



<http://duni0107-day.tistory.com>

A circular diagram with a gold-colored border. Inside the circle, the text '목 차' is centered. The circle is decorated with several small gold dots and arrows pointing clockwise along its perimeter.

## 목 차

A small horizontal line with dots at each end, centered above the first item.

1. 회원가입 정보를 DB에 저장

2. 워게임 풀이

A small horizontal line with dots at each end, centered below the second item.



회 원 가 입 정 보 를 D B 에 저 장



Account Register

NAME	
ID	
PASSWORD	
PASSWORD CHECK	
REGISTER	CANCEL





membersave.php



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

Method 방식은 post로 설정해주고  
action은 membersave.php가 실행되게 함

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

$name=$_POST['name'];
$userId=$_POST['userId'];
$userPw=$_POST['userPw'];
$userPw2=$_POST['userPw2'];

if($userPw == $userPw2) {
    $sql = "insert into person (name,userId, userPw)";
    $sql = $sql."values('$name', '$userId', '$userPw')";

    if($mysqli->query($sql)){
        echo "<script>alert('Success'); location.href='index.html';</script>";
    }else{
        echo "<script>alert('Failed');location.href='register.html';</script>";
    }
}
else {
    echo "<script>alert('no match');location.href='register.html';</script>";
}
?>
```

Db정보가 저장되어 있는 dbConnect.php를 연결해주고  
name,userId,userPw를 각각 db에 맞게 넣어줌



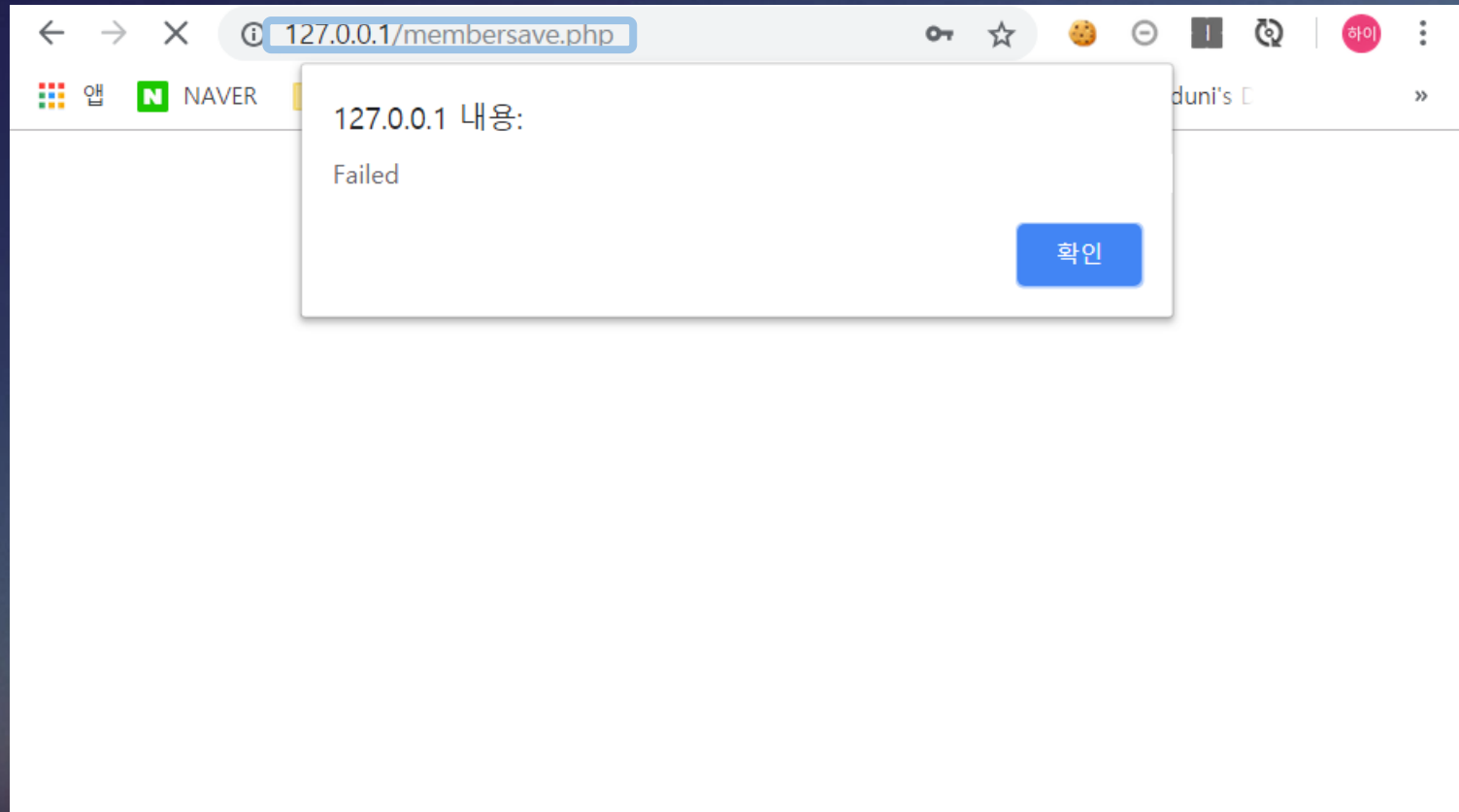
127.0.0.1/register.html/

A screenshot of a web browser window. The address bar shows '127.0.0.1/register.html' with a blue arrow pointing to it from the URL above. The browser's toolbar includes back, forward, refresh, and search icons, along with a star for bookmarks and a cookie icon. The page title is 'Account Register'. The background of the page is a dark space with various galaxies and stars. In the center, there is a registration form with four input fields. The first two fields contain the letter 'q', and the next two contain a single dot. Below the form are two buttons: 'REGISTER' and 'CANCEL'. The browser's taskbar at the bottom shows several open tabs, including 'NAVER', 'IE에서 가져온 북마크', '새 탭', 'Wargame.kr - 2.1', and 'duni's Day :: duni's'.



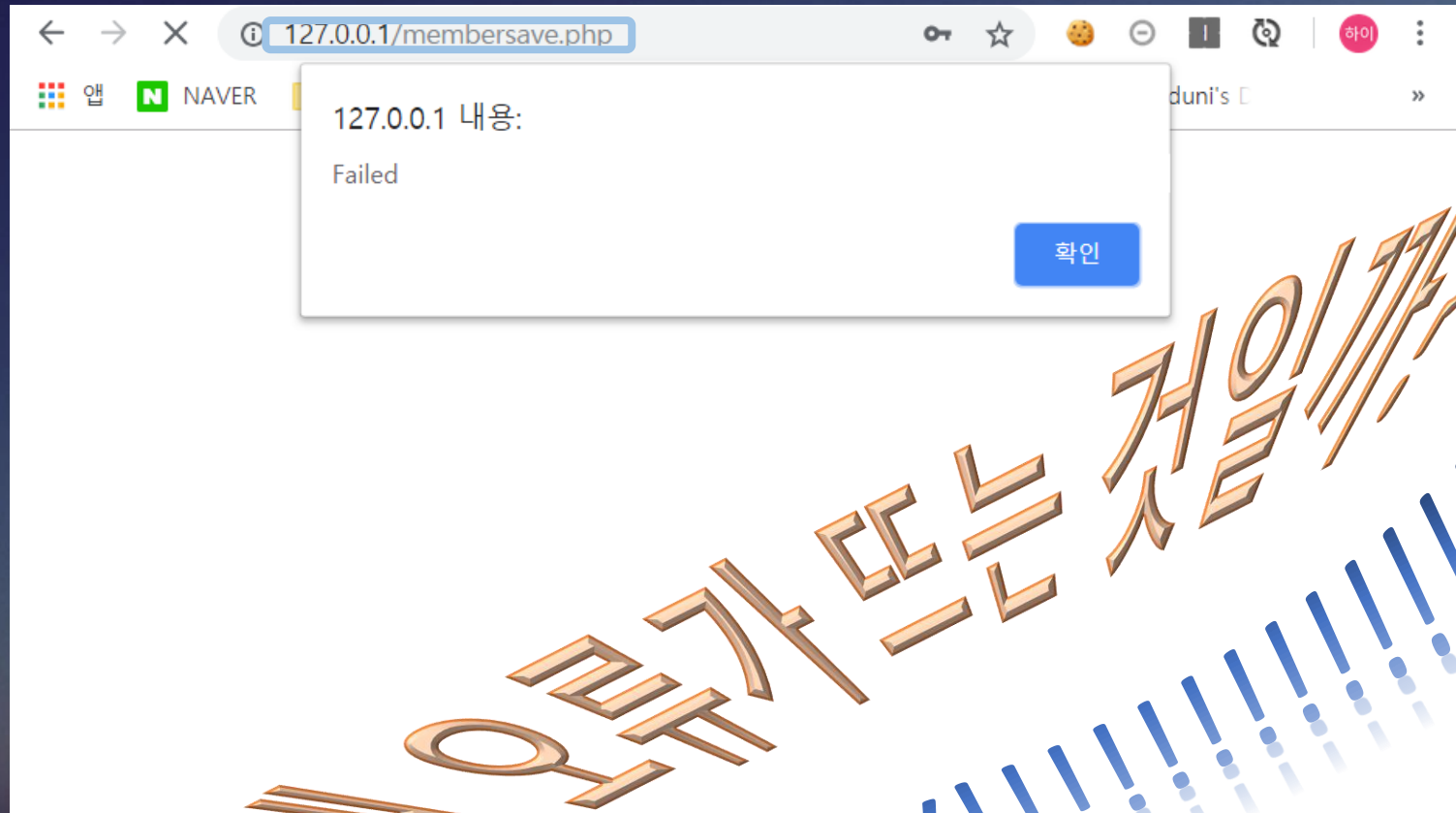


127.0.0.1/membersave.php/





127.0.0.1/membersave.php/



아냐! 곧 성공해서 담주엔  
실습할 수 있을꺼야!



남들은 쉬게 하던데 난  
왜이렇게 어렵지...?







W A R G A M E . k r 문제 풀이

md5\_compare



246point / bughela

JUST COMPARE ONLY.

with the other value :D

FLAG

Auth

Start

Close



VALUE 1 :

VALUE 2 :

[view-source](#)

```
<?php
    if (isset($_GET['view-source'])) {
        show_source(__FILE__);
        exit();
    }

    if (isset($_GET['v1']) && isset($_GET['v2'])) {
        sleep(3); // anti brute force

        $chk = true;
        $v1 = $_GET['v1'];
        $v2 = $_GET['v2'];

        if (!ctype_alpha($v1)) {$chk = false;}
        if (!is_numeric($v2)) {$chk = false;}
        if (md5($v1) != md5($v2)) {$chk = false;}

        if ($chk){
            include("../lib.php");
            echo "Congratulations! FLAG is : ".auth_code("md5_compare");
        } else {
            echo "Wrong...";
        }
    }
}

?>
<br />
<form method="GET">
    VALUE 1 : <input type="text" name="v1" /><br />
    VALUE 2 : <input type="text" name="v2" /><br />
    <input type="submit" value="chk" />
</form>
<br />
<a href="?view-source">view-source</a>
```



```
<?php
if (isset($_GET['view-source'])) {
    show_source(__FILE__);
    exit();
}

if (isset($_GET['v1']) && isset($_GET['v2'])) {
    sleep(3); // anti brute force

    $chk = true;
    $v1 = $_GET['v1'];
    $v2 = $_GET['v2'];

    if (!ctype_alpha($v1)) {$chk = false;}
    if (!is_numeric($v2)) {$chk = false;}
    if (md5($v1) != md5($v2)) {$chk = false;}

    if ($chk){
        include("../lib.php");
        echo "Congratulations! FLAG is : ".auth_code("md5_compare");
    } else {
        echo "Wrong...";
    }
}

?>
<br />
<form method="GET">
    VALUE 1 : <input type="text" name="v1" /><br />
    VALUE 2 : <input type="text" name="v2" /><br />
    <input type="submit" value="chk" />
</form>
<br />
<a href="?view-source">view-source</a>
```

Isset → 설정된 변수인지 확인

ctype\_alpha – 알파벳 문자 확인

Is\_numeric – 수나 수 문자열인지 확인

v1 입력에는 알파벳만,  
v2 입력에는 숫자만 입력

- md5로 출력한 hash 값이 같아야함

# magic hash 취약점

(실제로는 취약점이 아니라 특수 동작임)

1. 비교 연산할 때 Type Juggling을 이용해 서로 다른 값으로 인식되도록 하는 특수 동작
2. 항상 가능한 것은 아니고 특수한 경우 '0e' 시작하는 문자열일 때 가능



VALUE 1 : QNKCDZO  
VALUE 2 : 240610708  
  
[view-source](#)

Md5로 변환시 0e로 시작하는 알파벳 문자열과 숫자 문자열을 넣어주면  
두 수를 같게 인식함





Congratulations! FLAG is :

VALUE 1 :

VALUE 2 :

chk

[view-source](#)





FINISH