Security Alert

Cross-site Scripting ပြဿနာများ

Cross-site scripting (XSS) ကို အခြေခံတဲ့ တိုက်ခိုက်မှုတွေဟာ အသစ်မဟုတ်သေးမယ့် လူမှုရေး media တွေ ပေါ်ပေါက်လာတာက XSS တိုက်ခိုက်မှုအသစ်တွေ ထပ်ထုတ်နိုင်စေပါတယ်။

An XSS Primer

XSS တိုက်ခိုက်မှုနည်းလမ်းမှာ အသုံးအများဆုံးဟာ email ဖြစ်ပါတယ်။ ပြစ်မှုကျူးလွန်သူတစ်ယောက်ဟာ သာမန် URL တစ်ခုမှာ နိုင်ငံခြားဘာသာစကားလိုမျိုး အထူးအက္ခရာတွေကို တွဲဆက်လိုက်ပါတယ်။ ဒီအက္ခရာတွေဟာ လူလိမ်တွေ ပြုလုပ်ထားတဲ့ script တစ်ခုကိုလုပ်ဆောင်ဖို့ web server ကို ပြောပါလိမ့်မယ်။ ဥပမာ အားဖြင့်ပြောရရင် တိုက်ခိုက်သူတစ်ယောက်ဟာ ဘဏ်ရဲ့ URL မှာ ဒီလို script တစ်ခုကို တွဲဆက်ထားပြီး email ပို့လိုက်ပါတယ်။ ဒီ email ဟာ ဘဏ်ကနေ တရားဝင်ပို့တယ်လို့ ယုံကြည်ပြီး link ကို click နှိပ်ရင် browser ဟာ web server ဆီကို ဒီ script ပို့လိုက်ပါတယ်။ ဒါဆို code အမျိုးမျိုးကို လုပ်ဆောင်စေပြီး ဘဏ်ကို ဝင်ရောက်တဲ့ login အသေးစိတ်ဟာ browser cookie တစ်ခုကနေ တိုက်ခိုက်သူထံသို့ ရောက်ရှိသွားပါတယ်။ အဲဒီနောက် သူဟာ online ဘဏ်စာရင်းကို ဝင်ရောက်သွားနိုင်ပါပြီ။

နောက်ထပ် XSS တိုက်ခိုက် မှုအမျိုးအစားတစ်ခုဟာ အမျိုးမျိုးသော code တွေကို web server တစ်ခုမှာ သိုလှောင်ထားပါတယ်။ တိုက်ခိုက်သူဟာ e-commerce site တစ်ခုသို့ login ဝင်ရောက်ပြီး script တစ်ခုပါဝင်နေတဲ့ သတင်းစာသား တစ်ခုကို post တင်ထားပါတယ်။ ရက်အနည်းငယ်ကြာပြီးနောက် ဒီ site ကို login ဝင်တဲ့အခါ ဒီ post ကို ဖတ်ရပါမယ်။ အဲဒီမတိုင်ခင်က login သတင်းအချက်အလက်ပါရှိတဲ့ cookie ကို script က ခိုးယူပြီး အဲဒါကို လူလိမ်ထံ ပေးပို့ပါတယ်။ အဲဒီနောက် သူတို့ဟာ ကိုယ်ပုံစံ အယောင်ဆောင်နိုင်ပါလိမ့်မယ်။

တတိယအမျိုးအစား XSS တိုက်ခိုက်မှုဟာ web browser ကိုယ်တိုင်ပဲ ထိသွားနိုင်ပါတယ်။ ဒီအကြောင်းအစည်းမှာတော့ ကိုယ်သွားကြည့်မယ့် site တစ်ခုပေါ်မှာ တိုက်ခိုက်သူက အဆိပ်ရှိနေတဲ့ flash file တစ်ခုကို ထားထားပါတယ်။ Video တွေကို browser က download လုပ်တဲ့အခါ ဒီ file ဟာ browser ထဲမှာ script တစ်ခုကို ချိန်ကိုက်လုပ်ဆောင်စေပါတယ်။ အဲဒီနောက် တိုက်ခိုက်သူဟာ browser ထဲမှာရှိတဲ့ စာမျက်နှာတွေမှာ ပါဝင်တဲ့အရာတွေကို ထိန်းချုပ်နိုင်သွားပါပြီ။

Web 2.0 and XSS

ဒီကနေ့ website တွေဟာ ယေဘုယျ XSS တိုက်ခိုက်မှုတွေကို စစ်ထုတ်တဲ့အလုပ်ကို အရင် site တွေ ပြုလုပ်ခဲ့တာထက်စာရင် ပိုပြီး ကောင်းစွာလုပ်နိုင်ပေမယ့် ကွဲပြားတဲ့ content-filtering ပြုလုပ်ဖို့ အခြေအနေရှိတဲ့ site နှစ်ခုကို partner အဖြစ် ဆုံးဖြတ်ရင် ဘာဖြစ်လာနိုင်ပါသလဲ။

ပြောရမယ်ဆိုရင် site A ပေါ်ရှိ ကြော်ငြာတစ်ခုကို click နှိပ်လိုက်ပါတယ်။ မသိနိုင်တဲ့ အဖြစ်က ဒီကြော်ငြာမှာ XSS တိုက်ခိုက်မှုတစ်ခုပါဝင်နေပြီး browser ကို site B ဆီ ငြိမ်သက်စွာ ရောက်ရှိစေပါတယ်။ ခရီးသွား site တွေဟာ လူမှုရေးကွန်ရက် profile ကို အပြည့်အဝ ရယူနိုင်ပါတယ်။ XSS တိုက်ခိုက်မှုတစ်ခုနဲ့ site B ကို သွားရောက်ဖို့၊ အဲဒီမှာ login ဝင်ရောက်ဖို့၊ အဲဒီမှာရှိတဲ့အရာတွေကို click နှိပ်ဖို့မလိုပါဘူး။ ဒါမှမဟုတ် အဲဒီ site B ရှိနေတယ်ဆိုတာကိုတောင် မသိဘဲ ကိုယ့်ကို သားကောင် ဖြစ်လာစေပါတယ်။ ဘာကြောင့်လဲဆိုတော့ site B ဟာ လူမှုရေး ကွန်ရက် profile ကို (သူငယ်ချင်းရဲ့ သတင်းအချက်အလက်လည်း ဖြစ်နိုင်ပါတယ်) ရယူနိုင်ပြီးသားဖြစ်နေပြီး site A ပေါ်မှာရှိတဲ့ ကြော်ငြာရဲ့နောက်က ပြစ်မှုကျူးလွန်သူဟာလည်း ဒီသတင်းအချက်အလက်တွေကို ယခုရယူထားနိုင်နေပါပြီ။

ကံမကောင်းစွာဘဲ site တွေဟာ connection ကို encrypt လုပ်ထားရဲ့နဲ့ XSS တိုက်ခိုက်မှုကို ကြိုတင်ကာကွယ် မထားနိုင်ပါဘူး။ Encryption

သုံးထားတဲ့ site ကို ဝင်ရောက်ကြည့်တဲ့အခါမှာ သော့ခလောက်အသေးလေးဟာ toolbar ထဲမှာ ပေါ်လာကာ SSL (Secure Sockets Layer) ကို ဖော်ပြနေပြီး တိုက်ခိုက်မှုကိုပါ encrypt လုပ်နေတာပါပဲ။ ယေဘုယျအားဖြင့် site designer တွေဟာ XSS အပြည့်အဝအသုံးချမှုကို ကာကွယ်နိုင်ဖို့ site ကို ထိန်းချုပ်ထားပြီး ဖြစ်နေရပါမယ်။ အသုံးပြုသူတွေဟာ XSS တိုက်ခိုက်မှုကို ရှောင်ရှားနိုင်တဲ့ နည်း ၂ နည်း ရှိပါတယ်။ တစ်ခုကတော့ site တစ်ခုကနေ အခြားတစ်ခုကို link ချိတ်ထားတာတွေကို လျစ်လျူရှုထားလိုက်တာပါ။ ပြောရရင် link ကို click နှိပ်တာနဲ့ အခြား tab တစ်ခုထဲမှာ *somerandom-site.com* ကို တိုက်ရိုက်ရောက်ရှိသွားရမယ်။ Site ရဲ့ search လုပ်ဆောင်ချက်ကို အသုံးပြုပြီး စာမျက်နှာကို ရှာရမယ့်အစား site A ဟာ somerandomsite. com/page ဆီကို link ချိတ်ဆက်ထားပါတယ်။ ဒီနည်းလမ်းဟာ ချိတ်ဆက်ထားတဲ့ URL ထဲမှာ မြှုပ်နှံထားတဲ့ XSS တိုက်ခိုက်မှုတွေကို ထိရောက်စွာတားဆေးနိုင်မယ့် လည်း site ၂ ခုဟာ content တွေကို မျှဝေသုံးထားတဲ့အချိန်မှာ အကူအညီမပေးနိုင်ပါဘူး။ တခြားနည်း တစ်ခုကတော့ JavaScript လိုမျိုး scripting language တွေကို browser မှာ ပိတ်ထားဖို့ပါပဲ။ ဒါပေမဲ့ ဒါဟာ site တချို့မှာ လိုချင်တဲ့လုပ်ဆောင်ချက်တွေကိုပါ ပိတ်သွားစေနိုင်ပါတယ်။

အန္တရာယ်ရှိတဲ့ script တွေကို ပိတ်ဆို့ထားခြင်း

Internet Explorer 8 ဟာ script ပိတ်ထားတဲ့ XSS ကာကွယ်ပေးမှုပါရှိပြီးသားဖြစ်တဲ့ ပထမဦးဆုံး broswer ဖြစ်ခဲ့ပါတယ်။ ပြီးတော့ Google Chrome က နောက်က လိုက်လုပ်ဆောင်လာခဲ့ပါတယ်။ နှစ်ခု စလုံးဟာ web server တစ်ခုကနေလာတဲ့ script တစ်ခုကို malicious ဖြစ်နေလားလို့ ကြည့်ပါတယ်။ ဒီလိုသာ ဖြစ်နေခဲ့ရင် အဲဒါကို ပိတ်ထားလိုက်ပါတယ်။

Firefox အသုံးပြုသူတွေဟာ No-Script (*find.pcworld.com/70213*) ဆိုတဲ့ add-on ကို အသုံးချပြီး script တွေကို ရွေးချယ်ပိတ်ထားနိုင်ပါတယ်။ ဥပမာအားဖြင့် site ပေါ်မှာ တခြား script အစိတ်အပိုင်းတွေကို ပိတ်ထားချိန်မှာ flash video တစ်ခုကို မပိတ်ဘဲ ထားနိုင်စေပါတယ်။

NoScript ရဲ့ ပြဿနာတစ်ရပ်ကတော့ အသုံးပြုတွေအများစုဟာ script တစ်ခုခြင်းစီကို မပိတ်မိဖို့ လုပ်ဆောင်ရတဲ့ အဆင်မပြေနိုင်မှုပါပဲ။ ဒါကို မကြိုက်ကြပါဘူး။ ဒါပေမဲ့လည်း ပိတ်ခြင်း၊ မပိတ်ခြင်းဟာ ယေဘုယျ အားဖြင့် ဒုတိယဦးစားပေး လုပ်ဆောင်ချက်ပါပဲ။ တစ်ခုတည်း အတွက် ဒါမှမဟုတ် လုပ်ဆောင်ချက်အားလုံးကို သွားရောက် ကြည့်ရှုဖို့ ရွေးချယ်ထားတဲ့ site တစ်ခုပေါ်မှာ script တွေကို လုပ်ပိုင်ခွင့် သတ်မှတ်တာကိုလည်း လုပ်နိုင်ပါတယ်။

OS များကိုမဟုတ်ဘဲ အသုံးပြုသူတွေကို ပစ်မှတ်ထားတဲ့ လူလိမ်များ

ဘယ်သူ့ဆီမှာ အလုံခြုံဆုံး operating system ရှိနေပါသလဲ။ Apple လား၊ Google လား၊ Microsoft လား။ လုံခြုံရေးကျွမ်းကျင်သူတစ်ယောက် ပြောကြားမှုအရ တကယ့်အဓိက အကြောင်းအရာကတော့ OS ကို ဘယ်သူက အသုံးပြုနေသလဲဆိုတာပဲ ဖြစ်ပါတယ်။

"လက်ရှိမှာဖြစ်နေတဲ့ နည်းပညာပိုင်းအရ တိုက်ခိုက်ခံရနိုင်မှုအားလုံးကို Microsoft က လက်ဝါးကြီးအုပ်မထားနိုင်ပါဘူး" လို့ Symantec Security Response ရဲ့ နည်းပညာဒါရိုက်တာတစ်ယောက်က ဆိုပါတယ်။ ယနေ့ခေတ် online ပြစ်မှုကျူးလွန်မှုတွေက အသုံးပြုသူတွေရဲ့ အပြုအမူတွေပေါ်မှာ မူတည်တာ များပါတယ်။

လူတစ်ယောက်ကို အန္တရာယ်ရှိနေတဲ့ content တွေ ပါရှိနေတဲ့ attachment တစ်ခုကို ဖွင့်စေဖို့ နည်းပညာကျွမ်းနေဖို့ မလိုအပ်ပါဘူး။

လက်ရှိမှာတော့ နည်းပညာပိုင်းအားနည်းချက်တွေကို ပြည့်ဝစွာ အသုံးချသွားနိုင်တဲ့ malware ၃ ရာခိုင်နှုန်းကိုသာ Symantec က ရင်ဆိုင်တွေ့ရပါတယ်။ ကျန်ရှိတဲ့ ၉၇ ရာခိုင်နှုန်းဟာ social engineering လှည့်ဖျားကြစည်ချက်အမျိုးအစားတချို့ကနေ အသုံးပြုသူတစ်ယောက်ကို လှည့်စားနိုင်ဖို့ ကြိုးစားနေတာတွေ ဖြစ်ပါတယ်။

ဘာလုပ်နိုင်ပါသလဲ။ မေးမြန်းလာသမျှတွေကို သံသယစိတ်အပြည့် နဲ့ပဲ သဘောထားနိုင်ပါတယ်။ ဒီလိုဆိုရင်တော့ ဆက်သွယ်သမျှပုံစံအားလုံးကို သက်ရောက်သင့်ပါတယ်။ Email ကို သာမဟုတ်ဘဲ phone ခေါ်ဆိုမှုတွေကိုပါ သက်ရောက်သင့်ပါတယ်။

ဘယ် computer ၊ ဒါမှမဟုတ် ဘယ် operating system မဆို ၁၀၀ ရာခိုင်နှုန်း လုံခြုံတယ်လို့မရှိပါ။ လူတွေဟာ Microsoft ရဲ့ product တွေကို တိုက်ခိုက်နိုင်ဖို့ ကြိုးစားနေတာဟာ ဈေးကွက်ဝေစု ကြီးမားနေတဲ့အတွက် ကြောင့် ဖြစ်ပါတယ်။ ဒါပေမဲ့ Google ရဲ့ Chrome OS က စီးပွားရေးလုပ်ငန်းနဲ့ စားသုံးသူတွေရဲ့ ဈေးကွက်ကို ယူဆောင်လာနိုင်ခဲ့ရင် သူ့မှာလည်း ကြီးမားတဲ့ ပစ်မှတ်ကြီးတစ်ခု ရှိလာလိမ့်ပါမယ်။

Novice