5. XSS 공격

XSS(Cross-Site Scripting)란 **웹에서 많이 나타나는 취약점**의 하나이며, 게시판 웹 메일 등에 삽입된 악의적인 스크립트에 의해 페이지가 깨지거나 다른 사용자의 사용을 방해하거나 쿠키 및 기타 개인 정보를 특정 사이트로 전송시키는 공격이다.
웹 사이트의 **관리자가 아닌 일반 유저가 웹 페이지에 악성 스크립트를 삽입**할 수 있는 취약점이다.

5. XSS 공격

1. 실습 개요

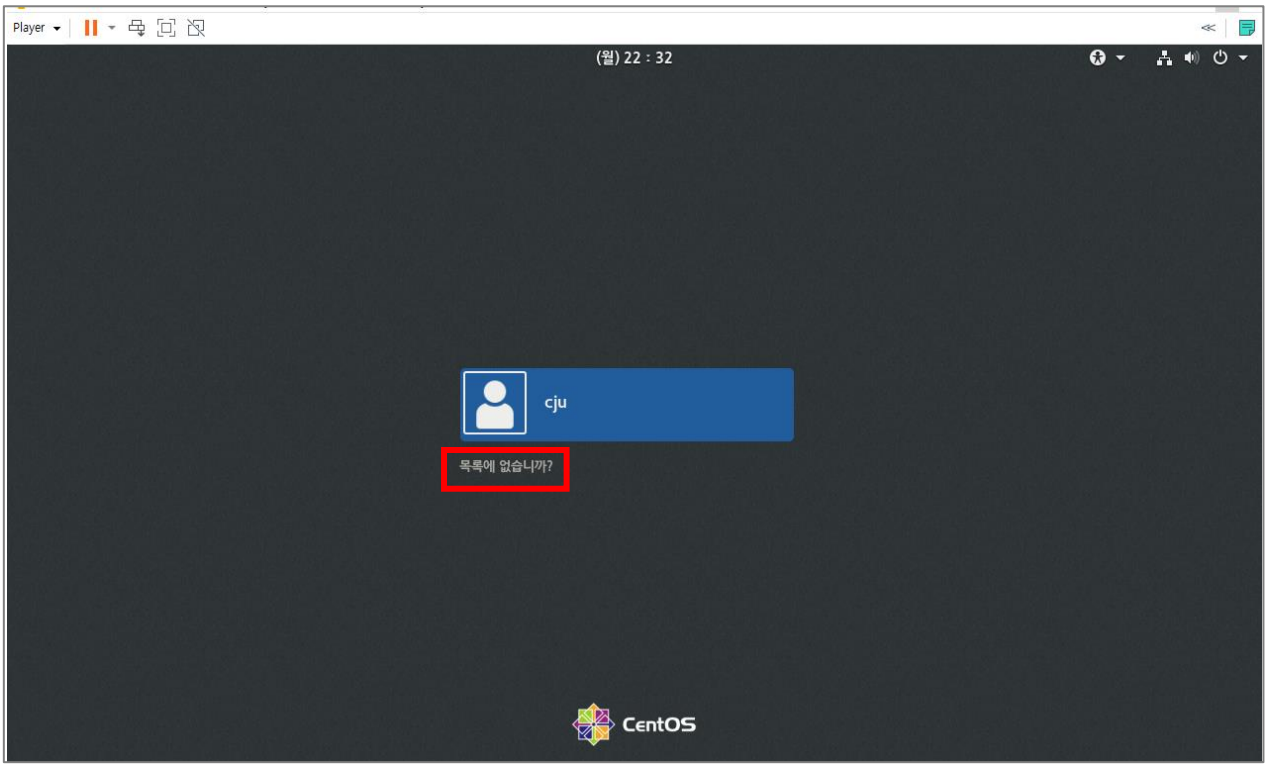
본 실습에서는 John the Ripper 도구를 이용한다. 흔히 쓰이는 패스워드를 모두 저장하여 대입해 보는 방식인 사전 공격/사전 대입 공격(Dictionary Attack) 기법으로 패스워드 크래킹을 진행한다.

2. 시스템 정보

* CentOS7_GWJ 계정 : root/root123

3. 문제풀이

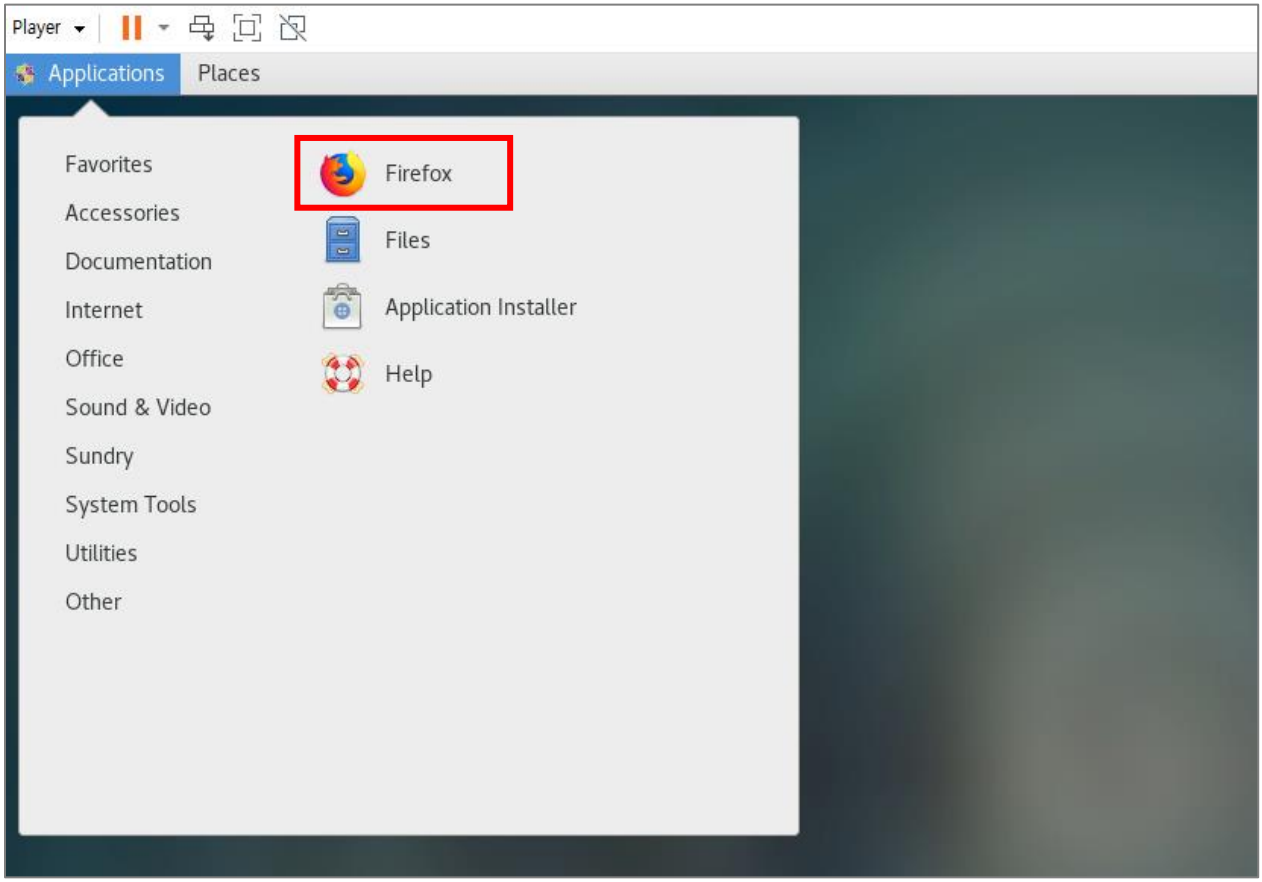
1) CentOS7_GWJ 로그인(root/root123)

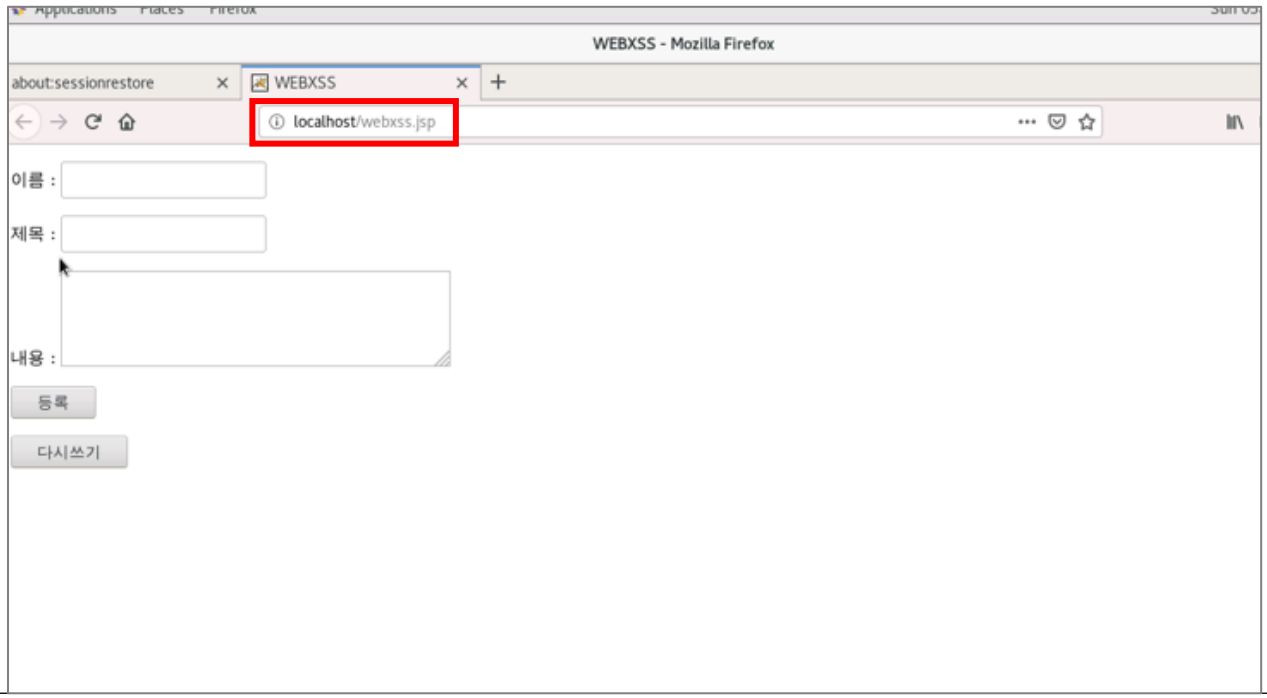


5. XSS 공격

[공격]

2) Firefox 실행 > XSS 실습 사이트로 접속
(주소: localhost/webxss.jsp)



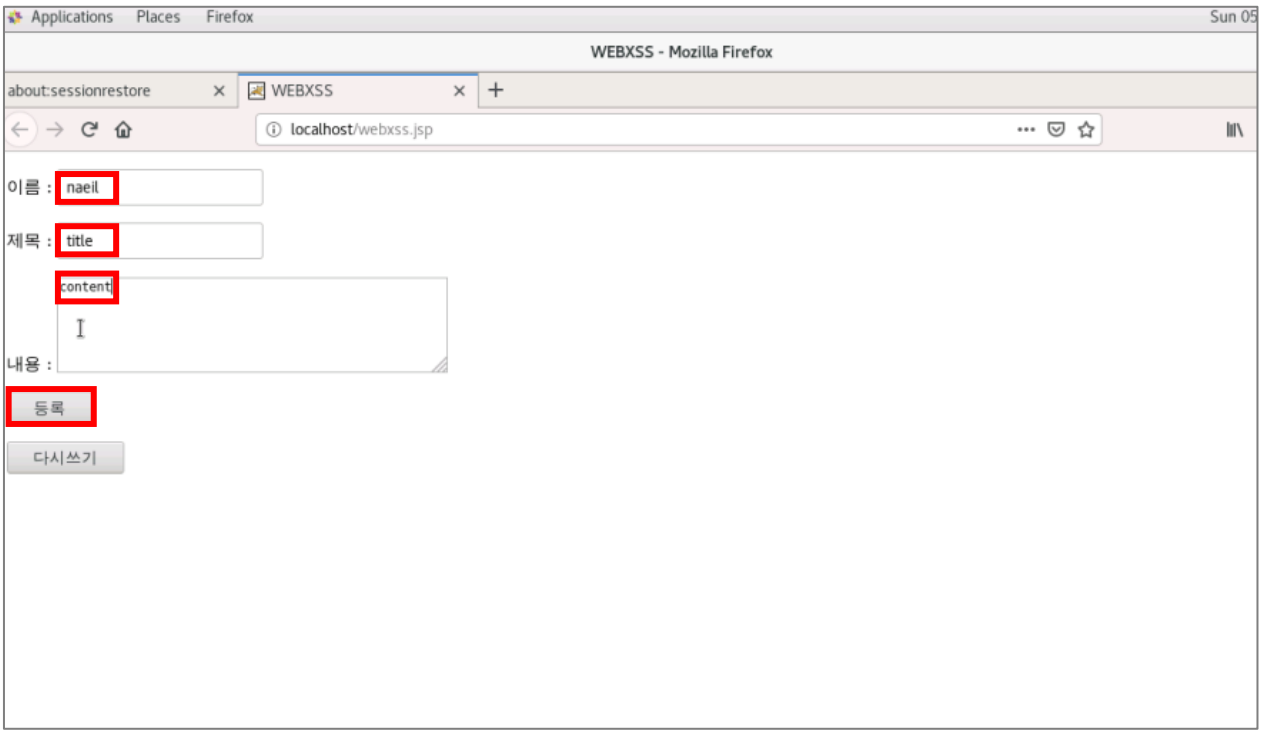


* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

5. XSS 공격

[공격]

3) 이름: naeil, 제목: title, 내용: content를 입력하고 [등록]버튼 클릭



4) 글 목록 리스트 출력, [내용보기] 클릭

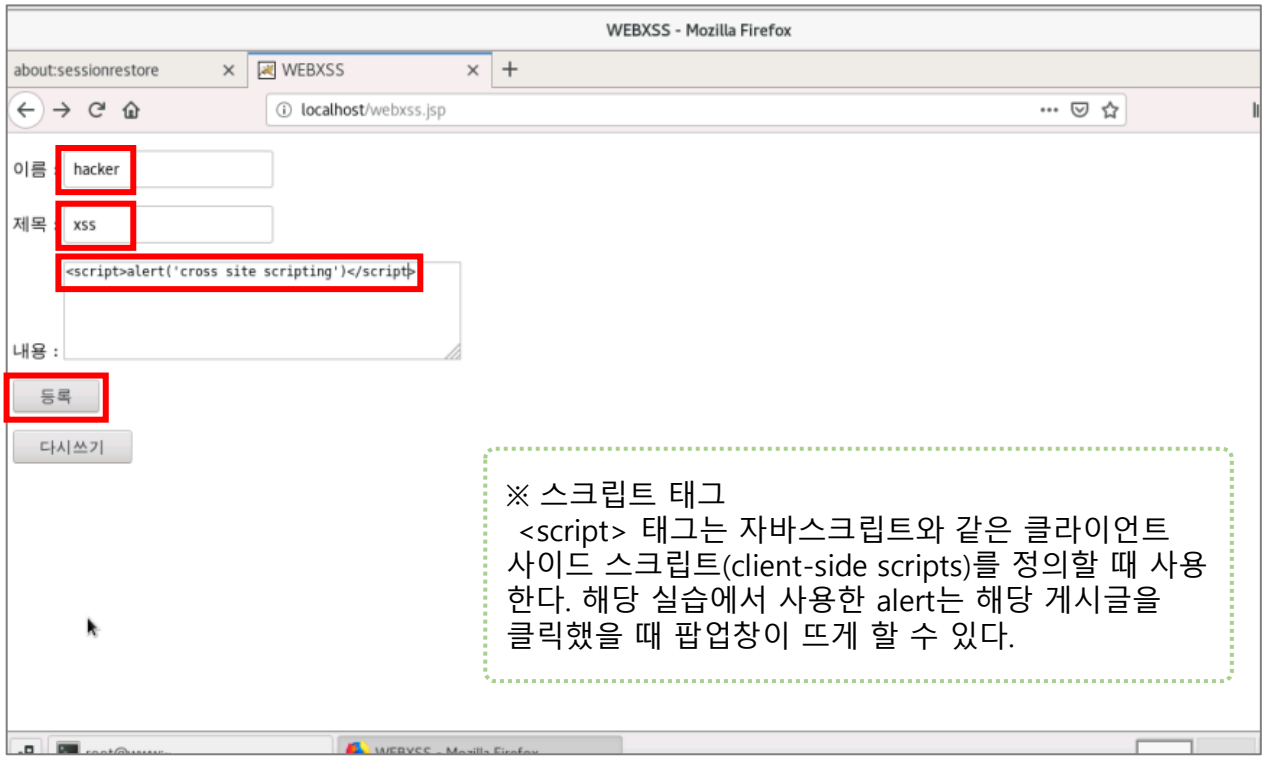
* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

5. XSS 공격

[공격]

5) 글 내용 출력, [글쓰기] 클릭

6) 이름: hacker, 제목: xss, 내용: <script>alert('cross site scripting')</script> 을 입력하고 [등록] 클릭



※ 스크립트 태그
<script> 태그는 자바스크립트와 같은 클라이언트 사이드 스크립트(client-side scripts)를 정의할 때 사용한다. 해당 실습에서 사용한 alert는 해당 게시글을 클릭했을 때 팝업창이 뜨게 할 수 있다.

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

5. XSS 공격

[공격]

7) 해당 글의 [내용보기]를 클릭하면 입력한 내용대로 경고창이 뜸