Team Name: Polaris

Team members:
Prajakta Shinde (1209404609)
Shibani Singh (1209404128)

Polaris: XSS Prevention for PHP files

CSE 545 - Software Security : Final Project

- **Problem statement:**

  As we have learnt in CSE 545, "We should never trust user input". There are many possible ways in which users can inject malicious code using input fields provided to him by a web application. Validating user input for all such cases is tedious and time consuming. So, we have developed a tool Polaris, which sanitizes user input on behalf of the developer to prevent XSS. Already available tools, that we have come across perform such checks at the run time. Whereas, in the case of Polaris, the developer just has to provide his PHP file and Polaris will create a new PHP file, which is more robust against XSS attacks. This new file can then be used directly by the developer.

- **Implementation Approach:**

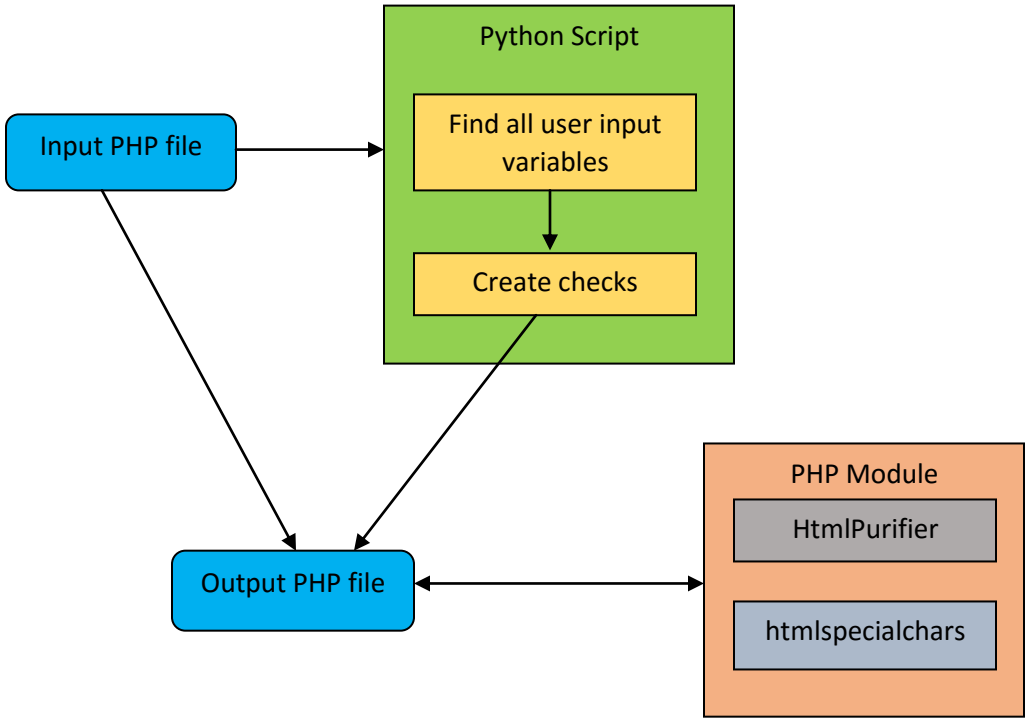
  One approach can be to sanitize the user input every time it is used. This approach is very inefficient because, if the user input is being used at many places and in different ways, we need to make sure, that it has been sanitized each time before being used.

  Second and the best approach to deal with XSS attacks would be to sanitize the user input as soon as it enters the server side and then this sanitized value can be used anywhere.

Polaris tool consists of a python script, which accepts a PHP file as an input and parses it to find all the user input variables. It then creates check statements that should be performed at run time and creates the output file using these statements and the original file.

These checks are performed using a separate PHP module, which acts as a wrapper and uses the original functionality of the libraries, HtmlPurifier and htmlspecialchars.

Fig.1 Flow Diagram



- **Usage:**

  Polaris is a package that contains :

  Setup.py : This is the first file to be executed and it needs to be executed only for the first time. It downloads and installs all the required libraries.

  Makefile : It creates executable file for the python script. This too has to be executed only once.

testxss.py : This script accepts 2 input arguments: input file name and desired name of the output file.

clean.php : This is the PHP module that wraps the functionality of 2 libraries: HtmlPurifier and htmlspecialchars.

- **Features:**
  - Escapes special characters such as: < > ' " & \ / etc.
  - Escapes comments.
  - Checks file type of the uploaded file using MIMETYPE and if there is a mismatch, it marks that file with a [WARNING].
  - Tackles attacks that use URL encoding.
  - Checks all the parameters that can be controlled by the user to perform XSS, like environment variables, cookies and server variables.

- **Limitations:**
  - Tool does not prevent the attacker from uploading malicious files. But it does mark files with a [WARNING] if a type mismatch is found. Developers should check such files before using them.
  - If multiple files are linked together, each file needs to be passed through the tool separately.
  - Designed only for Linux systems.

- **Future work:**
  - Functionality of the tool may be extended further to resolve internal linking between the PHP files by itself.
  - The tool can be modified to make it customizable.
  - More work could be done to increase the performance.
  - Sanitization can be extended for multimedia files.