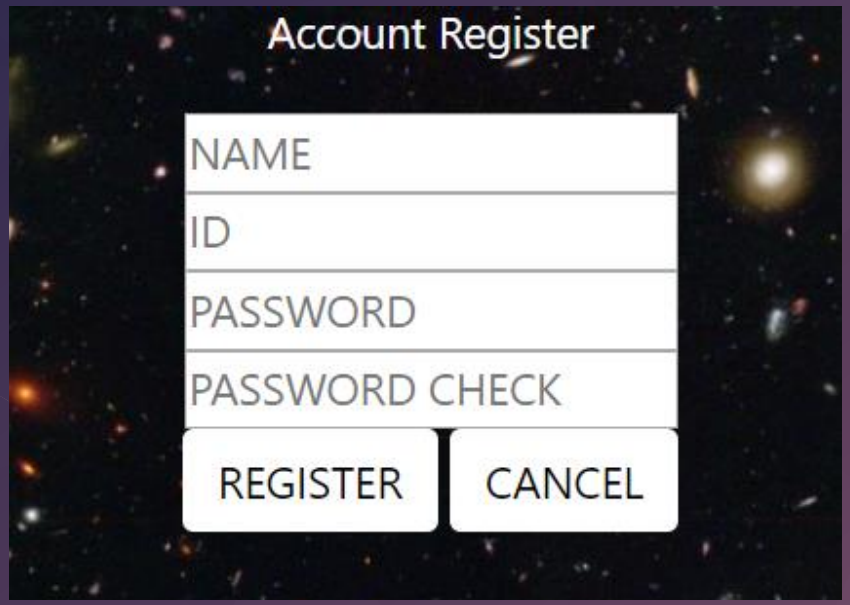

웹
D U N I 1 7
http://duni0107-day.tistory.com

목 차

회원가입 정보를 DB에 저장



membersave.php

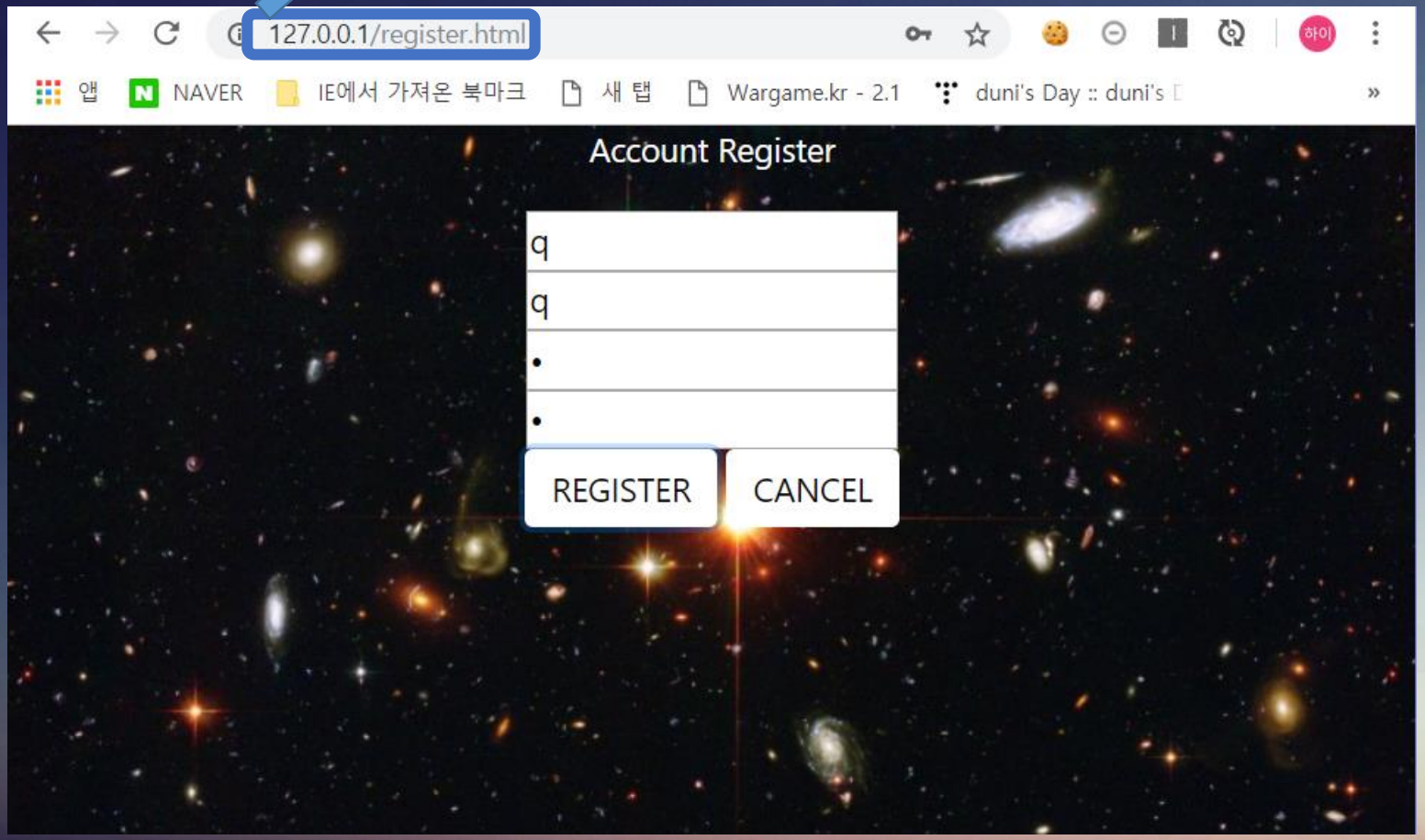
```
<form method="post" action="membersave.php">
```

Method 방식은 post로 설정해주고
action은 membersave.php가 실행되게 함

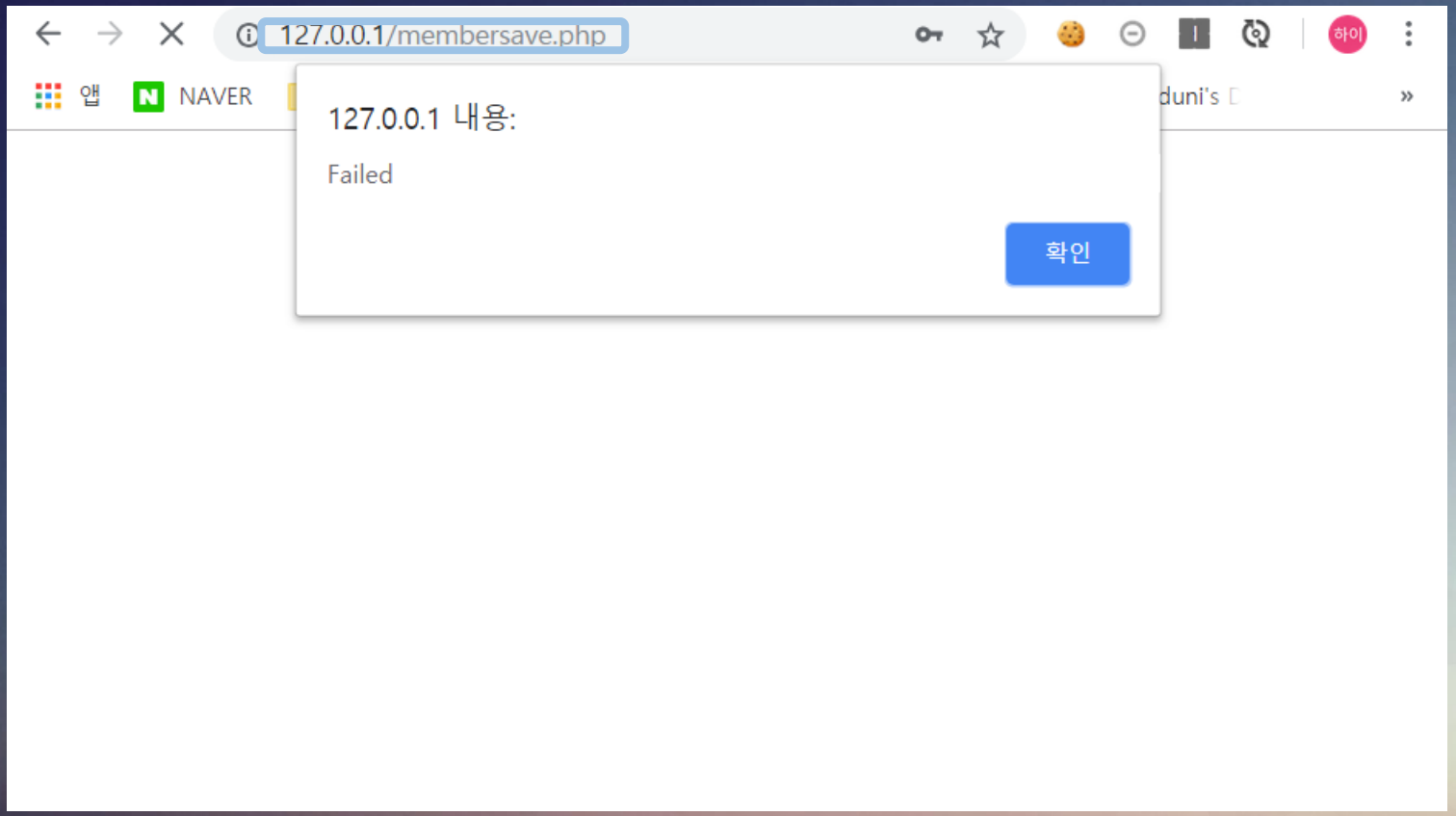
```php
<?php

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

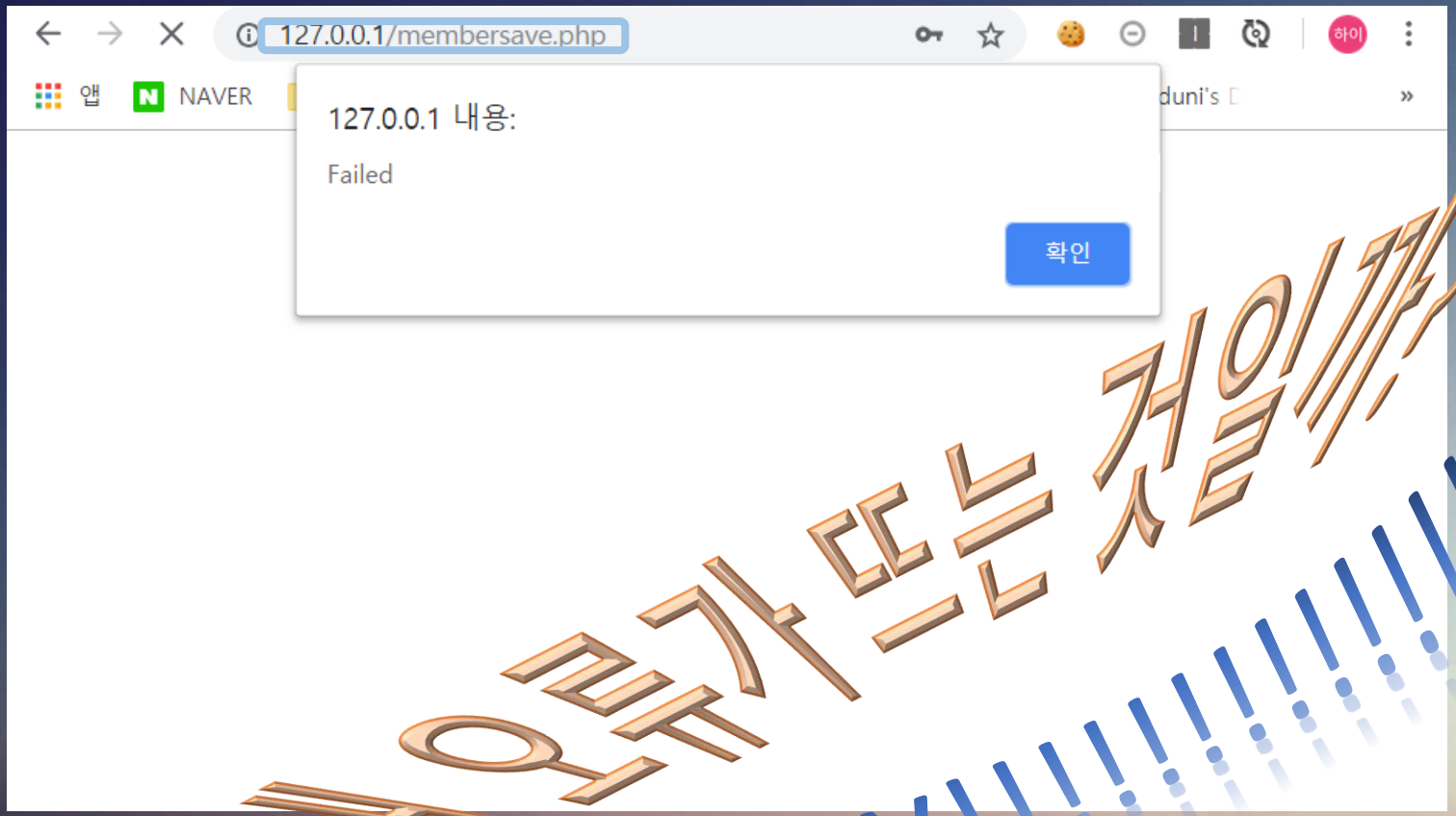
127.0.0.1/register.html/



127.0.0.1/membersave.php/



127.0.0.1/membersave.php/



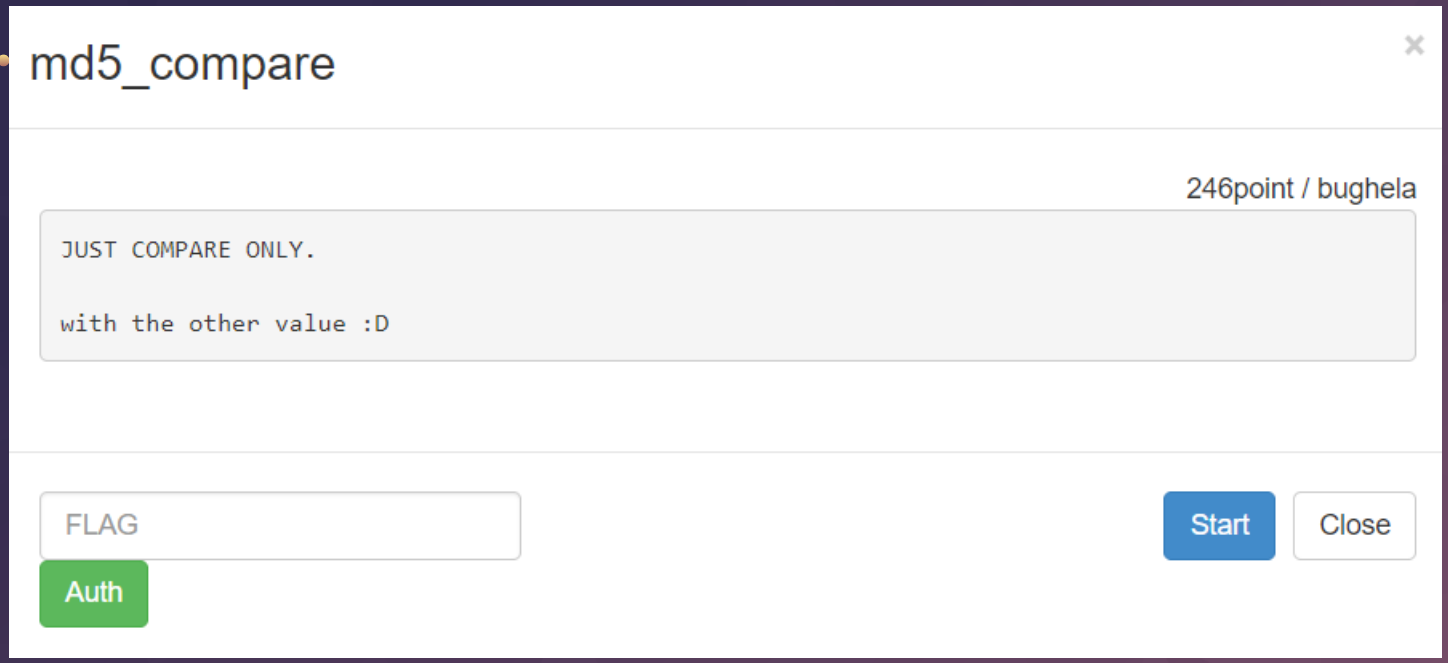
왜 오류가 뜨는 것일까?

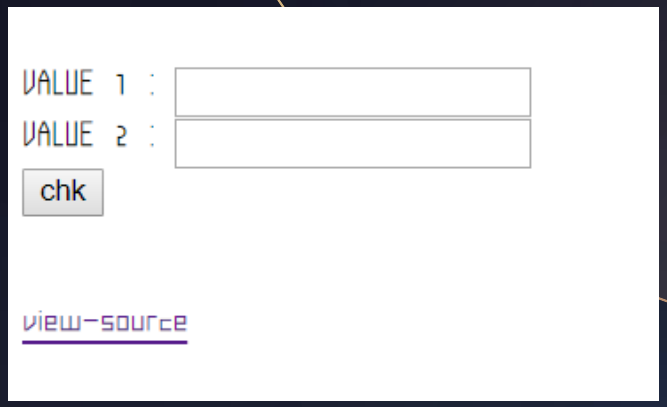
WHY!!!

아냐! 곧 성공해서 담주엔 실습할 수 있을꺼야!

남들은 쉽게 하던데 난 왜이렇게 어렵지..?

WARGAME.kr 문제 풀이






```php
<?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
<?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

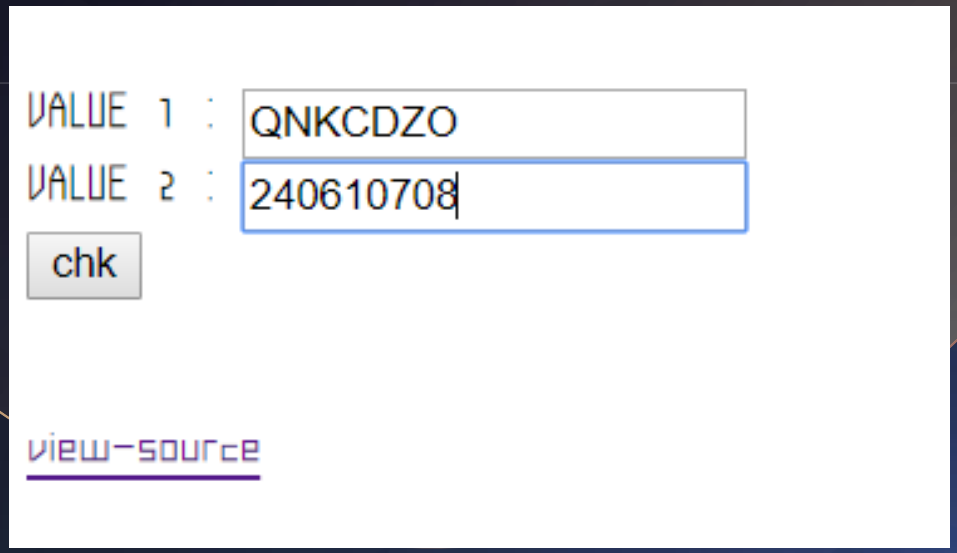
- md5로 출력한 hash 값이 같아야함

magic hash 취약점

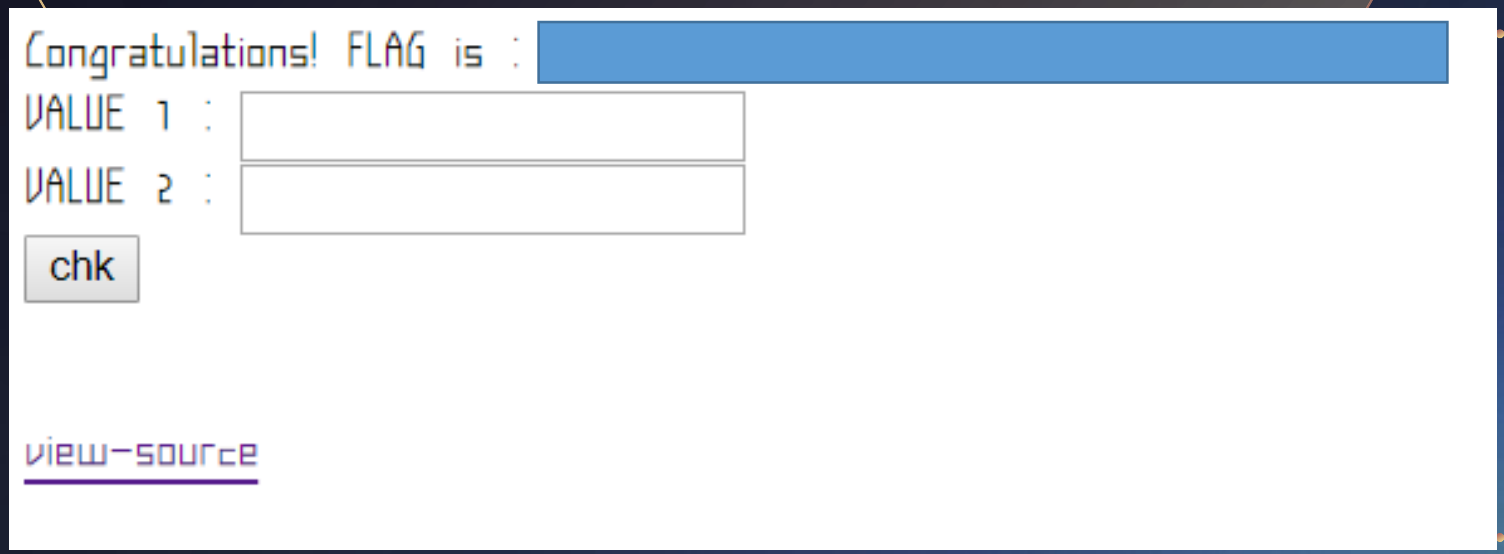
(실제로는 취약점이 아니라 특수 동작임)

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



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


Congratulations! FLAG is :
VALUE 1 :
VALUE 2 :
chk
view-source


FINISH