**# Red flag**

Project for DDOS, SQL injection version v.1

Group : 2

Name : Arun Khajuria, Iris Jangulli, Isaac Flores Osnaya.

**DDos attack** :

Slowloris is a type of denial of service attack tool invented by Robert "RSnake" Hansen which allows a single machine to take down

another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

**SQL injection blind** :

Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application's response. This attack is often used when the web application is configured to show generic

error messages but has not mitigated the code that is vulnerable to SQL injection. When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query's syntax is incorrect. The blind SQL injection

is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions.

This makes exploiting the SQL Injection vulnerability more difficult, but not impossible.

#Enviroment used: python 3.6, pyqt5

IDE used: pycharm

Download Python: https://www.python.org/downloads/

Installation:

pip install request

pip install pyqt5

# Usage:

* Run redflag\_main.py
* Url should have input query for SQL injection

example: <https://example.com/?q=>

* Url or IP address of the attacking machine for Slowris attack

Example: 193.90.55.111

* locate the data.txt location Redflag/UI/data.text. if need you want to input more malicious inputs append data file.
* Note : if there is any error in script redflag\_main.py access the attacking scripts in command prompt manually example : python sql.py.

#RUN :

