

Jayamsakthi

---

## **IMPLEMENTATION PLAN**

**Xss Hacker Tracking System**

---

# 1 DOCUMENT VERSION CONTROL

## 1.1.1 DOCUMENT HISTORY

Version	Date	Change log	Author
V0.01	09/May/2007	Initial version	Jayamsakthi

## 2 DETAILED PHASE DESCRIPTION

### 2.1 PREPARATION PHASE

This paragraph describes all steps in detail needed in the preparation phase.

Project(s) should support J2EE 1.3 Specification.  
Project should be of Web based one.

#### 2.1.1 STEP 1: DELIVERABLES OF NEW SOFTWARE RELEASE

This paragraph describes the actions to ensure delivery of Software.

1. Xss\_Tracking.jar
2. dbAccess.properties
3. Folder named "**xml**".
4. db script "security\_check.sql".
5. Hacked.jsp

### 2.2 IMPLEMENTATION PHASES

Steps to be followed for Implementing new Software which tracks hackers actions.

- 1) Run the **security\_check.sql** (table script ) on the your database which is connected by your application and grant sufficient privileges to that table.
- 2) Change the DB URL, UserName, Passwords of corresponding database in **dbAccess.properties** file.
- 3) Change the UserID variable used to login in your application in **dbAccess.properties** file  
Ex. USERID = userName.

- 4) Add Supplied **dbAccess.properties** to WEB-INF folder of existing application.
- 5) Modify **IED.properties** files for Lower Limit of Attempts, Max No. of Attempts, Time in Mins to block User for particular period.
- 6) Add Supplied **Xss\_Tracking.jar** to your application's CLASSPATH.
- 7) Add Supplied folder "**xml**" to **WEB-INF** folder of existing application.  
NOTE : xml folder contains three files called
  - **WhiteList.xml**
  - **BlackList.xml**
  - **Malicious.xml**
- 8) Add Supplied **Hacked.jsp** to Web Content folder of your existing application.
- 9) Add the following lines in your application's web.xml just before <servlet> ..</servlet>

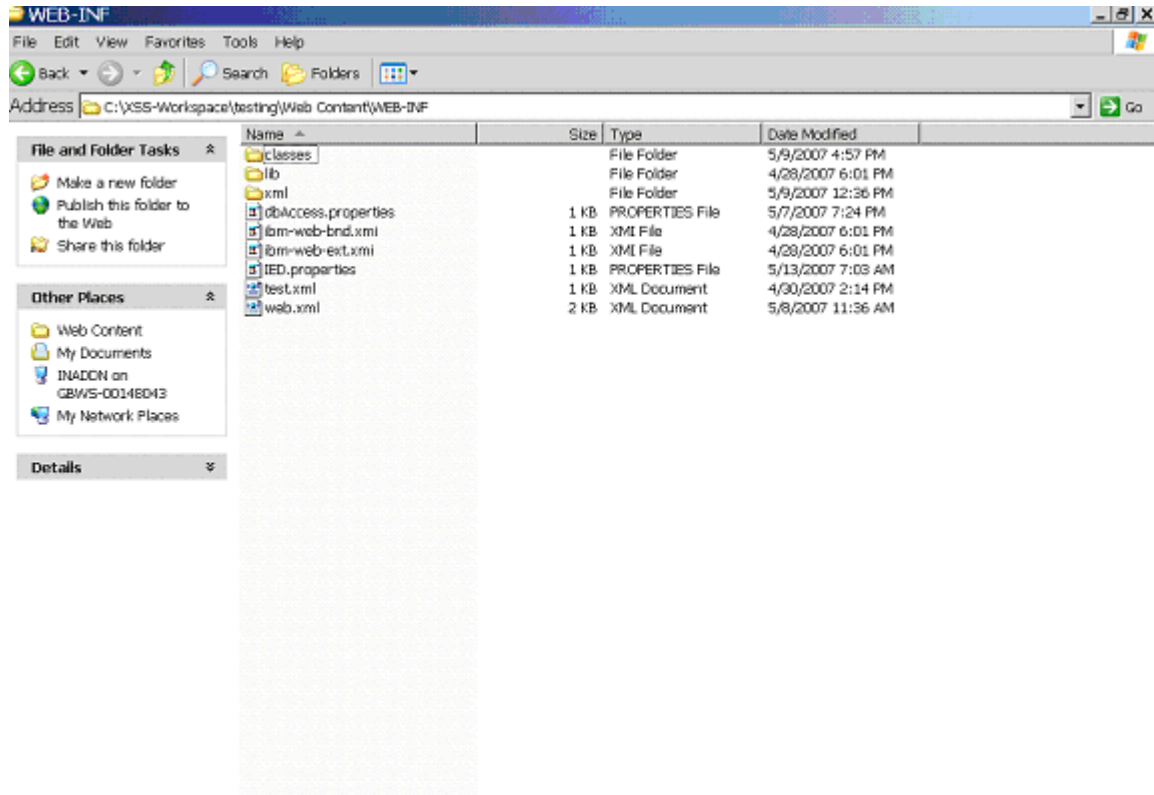
```
<filter>
  <filter-name>XSSPhaseOneFilter</filter-name>
  <filter-class>com.nonhacker.XSSPhaseOneFilter</filter-class>
</filter>
<filter-mapping>
  <filter-name>XSSPhaseOneFilter</filter-name>
  <url-pattern>*.do</url-pattern>
</filter-mapping>
```
- 10) Now Restart the Server.
- 11) Server should start without any errors.

Implementation has completed here.

## 2.3 POST IMPLEMENTATION PHASES

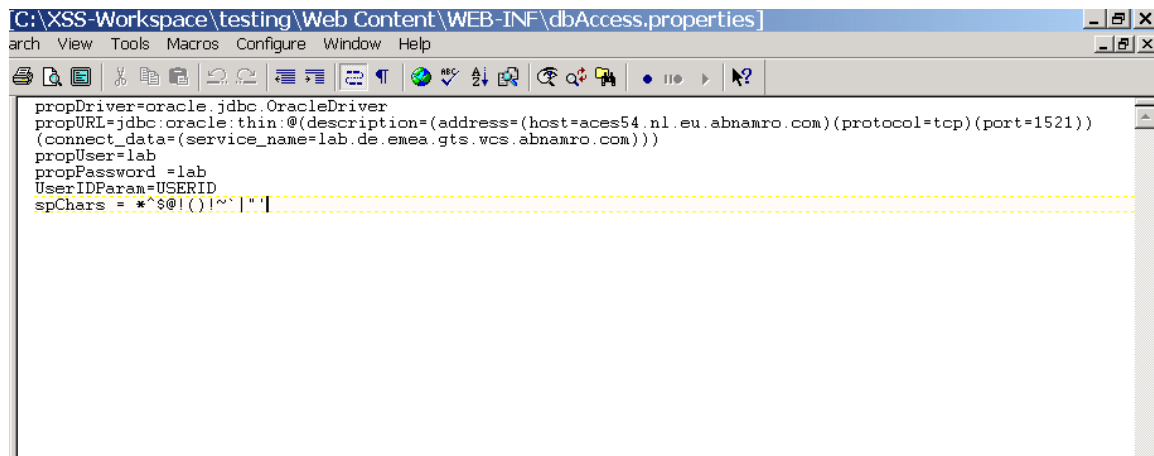
- 1) Access your application through web-browser.
- 2) Your application should run successfully.

- 1) This is the Place “WEB-INF” Folder(for any application) where Property files and xml folder would be kept.



- 2) dbAccess.properties file under WEB-INF folder and all the properties of Database would be there and sample is shown as below.

Application login userid should be given in this property file.

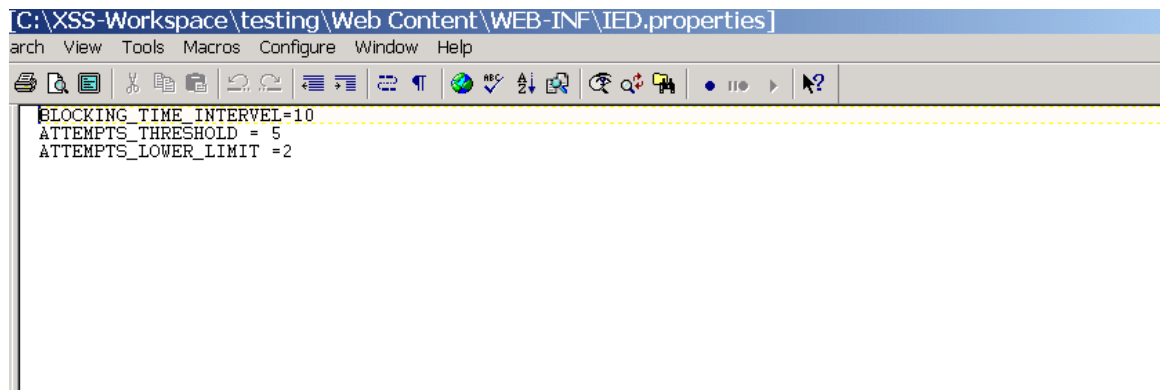


3) IED.properties file contains Time Interval which you want to block a User in case of Malicious attempts and Max No of Attempts and Lower limit of Attempts so that user can be put under Warning. The Description of parameters is as follows

BLOCKING\_TIME\_INTERVEL - No. of Mins for a User will be blocked.

ATTEMPTS\_THRESHOLD – Max No. of Attempts a User can be made , If User exceeds this limit, User status will changed to Blocked and He can't Access the Application anymore.

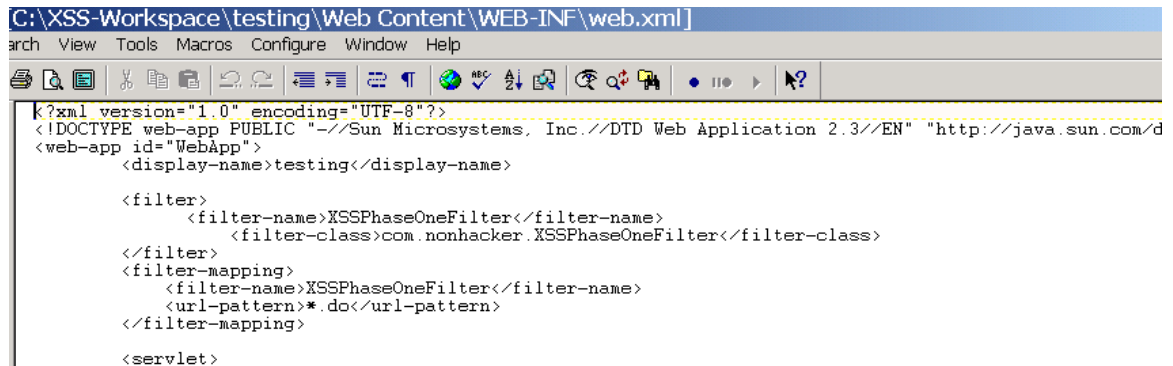
ATTEMPTS\_LOWER\_LIMIT – Min No. of Attempts a User can be made, If User exceeds this no. of Attempts User status will be changed to Warning



The screenshot shows a text editor window titled "C:\XSS-Workspace\testing\Web Content\WEB-INF\IED.properties". The window contains the following text:

```
BLOCKING_TIME_INTERVEL=10
ATTEMPTS_THRESHOLD = 5
ATTEMPTS_LOWER_LIMIT = 2
```

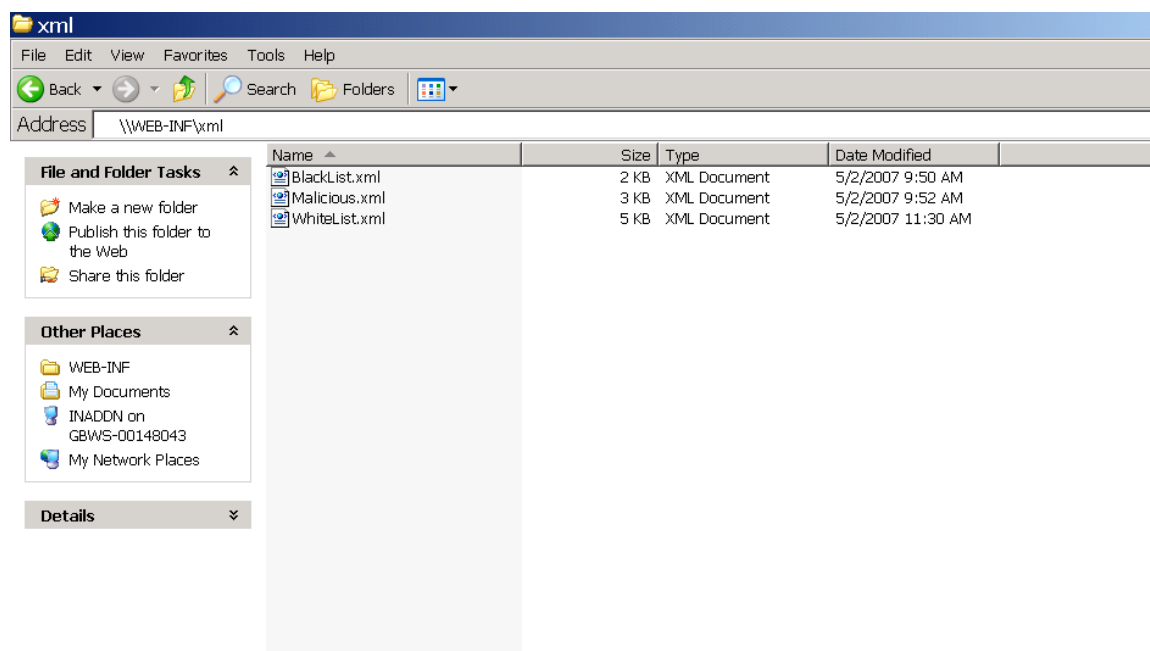
4) Sample web.xml ( which will be under WEB-INF) folder contains Filter Servlet Details.



The screenshot shows a text editor window titled "C:\XSS-Workspace\testing\Web Content\WEB-INF\web.xml". The window contains the following XML code:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN" "http://java.sun.com/d
<web-app id="WebApp">
  <display-name>testing</display-name>
  <filter>
    <filter-name>XSSPhaseOneFilter</filter-name>
    <filter-class>com.nonhacker.XSSPhaseOneFilter</filter-class>
  </filter>
  <filter-mapping>
    <filter-name>XSSPhaseOneFilter</filter-name>
    <url-pattern>*.do</url-pattern>
  </filter-mapping>
  <servlet>
```

5) Xml files which are put under WEB-INF/xml Folder which contains Tags of White , Black, Malicious Information.



6) Xml File of Black Listed Tags

```

[C:\xss-workspace\testing\web_content\WEB-INF\xml\BlackList.xml]
Search View Tools Macros Configure Window Help
[Icons]
<BlackList>
<Attack>
  <TagOrEvent>applet</TagOrEvent>
  <ClassName>HandleAbbr</ClassName>
  <Category>HtmlTagAttack</Category>
</Attack>

<Attack>
  <TagOrEvent>body</TagOrEvent>
  <ClassName>HandleEmbed</ClassName>
  <Category>HtmlTagAttack</Category>
</Attack>


<Attack>
  <TagOrEvent>embed</TagOrEvent>
  <ClassName>HandleEmbed</ClassName>
  <Category>HtmlTagAttack</Category>
</Attack>

<Attack>
  <TagOrEvent>frame</TagOrEvent>
  <ClassName>HandleEmbed</ClassName>
  <Category>HtmlTagAttack</Category>
</Attack>

<Attack>
  <TagOrEvent>script</TagOrEvent>
  <ClassName>HandleEmbed</ClassName>
  <Category>HtmlTagAttack</Category>
</Attack>

<Attack>

```

 Thank you for taking the time to evaluate TextPad  
Click Help to find out how to register, and stop this message from appearing.

You are welcome to try this program before you buy it.  
The software is fully functional, but you will be intermittently reminded that it is not free.

## 6) Xml File of Malicious Tags







LAB.SECURITY_CHECK	
USERID	VARCHAR2 (30)
IPADDRESS	VARCHAR2 (20)
USER_STATUS	VARCHAR2 (1)
USER_STATUS_TIMESTAMP	DATE
REC_ACTIVE	VARCHAR2 (1)
NR_OF_ATTEMPTS	NUMBER
TIMESTAMP	DATE