Chuckheads Final Paper

Team Chuckheads
Aaron Gardner
Zachary Priest
Matthew Crosby
Charles Burnell
Jay Capcha

April 30, 2017

1 Introduction

bla bla intro

2 Aaron’s attack

Injetion is classified by the Open Web Application Security Project as the top threat vector to web applications. An injection attack is defined by a malicious entity sends untrusted data to an interpreter as part of a command or query. This untrusted data can trick an interpreter into executing commands sent by the external malicious user, or accessing data without authorization.

SQL Injection attacks are application specific, targeted at applications running an SQL (Structured Query Language) database. Data that users enter, such as personal or financial data, is entered into a SQL database using pre-written SQL queries as strings, with the user supplied information being concatenated into the body of the query. This is very easy to exploit, as attackers simply send text that exploits SQL syntax. For example: consider a simple login screen. The user is presented with two text inputs, one for username and one for password. A normal user would simply type something like ”John Doe” as their username and ”myPass” as their password. The SQL query on the other end might look like this:

```
SELECT * FROM Users WHERE Name = ”John␣Doe” and Pass =”myPass”
```

A malicious user can exploit this SQL syntax in several ways, such as entering their username and password as ”’ or ””=”’. This would create the following query:

```
SELECT * FROM Users WHERE Name =”” or ””=”” AND Pass =”” or ””=””
```

Since the expression ’or ””=””’ is always true, this query is valid and will return all the rows from the Users table.

3 Zach's attack

4 Matt's attack

5 Jay's attack

6 Chuck's attack

7 Extra attack

8 Conclusion