Analysis of Brute Force, XSS, SQL Injection on Bank Management System

Information Security Analysis and Audit - CSE3501

Project Report

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Team Members:

Pranav Khurana - 18BCE2513

Shashank Shukla - 18BCE2522

Mihir Agarwal - 18BCE2526

Under the Guidance of:

Prof. Murali S

Associate Professor

School of Computer Science and Engineering

Abstract

Banking systems are highly vulnerable to attacks as they contain highly sensitive information. So in this project we will try to find vulnerabilities in an existing banking website and hack into the system using mentioned tools. Then we will try to monitor the attack using an intrusion detection system. Usage of e-services in our country is growing. However, the development and the deployment of these e-services on the Internet increase the likelihood of exposure to cyber-attacks.

We will be implementing our project by performing three attacks and providing solutions for them (prevention & detection) - Brute force attack, Cross-site scripting (XSS), and SQL Injection.

Attacks

1) Brute Force Attack

It is a web attack where the hacker tries different combinations of usernames and passwords repeatedly until it logs into the user's account. Used to gain unauthorized access to a system.

Tools used

- **Hydra:** In this attacking technique, the login credentials and important details of the user will be the main target in our banking website.
- **Splunk** is used to implement intrusion detection, it detects the attack and monitors logs.
- **Fail2Ban** is an incident response framework that monitors login attempts to system services and takes immediate action when it detects an IP address that behaves suspiciously - too many password failures. The account is blocked in that case.

2) Cross-Site Scripting (XSS):

Two types of XSS used- DOM-based XSS (Document Object Model), Reflected (non-persistent) XSS attack. We will be doing the following harm using XSS- Session-hijack, Capturing keystrokes by injecting a keylogger, Stealing information like current balance, transaction information, Stealing credentials by injecting a form into the vulnerable page.

Tools used

Attack- XSSER- It contains several options to try to bypass certain filters, and various special techniques of code injection. **Burp Suite-** It is used to intercept the request and then send intercepted data into Intruder.

Detection- XSS Scanner-The XSS Scanner uses the OWASP ZAP scanning engine.
XSStrike- XSStrike analyses the response with multiple parsers and then crafts payloads.

3) SQL Injection Attack

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field to get important information. In this project we will be implementing 2 types of SQL injection attacks –

1) Union based SQL injection
2) Blind based SQL injection

Tools used:

Attack: **SQLMap** - SQLMap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers

Detection and protection: Powerfuzzer: it is a highly automated and fully customizable web fuzzer capable of identifying many types of injections like SQL, LDAP, code, commands, and XPATH, **W3af** : An open source, web application attack and audit framework. It is powerful and can detect most of the vulnerabilities in a website.