A PROJECT REPORT ON

“Detecting SQL Injection Attacks using AST”

SUBMITTED BY

Miss. Kirti Chiplunkar	Exam No. 15
Miss. Sonal Dimbar	Exam No. 19
Miss. Stuti Thorat	Exam No. 74

UNDER THE GUIDANCE OF

PROF. PRADNYA GULHANE

सत्याला मरण नाही

DEPARTMENT OF COMPUTER ENGINEERING

ALL INDIA SHRI SHIVAJI MEOMRIAL SOCIETY’S
INSTITUTE OF INFORMATION TECHNOLOGY
KENNEDY ROAD, NEAR R.T.O. PUNE-411001

SAVITRIBAI PULE PUNE UNIVERSITY
2019-2020

ACKNOWLEDGMENT

It gives us immense pleasure in presenting the project report on “Detecting SQL Injection Attacks using AST” The success and the outcome of this report required a lot of guidance. We are very grateful to our guide **Prof. Pradnya Gulhane** who has provided expertise and encouragement. We thank ma’am who provided vision and knowledge that was very helpful throughout the research. All that we have done is only due to the great guidance. We also express our gratitude to **Dr. S.N. Zaware** Head of Computer Engineering Department, AISSMS Institute of Information Technology, for the valuable support.

We would also like to extend our sincere thanks to Principal Dr.P.B. Mane, for his dynamic and valuable guidance throughout the project and providing the necessary facilities that helped us to complete our dissertation work.

Miss. Kirti Chiplunkar
Miss. Sonal Dimbar
Miss. Stuti Thorat

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Overview

1.2 Problem Definition

A Python program to develop a new policy based Proxy Agent, which classifies the request as a scripted request or query based request, and then, detects the respective type of attack, if any in the request.

1.3 Objective

To detect both SQL injection attacks as well as the Cross-Site Scripting attacks.

1.4 Project Scope

- This system will be useful for finding SQL injection attacks as well as the Cross-Site Scripting attacks.

1.5 Methodology

A developer defines a SQL query to perform some database action necessary for their application to function. This query has an *argument* so that only desired records are returned, and the value for that argument can be provided by a user (for example, through a form field, URL parameter, web cookie, etc.).

A SQL attack plays out in two stages:

Research: Attacker tries submitting various unexpected values for the argument, observes how the application responds, and determines an attack to attempt.

Attack: Attacker provides a carefully-crafted input value that, when used as an argument to a SQL query, will be interpreted as part of a SQL command rather than merely data; the database then executes the SQL command as modified by the attacker.

.

Chapter 2

SOFTWARE REQUIREMENTS SPECIFICATION

2.1 Dependencies

Dependencies

Numpy, Python sqlite3, ast,re modules,Flask

.

2.2 System Requirements

2.2.1 Software Requirements(Platform Choice)

1. **Operating System:** Windows7 and higher / Linux
2. **IDE :** PyCharm
3. **Language Support :** Python 3.6 and higher

2.2.2 Hardware Requirements

1. **Disk Space:** Minimum disk space of 500 GB is expected for computations and storage means.
2. **Processor:** i5 CPU @1.60 GHz 1.80 GHz, 32-bit x32 OR 64-bit x64 pro- cessor is preferable.
3. **Memory:** 4 GB RAM and above , .
4. **Display:** 1600 * 900 minimum display resolution for better display.

Chapter 3

PROJECT IMPLEMENTATION

3.1 Tools and Technologies Used

.

1. **NumPy:**

   NumPy is a package in Python used for Scientific Comput- ing. NumPy package is used to perform different operations. The ndarray (NumPy Array) is a multidimensional array used to store values of same datatype. These arrays are indexed just like Sequences, starts with zero. NumPy uses much less memory to store data.

2. **Flask:**

   Flask is a lightweight WSGI web application framework. It is designed to make getting started quick and easy, with the ability to scale up to complex applications. It began as a simple wrapper around Werkzeug and Jinja and has become one of the most popular Python web application frameworks.

3. **Ast module :**

The ast module helps Python applications to process trees of the Python abstract syntax grammar. The abstract syntax itself might change with each Python release; this module helps to find out programmatically what the current grammar looks like. An abstract syntax tree can be generated by passing ast. Algorithm Details

- ## SQL injections

SQL injections is a code injection technique used to attack data driven applications in which malicious SQL statements are inserted into an entry field for execution.

SQL is one of the web attacks used by hackers to swipe data from organizations. It is an application layer attack. In this mechanism, a malicious SQL command is executed by the web application, exposing the backend database. An SQL injection attack can occur when a web application utilizes user supplied data without proper validation or encoding as part of a SQL query. Injected SQL interdiction can reform SQL statements and encompasses the security of web applications.

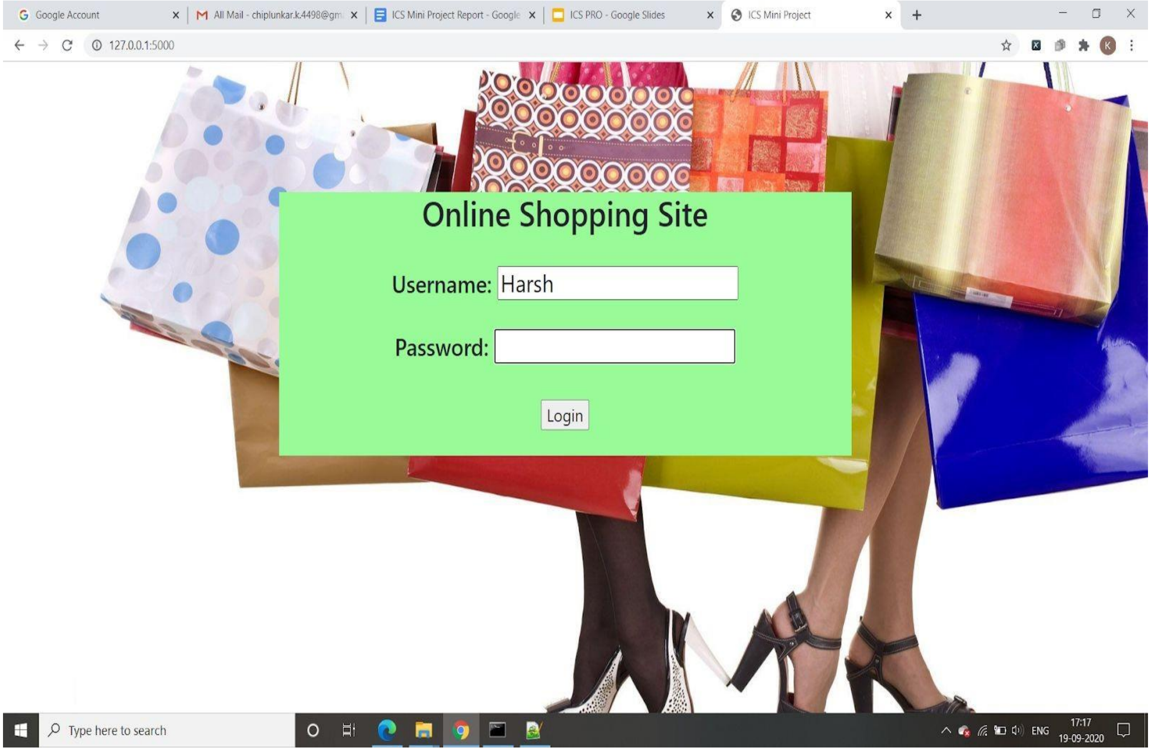
3.1.1 Algorithm 1 :

ABSTRACT SYNTAX TREE(AST)

- Python has a built-in AST module that lets you inspect ,parse and edit code.
- AST is a data structure that makes it easy to analyze ,inspect and edit programming language code.
- Abstract trees represents relation between objects, operators and language expressions
- After traversal of the ASTs if differences are found ,then an SQL injection is reported.

Chapter 4

4.1 Screenshots



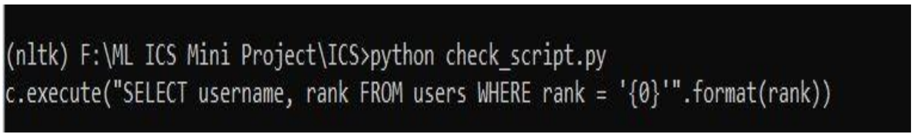
Online Shopping Site

Username: Harsh

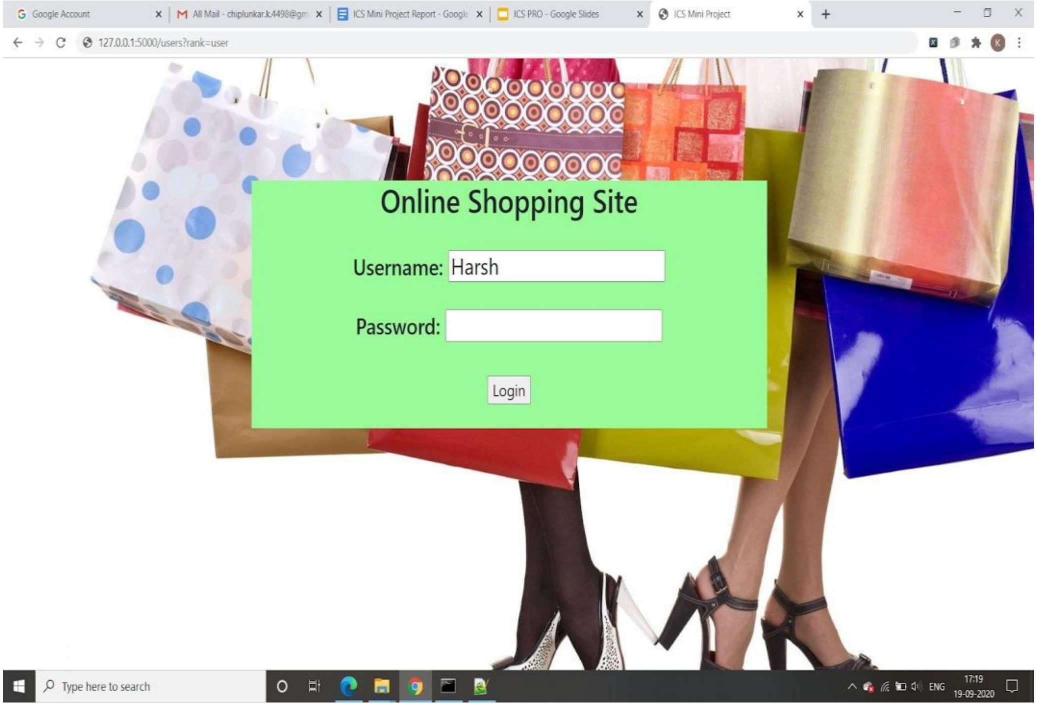
Password:

Figure 4.1:. Simple Shopping Site

Check_script.py used for checking dangerous queries using Python AST module.



```
(nltk) F:\ML ICS Mini Project\ICS>python check_script.py
c.execute("SELECT username, rank FROM users WHERE rank = '{0}'".format(rank))
```



127.0.0.1:5000/users?rank=user

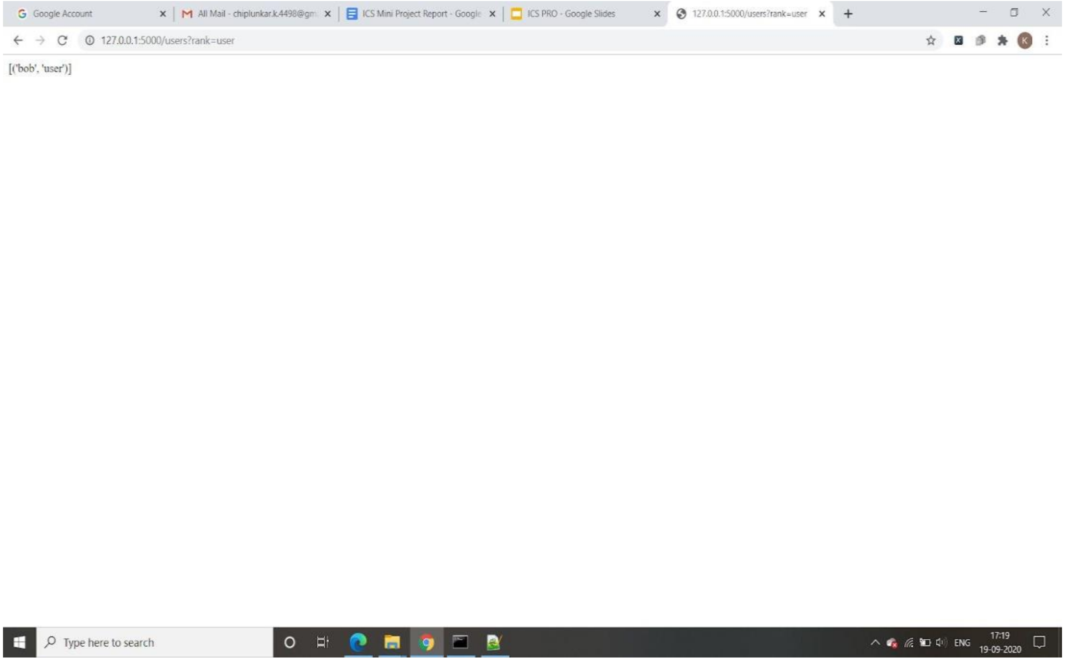
Online Shopping Site

Username: Harsh

Password:

Login

Figure 4.2:. Demonstrating SQL Injection



Google Account
All Mail - chiplunkar.k.4498@gm
ICS Mini Project Report - Google
ICS PRO - Google Slides
127.0.0.1:5000/users?rank=user
Type here to search
ENG
17:19
19-09-2020

127.0.0.1:5000/users?rank=user

```
[('bob', 'user')]
```

Figure 4.3:. SQL Injection

Chapter 5

CONCLUSIONS

5.1 Conclusion

It can be concluded that development of effective solutions for prevention and detection of SQL injection attacks is therefore of utmost importance to secure the web applications from being exploited by the attackers.Unfortunately ,these security aspects are often overlooked or given less priority during application development.As a result, theft of huge amounts of sensitive data using SQL injection attacks have become very common.So using the AST technique some of these threats can be detected and also be corrected at some extent.