< 웹해킹 4주차 과제 (16번, 20번) >

김수현

16번.

16번 문제를 보고 진짜 당황했다. 저 별표들은 무엇일까..라는 생각에 잠시 멍을 때렸지만 다시 정신줄을 붙잡고 익숙하게 페이지 소스보기를 클릭했다. 그랬더니 아래와 같은 소스코드가 떴다.

```
<html>
<head>
<title>Challenge 16</title>
<body bgcolor=black onload=kk(1,1) onkeypress=mv(event.keyCode)>
<font color=silver id=c></font>
<font color=yellow size=100 style=position:relative id=star>*</font>
<script>
document.body.innerHTML+="<font color=yellow id=aa style=position:relative;left:0;top:0>*</font>";
function mv(cd){
  kk(star.style.left-50,star.style.top-50);
  if(cd==100) star.style.left=parseInt(star.style.left+0,10)+50+"px";
  if(cd==97) star.style.left=parseInt(star.style.left+0,10)-50+"px";
  if(cd==119) star.style.top=parseInt(star.style.top+0,10)-50+"px";
  if(cd==115) star.style.top=parseInt(star.style.top+0,10)+50+"px";
  if(cd==124) location.href=String.fromCharCode(cd)+".php"; // do it!
}
function kk(x,y){
  rndc=Math.floor(Math.random()*9000000);
  document.body.innerHTML+="<font color=#"+rndc+" id=aa style=position:relative;left:"+x+";top:"+y+" onmouseover=this.innerHTML=''>*</font>";
}
</script>
</body>
</html>
```

잘 보면, 중간부분에 function mv(cd) 부분이 있는데, if문이 여러 개가 있는 것을 확인해볼 수 있다. 이 if문은 입력된 값에 따라 별이 움직이거나 페이지가 이동되는 것을 알 수 있다. 처음에는 이 숫자들이 무엇일까 고민을 해보았는데, 아스키코드 같아서 표를 통해 찾아보았다.

100 – d

97 – a

119 – w

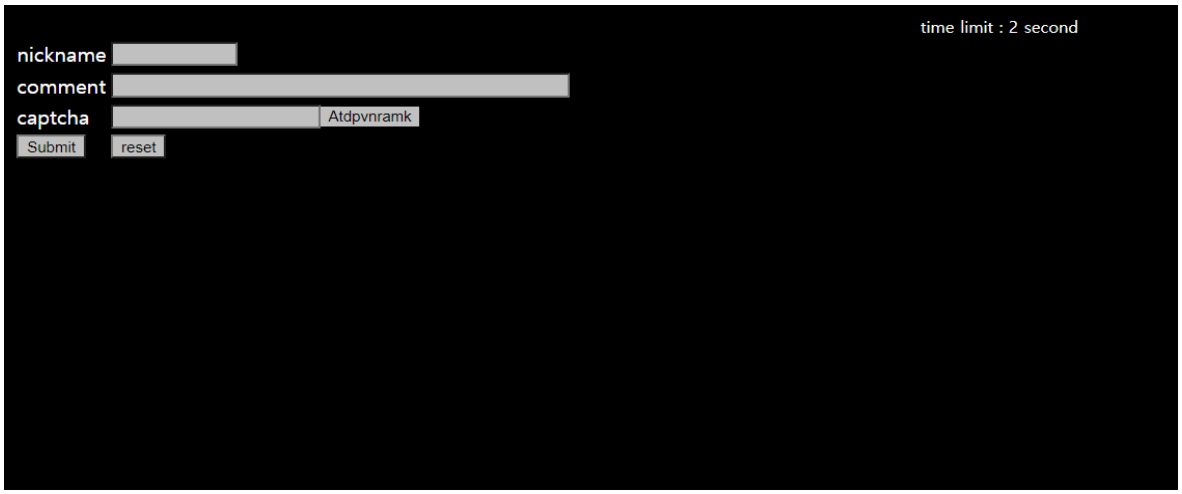
115 - s

124 - |

그런데, 소스코드에 보면 맨 마지막 if문 옆에 주석으로 "do it!" 이라고 써져 있어서 뭘 하라는 건지.... 그래서 위에 나온 문자들을 16번 문제 창에 입력했는데 맨 마지막에 | 부분에서 문제가 풀렸다고 뜨게 되었다. 알고 보니, 변수 값이 124이면 특정 페이지로 이동하는 코드였다.

old-16 Pwned. You got 10point. Congratz!

20번.



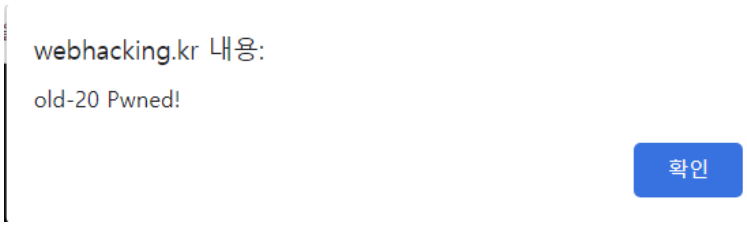
20번 문제는 nickname, comment, captcha를 입력하고 submit으로 제출하면 풀리는 문제인 듯 했다. 근데, 중간 맨 위에 time limit가 2초 인 것을 보고 2초 안에 제출해야 되나? 라는 생각이 들었다. 그래서 일단 소스코드부터 확인해보았다.

```
<html>
<head>
<title>Challenge 20</title>
<style type="text/css">
body { background:black; color:white; font-size:10pt; }
input { background:silver; color:black; font-size:9pt; }
</style>
</head>
<body>
<center><font size=2>time limit : 2 second</font></center>
<form name=lv5frm method=post>
<table border=0>
<tr><td>nickname</td><td><input type=text name=id size=10 maxlength=10></td></tr>
<tr><td>comment</td><td><input type=text name=cmt size=50 maxlength=50></td></tr>
<tr><td>captcha</td><td><input type=text name=captcha><input type=button name=captcha_ value="jwxU069flF" style="border:0;background=lightgreen"></td></tr>
<tr><td><input type=button value=Submit onclick=ck()></td><td><input type=reset value=reset></td></tr>
</table>
<script>
function ck(){
  if(lv5frm.id.value=="") { lv5frm.id.focus(); return; }
  if(lv5frm.cmt.value=="") { lv5frm.cmt.focus(); return; }
  if(lv5frm.captcha.value=="") { lv5frm.captcha.focus(); return; }
  if(lv5frm.captcha.value!=lv5frm.captcha_.value) { lv5frm.captcha.focus(); return; }
  lv5frm.submit();
}
</script>
</body>
</html>
```

function ck () 안에 if문이 여러 개가 있는데, 아무래도 id, cmt, captcha 값은 공백이면 안되고, cpatcha가 정확하지 않으면 return 된다는 것을 알 수 있다. 하지만 captcha길이가 길어서 time limit 2초안에 입력하기가 어렵기 때문에 크롬 콘솔창을 이용해주었다.

```
> lv5frm.id.value = "soo";
  lv5frm.cmt.value = "soo";
  lv5frm.captcha.value = lv5frm.captch_.value;
  lv5frm.submit();
```

위의 구문을 2초 안에 입력하기는 어려우니 메모장에 복사해 놓았다가 콘솔창에 2초안에 복사 붙여넣기를 해주었다. (id, cmt는 임의로 설정함.)



old-20 Pwned. You got 20point. Congratz!

문제가 풀린 것을 확인할 수 있었다. 뭔가 재미있던 문제였다.