POC – Hacker's dream Script #2
PDF파일 분석해서 숨겨진 패스워드 (또는 악성코드) 찾기

HACKING GROUP "OVERTIME"

woos55< wooshack55@gmail.com >2008.10.20

1 poc2008.pdf_로부터 스크립트 얻기.

poc2008.pdf_ 파일을 inflater.exe 를 이용해서 풀면 다음과 같은 스크립트를 얻을 수 있다.

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('PA(5){a=N.O.T();7 b=\'Z+/=\';7 m=[];I(i=0;i<5.d;i++){x=5.f(i);g(i%2==0)m[i]=x;B=a.d}g(B!=H){K L}5=m.z(\'\');7 k={v:(5.d%4!=0),b:CJ(\'[^\'+b+\']\').e(5),u:(/=/.e(5)&&(/=[^=]/.e(5)||/={3}/.e(5)))};g(k.v||k.b||k.u)G C S(\'U W\');7 9=[];7 c=0;X(c<5.d){7 w=b.h(5.f(c++));7 t=b.h(5.f(c++));7 l=b.h(5.f(c++));7 n=b.h(5.f(c++));7 j=(w<<Y)+(t<<M)+((l&F)<<6)+(n&F);7 D=(j&(p<<E))>>E;7 s=(l==y)?-1:(j&(p<<8))>>8;7 r=(n==y)?-1:(j&p);9[9.d]=q.o(D);g(s>=0)9[9.d]=q.o(s);g(r>=0)9[9.d]=q.o(r)}e=9.z(\'\');Q(e)}A(\'R=V=V\');',62,62,'|||||str||var||decoded||chars||length|test|charAt|if|indexOf||buf|invalid|i2|ee|i3|fromCharCode|255|String|b2|b1|i1|equals|strlen|i0|key|64|join|AhnLab_ASec|ss|new|b0|16|63|throw|1017|for|RegExp|return|false|12|arguments|callee|function|eval|dVmVFVyVIVHVAVgVPVSVAVnVUVGVFVzVcV3VdVvVcVmVQVgVaVXVMVgVIVkVRVvVIVFVUVgVSV2V5VvVdVyVBVBVUV0VVVDVPVyVIVnVOVwV|Error|toString|Invalid||data|while|18|ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789'.split('|'),0,{}))
```

2 다음 함수를 이용해서 위의 코드를 디코딩 한다.

```
function decode() {
 var code = document.getElementById('code').value;
 code = code.replace(/^eval/, '');
 document.getElementById('code').value = eval(code);
}
```

디코드한 결과는 다음과 같다. 여기서 빨간 부분을 주목하자. 스크립트를 분석해 보면 변수 a는 AhnLab_ASec() 본문을 받아서 스트링화한다. 그리고 변수 ss에 본문의 길이 값을 넣어주고 그것이 1017이 아니라면 (본문이 변조되었다면) false를 반환하여 함수를 종료시킨다.

하지만 나머지 스크립트 전체를 분석해보면 변수 a와 s가 추가적으로 이용되는 부분이 없으므로 본문의 변조를 체크하는 부분을 주석처리 하여준다.

```
function AhnLab_ASec(str){
a=arguments.callee.toString();
var
chars='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxy
z0123456789+/=';
var ee=[];
for(i=0;i<str.length;i++){
key=str.charAt(i);
if(i%2==0)
ee[i]=key;
ss=a.length
}
//if(ss!=1017){
return false}
str=ee.join('');
var invalid={strlen:(str.length%4!=0),
chars:new
RegExp('[^'+chars+']').test(str),equals:(/=/.test(str)&&(/=[^=]/.test(str)|
```

```
|/={3}/.test(str)))};
if(invalid.strlen||invalid.chars||invalid.equals)
throw new Error('Invalid data');
var decoded=[];
var c=0;
while(c<str.length){
var i0=chars.indexOf(str.charAt(c++));
var i1=chars.indexOf(str.charAt(c++));
var i2=chars.indexOf(str.charAt(c++));
var i3=chars.indexOf(str.charAt(c++));
var buf=(i0<<18)+(i1<<12)+((i2&63)<<6)+(i3&63);
var b0=(buf&(255<<16))>>16;
var b1=(i2==64)?-1:(buf&(255<<8))>>8;
var b2=(i3==64)?-1:(buf&255);
decoded[decoded.length]=String.fromCharCode(b0);
if(b1>=0)decoded[decoded.length]=String.fromCharCode(b1);
if(b2>=0)decoded[decoded.length]=String.fromCharCode(b2) }
test=decoded.join('');
eval(test)}

AhnLab_ASec('dVmVFVyVIVHVAVgVPVSVAVnVUVGVFVzVcV3VdVvVc
VmVQVgVaVXVMVgVIVkVRVvVIVFVUVgVSV2V5VvVdVyVBVBVUV0V
VVDVPVyVIVnVOVwV=V=V');
```

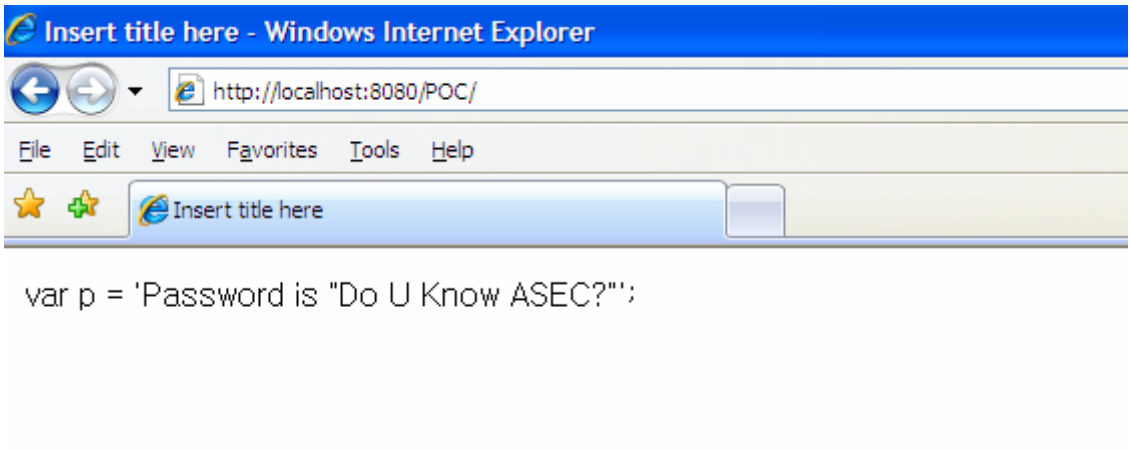
* 비밀번호 은닉 기법에 사용된 자바 스크립트 함수

fromCharCode() : 키값에 해당하는 아스키 문자를 얻습니다.

join(“”) : 괄호 안의 문자를 배열의 내용 사이에 추가하여 하나의 문자열로 만들어 줍니다.

3 패스워드 얻기

마지막으로 함수의 끝 부분에서 document.write(test) 를 추가해준뒤 함수를 실행하면 다음과 같은 결과를 얻을 수 있다.



PDF에 포함되어 있는 악성 스크립트 분석법 http://viruslab.tistory.com/324
PDF스크립트추출기http://blog.naver.com/31337guru?Redirect=Log&logNo=140056360251

하나은행 홈페이지 악성코드 사례 http://wwww.textcube.com/468
2 디코딩 함수 http://www.jb51.net/article/9705.htm