Hacking နှင့် ခလုတ်တိုက်ခြင်း

Thin Ba Shane (Luna Moon)

Legion of LOL

အမှာစာ

Techinical ဦးစားပေးရေးထားတဲ့ ဆောင်းပါးတစ်ခုမဟုတ်တဲ့အကြောင်းကို ဦးစွာအသိပေးချင်ပါတယ်။ Hacking သို့မဟုတ် Security အပိုင်းကို စိတ်ဝင်စားပြီး စတင်လေ့လာမယ့်သူများ ၊ စတင်လေ့လာနေပြီဖြစ်သော်လည်း အခက်ကြုံနေတဲ့သူများကို ကျနော့်အနေနဲ့ Information လေးပေးထားတဲ့ ဆောင်းပါးတစ်ခုသာဖြစ်ပါတယ်။ ဒါ့အပြင် ကျနော်ကိုယ်တိုင်လည်း Blog တွေသာရေးဖူးတဲ့သူ တစ်ယောက်ဖြစ်တာကြောင့် ကျနော့်ရဲ့ ပထမဆုံး နဲ့ အတတ်နိုင်ဆုံး စာရေးလေ့ကျင့်တဲ့ ဆောင်းပါးဆိုရင်လဲ မမှားပါဘူး။ ဒါကြောင့် ဒီဆောင်းပါးမှာ အမှားများပါဝင်နေရင် ကျနော့်အား အသိပေးနိုင်ကြောင်း ကြိုတင်ပြောကြားထားခြင်းဖြစ်ပါတယ်။

အားလုံးကိုလေးစားလျက်

မာတိကာ

0 - နိဒါန်း

1 - ခလုတ်တိုက်ခြင်း

2 - နိဂုံး

0 - နိဒါန်း

ပထမဦးစွာ ဒီဆောင်းပါးရဲ့ ခေါင်းစဉ်လေးကနေပဲစပြီးဆွေးနွေးချင်ပါတယ်။ ကျနော်ခေါင်းစဉ်ပေးတဲ့နေရာမှာ စာဖတ်သူစိတ်ဝင်စားအောင်လဲပေးချင်တာရယ် ၊ ရည်ရွယ်ချက်လေးလည်းပါဝင်အောင်ရယ် စဉ်းစားပြီးတော့ ပေးထားတာဖြစ်ပါတယ်။ ဒါကြောင့် ရည်ရွယ်ချက်လေးကို အရင်ဆုံးပြောပြချင်ပါတယ်။

ရည်ရွက်ချက်တွေကိုတော့ အောက်မှာစာရင်းလုပ်ပေးထားပါတယ်

- Hacking ရဲ့ ဆိုလိုရင်း အစစ်မှန်ကို စတင်လေ့လာသူများသိစေရန်
- Hacking က စတင်လေ့လာမယ့်သူအတွက် လုပ်သင့် ၊ မသင့် သိစေရန်
- Hacking လေ့လာရန် ဆုံးဖြတ်ထားသူတစ်ယောက်အတွက် အကြံဉာဏ်ရရှိစေရန်

စတဲ့ အချက်တွေကို အခြေခံပြီးရေးထားတာဖြစ်ပါတယ်။

0.1 - Hacking ဆိုတာဘာလဲ

Hacking ဆိုတာကို နေရာဒေသအမျိုးမျိုး ၊ သင်တန်းအမျိုးမျိုး ၊ ဆောင်းပါးအမျိုးမျိုးကနေ အဓိပ္ပါယ်တွေ အမျိုးမျိုးဖွင့်ဆိုထားကြတာကိုတွေ့ရပါတယ်။ ဒီလိုအဓိပ္ပါယ် ဖွင့်ဆိုမှုတွေများနေခြင်းက ဆိုလိုရင်းနဲ့ မူလအနှစ်သာရကို လူတိုင်းကမသိကြတော့ဘူး ၊ ကိုယ်ဖတ်မိတဲ့နေရာက အဓိပ္ပါယ်ကို အမှန်လို့ထင်သွားတဲ့သူတစ်ချို့အတွက် Hacking ကို အမျိုးမျိုးသတ်မှတ်ကုန်ကြတော့တာပါပဲ။ ဒါကြောင့်ပဲ ကျနော် Hacking ကို ကျနော်ဘယ်လိုသတ်မှတ်ထားလဲဆိုတာကို အကျိုးအကြောင်း ၊ သက်သေတချို့နဲ့ ဆွေးနွေးချင်တာဖြစ်ပါတယ်။

Dictionary က အဓိပ္ပါယ်ကိုအရင်ဆုံးကြည့်ကြည့်မယ်၊ (Definition in dictionary.com) မှာဖော်ပြထားတာကို ကျနော်တို့စကြည့်ကြမယ်။

- *to modify (a computer program or electronic device) or write (a program) in a skillful or clever way: Developers have hacked the app. I hacked my tablet to do some very cool things.*
- *to circumvent security and break into (a network, computer, file, etc.), usually with malicious intent: Criminals hacked the bank's servers yesterday. Our team systematically hacks our network to find vulnerabilities.*

- ပထမတစ်ခုက Computer Program တွေ Hardware Device တွေကို ပြင်ဆင်ရန် (သို့မဟုတ်) Program တစ်ခုကို အရည်အချင်းပြည့်ပြည့်နဲ့ လိမ်မာပါးနပ်စွာရေးသားခြင်းဖြစ်တယ် လို့ဆိုပါတယ်။
- ဒုတိယတစ်ခုက Computer ၊ Network ၊ File စတာတွေနဲ့ ပတ်သတ်တဲ့ လုံခြုံရေး (Security) ကို ဆိုးကျိုးများစေမဲ့ အရာတွေသုံးပြီးထိုးဖောက်ခြင်းဖြစ်တယ်လို့ဆိုပါတယ်။

ဒီလိုဆိုရင် ကျနော်စပြီးဆွေးနွေးမယ် ၊ Hacking ဆိုတဲ့ ဝေါဟာရတစ်ခုကို dictionary မှာဖော်ပြထားတာ ၂ ခုရှိတယ်မဟုတ်လား (ဒါတောင် computer နဲ့ဆိုင်တဲ့အရာသီးသန့်ပါ) ။ ဒီဖော်ပြချက် ၂ခုထဲမှာမှ ၂ ခုကိုလုံးကိုမှတ်ထားတာက ဘယ်လောက်များမလဲ ၊ ပထမတစ်ခုကိုပဲမှတ်မိနေမယ့်သူက ဘယ်လောက်များမလဲ ၊ ဒုတိယတစ်ခုကိုပဲမှတ်မိနေမယ့်သူက ဘယ်လောက်များမလဲ ။

အဓိပ္ပါယ်က ဘယ်လိုပဲဖြစ်နေဖြစ်နေ ပထမ ဖော်ပြချက်ထဲကလို Software / Program / Hardware စတာတွေကို ပိုပြီးအသုံးဝင်အောင် မွမ်းမံမယ် ၊ ပိုပိုသစ်ဆန်းပြီး လူတွေအတွက်အရမ်းအကျိုးရှိစေမယ့် အရာတွေကို ဖန်တီးမယ် ဆိုတဲ့လူတွေအတွက်ကတော့ အဲဒါတွေဟာ Hacking ပဲဖြစ်ပါတယ်။ ဒါကြောင့် သူတို့ဟာ Hacker တွေလဲဖြစ်ပါတယ်။ ဒီလိုအလုပ်တွေကို လုပ်ဆောင်ဖို့ဆိုတာ " လုပ်မယ်ဟေ " ဆိုပြီး စလုပ်လို့ရတဲ့အရာတွေ မဟုတ်ဘူးဆိုတာတော့ သိပြီးဖြစ်မှာပါ။

ရှိပြီသားအရာတွေထက် ပိုကောင်းပြီး ဆန်းသစ်တဲ့ အရာတစ်ခုဖြစ်ဖို့ဆိုတာ သေချာတာတော့ Creation ရှိတဲ့သူတွေမှသာလုပ်ဆောင်နိုင်တာဖြစ်ပါတယ်။ ဒါကြောင့် ဒီလိုဖန်တီးနိုင်တဲ့သူတွေကိုလဲ Hacker လို့သတ်မှတ်ကြပါတယ်။ ဒီအတွက် ကျနော့်မှာ သက်သေပြစရာရှိပါတယ်

Linux Operating System တစ်ခုဖြစ်ပေါ်လာတဲ့အတွက် ဘယ်လောက် ကောင်းကျိုးတွေဖြစ်ထွန်းခဲ့တယ် ၊ ဖြစ်လဲဖြစ်နေတုန်းပဲဆိုတာတော့ အားလုံးငြင်းကြမယ်မထင်ပါဘူး။ ဒီ Operation System ဖြစ်လာတဲ့အကြောင်းကို Linux Torvalds ကိုယ်တိုင်ပါဝင်ရေးသားထားတဲ့ " Just for fun : The Story of an Accidental Revolutionary " စာအုပ်ထဲမှာ ဒီလိုမျိုး ဖန်တီးတဲ့သူတွေကို Hacker လို့သုံးနှုံးထားတာကိုတွေ့ရပါလိမ့်မယ်။ Linux ကိုဖန်တီးတဲ့သူမှမဟုတ်ပါဘူး ၊ Linux ကို ပိုမိုကောင်းမွန်လာအောင် Support ပိုင်းပေးကြတဲ့သူတွေကိုလည်း Linus Torvalds က Hacker တွေလို့ပဲ သုံးနှုန်းထားတာကိုတွေ့ရပါလိမ့်မယ်။

ဒါကြောင့် ကျနော်ဆိုလိုချင်တာဟာ Hacking ဟာ ဘယ်မှာမဆိုရှိနိုင်ပါတယ်။ အကြောင်းအရာတစ်ခုကို သာမာန်ထက်ပိုနားလည်ပြီး ကောင်းတဲ့အရာတွေကို ဖန်တီးတဲ့သူတွေကလည်း Hacker ဖြစ်သလို ၊ ထိုအကြောင်းအရာတစ်ခုကိုပဲ သာမာန်ထက်ပိုမိုနားလည်ပြီး မကောင်းတဲ့အရာတွေကို ဖန်တီးချင်တဲ့သူတွေကိုလည်း Hacker လို့ပဲ သတ်မှတ်ပါတယ်။ ဒီနေရာမှာ လူသားတို့ရဲ့ ထုံးစံအတိုင်း အကောင်းထက် အဆိုးကိုသာ အသိအမှတ်ပြုကြတာပေါ့။

ဥပမာ - လက်ရှိမြန်မာပြည်မှာဆိုပါတော့ " **ဘယ် Celebrity တစ်ယောက်ရဲ့ Acc ကို ဘယ် အဖွဲ့က Hack လိုက်တယ်**" ဆိုတဲ့ သတင်းမျိုး နဲ့ "**ဘယ်ကျောင်းမှာတက်နေတဲ့ ဘယ်အရွယ်ကျောင်းသားတစ်ယောက်က လူအကျိုးပြုမယ့် အရာတစ်ခုကိုဖန်တီးလိုက်တယ်**" ဆိုတဲ့ သတင်း

၂ခုမှာ လူအများစုက ဘယ်သတင်းကို ပိုမှတ်မိပြီး ဘယ်သတင်းကို စိတ်ဝင်စားမလဲဆိုတာ ကိုယ်တိုင်စဉ်းစားကြည့်ပါ။

0.2 - Hacking ကိုလေ့လာသင်သလား ?

Hacking ကို ကျနော်နားလည်ထားသလို ရှင်းပြပြီးပြီဖြစ်တာကြောင့် စာဖတ်သူအနေနဲ့ သိသင့်သလောက်တော့ သိထားပြီလို့ယူဆလိုက်ပါမယ်။ ကျနော် လက်ရှိမြန်မာနိုင်ငံပေါ်မူတည်ပြီး စဉ်းစားရမယ့် အချက်လေးတွေ အောက်မှာပြထားပေးပါမယ် ၊ စဉ်းစားရမှာက သင့်အလုပ်ဖြစ်ပါတယ်။

- Hacking က သူများထက်တော့ ပိုကြိုစားရမှာသေချာတယ် ၊ ဒါကတော့ ဆုံးဖြတ်ချက်အပေါ်မူတည်ပါတယ်။
- Hacking မှာ creation က အရေးပါတာဖြစ်တဲ့အတွက် ကိုယ်ကဖန်တီးချင်သူလား ၊ ဟိုယောင်ဒီယောင်ပဲလား။
- ဘယ်အကြောင်းအရာမဆို သာမာန်လူတွေထက်တော့ ပိုပြီးနားလည်ရမှာဖြစ်တဲ့အတွက် လေ့လာရမှာ ကိုပျင်းတဲ့သူလား ၊ ပျော်တဲ့သူလား။
- ခုမှ စလေ့လာမယ်ဆိုလဲ နောက်မကျသေးပါဘူး ၊ ဒါပေမဲ့ ပြန်တွက်ရမှာက အချိန်ရောပေးနိုင်ပါ့မလား၊ ပုံမှန်ရောလေ့လာနိုင်ပါ့မလား။
- Hacking နဲ့ အသက်မွေးဝမ်းကြောင်းထိလုပ်မှာလား ၊ အပျော်လား။
- Creation တွေဘာတွေ လုပ်မယ်ဆိုတည်းက သေချာပေါက် Programming လိုတယ်။
- ဒီ Hacking နဲ့ မရပ်တည်နိုင်ခဲ့ရင် ဘယ်လိုအဆင်ပြေနိုင်မလဲ။

အခုမှစတဲ့သူတွေကို စဉ်းစားစေချင်တာဖြစ်ပါတယ်။ သူငယ်ချင်းတွေကြားမှာ နာမည်ကြီးတာမျိုးလောက်ဆိုရင်တော့ အဲ့ဒါလုပ်မယ့် အချိန်တွေကို မဖြုန်းသင့်ဘူးပေါ့။ ဒီလိုမှမဟုတ်ပဲ ကျနော့်လို လူတန်းစားတစ်ရပ်ဖြစ်တဲ့ ဘာမှမရရင်လဲနေ ၊ ဘာမှဖြစ်စရာလဲမလိုဘူး ၊ သိချင်တာတွေ သိရရင်ကျနပ်ပြီ ၊ အဲ့အတွက်လဲ အားထုတ်မယ်ဆိုရင်တော့ ဒီစာအုပ်ဖတ်ပြီးရင် စလုပ်လိုက်တော့လို့ပြောချင်ပါတယ်။

1 - ခလုတ်တိုက်ခြင်း

ကျနော် Facebook သုံးတုန်းကပေါ့ ၊ ကျနော့်အသိ အုပ်ထိန်းသူတစ်ယောက်က ကျနော့်ကိုမေးတယ် ၊ သူ့ကလေးကို လမ်းညွှန်ပေးပါတဲ့ ။ တကယ်ပါ ဘာလမ်းညွှန်ရမှန်းကို မသိပါဘူး ။ ဒါ့အပြင် အခြားစလုပ်တော့မလို လူငယ်တွေထဲကလဲ ဒီလိုမေးခွန်းမျိုးကိုမေးကြပါသေးတယ်။ ဒီတော့ အားလုံးအတွက် ကျနော်အဖြေလေးတစ်ခုတော့ ပေးဖြစ်တယ် ' ခလုတ်တိုက်မိသမျှ အကုန်စလုပ်တော့ ' လို့ ပြောလိုက်တာဖြစ်ပါတယ်။ တချို့ကလဲ စနောက်နေတယ်ထင်ပါရဲ့ ၊ ပေါ်မလာတော့ပါဘူး။

နိဒါန်းမှာ ပြောပြထားတာကြောင့် Hacking ဆိုတဲ့ လမ်းကိုလျောက်တော့မယ်ဆိုရင် မလွယ်ကူလောက်ဘူးဆိုတာတော့ ရိပ်မိထားလောက်မှာဖြစ်ပါတယ်။ ဒါပေမဲ့လည်း ဒီလမ်းကိုမှ လျောက်မယ်စိတ်ကူးထားတယ်ဆိုတဲ့ သူတစ်ယောက်အတွက်တော့ လမ်းဘယ်လောက်ကြမ်းကြမ်းလျောက်ရမှာပဲပေါ့။ ဒီတော့ ပန်းတိုင် မဟုတ်တောင်မှ အတိုင်းအတာတစ်ခုကိုရောက်ချင်တယ်ဆိုရင်တော့ ကြမ်းပါတယ်ဆိုတဲ့လမ်းပေါ်က တိုက်သမျှခလုတ်ကို ရှင်းရတော့မှာဖြစ်ပါတယ်။

1.1 – First problem ever

ကိုယ့်အလုပ်ကိုယ်လုပ်လာရင်းနဲ့မှ အတွေ့အကြုံ ၊ အချိန် ၊ အဆက်မပြတ်လေ့လာမှု စတာတွေကြောင့် အလိုလိုနေရင်း သိလာတဲ့ သူတွေမှာ ဒီပြဿနာမရှိပေသော်လည်း အသက်အရွယ်ငယ်ငယ် ၊ ဘာကိုဝါသနာပါမှန်းလဲမသိ ၊ ဘာလုပ်ချင်လို့လုပ်ချင်မှန်းလဲမသိ ၊ ရည်ရွယ်ချက်တွေကျတော့လဲ အကြီးကြီး စတာတွေကြောင့် ဟိုစပ်စပ် ၊ ဒီစပ်စပ် ဖြစ်နေတဲ့အခိုက်အတန့်ဟာ ပထမဆုံး ခလုတ်ကသင်းပဲပေါ့။ အဲဒီခလုတ်ကသင်းက တော်တော်လဲဒုက္ခပေးပါတယ် ၊ တချို့ဆို အဲ့မှာတည်းက ရပ်သွားကြတာမြင်ဖူးပါလိမ့်မယ်။

' ဒီတော့ ဘယ်လိုရှင်းမလဲ ' ဆိုတဲ့ မေးခွန်းအတွက် ကျနော်ရှင်းတဲ့ ပုံစံလေးပြောပြပါမယ်။ အမှန်တရားလို့ မဆိုလိုပါဘူး ၊ သဘောကျတယ်ဆိုရင်တော့ ယူသုံးလို့ရအောင်ဖြစ်ပါတယ်။ ကျနော်တုန်းကတော့ ဒီအချိန်မှာ အနည်းငယ်တွက်ချက်မှုလေးတွေရှိခဲ့တယ်။ အောက်ကလို မေးခွန်းလေးတွေမေးပြီး ပြန်ဖြေကြည့်ပေါ့။

အမေး။ ။ ဘာဝါသနာပါတာလဲ

အဖြေ။ ။ သေချာမသိဘူး ၊ ဟိုဟာဆိုလဲ လုပ်ချင် ဒီဟာဆိုလဲလုပ်ချင်

အမေး။ ။ Hacking တွေထဲမှာ ဘယ်ဟာကိုကြိုက်လဲ

အဖြေ။ ။ သိသလောက်တော့ အကုန်လုံးက ကြိုက်ချင်စရာတွေချည်းပဲ

ဆိုလိုချင်တာက ကျနော်လဲ ဘာမှကြိုတင်တွေးထားတာမဟုတ်ဘူး ၊ တိတိကျကျပြောရရင်တော့ ဘယ်ဟာကဘာမှန်းမှမသိတာ ဘယ်လိုလုပ်ဆုံးဖြတ်လို့ရနိုင်မှာလဲ။ ဒီတော့ အသစ်ပြန်မေးမယ်။

အမေး။ ။ ဘာပဲဖြစ်ဖြစ် စမ်းကြည့်မလား

အဖြေ။ ။ စမ်းမယ် ၊ Ready !

အမေး။ ။ Computer နဲ့ ပတ်သတ်ပြီး ဘယ်လောက်သိလဲ

အဖြေ။ ။ Game တောင် Uninstall ပြန်မလုပ်တတ်သေးဘူး။

အစ်ကိုတစ်ယောက်ရဲ့ လမ်းညွှန်မှုကြောင့် Network Engineering အခြေခံသင်တန်းသွားတက်ဖြစ်တယ်။ ဘာမှမရှိရင်တော့ တစ်ခုခုရှိအောင်လုပ်တာကောင်းပါတယ်။ ဘာမှမရှိတာက ဘာအပေါ်မှအခြေခံလို့မရဘူး ဖြစ်နေရာကနေ ကျနော်ဟာ Networking အခြေခံလောက်ကို သိထားတဲ့ IT သမားပေါက်စလေးတော့ဖြစ်သွားတာပေါ့။ အဲ့ကစပြီးတော့ Hacking / Hacker ဆိုတဲ့ စာလုံးပါသမျှက ကျနော်နဲ့ဆိုင်တယ်လို့ ကျနော်က ယူဆလိုက်ပြီ။

မြန်မာလိုရေးထားတဲ့ စာအုပ်တွေ Hacking , Virus , Hacker ဘာလာလာအကုန်ဖတ် ၊ အကုန်စမ်းပေါ့။ သတင်းစာထဲမှာပဲဖြစ်ဖြစ် Ethical Hacking သင်တန်းများတွေ့လို့ကတော့ အနည်းဆုံးဖုန်းလေးတော့ လှမ်းဆက်လိုက်ရမှ နေသာထိုင်သာရှိတဲ့ အချိန်ကာလပေါ့။ ကျနော်အဲ့လိုတွေလုပ်ပြီး ကိုယ်ဘာကိုရွေးရမယ်ဆိုတာကို ကိုယ့်ဘာကိုမြင်လာတယ်။ ကိုယ့်ရှေ့မှာရွေးစရာလေးရှိမှလဲ ကောင်းနိုးရာရာရွေးရသေးတာမဟုတ်လား။ မေးခွန်းလေးတွေပြန်မေးဖြေရတယ်။

အမေး။ ။ Network engineer အနေနဲ့ ဆက်လုပ်မလား

အဖြေ။ ။ မလုပ်ချင်ဘူး ၊ Hacker ပဲ တစ်ပြားမှ မလျှော့ဘူး

အမေး။ ။ Programming ရောလေ့လာမှာလား

အဖြေ။ ။ Hacking မှာလိုတယ်ဆိုရင် လုပ်မယ်

အမေး။ ။ Network Hacking လား ၊ Web Hacking လား

အဖြေ။ ။ အဲ့ ၂ ခုလောက်ရှိတယ်ထင်ထားတာ ၊ Network က device တွေမရှိဘူး ၊ Web ပဲရွေးလိုက်မယ် (လောလောဆယ် browser တစ်ခုလောက်နဲ့စလို့ရမယ့်အရာ)

ကျနော်ဆိုလိုချင်တာကတော့ ရိုးရှင်းပါတယ် ၊ ကိုယ့်အခြေအနေပေါ်မူတည်ပြီး အကောင်းဆုံးလို့ကိုယ်ထင်တဲ့အရာကိုရွေးပါ။ ရွေးပြီးပြီဆိုရင်တော့ ဆက်လျှောက်ယုံပဲပေါ့။ အဓိကမလုပ်မိစေဖို့ကတော့ ဘာမှမလုပ်ပဲ ကျနော်က Forensic လုပ်ချင်တာဗျ ဆိုတာမျိုးပေါ့။ ဟိုဟာလိုလို ၊ ဒီဟာလိုလို အကြောင်းပြချက်တွေနဲ့ဘာမှမလုပ်ဖြစ်ရင်တော့ ' **ဖောရှော** ' တော့ဖြစ်ပါလိမ့်မယ်။

1.2 - A message from Hackers

လမ်းကြောင်းရွေးပြီးပြီဆိုရင် နောက်ထပ်ကြုံရမယ့်အရာလေးတွေရှိသေးတယ်။ နောက်ထပ်ရှင်းရမယ့် ခလုတ်တွေပေါ့ ၊ ကြိုးပြီးတော့ စီလျက်သားကိုရှိနေတာဖြစ်ပါတယ်။ ဒါပေမဲ့လည်း အဲ့ခလုတ်တွေကို မမြင်ပဲ ၊ ပေါက်တတ်ကရတွေလျှောက်လုပ်နေမိတတ်ပါတယ်။ (ကျနော်ကတော့ လုပ်ကိုလုပ်ခဲ့တာ) ဘာတွေလုပ်ခဲ့တယ်ဆိုတောတော့ ပြောစရာမလိုလို့မပြောတော့ဘူး။ ဒါကြောင့် နောက်လူတွေကျရင်တော့ ဒါလေးတွေကို ရှင်းရင်ကောင်းမယ်ဆိုတာ အကြံပေးချင်ပါတယ်။

Don't Learn to Hack, Hack to Learn ဆိုတဲ့ စကားကိုကြားဖူးမှာပါ၊ အဲဒီဆိုလိုရင်းကို စစချင်းလုပ်တဲ့အနေနဲ့ တော်တော်နားလည်ရခက်ပါလို့မ်မယ်၊ ကျနော်တုန်းကတော့ တကယ်ကို ဘာစကားကြီးမှန်းကိုမသိတာပါ။ အခုနားလည်ထားတာလေးကတော့ ` **How to hack လိုမျိုးတွေကို လေ့လာမယ့်အစား ၊ Target တစ်ခုထားပြီး လိုတာတွေကိုလေ့လာသွားတာပိုကောင်းတယ်** ` လို့နားလည်လိုက်ပါတယ်။ ဒါကြောင့် ပိုရှင်းသွားအောင် Web Security ဆိုတဲ့ Target လေးထားလိုက်မယ်ဆိုရင် ဘာတွေသင်ယူရမယ်ဆိုတာ အများကြီးပေါ်လာတာကိုတွေ့ရပြီပေါ့။

1.3 - Hack to Learn

ဒီအပိုင်းမှာတော့ ကျနော်တို့ Target ကို Web Hacking ကိုအရင်ဆုံးရွေးကြည့်လိုက်မယ်။ Web Application တစ်ခုကို Hack မယ်လို့စတွေးလိုက်ရင် " **How to hack a website** " ကိုဘယ်တော့မှ မစမိရင်ပိုကောင်းမယ်ထင်ပါတယ်။ keyword ကိုက အဲဒါ Hack to learn မဟုတ်တော့ဘူးလို့ဆိုရမှာဖြစ်တယ်။ အရင်ဆုံး အောက်မှာပြထားသလို မေးခွန်းတွေထုတ်လိုက်မယ် ၊ ပြီးရင် ကိုယ့်မေးခွန်းကို ကိုကိုယ်တိုင်ပဲ ကိုယ်စိတ်ကျေနပ်တဲ့ထိ အဖြေလိုက်ရှာရမှာဖြစ်တယ်။

ဥပမာ။ ။ အောက်ကမေးခွန်းကိုကြည့်ပါ

1. Web Application ဆိုတာဘာလဲ ?
    - Wiki မှာ ဖတ်မယ်
    - Blog တွေမှာ ဖတ်မယ်
    - ပုံတွေလိုက်ကြည့်မယ်
    - Youtube က Video တွေမှာကြည့်မယ်
    - Ebook တွေမှာဖတ်မယ်
    - ကိုယ့်ကို ရှင်းပြနိုင်မယ့်သူကိုမေးမယ် (forums)

ကျနော့်အနေနဲ့ကတော့ အပေါ်မှာပြထားတဲ့ အဆင့်အတိုင်းပဲ အဖြေရှာစေချင်တယ် ၊ အတတ်နိုင်ဆုံးတော့ သူများကိုမေးရတာကို နောက်ဆုံးမှပဲလုပ်စေချင်ပါတယ်။ အပေါ်ကအချက်တွေကနေ ကြိုးစားအားထုတ်မှုမရှိပဲနဲ့ သူများကိုသွားမေးတာက သူများအပေါ်လည်း မတရားရာ ကျပါတယ်။

1.4 – Advice from a Noob

ကျနော် အခြေခံသိသင့်တဲ့အရာတွေ မသိပဲ SQL Injection ကို ၆ လလောက်လေ့လာဖူးပါတယ်။ အမှန်တိုင်းပြောရရင် ကျနော် Web Technology ကိုတောင် သေသေချာချာမသိပါဘူး။ ကျနော် SQL Injection ကို Myanmar Security Forum မှာ Basic tutorial လိုတစ်ခုကိုစစမ်းပြီးတော့ တစ်ချိန်လုံး Online မှာ လိုက်စမ်းနေခဲ့တယ်၊ SQL Injection challenge တွေကိုလည်း ညတိုင်းလိုလိုဖြေဖြစ်တယ်။ ကျနော် အခြေခံတွေကို မလုပ်ခဲ့တဲ့အတွက် ကျနော်ဟာ သူများပြောပြတာတွေကိုသာလိုက်မှတ်ရပါတယ် ၊ ဒီလိုမှမဟုတ်လဲ ကြက်ကန်းဆန်အိုးတိုးပြီး challenge ဖြေနိုင်သွားတာမျိုးလဲ ရှိချင်ရှိမယ်။

အချိန်တွေလဲကုန်ရော ကျနော်အမြင်မှန်အောက်ကလိုရလာတယ်။

- Web Technology ကို အရင်ဆုံးနားလည်သင့်တယ်
- Web App တစ်ခုကို HTML နဲ့ ဘယ်လို structure ချထားသလဲ

- CSS နဲ့ ဘယ်လို decoration လုပ်ထားလဲ
- JavaScript / JQuery စတာတွေနဲ့ User Interface ကို ဖန်တီးထားသလဲ
- Database မှာသုံးတဲ့ SQL Queries တွေကဘာတွေလဲ
- Server side မှာ PHP က ဘယ်လိုတွေအလုပ်လုပ်လဲ

စတဲ့ အခြေခံလိုအပ်ချက်တွေကို ပြန်လေ့လာရပါတယ်။ ဒါကြောင့် ကျနော့်လို အချိန်မကုန်ချင်ရင်တော့ အဲ့ဒီအရာတွေကို အရင်ဆုံးလေ့လာပါလို့အကြံပေးချင်ပါတယ်။

ဒီအခြေခံတွေနားလည်ပြီးနောက်မှာ ကျနော် လူသိများတဲ့ SQL Injection ၊ XSS ၊ File Inclusion တို့လို Vulnerabilities တွေကို Source Code နဲ့အတူပြန်လေ့လာဖြစ်ပါတယ်။ Source code ကိုနားလည်နိုင်ပြီဆိုရင်တော့ Why ဆိုတဲ့မေးခွန်းတွေအတွက် အဖြေတွေရှိနေပြီပေါ့။ ကျနော် ဘယ်ဟာကိုအားနည်းတယ်ဆိုတာ ကျနော်အသိဆုံးဖြစ်တယ်မဟုတ်လား။ ကျနော် Shell upload တင်တာတွေကို သိပ်မရဘူးဆိုပါတော့ ။ HTML နဲ့ PHP ကို သုံးပြီး File Upload Form တွေဘယ်လိုအလုပ်လုပ်တယ်ဆိုတာကို ကျနော် နားမလည်မချင်းနေရာစုံက လေ့လာပါတယ်။ Code တွေကို ပြန်စမ်းရေးတယ် ၊ Bypass ဘယ်လိုလုပ်ကြလဲဆိုတာကိုရှာဖတ်ပြီးစမ်းတယ် ၊ ဘယ်လိုကာရလဲဆိုတာ ထပ်လေ့လာတယ် ၊ Bypass ပြန်ရှာတယ်။ ဒီလိုနည်းနဲ့ လေ့လာလို့အပြီးမှာတော့ ကျနော့်ဆီမှာ စမ်းထားတဲ့ code လေးတွေကျန်ခဲ့ပြီပေါ့။

ကျနော် စမ်းထားတဲ့ code တွေကို ကျနော့်ကိုအမြဲတမ်းအကြံကောင်းတွေပေးတဲ့ Ko Ye Yint Min Thu Htut (YEHG) ကိုပြဖြစ်တယ်။ သူ့ရဲ့ အကြံပေးချက်ကြောင့် အခုအဲ့ဒီ code တွေက Damn Vulnerable File Upload Lab ဖြစ်သွားပါတယ်။ ကျနော့်အတွက် ဂုဏ်အယူဆုံးကတော့ SQL Injection ကို ကျနော်သေချာသိအောင် လေ့လာခဲ့တဲ့ SQLi-Labs ရဲ့ Audi-1 က ကျနော့် File Upload Lab လေးကို github မှာ star ပေးသွားတာပဲဖြစ်တယ်။ ဒါကြောင့် ကျနော့်အနေနဲ့ အခြေခံတွေကိုလုံးဝကျော်မသွားဖို့နဲ့ ကိုယ့်ကိုယ်ကို မလိမ်မိဖို့ အကြံပေးချင်ပါတယ်။ သို့ပေမဲ့ ကျနော်က Noob တစ်ယောက်သာဖြစ်တဲ့အတွက် Noob တစ်ယောက်ရဲ့ အကြံလို့ပဲသုံးလိုက်ခြင်းဖြစ်ပါတယ်။

1.5 – Programming Advantages

Programming ကို ကြောက်နေတယ်ဆိုရင်တော့ Hacking ဆိုတာကြီးနဲ့ ဝေးနေရဦးမှာပါ။ ဥပမာလေးတစ်ခုနဲ့ ပြောပြချင်ပါတယ်။ PHP နဲ့ ရေးထားတဲ့ Web App တစ်ခုမှာ Code Injection Vulnerability ရှိတယ်ဆိုပါတော့။ အောက်မှာပြထားတာက အရိုးရှင်းဆုံး vulnerable code ပါ

```
<?php
eval($_GET['code']);
?>
```

Code Injection ကိုသိတဲ့အတွက် filename.php?code=phpinfo(); လို့ inject လုပ်လို့ရတယ်ဆိုတာကို ကျနော်သိပါတယ်။ Remote Code Execution (RCE) အဖြစ်ကိုပြောင်းဖို့အတွက် system("uname -a"); လိုသေးတယ်ဆိုတာလောက်ထိ OWASP တို့လို သေသေချာချာရေးထားတဲ့ Document တွေကြောင့် သိနိုင်သေးပါတယ်။ ဒါပေမဲ့ system() , exec() တို့လို Command Execution functions တွေကို disable လုပ်ထားတာမျိုးဆိုရင် PHP Programming ကို သိခြင်းမသိခြင်းက တဖြည်းဖြည်းသိသာလာပါလိမ့်မယ်။

ကျနော် ဘာဆက်လုပ်ရမှန်းမသိတုန်းက Ko Someone ကို ကျနော်မေးဖူးပါတယ် ၊ သူက PHP ကိုကောင်းကောင်းရတော့ ကျနော်မသိတဲ့ တခြား function တစ်ခုကိုပြောင်းသုံးပေးလိုက်တယ်။ အရမ်းရိုးရှင်းပါတယ်။ ဒီတော့ တကယ်စိတ်ဝင်တစားလုပ်မယ်ဆိုရင်တော့ Programming သိထားတာကပိုပြီးကောင်းတယ်ဆိုတာကို အကြံပေးချင်ပါတယ်။ Programming မရရင် သေချာပေါက်လုပ်လို့မရတဲ့ အရာတစ်ခုရှိပါသေးတယ်။ အဲဒါကတော့ Code Auditing လို့ခေါ်တဲ့ Source code ကို Analysis လုပ်ခြင်းပဲဖြစ်ပါတယ်။ Soure code နားမလည်မှတော့ အလှပဲထိုင်ကြည့်လို့ရတော့မှာပေါ့။

2 - နိဒါန်း

အဆုံးသတ် အနေနဲ့ ပြောချင်တာကတော့ ကျနော်က စာရေးတာရယ် ၊ Hacking ရယ်ကို ဝါသနာပါတဲ့သူတစ်ယောက်ဖြစ်တာကြောင့် Hacking နဲ့ ဆိုင်တဲ့ စာတွေရေးဖြစ်တာဖြစ်ပါတယ်။ ဒီဆောင်းပါးက ကျနော့်ရဲ့ ပထမဆုံးစာအုပ်ဖြစ်တာကြောင့် မယဉ်ကျေးတဲ့အသုံးနှုန်းများပါဝင်ခဲ့တယ်ဆိုရင် တောင်းပန်အပ်ပါတယ်။ စာအုပ်ထဲမှာ ပါဝင်တဲ့ အကြောင်းအရာကြောင့် သင့်အတွက် မှတ်သားစရာတစ်ခုခုရတယ် ၊ ဒါမှမဟုတ် ကျနော့်ကို အကြံပေးချင်တဲ့ အကြောင်းအရာတွေရှိတယ်ဆိုရင်တော့ အောက်မှာပေးထားတဲ့ contact များကနေ ဆက်သွယ်နိုင်ပါတယ်။

2.1 - Contacts

Email – thinbashane@gmail.com

Website – http://location-href.com

WeChat ID – swiftfanboy

Twitter - @arf0flunam00n

2.2 - Thanks

ကျနော်ကျေးဇူးတင်ရမယ့် သူတွေရော ၊ လေးစားရတဲ့သူတွေရော အရမ်းများတဲ့အတွက် ဒီကနေအားလုံးကို ဂါရဝပြုလိုက်ပါတယ်။

လူသားအားလုံးကို လေးစားပါတယ်


LEGION
OF
LOL