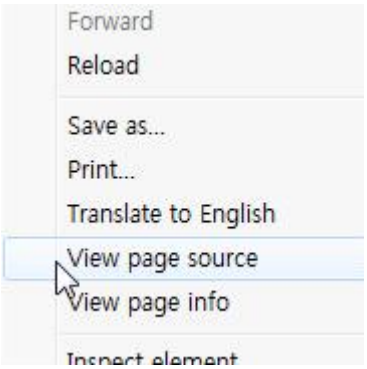
webhacking.kr 12번문제

B1ackZer0
2011.04.26

code3.html의 자바스크립트를 분석하라고 한다.
code3.html의 자바스크립트를 분석하세요.

우선 소스를 보자.



다음은 소스이다.
eval(); 은 안의 수식을 계산하는 함수이다.
String.fromCharCode()는 안의 아스키 값을 문자열로 바꾸는 함수이다.
<!--hello world-->

```
<html>
<head>
<title>Challenge 12</title>
</head>
<body>

<script>
wtf=String.fromCharCode(118,97,114,32,101,110,99,111,61,39,39,59,13,10,118,97,114,32,101,1
10,99,111,50,61,49,50,54,59,13,10,118,97,114,32,101,110,99,111,51,61,51,51,59,13,10,118,97,11
4,32,99,107,61,100,111,99,117,109,101,110,116,46,85,82,76,46,115,117,98,115,116,114,40,100,1
11,99,117,109,101,110,116,46,85,82,76,46,105,110,100,101,120,79,102,40,39,61,39,41,41,59,13,1
0,32,13,10,32,13,10,102,111,114,40,105,61,49,59,105,60,49,50,50,59,105,43,43,41,13,10,123,13,1
0,101,110,99,111,61,101,110,99,111,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,11
```

4,67,111,100,101,40,105,44,48,41,59,13,10,125,13,10,32,13,10,102,117,110,99,116,105,111,110,3
2,101,110,99,111,95,40,120,41,13,10,123,13,10,114,101,116,117,114,110,32,101,110,99,111,46,9
9,104,97,114,67,111,100,101,65,116,40,120,41,59,13,10,125,13,10,32,13,10,105,102,40,99,107,61
,61,34,61,34,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,10
1,110,99,111,95,40,50,52,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,
67,111,100,101,40,101,110,99,111,95,40,50,50,48,41,41,43,83,116,114,105,110,103,46,102,114,1
11,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,51,50,41,41,43,83,116,114,105,
110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,49,57,50,41,
41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,1
11,95,40,50,50,54,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,10
0,101,40,101,110,99,111,95,40,50,48,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,
104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,48,52,41,41,43,83,116,114,105,110,103,4
6,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,50,50,45,50,41,41,4
3,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,9
5,40,49,57,56,41,41,43,34,126,126,126,126,126,126,34,43,83,116,114,105,110,103,46,102,114,11
1,109,67,104,97,114,67,111,100,101,40,101,110,99,111,50,41,43,83,116,114,105,110,103,46,102,
114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,51,41,41,13,10,123,13,10,97,108,1
01,114,116,40,34,80,97,115,115,119,111,114,100,32,105,115,32,34,43,99,107,46,114,101,112,108
,97,99,101,40,34,61,34,44,34,34,41,41,59,13,10,125,13,10);

eval(wtf);

</script>

code3.html의 자바스크립트를 분석하세요.
</body>
</html>

String.fromCharCode()으로 자동으로 바꿔주지만 우리가 보기 편하게 우선 바꿔보았다.

```
var enco='';
var enco2=126;
var enco3=33;
var ck=document.URL.substr(document.URL.indexOf('='));

for(i=1;i<122;i++){
enco=enco+String.fromCharCode(i,0);
}

function enco_(x){
return enco.charCodeAt(x);
}
```

```
if(ck=="="+String.fromCharCode(enco_(240))+String.fromCharCode(enco_(220))+String.fromCharCode(enco_(232))+String.fromCharCode(enco_(192))+String.fromCharCode(enco_(226))+String.fromCharCode(enco_(200))+String.fromCharCode(enco_(204))+String.fromCharCode(enco_(222-2))+String.fromCharCode(enco_(198))+"~~~~~~"+String.fromCharCode(enco2)+String.fromCharCode(enco3)){
alert("Password is "+ck.replace("=",""));
}
```

위의 것도 분석하면되지만, 그냥 프로그래밍을 해서 바로 답을 구하기로 했다.
key 변수에 넣고 출력하면 패스워드가 나올 것이다.

```
key="="+String.fromCharCode(enco_(240))+String.fromCharCode(enco_(220))+String.fromCharCode(enco_(232))+String.fromCharCode(enco_(192))+String.fromCharCode(enco_(226))+String.fromCharCode(enco_(200))+String.fromCharCode(enco_(204))+String.fromCharCode(enco_(222-2))+String.fromCharCode(enco_(198))+"~~~~~~"+String.fromCharCode(enco2)+String.fromCharCode(enco3)
alert("Password is "+key.replace("=",""));
```

패스워드를 얻었고 인증에 성공했다.