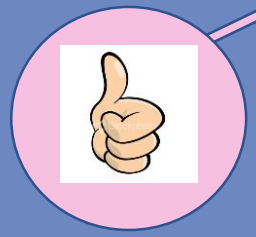
Ok 계획대로
안되고있어



안녕하세요
웹개발이예요

Https://duni0107-dau.tistoru.com/

좋아요와 구독...

지금까지 완성된 것

1. 로그인, 회원가입, 게시판, 글쓰기 폼(html) 작성
2. 회원가입 정보 DB에 저장

1/18~1/30 계획

1. 로그인 성공 후 실행 화면 만들기
2. 로그아웃 성공 후 화면 만들기
3. 게시판 글쓰기 정보 DB에 저장시키기
4. 저장된 글 list에 호출시키기
5. SQL Injection 실행환경 구축하기

피용적 START

글쓰기 정보 DB에 저장시키기

board.html

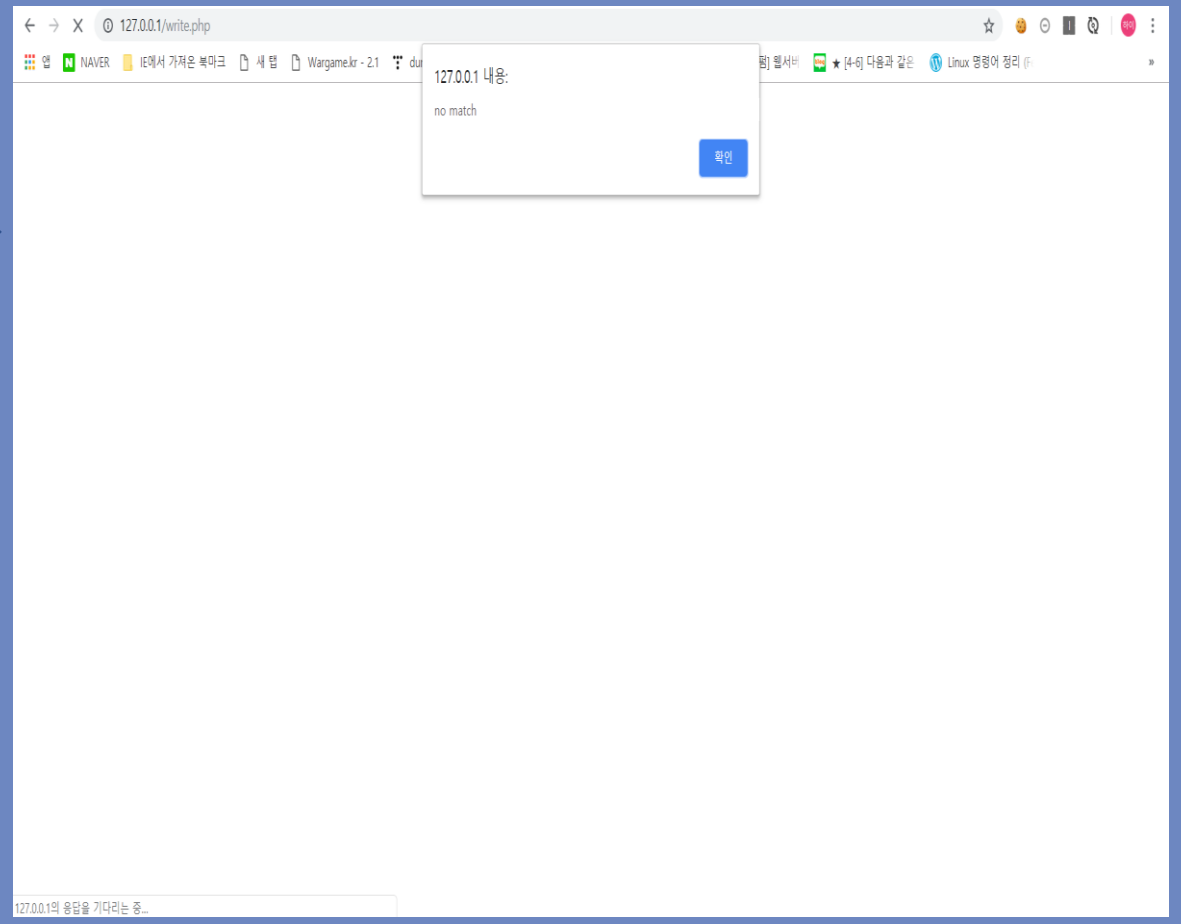
```
<form action="write.php" method="post">

        <tr>
          <th>아이디</th>
          <td><input type="text" name="userId" placeholder="아이디를 입력하세요"></td>
        </tr>
        <tr>
          <th>비밀번호</th>
          <td><input type="password" name="userPw" placeholder="비밀번호를 입력하세요"></td>
        </tr>
        <tr>
          <th>제목</th>
          <td><input type="text" name="title" placeholder="제목을 입력하세요"></td>
        </tr>
        <tr>
          <th>내용</th>
          <td><textarea cols="40" rows="10" name="content" placeholder="내용을 입력하세요"></textarea></td>
        </tr>
    </table>

        <button class="btn btn-default"><a href="write.php>WRITE</a></button>
        <button class="btn btn-default"> <a href="list.php">BOARD LIST</a></button>

        </form>
```

dbConnect2.php

```php
<?php
$host = 'localhost';
$user = 'root';
$pw = [redacted]
$dbName = 'board';

$mysqli = new mysqli($host, $user, $pw, $dbName);

$userId=$_POST['userId'];
$userPw=$_POST['userPw'];
$title=$_POST['title'];
$content=$_POST['content'];

if($db) {
        echo '[연결실패] : '.mysql_error().'';
} else {
        echo '[연결성공]';
}

?>
```

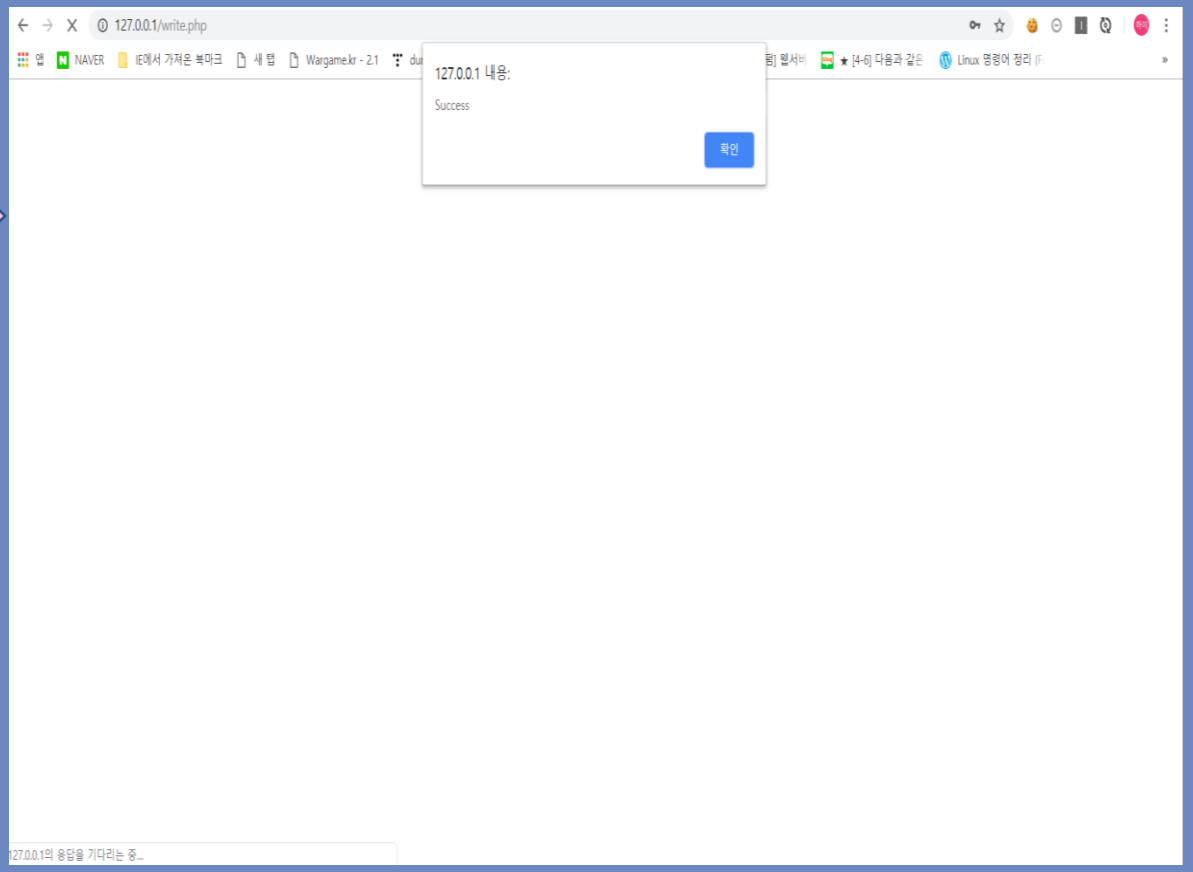
write.php

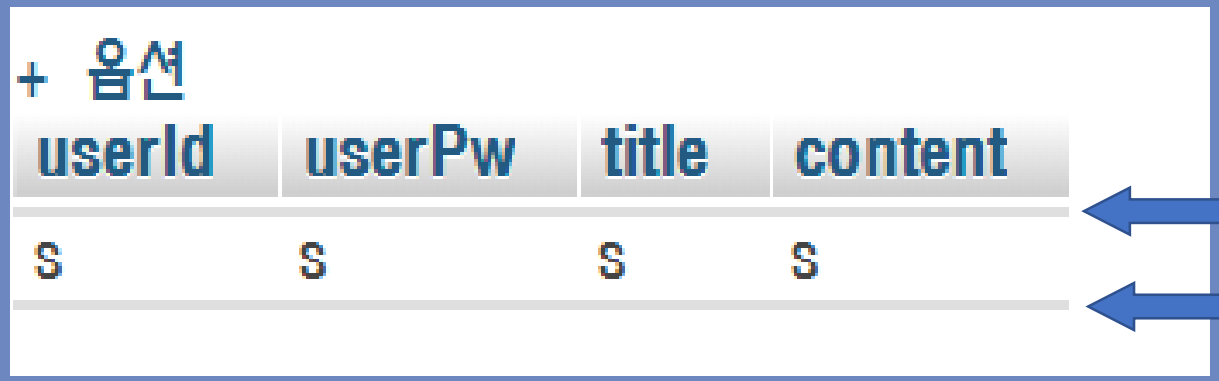
```php
<?php

include "dbConnect2.php";

   if($userId != null)
   {
      $sql = "insert into store (userId, userPw, title, content)";
      $sql = $sql."values('$userId', '$userPw', '$title', '$content')";

      if($mysqli->query($sql)){
         echo "<script>alert('Success'); location.href='index.html';</script>";

      }else{
         echo "<script>alert('Failed');location.href='index.html';</script>";
      }
   }
   else {
         echo "<script>alert('no match');location.href='board.html';</script>";
   }

?>
```



write.php

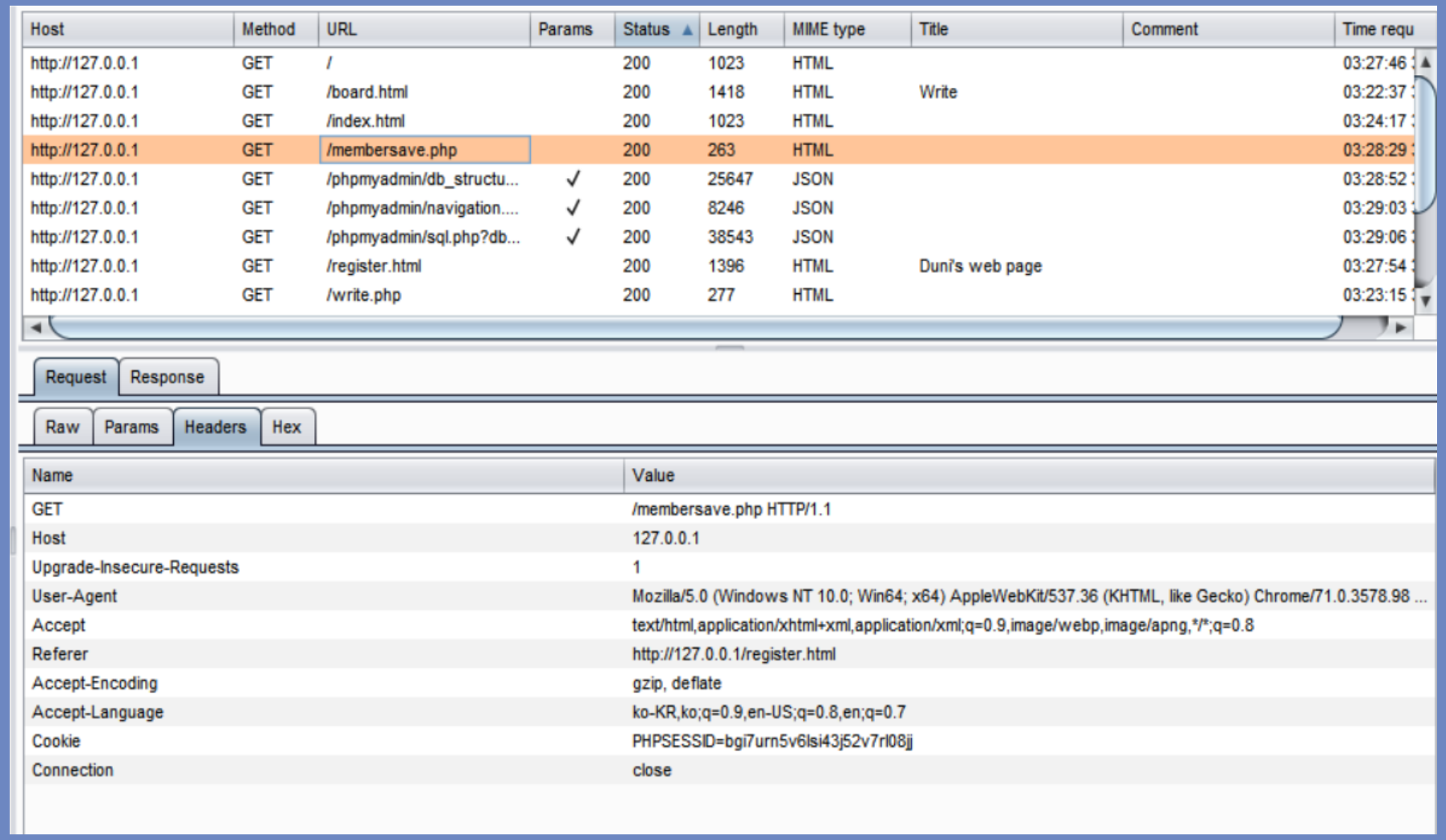
```
<?php

include "dbConnect2.php";

   if($userId == null)
   {
      $sql = "insert into store (userId, userPw, title, content)";
      $sql = $sql."values('$userId', '$userPw', '$title', '$content')";

      if($mysqli->query($sql)){
         echo "<script>alert('Success'); location.href='index.html';</script>";

      }else{
         echo "<script>alert('Failed');location.href='index.html';</script>";
      }
   }
   else {
         echo "<script>alert('no match');location.href='board.html';</script>";
   }

?>
```





이 피가 저장된 데이터임

그렇다면 왜??? 대체 왜 DB에 null 값으로 저장이 된 것일까?



Host	Method	URL	Params	Status ▲	Length	MIME type	Title	Comment	Time requ
http://127.0.0.1	GET	/		200	1023	HTML			03:27:46
http://127.0.0.1	GET	/board.html		200	1418	HTML	Write		03:22:37
http://127.0.0.1	GET	/index.html		200	1023	HTML			03:24:17
http://127.0.0.1	GET	/membersave.php		200	263	HTML			03:28:29
http://127.0.0.1	GET	/phpmyadmin/db_structu...	✓	200	25647	JSON			03:28:52
http://127.0.0.1	GET	/phpmyadmin/navigation....	✓	200	8246	JSON			03:29:03
http://127.0.0.1	GET	/phpmyadmin/sql.php?db...	✓	200	38543	JSON			03:29:06
http://127.0.0.1	GET	/register.html		200	1396	HTML	Duni's web page		03:27:54
http://127.0.0.1	GET	/write.php		200	277	HTML			03:23:15

Request | Response

Raw | Params | Headers | Hex

Name	Value
GET	/membersave.php HTTP/1.1
Host	127.0.0.1
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 ...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer	http://127.0.0.1/register.html
Accept-Encoding	gzip, deflate
Accept-Language	ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie	PHPSESSID=bgi7urn5v6lsi43j52v7rl08jj
Connection	close

Burpsuite를 이용해 확인해봄

membersave.php가 실행되는 과정에서 post가 실행되지 않고 있음이 확인됨

```
<form action="write.php" method="post">
```

Method 방식은 post로 설정되어있고 action 으로 write.php가 실행되게 되어있음

board.html

```
    <tr>
      <th>아이디</th>
      <td><input type="text" name="userId" placeholder="아이디를 입력하세요"></td>
    </tr>
    <tr>
      <th>비밀번호</th>
      <td><input type="password" name="userPw" placeholder="비밀번호를 입력하세요"></td>
    </tr>
    <tr>
      <th>제목</th>
      <td><input type="text" name="title" placeholder="제목을 입력하세요"></td>
    </tr>
    <tr>
      <th>내용</th>
      <td><textarea cols="40" rows="10" name="content" placeholder="내용을 입력하세요"></textarea></td>
    </tr>
  </table>

    <button class="btn btn-default”><a href=”write.php>WRITE</a></button>
    <button class="btn btn-default"> <a href="list.php">BOARD LIST</a></button>

    </form>
```

Write.php가 submit이 아닌 링크로 걸려있음

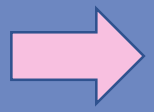
이 부분을 수정해주자

board.html

```
<form action="write.php" method="post">

        <tr>
          <th>아이디</th>
          <td><input type="text" name="userId" placeholder="아이디를 입력하세요"></td>
        </tr>
        <tr>
          <th>비밀번호</th>
          <td><input type="password" name="userPw" placeholder="비밀번호를 입력하세요"></td>
        </tr>
        <tr>
          <th>제목</th>
          <td><input type="text" name="title" placeholder="제목을 입력하세요"></td>
        </tr>
        <tr>
          <th>내용</th>
          <td><textarea cols="40" rows="10" name="content" placeholder="내용을 입력하세요"></textarea></td>
        </tr>
    </table>

    <button class="btn btn-default" input type="submit">WRITE</button>
    <button class="btn btn-default"> <a href="list.php">BOARD LIST</a></button>

        </form>
```

write.php

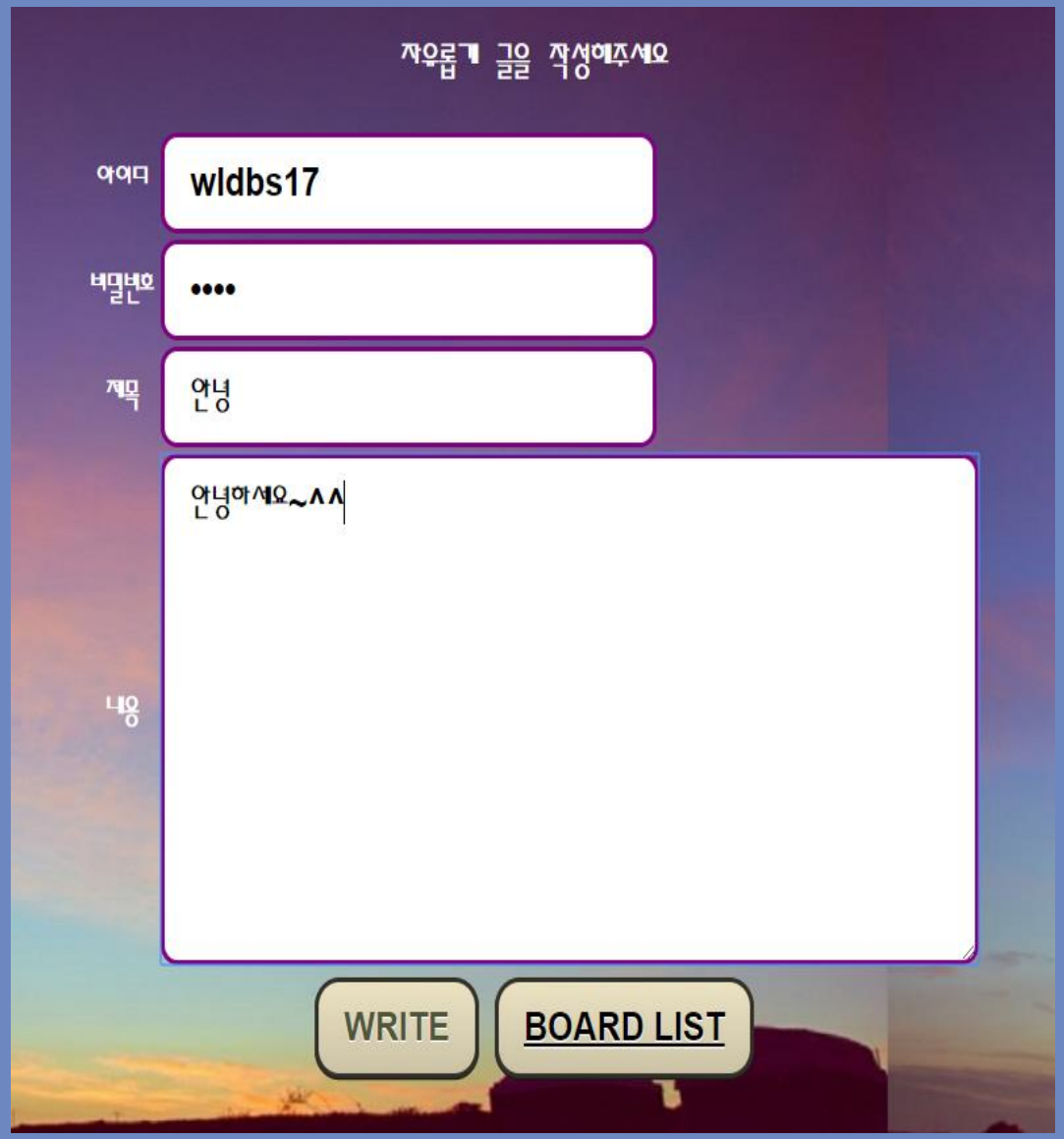
```php
<?php

include "dbConnect2.php";

   if($userId == null)
   {
      $sql = "insert into store (userId, userPw, title, content)";
      $sql = $sql."values('$userId', '$userPw', '$title', '$content')";

      if($mysqli->query($sql)){
         echo "<script>alert('Success'); location.href='index.html';</script>";

      }else{
         echo "<script>alert('Failed');location.href='index.html';</script>";
      }
   }
   else {
         echo "<script>alert('no match');location.href='board.html';</script>";
   }

?>
```



write.php

```php
<?php

include "dbConnect2.php";

   if($userId != null)
   {
      $sql = "insert into store (userId, userPw, title, content)";
      $sql = $sql."values('$userId', '$userPw', '$title', '$content')";

      if($mysqli->query($sql)){
         echo "<script>alert('Success'); location.href='index.html';</script>";

      }else{
         echo "<script>alert('Failed');location.href='index.html';</script>";
      }
   }
   else {
         echo "<script>alert('no match');location.href='board.html';</script>";
   }

?>
```

원상복귀



userId	userPw	title	content
wldbs17		안녕	안녕하세요~^^

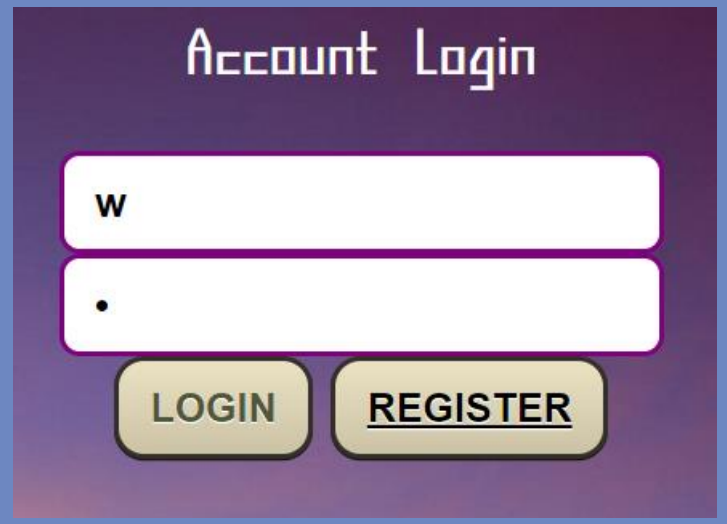
마찬가지로 회원가입에서도 post 부분을 수정해줌

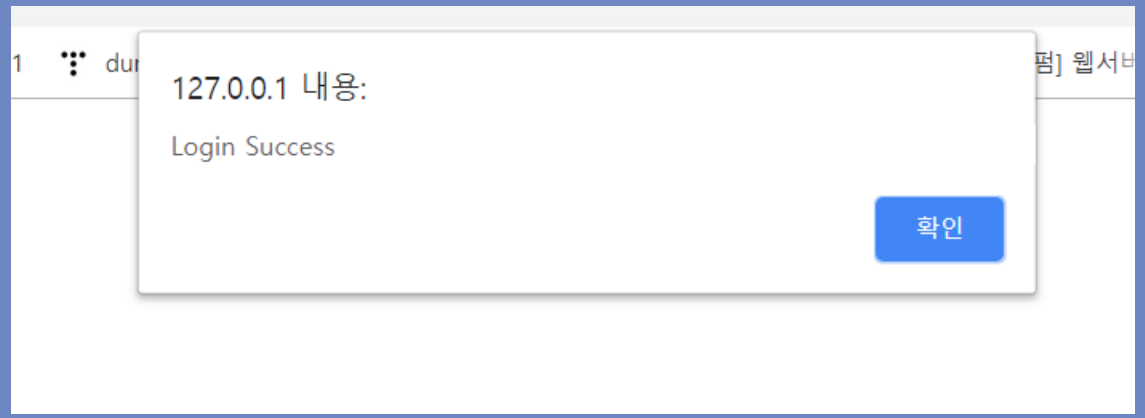
1/18~1/30 계획

1. 로그인 성공 후 실행 화면 만들기
2. 로그아웃 성공 후 화면 만들기
3. ~~게시판 글쓰기 정보 DB에 저장시키기~~
4. 저장된 글 list에 호출시키기
5. SQL Injection 실행환경 구축하기

signIn.php

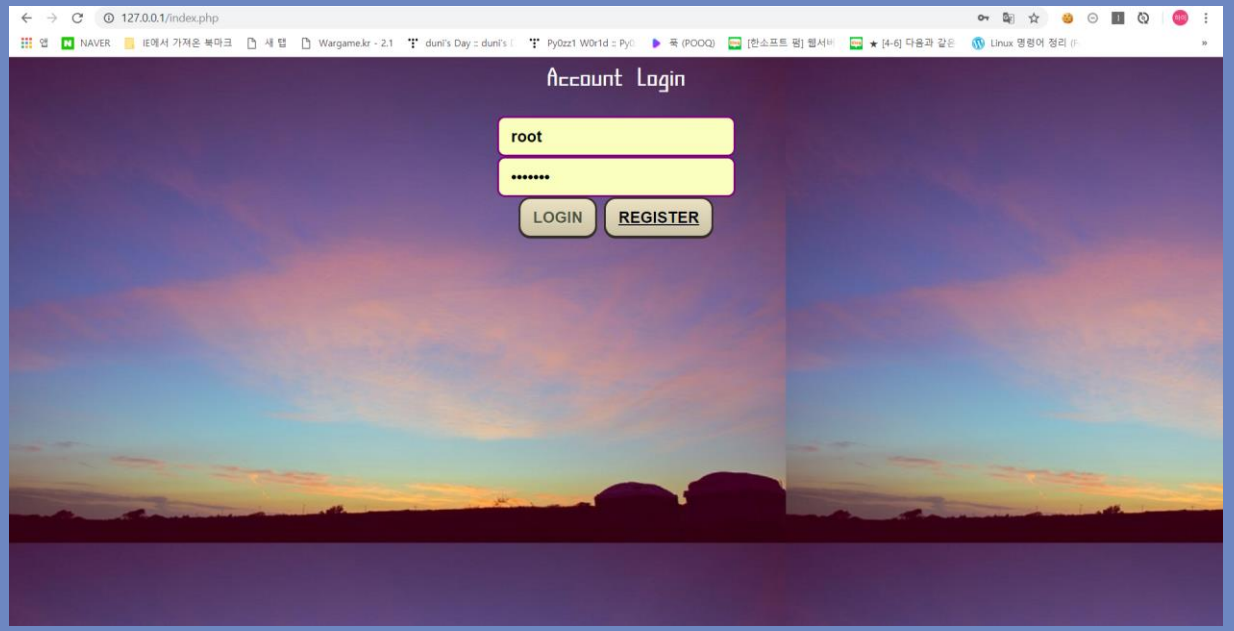
```php
<?php
  include "session.php";
  include "dbConnect.php";

  $check="select * from member where userId='$userId'";
  $result=$mysqli->query($check);
  if($result->num_rows==1){
    $row=$result->fetch_array(MYSQLI_ASSOC);
    if($row['userPw']==$userPw){
      $_SESSION['userId']=$userId;
      if(isset($_SESSION['userId'])) {
        echo "<script>alert('Login Success');
location.href='main.html';</script>";
      }
      else {
        echo "세션 저장 실패";
      }
    }
    else{
      echo "wrong id or pw";
    }
  }
  else{
    echo "wrong id or pw";
  }

 ?>
```





signOut.php

```
<?php
		include "session.php";
		$res=session_destroy();
		if($res){
			echo "<script>alert('Logout Success');
location.href='index.php';</script>";
		}
?>
```



1/18~1/30 계획

~~1. 로그인 성공 후 실행 화면 만들기~~

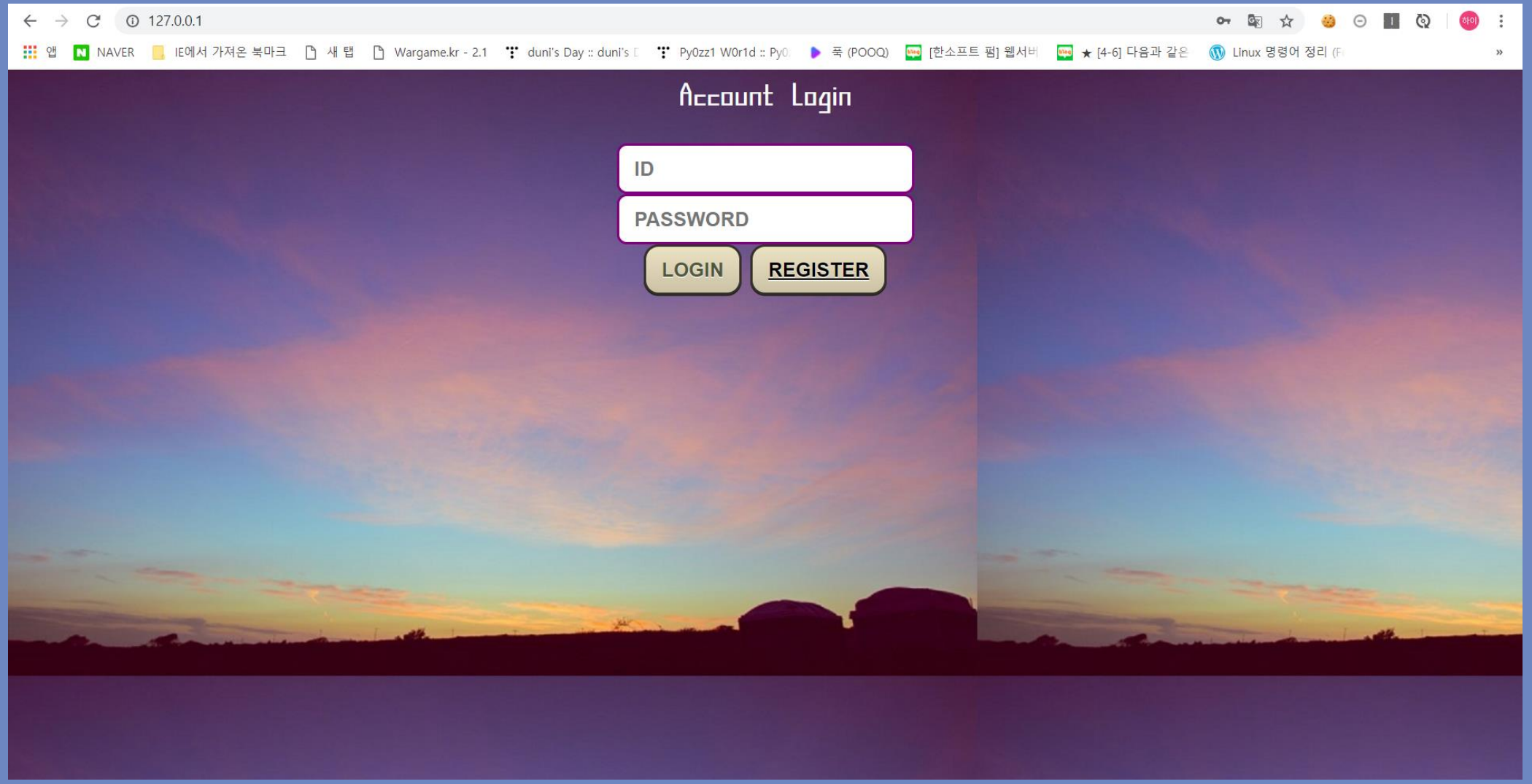
~~2. 로그아웃 성공 후 화면 만들기~~

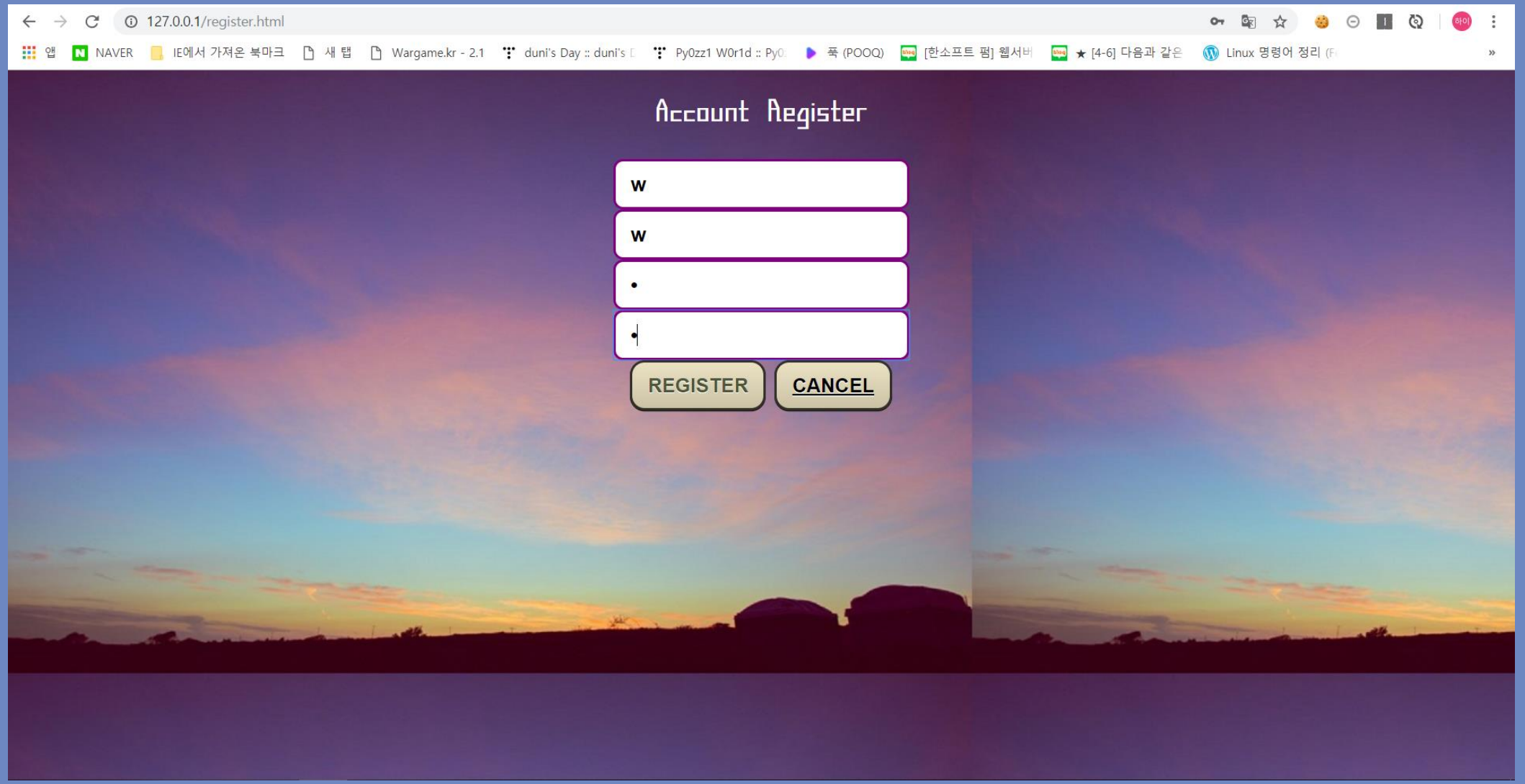
~~3. 게시판 글쓰기 정보 DB에 저장시키기~~

4. 저장된 글 list에 호출시키기

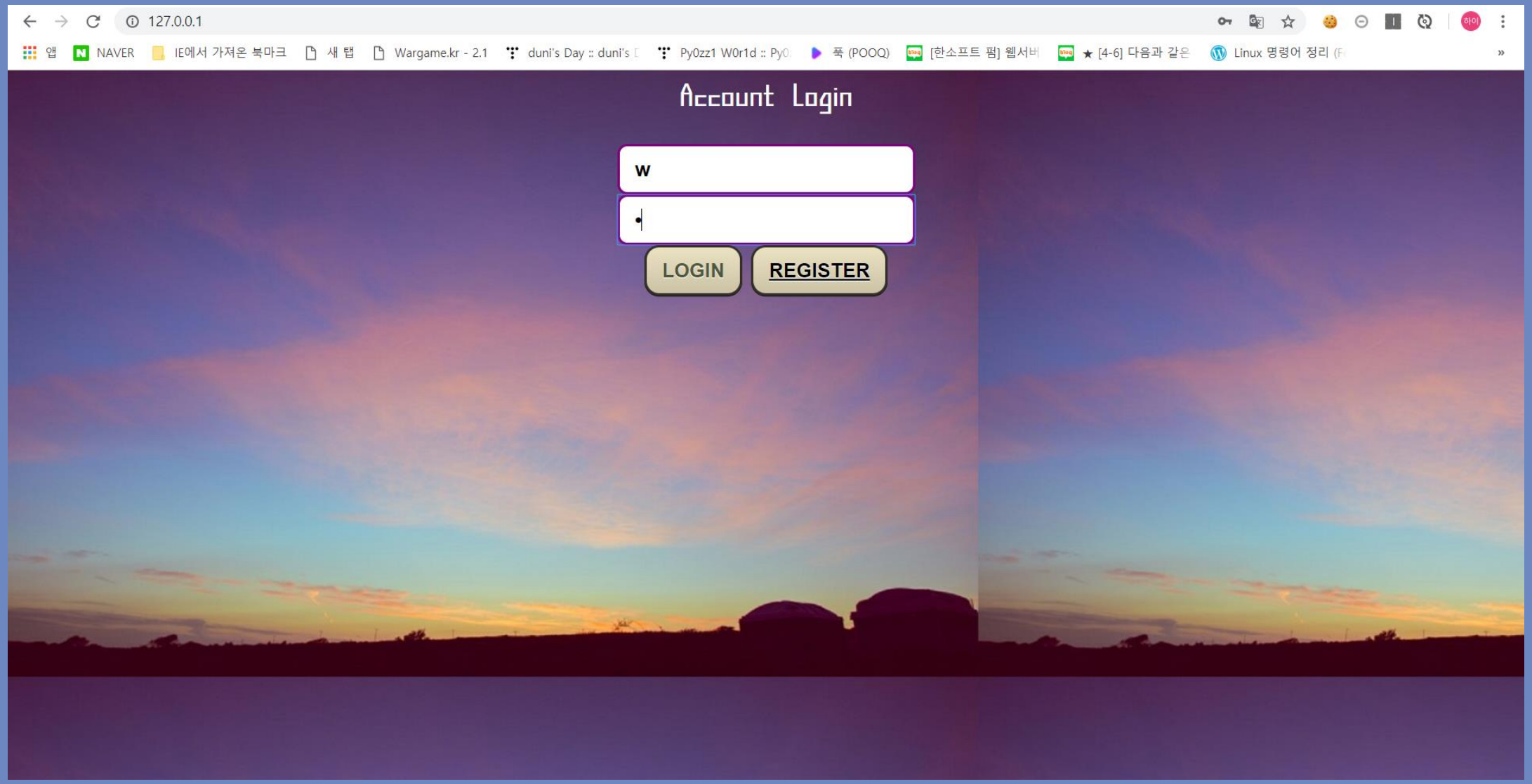
5. SQL Injection 실행환경 구축하기

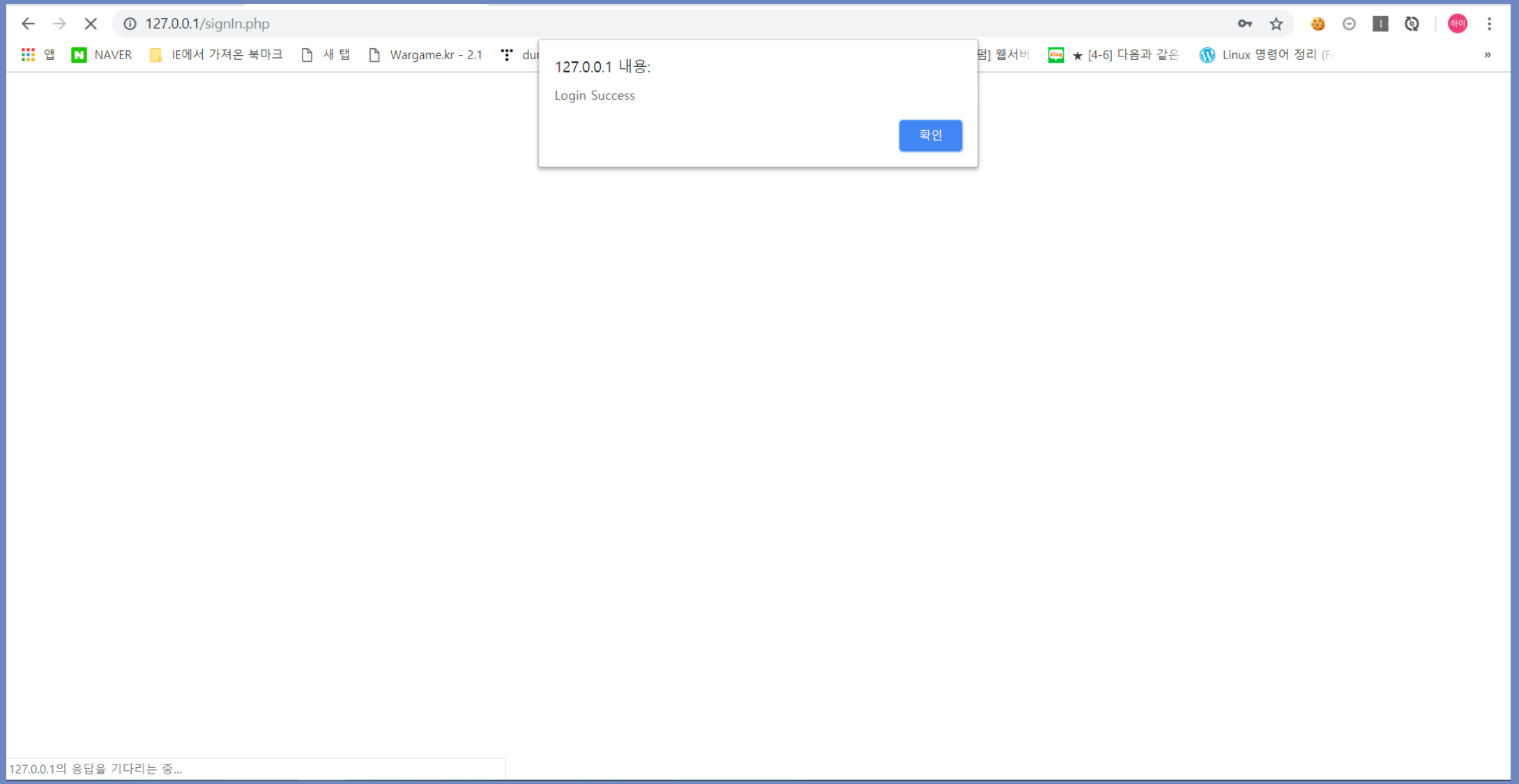
지금까지 완성된 무료 공개!

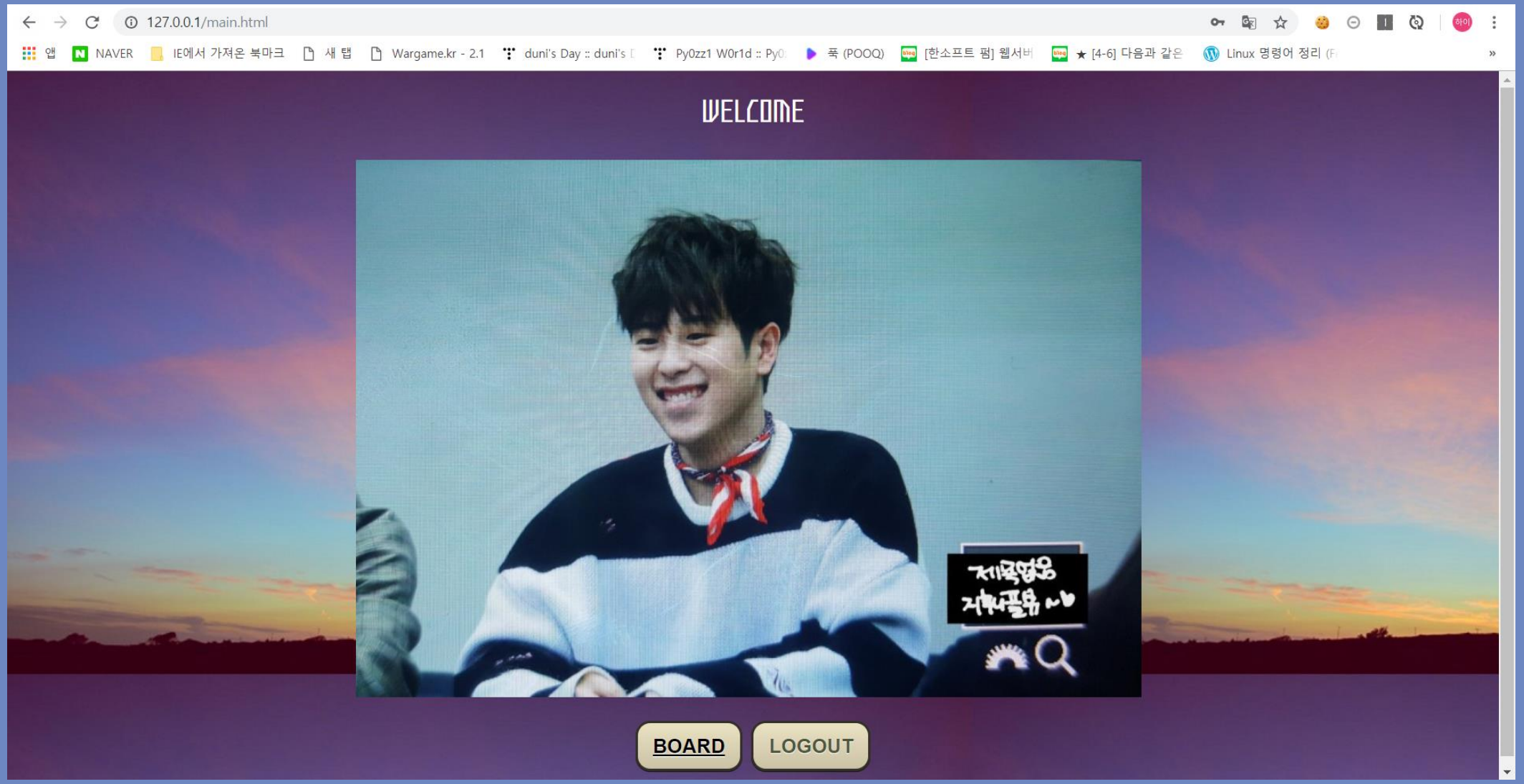

127.0.0.1
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
duni's Day :: duni's
Py0zz1 W0r1d :: Py0
푹 (POOQ)
[한소프트 펌] 웹서버
★ [4-6] 다음과 같은
Linux 명령어 정리
Account Login
ID
PASSWORD
LOGIN
REGISTER

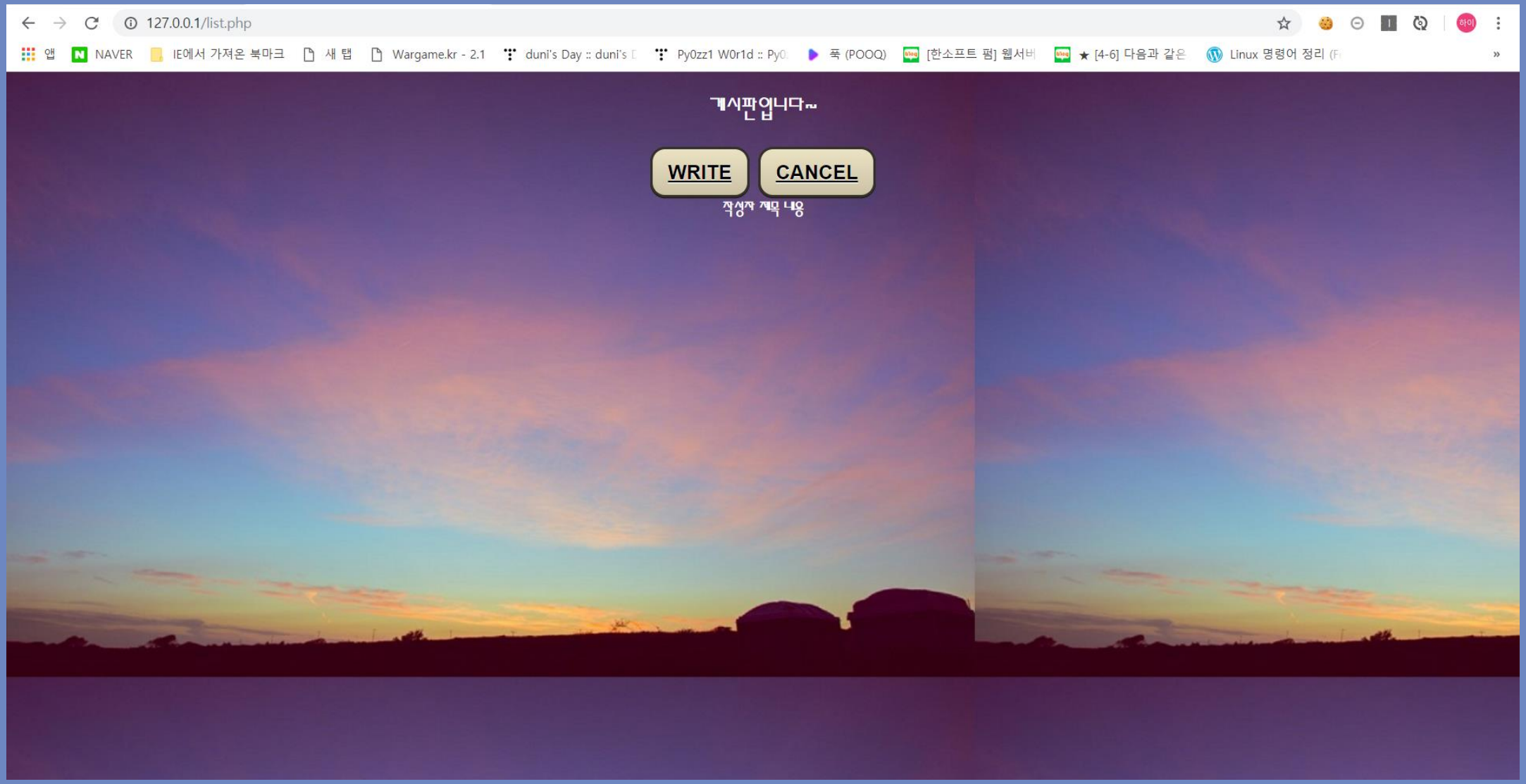

127.0.0.1/register.html
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
duni's Day :: duni's
Py0zz1 W0r1d :: Py0
푹 (POOQ)
[한소프트 펌] 웹서버
★ [4-6] 다음과 같은
Linux 명령어 정리
Account Register
w
w
REGISTER
CANCEL

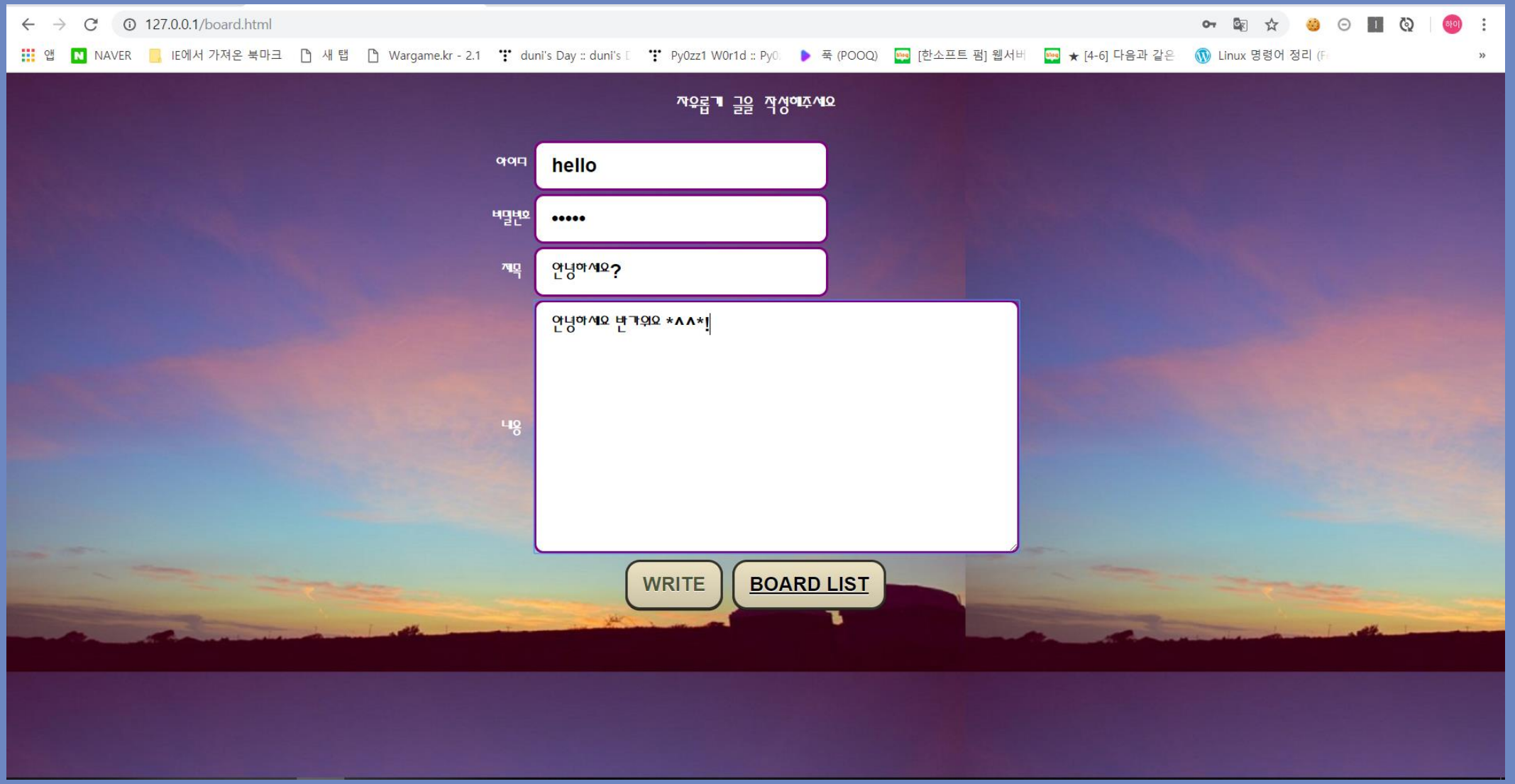
name	userId	userPw
[redacted]	[redacted]	[redacted]
w	w	w


127.0.0.1
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
Py0zz1 W0r1d :: Py0
푹 (POOQ)
[한소프트 펌] 웹서버
★ [4-6] 다음과 같은
Linux 명령어 정리
Account Login
w
LOGIN
REGISTER

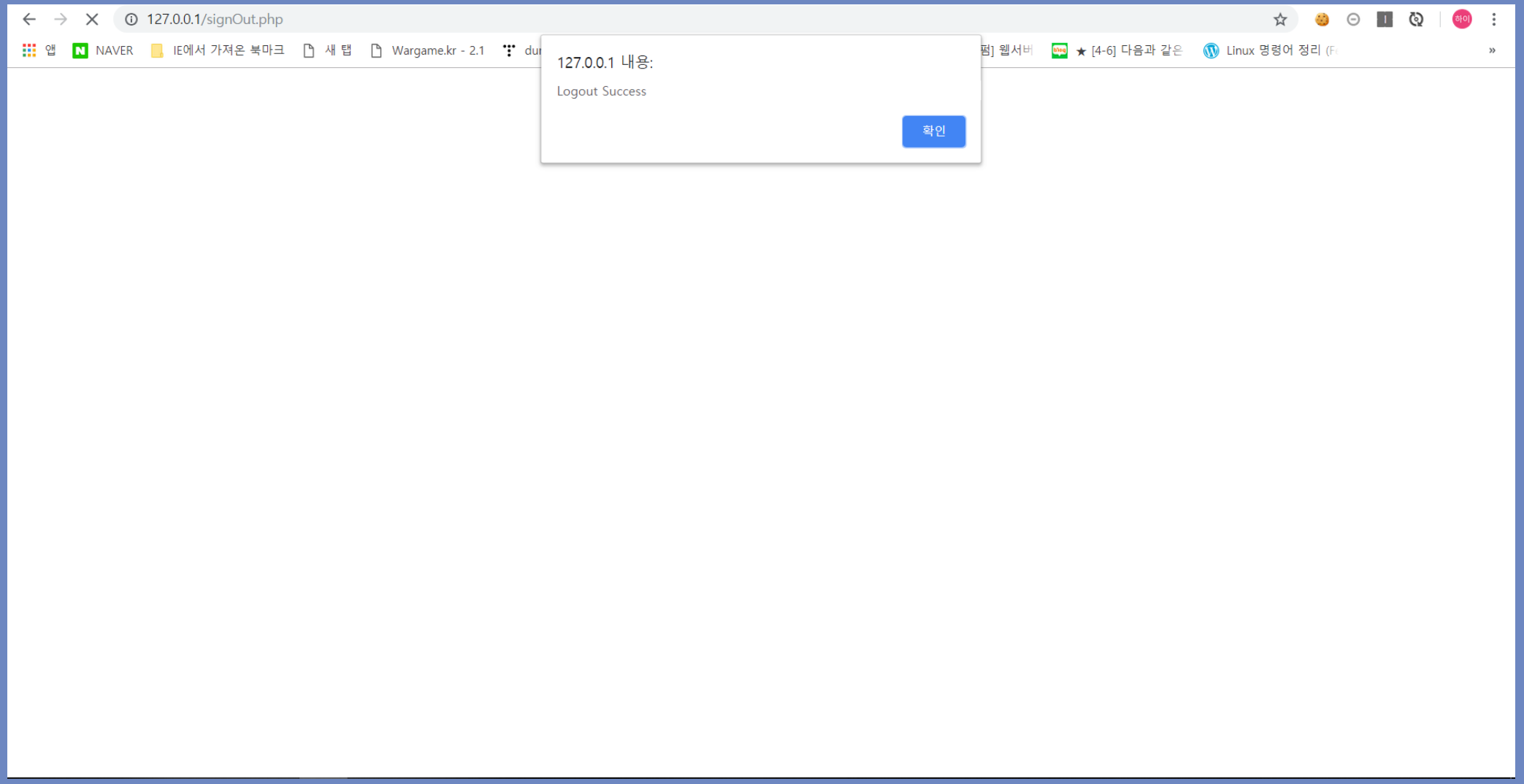

127.0.0.1/signIn.php
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
127.0.0.1 내용:
Login Success
확인
127.0.0.1의 응답을 기다리는 중...


127.0.0.1/main.html
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
duni's Day :: duni's
Py0zz1 W0r1d :: Py0
푹 (POOQ)
[한소프트 펌] 웹서버
★ [4-6] 다음과 같은
Linux 명령어 정리
WELCOME
BOARD
LOGOUT


127.0.0.1/list.php
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
duni's Day :: duni's
Py0zz1 W0r1d :: Py0
푹 (POOQ)
[한소프트 펌] 웹서버
★ [4-6] 다음과 같은
Linux 명령어 정리
게시판입니다..
WRITE
CANCEL
작성자 제목 내용


127.0.0.1/board.html
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
duni's Day :: duni's
Py0zz1 W0r1d :: Py0
푹 (POOQ)
[한소프트 펌] 웹서버
★ [4-6] 다음과 같은
Linux 명령어 정리
자유롭게 글을 작성해주세요
아이디
hello
비밀번호
•••••
제목
안녕하세요?
내용
안녕하세요 반가워요 *^^*!
WRITE
BOARD LIST

userId	userPw	title	content
s	[illegible]	s	s
s	[illegible]	s	s
w	[illegible]	w	w
z	[illegible]	안녕	안녕하세여
wwwwww	[illegible]	ww	ww
wldbs17	[illegible]	안녕	안녕하세요~^^
root	[illegible]		
hello	[illegible]	안녕하세요?	안녕하세요 반가워요 *^^*!


127.0.0.1/signOut.php
앱
NAVER
IE에서 가져온 북마크
새 탭
Wargame.kr - 2.1
127.0.0.1 내용:
Logout Success
확인
★ [4-6] 다음과 같은
Linux 명령어 정리

끝(질문은 없겠지...)

정모.. 나 진짜 최선을 다했어…
난 여기까지인가봐…