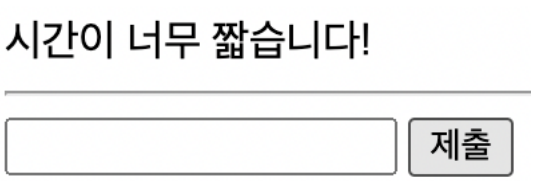
HackCTF time

```php
<?php
$flag = "???";
if(isset($_GET['time'])) {
    if(!is_numeric($_GET['time'])) {
        echo '시간은 숫자만 됩니다!';
    } else if($_GET['time'] < 60 * 60 * 24 * 30 * 2) {
        echo '시간이 너무 짧습니다!';
    } else if($_GET['time'] > 60 * 60 * 24 * 30 * 3) {
        echo '시간이 너무 깁니다!';
    } else {
        sleep((int)$_GET['time']);
        echo "flag is ",  $flag;
    }
    echo '<hr>';
}
?>
```

제출

가장 먼저 들어가면 보이는 화면입니다. time이 숫자인지 확인 후 주어진 범위를 충족시키면 time만큼 sleep후에 플래그를 출력합니다.

숫자 10을 제출하게 되면



이와 같이 나타나게 됩니다.

여기서 생각해볼 수 있는 것은 time은 is_numeric을 통과해야하고 주어진 범위 이내여야 하는 데 범위 내로 숫자가 들어가게 되면 숫자가 너무 커져 너무 오랜 시간 sleep을 하게 됩니다. 여기서 어떤 형식들이 is_numeric을 통과하는 지 확인해 보겠습니다.

```php
$tests = array(
    "42",
    1337,
    0x539,
    02471,
    0b10100111001,
    1337e0,
    "0x539",
    "02471",
    "0b10100111001",
    "1337e0",
    "not numeric",
    array(),
    9.1,
    null,
    '',
);
```

```
'42' is numeric
1337 is numeric
1337 is numeric
1337 is numeric
1337 is numeric
1337.0 is numeric
'0x539' is NOT numeric
'02471' is numeric
'0b10100111001' is NOT numeric
'1337e0' is numeric
'not numeric' is NOT numeric
array (
) is NOT numeric
9.1 is numeric
NULL is NOT numeric
'' is NOT numeric
```

여기서 주목해야할 부분은 지수형식입니다. 지수형식은 is_numeric을 통과하게 되고

```php
sleep((int)$_GET['time']);
```

여기서 int형변환을 통해 소수점 뒤의 부분은 없어지게 됩니다.
예를 들면 12.1e3 같은 경우 값의 경우 12100이지만 int형변환을 하게 되면 소수점 뒤의 부분이 없어지게 되어 12가 됩니다.
따라서 5184000과 7776000 사이의 수인 5185000를 지수형식으로 나타낸 5.185e6을 입력하게 되면 is_numeric과 범위를 통과하고 int형변환 후 5가 되어 5만큼 sleep 후 플래그가 나타나게 됩니다.

flag is HackCTF{1_w4nt_t0_sp3nd_m0r3_t1m3}