DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (OIST)

A NOVEL TECHNIQUE TO PREVENT SQL INJECTON AND XSS ATTACKS USING KMP STRING MATCH ALGORITHM

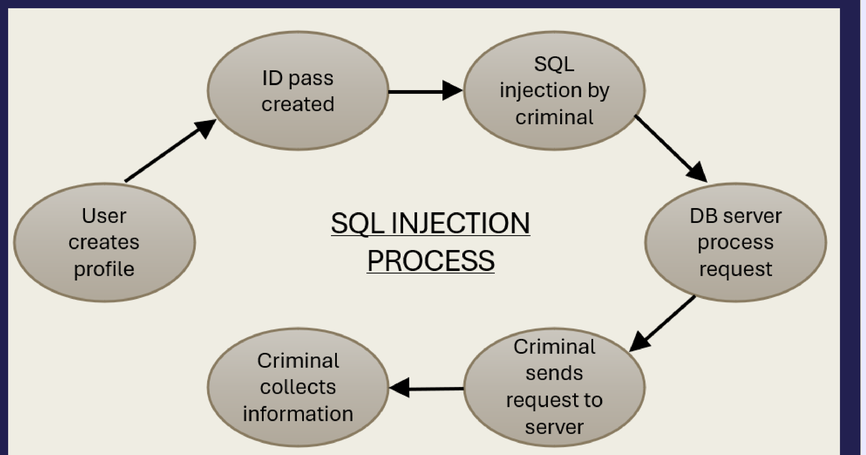
Abstract

Structured Query Language (SQL) injection and cross-site scripting remain a major threat to data-driven web applications. Instances where hackers obtain unrestricted access to back-end database of web applications so as to steal, edit, and destroy confidential data are increasing. This project presents a technique for detecting and preventing these threats using Knuth-Morris-Pratt (KMP) string matching algorithm

SQL Injection Attacks

SQL injection is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application's web server.

- Boolean-based SQL injection or tautology attack
- Union-based SQL injection
- Error-based SQL injection
- Batch query SQL injection/piggy backing attacks
- Hexadecimal/decimal/binary variation attack



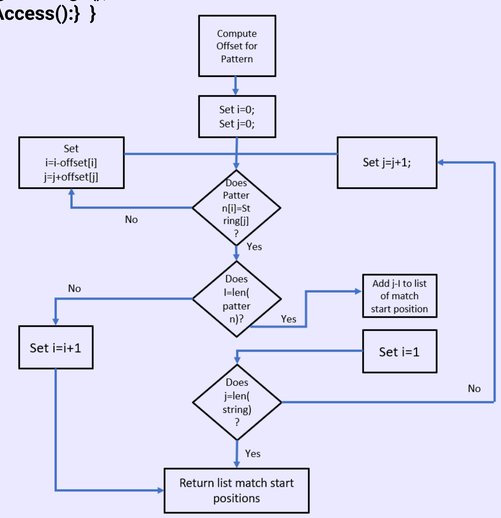
Objective

- Validate the effectiveness of the proposed technique in mitigating SQL injection and XSS attacks.
- Measure security levels through various test cases including SQL injection, XSS, and encoded injection attacks.
- Address the threats posed by SQL injection and cross-site scripting (XSS) in data-driven web applications.
- Develop a detection and prevention technique using the Knuth-Morris Pratt (KMP) algorithm.

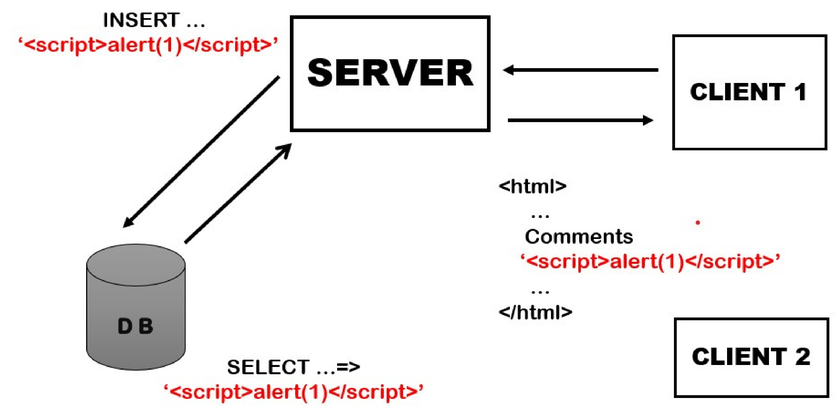
KMP Algorithm

KMP string matching algorithm is used to compare user's input string with different SQL injection and XSS attacks patterns that have been formulated. The algorithm goes thus:

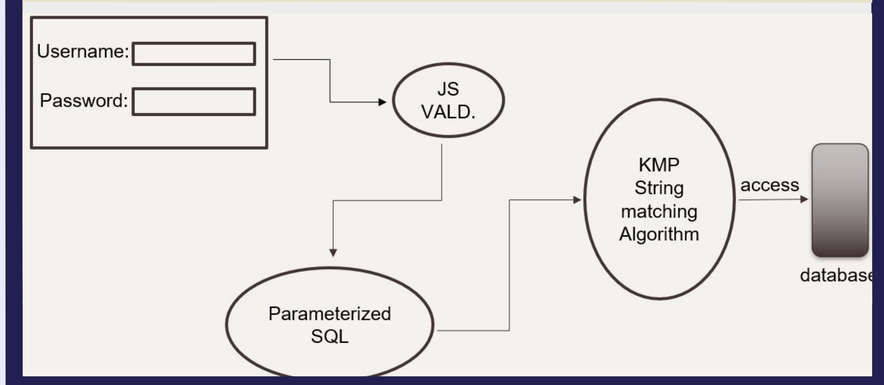
```
I=\sum_{i=0}^{n}f_{i}
Where f is the user's input from each form text field  filter (1) {data = convert
ASCIItoString(1):
            if (data < >" ") {
                a = checkBooleanBasedSqli(data);
                b = checkUnionBasedSqli(data);
                c = checkErrorBasedSqli (data);
                d = checkBatchQuerySqli(data);
                e = checkLikeBasedSqli(data);
                f = checkXss(data);
    if (true (a||b||c||d||e||f)){
        blockUser();
        resetHTTP();
        warning Message()}
    else (grant Access():} }
```



Cross Site Scripting



Flow of Project



Conclusion

This project presents a fresh approach aimed at identifying and halting SQL injection and XSS attacks effectively Initially, it delved into studying different attack types and their patterns. It then devised a parse tree to visually represent these patterns. Leveraging this tree, a filter() function was created, employing the KMP string matching algorithm, which proved capable of both detecting and preventing these malicious attacks

TEAM MEMBERS: Ayush Verma , Aditya Raj, Anjali Verma , Esha Sharma

GUIDE: Prof. Swati Shilpi