







```
MSAT Interface 🗿
                                                                                                                                                                                                                                                                                                                         <u>O</u> (B) (S)
 Project Structure
                                                       Project: Alpha - (file_path)/XSSRequestWrapper.java
                                                              import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper
 D:\varma\project_alpha
   > idea
                                                              public class XSSRequestWrapper extends HttpServletRequestWrapper {
    √ es src
                                                                public XSSRequestWropper(HttpServletRequest servletRequest) {
   super(servletRequest);
}

√ scripts_module

         XSSFilter.java
                                                                @Override
public String[] getParameterValues(String parameter) {
    String[] values = super.getParameterValues(parameter);
        XSSScan.java
XSSRequestWrapper.jav
                                                                    if (values == null) {
return null;
                                                                    }
                                                                     int count = values length,

String[] encoded Values = new String[count];

for (int i = 0, i < count; i++) {

   encoded Values[i] = stripXSS(values[i]);
                                                                    return encodedValues;

    Override
    public String getParameter(String parameter) {
        String value = super.getParameter(parameter)

                                                                    return stripXSS(value);
                                                                 @Override public String getHeader(String name) {
                                                                     String value = super.getHeader(name);
return stripXSS(value);
                                                                 private String stripXSS(String value) {
```

```
MSAT Interface ②
                                                                                                                                                                                                                                                                                                                                                              Project Structure
                                                                Project: Alpha - (file_path)/XSSRequestWrapper.java =
                                                                              return encodedValues;
   D:\varma\project_alpha
       idea idea
       v src
                                                                               public String getParameter(String parameter) {
   String value = super.getParameter(parameter);
                                                                             return stripXSS(value);

✓ scripts_module

            XSSFilter.java
                                                                              @Override
public String getHeader(String name) {
   String value = supergetHeader(name),
   return stripXSS(value);
}
            XSSScan.java
            XSSRequestWrapper.jc
                                                                             private String stripXSS(String value) {
    if (value = null) {
        // NOTE: It's highly recommended to use the ESAPI library and uncomment the following line to
        // avoid encoded attacks.
    // value = ESAPI.encoder().canonicalize(value);
                                                                                      // Avoid null characters
value = value.replaceAll("", "");
                                                                                       // Avoid anything between script tags
Pattern scriptTattern = Pattern compilet("script>("?)</script>", Pattern.CASE_INSENSITIVE);
volue = scriptTattern andcher(value) replaceAll("");
                                                                                       // Avoid anything in a src='...' type of expression scriptPattern = Pattern.compile("src[r]=[]\\\('.*?)\\", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL); value = scriptPattern.matcher(value).replaceAll("");
                                                                                       scriptPattern = Pattern.compile("src[]^=()]^* \setminus "(^*/^*) \setminus "", Pattern.CASE\_INSENSITIVE | Pattern.MULTILLINE | Pattern.DOTALL); value = scriptPattern.matcher(value) replaceAll(""); 
                                                                                       // Remove any lonesome </script> tag
scriptPattern = Pattern.compile("</script>", Pattern.CASE_INSENSITIVE);
value = scriptPattern.matcher(value).replaceAll("");
```

```
MSAT Interface ①
                                                                                                                                                                                                                                                                                                                                 \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc
  Project Structure
                                                          Project: Alpha - (file_path)/XSSRequestWrapper.java -
                                                           // Avoid expression(_) expressions
scriptPattern = Pattern.compile("expression\((.*?)\)", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);
value = scriptPattern.matcher(value).replaceAll("");
   D:\varma\project_alpha
     idea .idea
                                                                      // Avoid javascript...expressions scriptPattern = Pattern.compile("javascript.", Pattern.CASE_INSENSITIVE); value = scriptPattern.matcher(value).replaceAll("");
     √ Em src

✓ scripts_module

                                                                      // Avoid vbscript:... expressions scriptPattern = Pattern.compile("vbscript", Pattern.CASE_INSENSITIVE); value = scriptPattern.matcher(value).replaceAll("");
          XSSFilteriava
           XSSScan.java
                                                                      // Avoid onload= expressions scriptPattern = Pattern.compile("onload(.*?)=", Pattern.CASE_INSENSITIVE | Pattern.MULTIL.INE | Pattern.DOTALL.); value = scriptPattern.matcher(value).replaceAll("");
          XSSRequestWrapper.ja
                                                                   return value;
                                                          }
```