

다음과 같은게 보인다.

Wrong IP! 를 출력한다.

client ip	123.142.203.94
agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MASM; InfoPath.2)

Wrong IP!

소스를 한번 보자.



아래는 소스보기를 통해 본 소스이다.

```
<html>
<head>
<title>Challenge 24</title>
</head>
<body>
<table border=1><tr><td>client ip</td><td>123.142.203.94</td></tr><tr><td>agent
</td><td>Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MASM;
InfoPath.2)</td></tr></table><p><hr><center>Wrong IP!</center><hr>
```

```
<!--
```

```
source : index.php
```

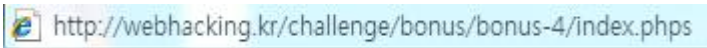
```
-->
```

```
</body>
```

```
</html>
```

주석으로 index.php 가르킨다.

index.php를 가서 소스를 보자.



이것이 원본 소스이다.

대충 살펴보면 쿠키에서 REMOTE_ADDR변수의 값을 필터링을 통해 127.0.0.1일 경우 패스워드를 출력하는 것이다.

```
<html>
```

```
<head>
```

```
<title>Challenge 24</title>
```

```
</head>
```

```
<body>
```

```
<?
```

```
$answer="????";
```

```
extract($_SERVER);
```

```
extract($_COOKIE);
```

```
$ip=$_REMOTE_ADDR;
```

```
$agent=$_HTTP_USER_AGENT;
```

```
if($_COOKIE[REMOTE_ADDR])
```

```
{
```

```
$ip=str_replace("127", "", $ip);
```

```
$ip=str_replace("7.", "", $ip);
```

```
$ip=str_replace("0.", "", $ip);
```

```
}
```

```
echo("<table                                border=1><tr><td>client
ip</td><td>$ip</td></tr><tr><td>agent</td><td>$agent</td></tr></table>");
```

```
if($ip=="127.0.0.1")
{
echo("<p><hr><center>Congratulation! Password is $answer</center><hr>");
}
```

```
else
{
echo("<p><hr><center>Wrong IP!</center><hr>");
}
?>
```

<!--

source : index.phps

-->

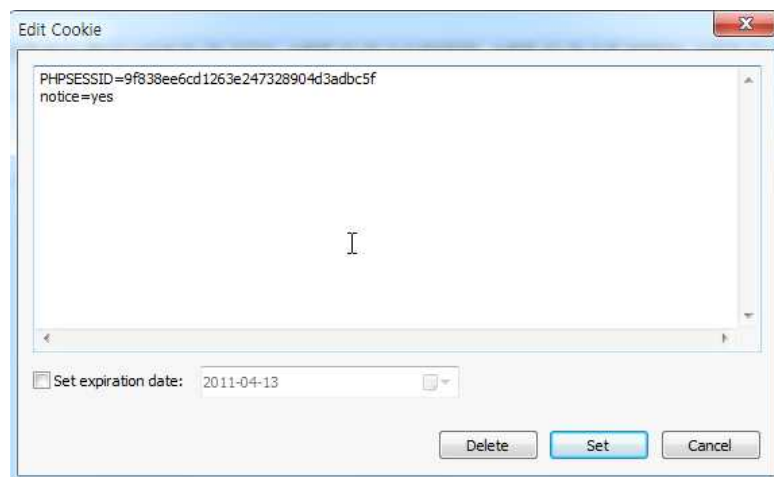
</body>

</html>

쿠키의 Edit Cookie를 눌러주자.



다음과 같이 쿠키가 보여지고, 수정이 가능하다.



다음이 필터링 소스이다.

12, 7., 0.을 공백으로 치환한다.

```
$ip=str_replace("12","", $ip);
```

```
$ip=str_replace("7.", "", $ip);
```

```
$ip=str_replace("0.", "", $ip);
```

이 치환을 이용해서 필터링을 우회하게 입력하자.

REMOTE_ADDR에 필터링을 우회하기 위해 10.270..00..00..1을 입력했다.



그러면 127.0.0.1으로 ip가 입력되고 패스워드가 출력된다.

Congratulation! Password is V2ryyyyyyyyyy_EasYYY!
