We are working on three different exploits in this project which include

1. SQL Injection with Kali
2. CSRF attack with Kali
3. XSS attack with Kali

***SQL Injection:***

1. We use SQL Map which is a pen test tool comes with the Kali Linux operating system, we use this to hack vulnerable website and get access to a database.
2. It supports a wide range of Relational databases like MySQL, Oracle, and SQL Server etc.,

SQL Map Steps:

1. Target/Vulnerable website: DVWA installed on Ubuntu Machine
2. **Checking if site is vulnerable to SQL Injection:**
   * 1. Give a ‘ or “ at the end of URL if it return a SQL error, then the website is vulnerable to SQL injection.
3. **Finding the DB used using SQLMAP:** 
   * 1. Type sqlmap -u <http://localhost:8080/> --dbs from kali terminal to find the name of database and schemas available.
     2. Logs will be saved under /usr/share/sqlmap/output/ folder.
4. **Finding Tables in the DB using SQLMAP:**
   * 1. Type **sqlmap -u** <http://localhost:8080/> -D **name\_of\_the\_schema –tables** from kali terminal to find the name of tables available.
5. **Finding columns on Tables in the DB using SQLMAP:**
   * 1. **Type sqlmap -u** <http://localhost:8080/> **-D name\_of\_the\_schema –tables name\_of\_the\_table –columns** from Kali Terminal
6. **Getting data from Columns:**
   * 1. Type **sqlmap -u http://localhost:8080/ -D name\_of\_the\_schema -T name\_of\_the\_table -C name\_of\_the\_column –dump** from Kali terminal.
7. **Cracking Hashed Passwords:** Kali Linux has a in-built stock tools to find the type of hash and it can be identified using hash-identifier command followed by the hash value. Based on the type of hash we can proceed further.

***CSRF (Cross-Script Request Forgery):***

This attack exploits the trust of website owner on the site user.

Brief description of how to do this attack.

***Scenario***: Changing the password of the admin without having actual access.

1. Just copy the **change password code** enclosed in the form tag and save it in the local.
2. Run the html form saved in the local and then the same text fields will appear to change the password.
3. Since the form tag in the local html file will have the actual service which will make password changes it will make the change to actual password of the admin.

We need work on filtering keyword needed to be included in the Bro Scripts.