I. The Vulnerable Site

A. Setup

1. Extract files to site's directory
2. Configure server2.py to the desired port (line 33)
3. Run python3 server2.py

B. Components

1. server2.py (the python server that hosts the site)
2. Index.html (the html for the site)
3. Static (contains jquery library)
4. Post.html contains the information submitted by the user

C. Protections

1. To prevent this attack, we decided to validate the input. The user is not able to submit text in the discussion post box that contains < or > to prevent scripts from being injected. The version with the modified security is named secure.html

II. The Attacker Server

A. Setup

1. Extract files to server's directory
2. Configure server2.py to the desired port (line 29)
3. Run python3 server2.py
4. Have the index.php file in the same directory as the PHP server
5. When the index.php file receives the PHP request from the server, it puts the output of the file into test.txt

III. The Key Logging Program

A. How it works technically

1. Uses variable typedString to collect user input
2. Creates event listeners for keydown and click
3. For keydown events, the keypresses are added to the typedString variable
4. When the user hits enter or clicks, the typedString is sent to the attacker server using PHP
5. After the post request, the typedString variable is reset.

B. Role in demo

1. The keylogger script is injected through cross site scripting and sends user input to the attacker's server.

C. Setup

1. Paste the keylogger script into the forum input
2. Hit enter