Challange6

페이지를 들어가면 ID : guest, PW : 123qwe를 확인할 수 있다.

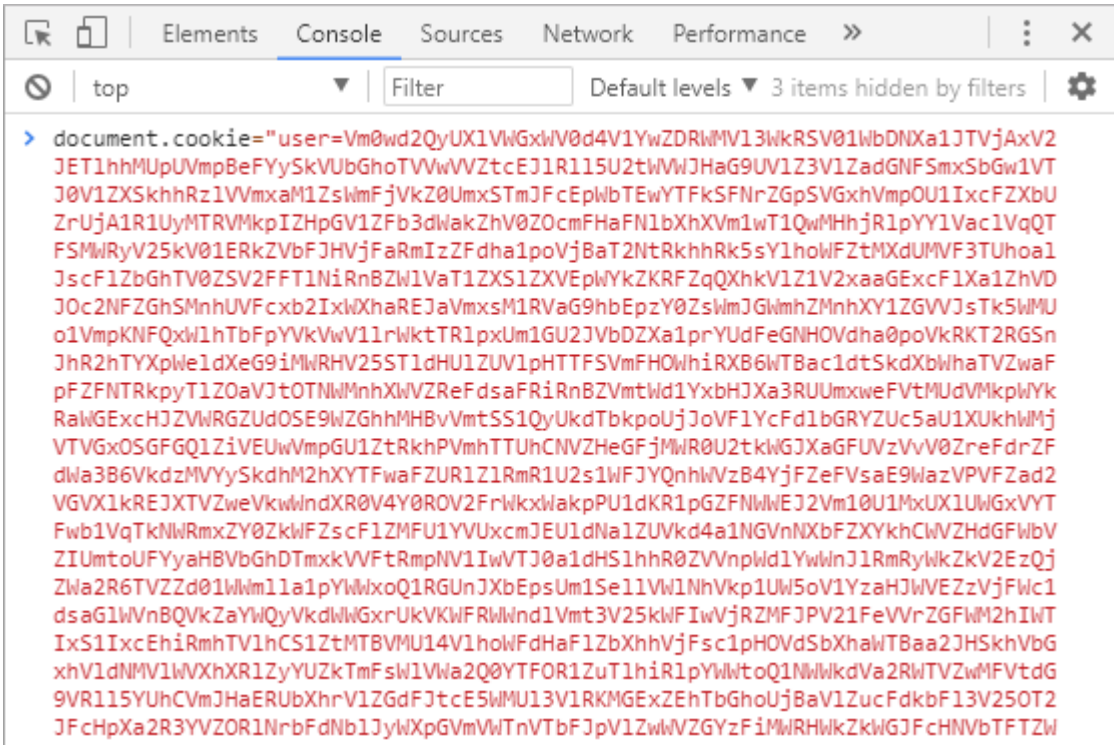
Index.phps를 확인해보면 guest와 123qwe를 변수에 입력한 뒤 Base64로 20번 인코딩한 뒤 #str_replace로 인해 "1" 이라는 값이 $var_id에 저장되있으면 "!" 로 치환해서 $val_id에 저장(이하 동일) 한 뒤 쿠키에 저장한다는 것 을 확인할 수 있다.

```php
<?php
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>");
}
?>
```

다음 소스를 보면 치환하였던 숫자를 다시 숫자로 치환한 뒤 20번 디코딩 그리고 user와 password가 admin인지 비교하는 구문이 있다.

```php
<?

$decode_id=$_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("<font style=background:silver;color:black>  HINT : base64  </font><hr><a href=index.phps style=color:yellow;>index.phps</a><br><br>");
echo("ID : $decode_id<br>PW : $decode_pw<hr>");

if($decode_id=="admin" && $decode_pw=="admin")
{
    @solve(6,100);
}


?>
```

현재 guest, 123qwe가 base64로 20번 인코딩 되어 저장되어 있는 쿠키 값을 admin을 base64로20번인코딩한 값으로 변경하면 된다.



그리고 다시 페이지로 돌아가 확인을 해보면 ID와 PW가 admin으로 바뀐 것을 확인할 수 있다.