**PROJECT PROPOSAL**

**Team Members and ID:**

1. **Joseph Strickland - 801078219**
2. **Shruti Rabara - 801075189**
3. **Eric Baca - 801166050**

**Tool and its Summary:**

Laravel is a PHP framework which includes a variety of helpful tools. The Query Builder automatically parameterized/sanitizes input making it penetration proof with very little effort from a development standpoint. By using this tool in an application, you can prevent harmful SQL injections that could endanger the integrity of the application’s data. By utilizing the easy-to-use framework syntax, laravel provides protection against SQL injections with little effort.   
  
Laravel also provides other security-based features for development such as authentication and authorization. While we will not demonstrate some of these additional security features, laravel should be considered when developing a web application due to its extensive and useful security features. We will be focusing our project on laravel’s query building security functionality.

**Motivation:**

Our motivation for using Laravel as the tool for our penetration testing demo is because it provides a good defense against SQL injection attacks on web applications through its database query builder tool. More specifically, it uses PDO, PHP data object, parameter binding to correctly pass in the clean and sanitized strings into the query builder as query bindings. Therefore, this query builder tool not only makes it convenient to create and run database queries but also makes it safe for us to do so without worrying about SQL injection attacks.

**Presentation Approach:**

We are going to create a very simple web application to demonstrate the secure programming framework laravel. For the front end, we are going to create simple HTML views that will showcase inputs from the user via a form. This form will allow for different types of inputs such as text, date, and other relevant information to be placed into a database. We are going to style the HTML pages with CSS to make them look professional.

After having created the frontend HTML and CSS, we are going to utilize a PHP backend to send information to the database. This backend will be where we demonstrate the laravel framework and how it combats SQL injections. The backend will also demonstrate any interactivity we have on the simple web application’s front end. On top of utilizing PHP with the laravel framework, we will create a simple MySQL database that has a schema designed for the frontend form submission.

The actual presentation will be a video that demonstrates this basic web application. We will showcase the basic functionality through the front-end HTML pages and then submit a form to the database. In the presentation, we will try malicious and legitimate inputs to show the reaction from the application. When testing the malicious inputs, we will have an error message occur due to the laravel framework catching the malicious input and rejecting it. We will also showcase correct inputs and how the application handles processing the information. Finally, the presentation will showcase some of the source code relating to laravel and how it prevents malicious inputs from being submitted to the database. By demonstrating the simple web application and displaying the laravel source code, we will be able to effectively showcase the secure programming framework laravel, and how stopping SQL injections are important for the integrity of every piece of software.