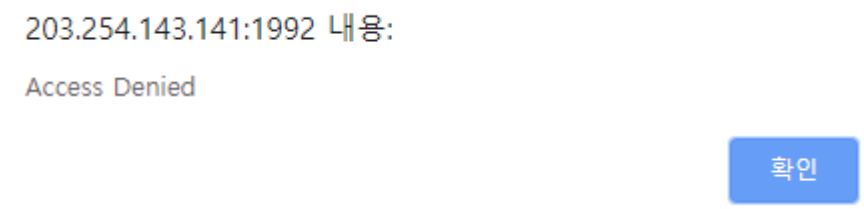
Password Solution.



Host : 203.254.143.141:1992

/password 를 들어가면 다음 사진과 같이 자바스크립트가 실행된다. 방해 되므로 자바스크립트를 끄고 다시 접속하면

이러한 form이 나온다.

텍스트박스에 아무 내용이나 적고 버튼을 누르면 that's wrong이 나오는데

203.254.143.141:1992/password.php?pasword=a

주소창을 보니 get 방식으로 데이터가 넘어가는 것을 알 수 있다.

문제 이름이 find password 이므로 password로 바꾸고 데이터를 넘기면 똑같이 that's wrong이 나오는데 개발자 도구로 페이지를 뜯어보니

Password = password 라는 힌트가 있다

주소창에서 password=password를 보내게 되면

Find the password

search

Don't you think it's too easy?
No answer

Hint : view-source

이렇게 나오는데 소스를 한번 보자.

```
<?php
$answer = $_GET["password"];
if( htmldecode(urldecode($answer)) == "password")
{
echo flag();
}
else if("password"==$answer)
{
        echo "Don't you think it's too easy?<br>No answer<br><br>";
        echo "Hint : <a href='view-source.txt'>view-source</a>";
}
else if(empty($answer) and empty($_GET["pasword"]))
{
echo "";
}
else
{
echo "<br>That's wrong!";
}
?>
```

이렇게 나온다. 답을 보아하니 password를 html인코딩을 한 후 url인코딩을 한 값을 넘기면 flag가 나오는 것 같다.

Password를 html 인코딩 하면 password

이를 url 인코딩 하면

%26%23112%3B%26%2397%3B%26%23115%3B%26%23115%3B%26%23119%3B%26%23111%3B%26%23114%3B%26%23100%3B

203.254.143.141:1992/password.php?password=%26%23112%3B%26%2397%3B%26%23115%3B%26%23115%3B%26%23119%3B%26%23111%3B%26%23114%3B%26%23100%3B

이렇게 보내면

답이 나온다.

Find the password

search

flag:PaSs_worD