webhack.teamtmp 10 번문제

Xero
박준혁 (한국디지털미디어고등학교 2 학년)
2012-06-19
wnsgurzxc@nate.com

다음과 같이 폼 하나가 있고 Check 버튼 하나가 있다.

소스를 보면 다음과 같이 ./js.js 파일을 포함한다.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
<title>Level 10</title>
</head>
<form name="frm" method="GET" action="index.php">
<input name="pass" />
<button onclick=submit();>Check</button><br><br>
</form>
<script type='text/javascript' src='./js.js'></script>
</html>
```

http://webhack.teamtmp.org/level10/js.js 주소로 들어가면 다음과 같이 난독화 되어있는 자바스크립트 소스를 볼 수 있다.

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(c/a))+String
d[e]}];e=function(){return'₩[₩xa1-₩xff]+'};c=1};while(c--){if(k[c]){p
{d[c]=k[c]||c}k=[È(e){ç d[e]}];e=È(){ç₩'₩₩₩₩w+₩'};c=1};ê(c--){è(k[c])
((¡=¡%µ)>æ?ò.ú(¡+å):¡.¢º(ç))};Þ(!₩₩₩'₩₩₩'.Ý(/^/,ò)){Ô(¡--){²
¥(¡)+₩₩₩'₩₩₩₩₩₩₩₩₩¿₩₩₩',₩₩₩'ð₩₩₩'),©[¡]}}}Ê ¬}(₩₩₩'¢©(¹ (¬,µ,¡,©,
₩₩₩₩₩₩₩₩'₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩Ò+₩₩₩₩₩₩₩₩₩'};¡=1};ë(¡--){ï(©[¡]){¬=¬.í(¢¨
(₩₩₩₩₩₩₩₩'ô(¼(É,¢Ã,¨,¶,±,Ë){±=¼(¨){½ ¨};Ô(!₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩'₩₩
₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩'₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩¢¹ +₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩'}
(¨)+₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩'₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩Ö₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩
₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩'₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩':¤(¢
{ä(¢--){³ [¤(¢)]=ª[¢]||¤(¢)}ª=[Ã(¤){Ä ³[¤]}];¤=Ã(){Ä₩₩₩₩₩₩₩₩₩₩
```

http://jsbeautifier.org/ 사이트를 이용해 복호화시키니 다음의 소스가 나왔다.

```
function yafeelsogood(str) {
    var pwd = "fj12905mg012mvn120ABF₩Q0!912409GJ190";
    var prand = "";
    for (var i = 0; i < pwd.length; i++) {
        prand += pwd.charCodeAt(i).toString()
    }
    var sPos = Math.floor(prand.length / 5);
    var mult = parseInt(prand.charAt(sPos) + prand.charAt(sPos * 2) + prand.charAt(sPos * 3) + prand.charAt(sPos * 4) + prand.charAt(sPos * 5));
    var incr = Math.round(pwd.length / 2);
    var modu = Math.pow(2, 31) - 1;
    var salt = parseInt(str.substring(str.length - 8, str.length), 16);
    str = str.substring(0, str.length - 8);
    prand += salt;
    while (prand.length > 10) {
        prand = (parseInt(prand.substring(0, 10)) + parseInt(prand.substring(10, prand.length))).toString()
    }
    prand = (mult * prand + incr) % modu;
    var enc_chr = "";
    var enc_str = "";
    for (var i = 0; i < str.length; i += 2) {
        enc_chr = parseInt(parseInt(str.substring(i, i + 2), 16) ^ Math.floor((prand / modu) * 255));
        enc_str += String.fromCharCode(enc_chr);
        prand = (mult * prand + incr) % modu
    }
    return enc_str
}
if (document.frm.pass.value == yafeelsogood("82ffbc625fc6bb55fc9cb7c0103a07f04e33b1acc0f6e1057d13c4")) {
    location.href = 'index.php?pw=' + document.frm.pass.value
}
```

yafeelsogood() 에 82ffbc625fc6bb55fc9cb7c0103a07f04e33b1acc0f6e1057d13c4 라는 값을 전달해서 나온 값이 입력 값과 같으면 답을 출력한다.

다음의 소스를 추가시키니 jSUnP4ckaNdx0R3cRypTi0n 라는 값이 나왔다.
document.write(yafeelsogood("82ffbc625fc6bb55fc9cb7c0103a07f04e33b1acc0f6e1057d13c4"));

jSUnP4ckaNdx0R3cRypTi0n 를 입력하니 다음과 같이 답이 출력되었다.

Check

PW : 111c8878c25abbf30191a0f360f4163d

Key : 111c8878c25abbf30191a0f360f4163d