webhacking.kr 38번문제

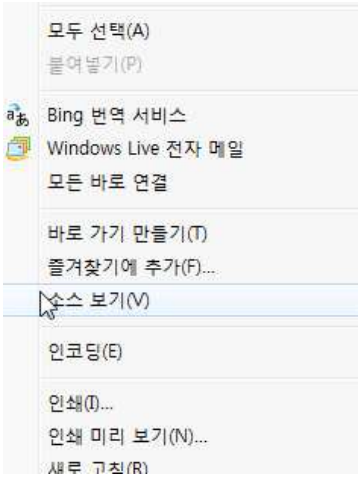
B1ackZer0
2011.04.15

다음과 같은 폼이있다.
로그 인젝션이라고한다.

LOG INJECTION

Login Admin

소스를 한번 보자.



다음이 소스이다.
주석으로 admin.php를 알려준다.
하지만, 소스를 보지 않았어도 이미 폼에 admin버튼이 있고 누르면 admin.php로 이동되는 것을 볼 수 있다.

```
<html>
<head>
<title>Challenge 38</title>
</head>
<body>
<h1>LOG INJECTION</h1>
<!-- admin.php -->
```

<form method=post action=index.php>
<input type=text name=id size=20>
<input type=submit value='Login'><input type=button value='Admin' onclick=location.href='admin.php'>
</form>
</body>
</html>

대충 aaaa를 넣어서 Login을 해서 로그를 남겨보았다.

admin페이지로 가서 로그를 확인해보았다.

로그에 아이피와 로그인한 아이디가 보인다.

admin으로 로그인해보았다.

예상대로 다음과 같이 로그인이 안된다고 뜬다.

url인코딩이 되는지, 인젝션이 되는지 등등 확인을 위해 특수문자들을 넣어보았다.

다음과 같이 url인코딩, 인젝션등등이 먹히는않는 것을 볼 수 있다.

log
123.142.203.94:aaaa
123.142.203.94:%0a ' # <!--

풀이방법을 못 찾고 헤메다가 우연히 생각나서 시도해봤다.
로그가 뜨고, 그것을 인식하여 admin인지 확인하는 방식이라는 가정하에 시도해 본 방법이다.
가정이 맞다면, 로그는 123.142.203.94: <--공백
123.142.203.94:admin
다음과 같이 뜨게 되어 로그 인젝션에 할것이다.

password 값을 얻었고, 인증에 성공했다.

log
123.142.203.94:aaaa
123.142.203.94:%0a ' # <!--

Password is 3aab802ec9a2b7124aa49906954ef60d