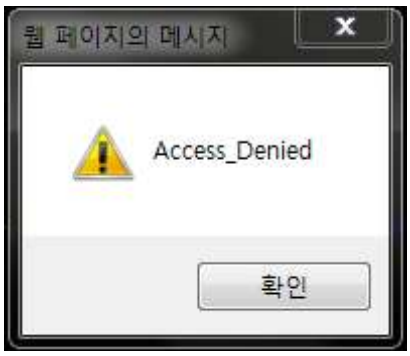
webhacking.kr 5번문제

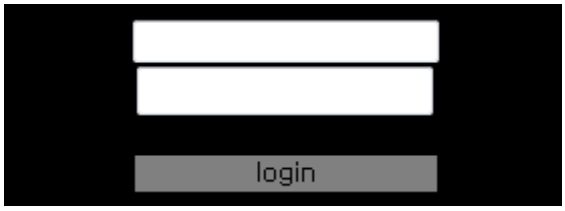
Infini45T
2011.08.05

다음과 같이 Login과 Join이 보인다.
Join을 눌러 회원가입 창을 보자.

다음과 같이 Access_Denied라는 에러창이 뜬다.



로그인 창을 한번 보았다.



로그인 창의 주소는 다음과 같았다.
http://webhacking.kr/challenge/web/web-05/mem/login.php

게싱을 하여 회원가입 창의 주소를 알아내었다.

http://webhacking.kr/challenge/web/web-05/mem/join.php

회원가입 창에 들어가니 까만배경에 아무것도 있지 않았다.
소스를 보니 소스가 다음과 같았다.

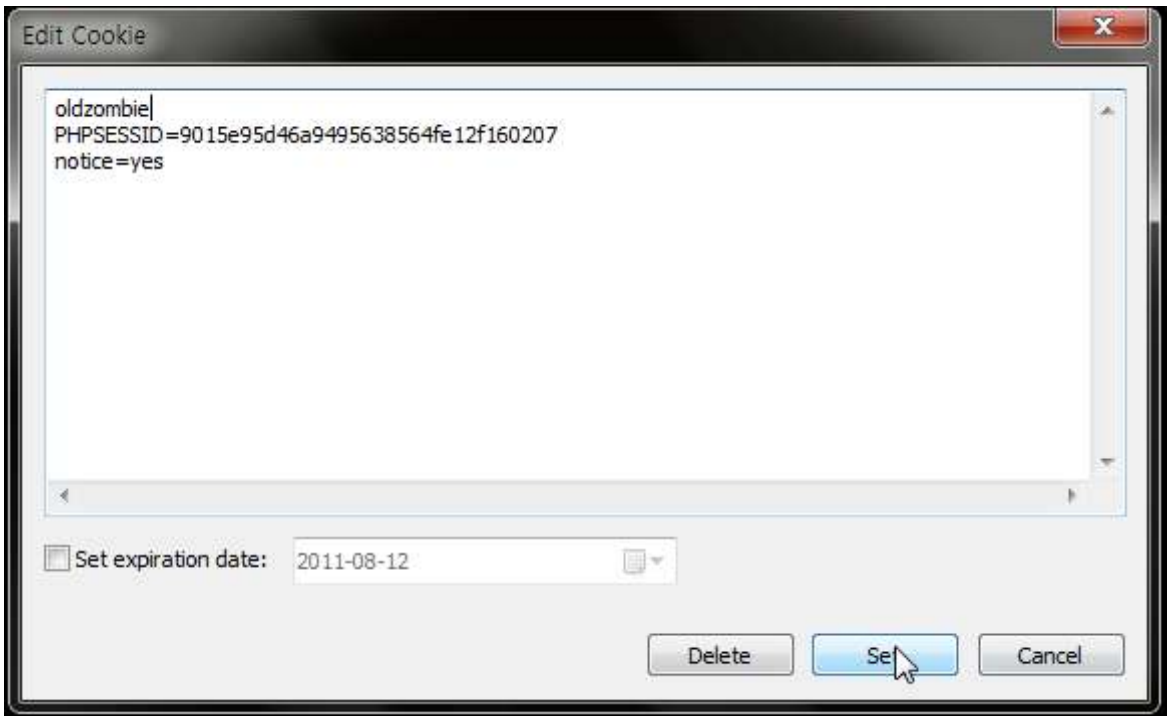
```
<html>
<title>Challenge 5</title></head><body bgcolor=black><center>
<script>
l='a';ll='b';lll='c';llll='d';lllll='e';llllll='f';lllllll='g';llllllll='h';lllllllll='i';llllllllll='j';lllllllllll='k';llllllllllll='l';llll
lllllllll='m';llllllllllllll='n';lllllllllllllll='o';llllllllllllllll='p';lllllllllllllllll='q';llllllllllllllllll='r';lllllllllllllllllll='s';llllllll
llllllllllll='t';lllllllllllllllllllll='u';llllllllllllllllllllll='v';lllllllllllllllllllllll='w';llllllllllllllllllllllll='x';lllllllllllllllllllllllll='y
';llllllllllllllllllllllllll='z';I='1';II='2';III='3';IIII='4';IIIII='5';IIIIII='6';IIIIIII='7';IIIIIIII='8';IIIIIIIII='9';IIIIIIIIII='
0';li='.';ii='<';iii='>';lIIlIIlIIlIIlIIlIIlIIlIIlI=lllllllllllllll+llllllllllll+llll+llllllllllllllllllllllllll+lllllllllllllll+lllllllllllll+l
l+lllllllll+lllll;
lIIIIIIIIIIIIIIIIIl=llll+lllllllllllllll+lll+lllllllllllllllllllll+lllllllllllll+lllll+llllllllllllll+llllllllllllllllllll+li+lll+lllllllllllllll+
lllllllllllllll+lllllllllll+lllllllll+lllll;if(eval(lIIIIIIIIIIIIIIIIIl).indexOf(lIIlIIlIIlIIlIIlIIlIIlIIlI)==-1) { bye;
}if(eval(llll+lllllllllllllll+lll+lllllllllllllllllllll+lllllllllllll+lllll+llllllllllllll+llllllllllllllllllll+li+'U'+'R'+'L').indexOf
(lllllllllllll+lllllllllllllll+llll+lllll+'='+I)==-1){alert('access_denied');history.go(-1);}else{document.writ
e('<font size=2
color=white>Join</font><p>');document.write('.<p>.<p>.<p>.<p>.<p>');document.write('<f
orm method=post action='+llllllllll+lllllllllllllll+lllllllll+llllllllllllll+li+llllllllllllllll+llllllll+llllllllllllllll
+'>');document.write('<table border=1><tr><td><font
color=gray>id</font></td><td><input type=text name='+lllllllll+llll+'
maxlength=5></td></tr>');document.write('<tr><td><font
color=gray>pass</font></td><td><input type=text name='+llllllllllllllll+lllllllllllllllllllllll+'
maxlength=10></td></tr>');document.write('<tr align=center><td colspan=2><input
type=submit></td></tr></form></table>');}
</script>
</body>
</html>
```

일일히 원래 소스로 바꿔보았다.

```
<html>
<title>Challenge 5</title></head><body bgcolor=black><center>
<script>if(eval(document.cookie).indexOf(oldzombie)==-1) { bye;
}if(eval(d+o+c+u+m+e+n+t+.+'U'+'R'+'L').indexOf(m+o+d+e+'='+1)==-1){alert('access_deni
ed');history.go(-1);}else{document.write('<font size=2
color=white>Join</font><p>');document.write('.<p>.<p>.<p>.<p>.<p>');document.write('<f
orm method=post action='+j+o+i+n+.+p+h+p
+'>');document.write('<table border=1><tr><td><font
color=gray>id</font></td><td><input type=text name='+i+d+'
maxlength=5></td></tr>');document.write('<tr><td><font
color=gray>pass</font></td><td><input type=text name='+p+w+'
maxlength=10></td></tr>');document.write('<tr align=center><td colspan=2><input
```

type=submit></td></tr></form></table>');}
</script>
</body>
</html>

대충 해석해보자면 Join의 내용을 뜨게 하려면 다음과 같이 쿠키에 oldzombie를 넣고 http://webhacking.kr/challenge/web/web-05/mem/join.php?mode=1 이 주소로 들어가면 된다.

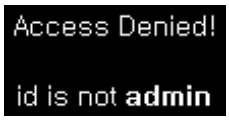


그러자 다음과 같이 폼이 나타났다.

다음과 같이 폼에 값을 넣고 쿼리를 전송 해 보았다.

다음과 같이 출력되었다.

위의 아이디로 로그인을 해보았으나 다음과 같이 뜨고 되지 않았다.



파로스로 잡아서 다음과 같이 값을 변경하여 전송하였다.

```
id=admin                                *&pw=asdf123
```

다음과 같이 sign up이라고 출력되었다.

```
<html>
<title>Challenge 5</title></head><body bgcolor=black><center>
<font size=2 color=white>sign up</font>
```

그리고 로그인을 하니 로그인이 되었고 문제를 풀었다.
이것은 mysql상의 길이 오류이다.
위의 폼에서 길이제한을 5로 두어서 불가능했지만 파로스로 길이를 변경하여 우회에 성공하였다.
위의 취약점은 서버스크립트단에서 길이체크를 하면 손쉽게 막을 수 있다.
참조 글: http://teamcrak.tistory.com/54