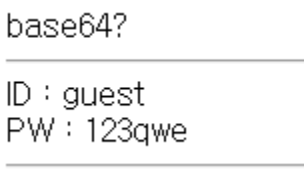
webhacking.kr 6번문제

B1ackZer0
2011.04.04

다음과 같은 글이 있다.



위의 그림만으론 문제를 풀 수 없으니 단서를 구해보자.
아래는 소스보기를 하여 본 소스이다.
주석으로 index.phps가 있다.
한번 들어가 보자.

```
<html>
<head>
<title>Challenge 6</title>
</head>
<body>

base64?<hr>ID : guest<br>PW : 123qwe<hr>
<!--

index.phps

-->


</body>
</html>
```

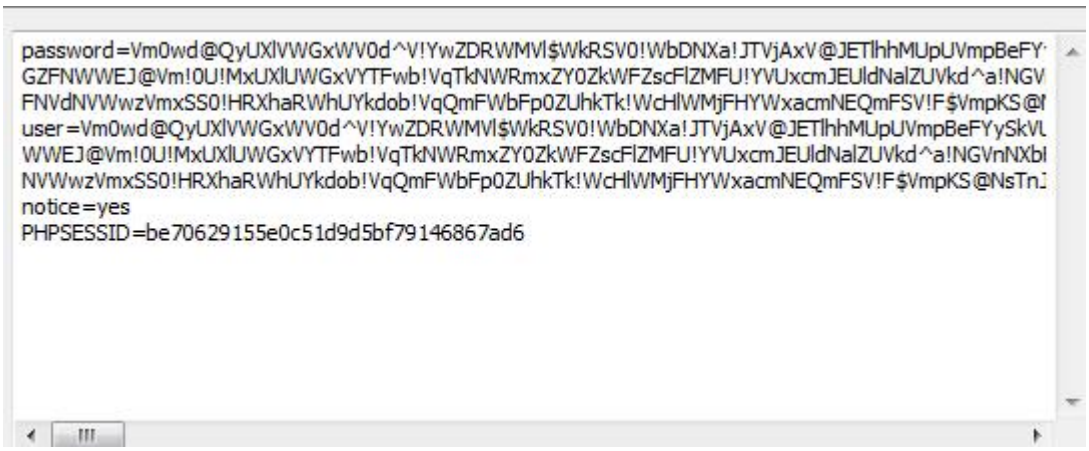
```
<html>
<head>
<title>Challenge 6</title>
</head>
<body>
```

index.phps로 들어가서 본 index.php의 소스이다.

```
<?

if(!$_COOKIE[user])
{
$val_id="guest";
$val_pw="123qwe";

for($i=0;$i<20;$i++)
{
$val_id=base64_encode($val_id);
$val_pw=base64_encode($val_pw);

}

$val_id=str_replace("1","!",$val_id);
$val_id=str_replace("2","@",$val_id);
$val_id=str_replace("3","$",$val_id);
$val_id=str_replace("4","^",$val_id);
$val_id=str_replace("5","&",$val_id);
$val_id=str_replace("6","*",$val_id);
$val_id=str_replace("7","(",$val_id);
$val_id=str_replace("8",")",$val_id);

$val_pw=str_replace("1","!",$val_pw);
$val_pw=str_replace("2","@",$val_pw);
$val_pw=str_replace("3","$",$val_pw);
$val_pw=str_replace("4","^",$val_pw);
$val_pw=str_replace("5","&",$val_pw);
$val_pw=str_replace("6","*",$val_pw);
$val_pw=str_replace("7","(",$val_pw);
$val_pw=str_replace("8",")",$val_pw);



Setcookie("user",$val_id);
Setcookie("password",$val_pw);

echo("<meta http-equiv=refresh content=0>");
}
?>

<html>
<head>
<title>Challenge 6</title>
</head>
<body>

<?

$decode_id=$_COOKIE[user];
$decode_pw=$_COOKIE[password];
```

```
$decode_id=str_replace("!","1",$decode_id);
$decode_id=str_replace("@","2",$decode_id);
$decode_id=str_replace("$","3",$decode_id);
$decode_id=str_replace("^","4",$decode_id);
$decode_id=str_replace("&","5",$decode_id);
$decode_id=str_replace("*","6",$decode_id);
$decode_id=str_replace("(","7",$decode_id);
$decode_id=str_replace(")","8",$decode_id);

$decode_pw=str_replace("!","1",$decode_pw);
$decode_pw=str_replace("@","2",$decode_pw);
$decode_pw=str_replace("$","3",$decode_pw);
$decode_pw=str_replace("^","4",$decode_pw);
$decode_pw=str_replace("&","5",$decode_pw);
$decode_pw=str_replace("*","6",$decode_pw);
$decode_pw=str_replace("(","7",$decode_pw);
$decode_pw=str_replace(")","8",$decode_pw);




for($i=0;$i<20;$i++)
{
$decode_id=base64_decode($decode_id);
$decode_pw=base64_decode($decode_pw);
}

echo("ID : $decode_id<br>");
echo("PW : $decode_pw<br>");



if($decode_id=="admin" && $decode_pw=="admin")
{

$answer="????";

echo("<hr>Congratulation!<p>Password is <b>$answer</b><hr>");
}


?>

<!--

index.php.bak

-->

</body>
</html>
```

대충 해석하자면 이렇다.
쿠키의 값을 20번 base64인코드한 후, 치환한것이다.
패스워드를 얻으려면 거꾸로 절차를 밟으면 된다.
admin을 base64 인코드를 20번하고, 치환을 한 값을 쿠키에 넣으면 클리어된다.
쿠키를 admin을 base64 인코드를 20번하고 치환한 값으로 설정해보자.



admin으로 로그인에 성공했고 패스워드를 알아냈다.

base64?

ID : admin
PW : admin

Congratulation!

Password is **tlqkfdkaghanjffhgodiehlwl**