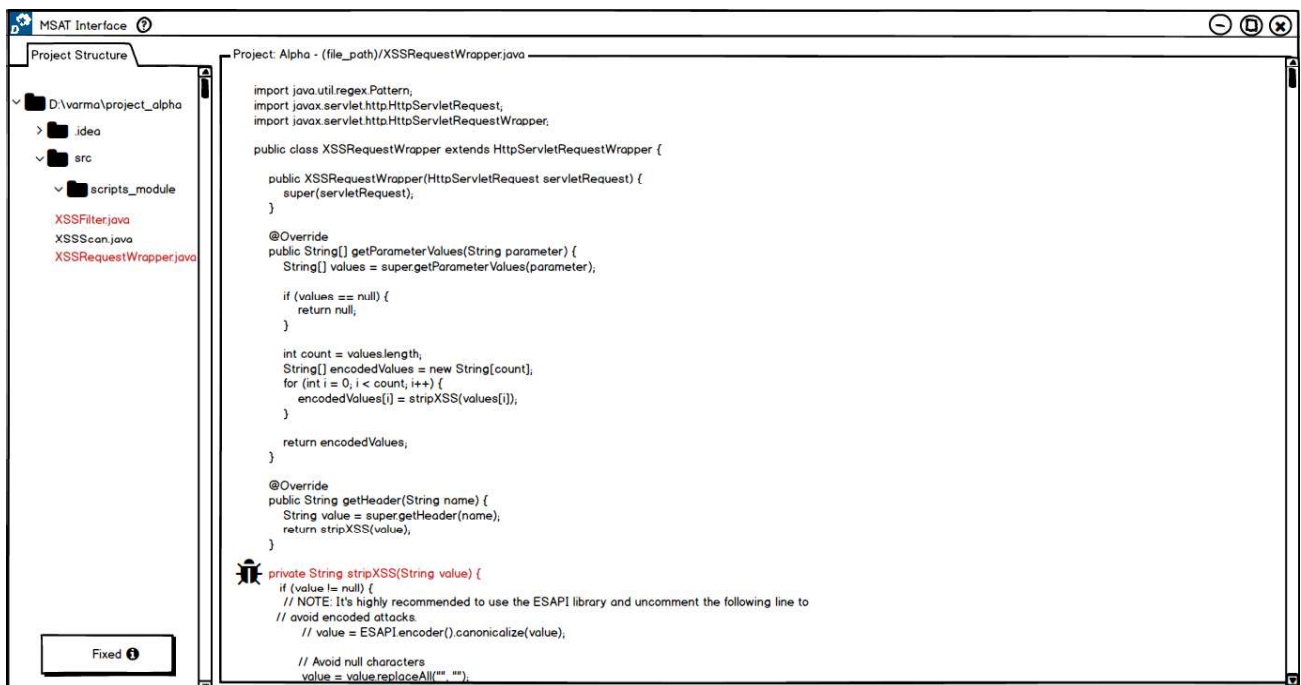
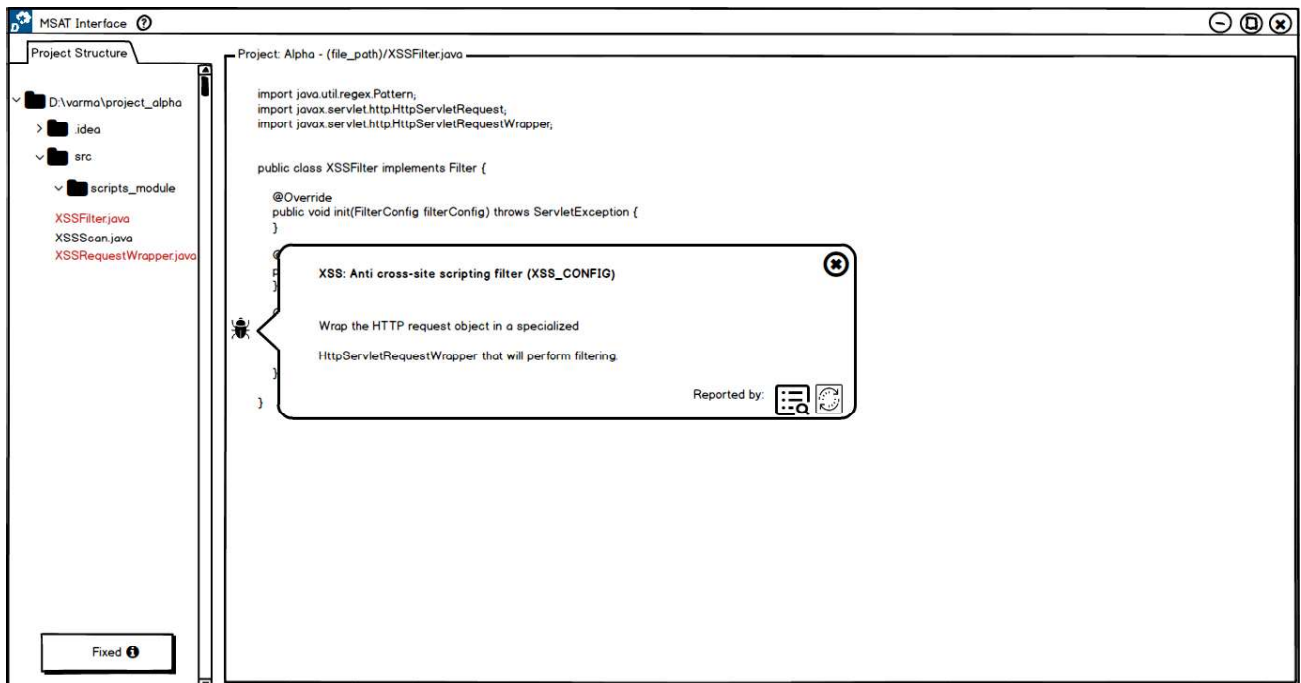
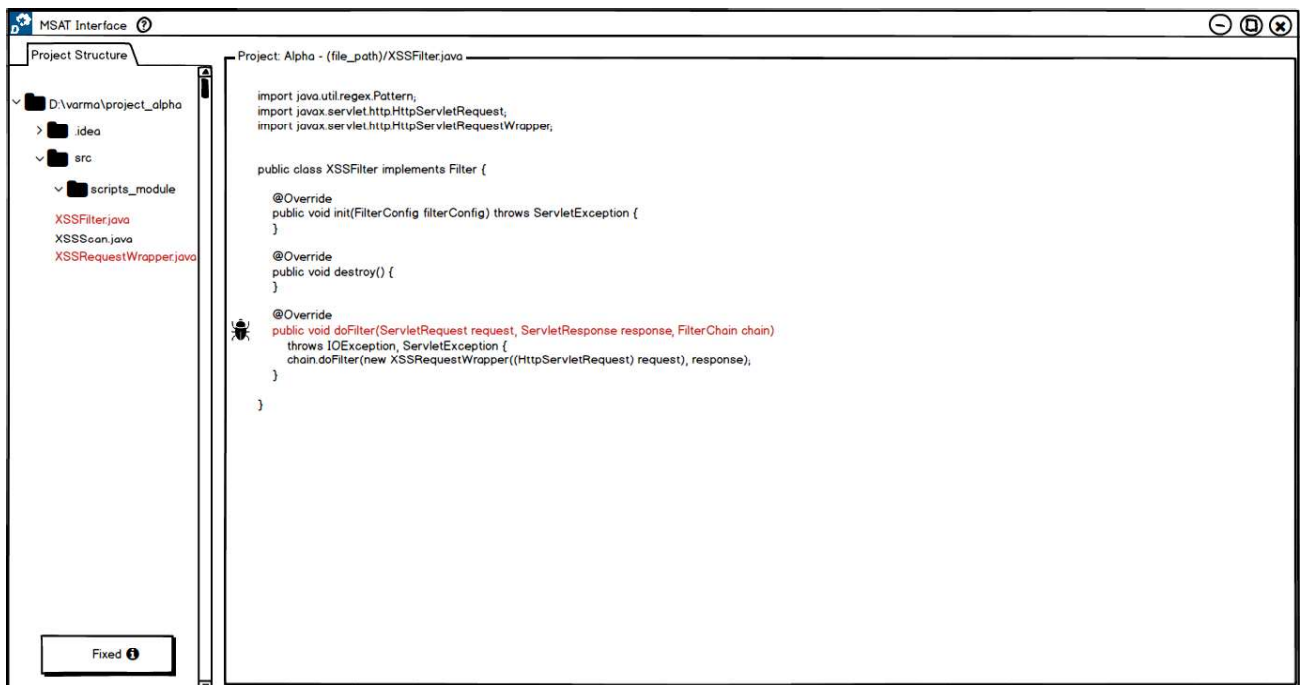
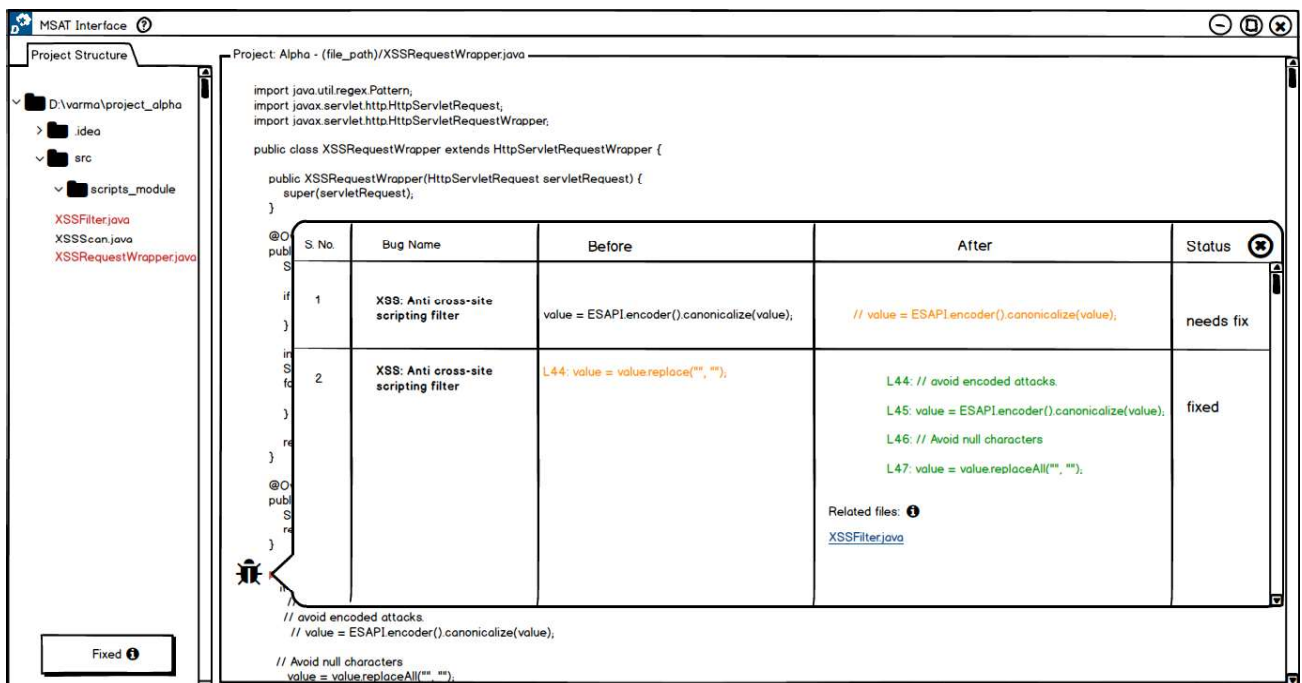


UXD Cycle 3 - RQ 3 - Table View







MSAT Interface

Project Structure

D:\varma\project_alpha

idea

src

scripts_module

XSSFilter.java

XSSScan.java

XSSRequestWrapper.java

Fixed

Project: Alpha - (file_path)/XSSRequestWrapper.java

```

import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper;

public class XSSRequestWrapper extends HttpServletRequestWrapper {

    public XSSRequestWrapper(HttpServletRequest servletRequest) {
        super(servletRequest);
    }

    @Override
    public String getParameter(String name) {
        if (name != null) {
            String value = getParameter(name);
            if (value != null) {
                value = value.replaceAll("<script.*>", "");
            }
        }
        return value;
    }

    // avoid encoded attacks
    // value = ESAPI.encoder().canonicalize(value);

    // Avoid null characters
    value = value.replaceAll("&#0000", "");

```

S. No	Bug Name	Before	After	Status
1	XSS: Anti cross-site scripting filter	value = ESAPI.encoder().canonicalize(value);	// value = ESAPI.encoder().canonicalize(value);	needs fix
2	XSS: Anti cross-site scripting filter	L44: value = value.replaceAll("<script.*>", "");	L44: // avoid encoded attacks canonicalize(value);	fixed

Related files are program files where the changes are made in addition to current file where bug is identified.

Related files: [XSSFilter.java](#)

MSAT Interface

Project Structure

D:\varma\project_alpha

idea

src

scripts_module

XSSFilter.java

XSSScan.java

XSSRequestWrapper.java

Fixed

Project: Alpha - (file_path)/XSSRequestWrapper.java

```

import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper;

public class XSSRequestWrapper extends HttpServletRequestWrapper {

    public XSSRequestWrapper(HttpServletRequest servletRequest) {
        super(servletRequest);
    }

    @Override
    public String getParameter(String name) {
        if (name != null) {
            String value = getParameter(name);
            if (value != null) {
                value = value.replaceAll("<script.*>", "");
            }
        }
        return value;
    }

    // avoid encoded attacks
    // value = ESAPI.encoder().canonicalize(value);

    // Avoid null characters
    value = value.replaceAll("&#0000", "");

```

S. No	Bug Name	Before	After	Status
2	XSS: Anti cross-site scripting filter	L44: value = value.replaceAll("<script.*>", "");	L44: // avoid encoded attacks. L45: value = ESAPI.encoder().canonicalize(value); L46: // Avoid null characters L47: value = value.replaceAll("�", "");	fixed
3	SA: Self comparison of value with itself	L44: value = value.replaceAll("<script.*>", "");	L44: value = value.replaceAll("<script.*>", ""); L34: // value = ESAPI.encoder().canonicalize(value);	fixed

Related files are program files where the changes are made in addition to current file where bug is identified.

Related files: [XSSFilter.java](#)

MSAT Interface

Project Structure

D:\varma\project_alpha

idea

src

scripts_module

XSSFilter.java

XSSScan.java

XSSRequestWrapper.java

Fixed

Project: Alpha - (file_path)/XSSRequestWrapper.java

```

import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper;

public class XSSRequestWrapper extends HttpServletRequestWrapper {

    public XSSRequestWrapper(HttpServletRequest servletRequest) {
        super(servletRequest);
    }

    @Override
    public String getParameter(String name) {
        if (name != null) {
            String value = getParameter(name);
            if (value != null) {
                value = value.replaceAll("<script.*>", "");
            }
        }
        return value;
    }

    // avoid encoded attacks
    // value = ESAPI.encoder().canonicalize(value);

    // Avoid null characters
    value = value.replaceAll("&#0000", "");

```

S. No	Bug Name	Before	After	Status
2	XSS: Anti cross-site scripting filter	L44: value = value.replaceAll("<script.*>", "");	L44: // avoid encoded attacks. canonicalize(value);	fixed
3	SA: Self comparison of value with itself	L44: value = value.replaceAll("<script.*>", "");	L44: value = value.replaceAll("<script.*>", ""); L34: // value = ESAPI.encoder().canonicalize(value);	fixed

Related files are program files where the changes are made in addition to current file where bug is identified.

Related files: [XSSFilter.java](#)