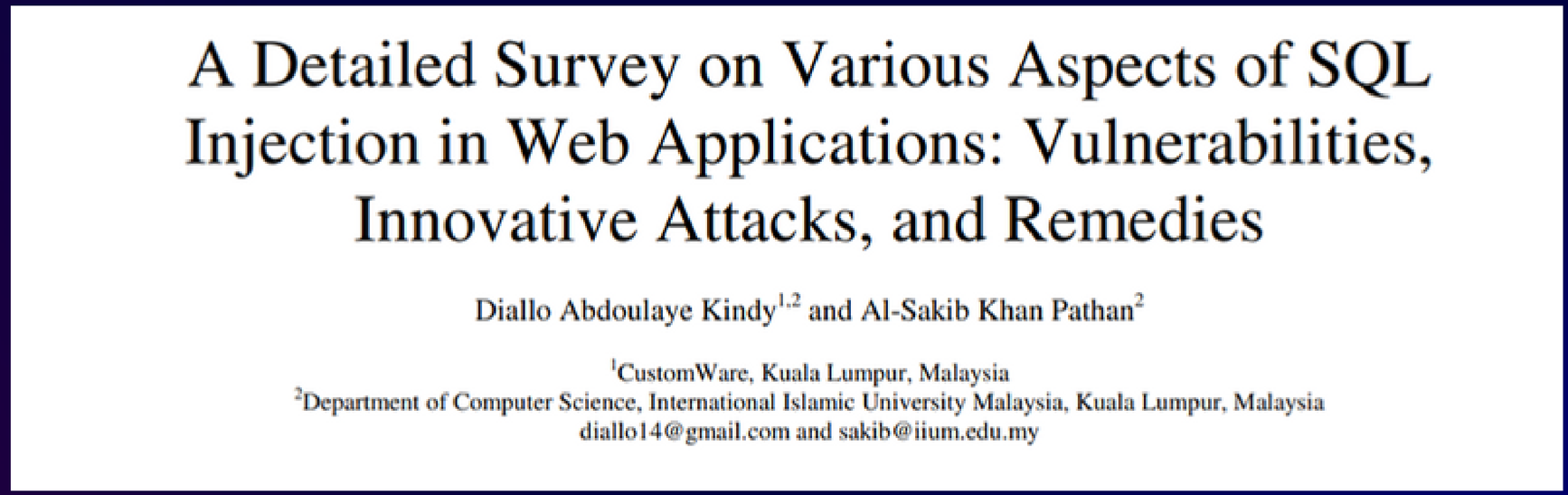
2. Least Privilege Principle

3. Web Application Firewalls (WAFs)

4. Regular Security Testing

CRS

Base Paper



A Detailed Survey on Various Aspects of SQL Injection in Web Applications: Vulnerabilities, Innovative Attacks, and Remedies

Diallo Abdoulaye Kindy[1,2] and Al-Sakib Khan Pathan[2]

[1]CustomWare, Kuala Lumpur, Malaysia
[2]Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia
diallo14@gmail.com and sakib@iium.edu.my

Link : https://arxiv.org/ftp/arxiv/papers/1203/1203.3324.pdf

CRS

References

1	MITRE, Common Weakness Enumeration. https://cwe.mitre.org/data/index.htmlHalfond W. G., Viegas, J., and Orso, A., A Classification of SQL-Injection Attacks and Countermeasures. In Proc. of the Intl. Symposium on Secure Software Engineering, Mar. 2006.
2	Damn Vulnerable Web Application (DVWA), available at: http://www.dvwa.co.uk/, last accessed 11 June, 2013.
3	"OWASPD – Open Web Application Security Proj ect. Top ten most critical web application vulnerabilities," 2005.
4	L. Auronen, "Tool-Based Approach to Assessing Web Application Security," Helsinki University of Technology, November, 2002

CRS