

webhacking.kr 12번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-03-31

Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

Javascript challenge라고 한다.

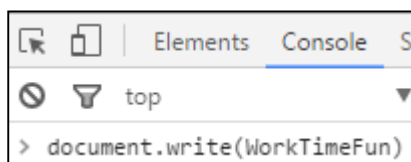
javascript challenge

중요 소스를 보면 다음과 같다.

WorkTimeFun에 아스키코드로 문자들을 주고 그것을 실행한다.

```
WorkTimeFun = String.fromCharCode(118, 97, 114, 32, 101, 110, 99, 111, 61, 39, 39, 59, 13, 10, 118, 97, 114, 32, 101, 110, 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, 114, 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, 111, 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, 10, 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, 10, 101, 110, 99, 111, 61, 101, 110, 99, 111, 43, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 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, 32, 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, 99, 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, 101, 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, 111, 109, 67, 104, 97, 114, 67, 111, 110, 100, 101, 40, 101, 110, 99, 111, 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, 100, 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, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 101, 110, 99, 111, 95, 40, 49, 57, 56, 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, 51, 41, 41, 13, 10, 123, 13, 10, 97, 108, 101, 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(WorkTimeFun);
```

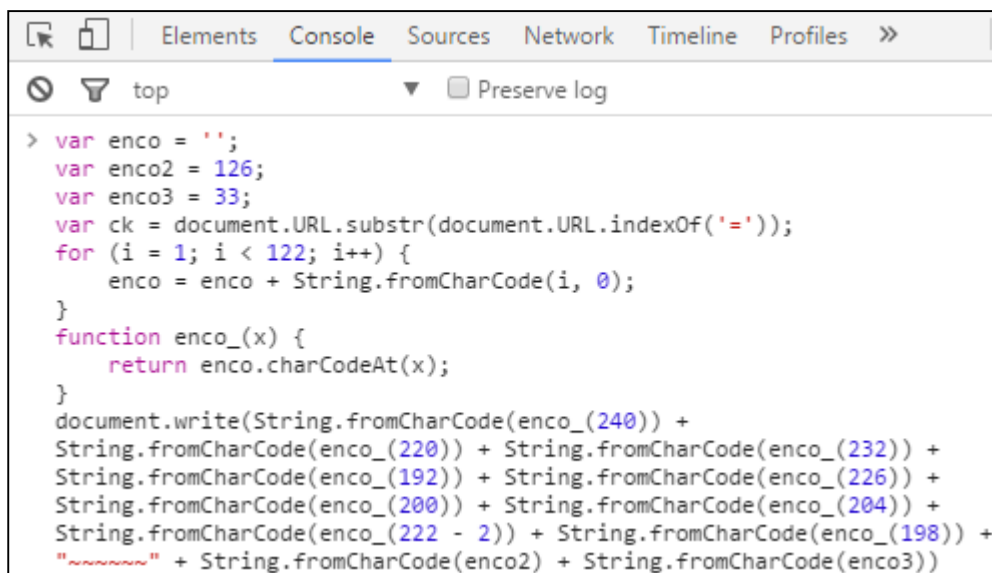
직접 해석하기 싫으니 크롬의 개발자 도구를 이용해서 WorkTimeFun을 출력해보았다.



그러자 다음과 같은 소스가 나왔다.

```
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("=", ""));
}
```

ck와 뒤의 값을 비교하니 뒤의 값을 다음과 같이 document.write로 출력해보았다.



```
> 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);
}
document.write(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))
```

그러자 다음과 같이 youaregod~~~~~!이 출력되었다.

youaregod~~~~~!

Auth에 인증하면 클리어된다.



KEY : youaregod~~~~~!