Table of Contents

Introduction

ဒီစာအုပ်ကို Real World SQL Injection ဆိုတဲ့နာမည်နဲ့ Education and Ethical Hacking အတွက်ရည်ရွယ်ပြီး ရေးသားသွားမှာဖြစ်ပါတယ်။ ဒီစာအုပ်သည် IT Security နဲ့ပတ်သက်သော Knowledge ကိုအပြည့်အဝပေးနိုင်ပေမယ့် IT Security ရဲ့တစ်စိပ်တစ်ပိုင်းအဖြစ် SQL(Structured Query Language) Injection နဲ့ပတ်သက်တဲ့ Knowledge တွေကိုတော့ တတ်နိုင်သမျှ, လက်လှမ်းမှီသမျှ, Public သုံးစာမျက်နှာပေါ်မှာ တင်နိုင်သမျှသော အကြောင်းအရာ အချက်အလက်များကို Lab နဲ့တွဲပြီး အကောင်းဆုံး ရှင်းလင်းပြပေးသွား မှာဖြစ်ပါတယ်။ ဒီစာအုပ်မှာ အဓိကအားဖြင့်အပိုင်း ၃ ပိုင်းခွဲပြီးရေးသားသွားမှာ။

ပထမပိုင်းအနေနဲ့ SQL Injection Methodology and Research အပိုင်းကို Sample ပုံစံများနဲ့ ရှင်းပြသွားမှာဖြစ်ပါတယ်။

ဒုတိယပိုင်းအနေနဲ့ကတော့ SQL Injection ကို Offline Site and Real World Site များဖြင့် Lab များလုပ်ပြပေးသွားမှာ ဖြစ်ပြီးတော့၊

တတိယပိုင်းအနေနဲ့ကတော့ SQL Injection မှာသိသင့်သိထိုက်သော DIOS ရေးနည်းများအပါအဝင် SQL Injection နဲ့ပတ်သက် သက်ဆိုင်သမျှ Knowledge တွေကို နောက်ဆက်တွဲ အပိုင်းအနေနဲ့ရေးသားသွားမှာဖြစ်ပါတယ်။

ဒီသုံးပိုင်းဟာ တခုနဲ့တခု ပတ်သက်ဆက်စပ်နေမှာပါ၊ ဘာကြောင့်လည်းဆိုတော့ ပထမပိုင်းက Concept တွေကို သိရှိနားလည်ထားမှသာ ဒုတိယပိုင်း Lab တွေကို ရင်နှီးကျွမ်းကျင်စွာနားလည်နိုင်မှာ ဖြစ်ပါတယ်။ SQL Injection ရဲ့ Concept တွေ SQL Injection Type တွေရဲ့ပြောင်းလဲတတ်ပုံ သဘောတရားတွေကိုမသိထားရင် Lab တွေမှာလုပ်ပြသမျှကို ဘာကြောင့် တခုနဲ့တခုမတူပဲပြောင်းလဲ သွားရတယ်ဆိုတာကို စာဖတ်သူတွေအနေနဲ့ လက်လှမ်းမှီလိုက်မှာမဟုတ်ပါဘူး။ ဒါကြောင့် Concept ဟာလည်း သိပ်ကိုအရေးပါပါတယ်။ Concept ဟာအရေးကြီးတဲ့အပိုင်းဖြစ်တာကြောင့် စာရေးသူအနေနဲ့ Concept ပိုင်းကို နားလည်နိုင်သမျှနားလည်အောင် Real World Style Sample တွေနဲ့ရော မိမိတို့ Inject လုပ်လိုက်တဲ့ Quote, Query တွေဟာ Database အတွင်းကိုဘယ်လိုဝင်ရောက်သွားသလဲဆိုတဲ့ Database Execute Sample လေးတွေပါ ထည့်ပြီးရေးသားသွားမှာဖြစ်ပါတယ်။

ဒုတိယဖြစ်တဲ့ Lab ခန်းမှာတော့ Offline and Online Site တွေနဲ့ SQL Injection Method တွေကိုစုံနိုင်သမျှ စုံအောင်ရှာဖွေထားပါတယ် ထို့အတူ မတူညီတဲ့ Database တွေနဲ့လည်း Labs လုပ်ပြထားမှာဖြစ်ပါတယ် Real World ဆိုတဲ့အတိုင်း Ethics ကိုအတတ်နိုင်ဆုံးထိန်းသိမ်းပြီး Offline and Online Lab တွေကို Screen Capture တွေနဲ့အတိုအကျရှင်းပြ လုပ်ပြသွားမှာပါ၊ Website တွေဟာအသုံးပြုထားတဲ့ Database တို့ WAF(Web Application Firewall) တို့မတူရင် Inject လုပ်ရတဲ့ Method and Query တွေဟာလည်း

မတူညီတော့ပါဘူး၊ အဲ့ဒီလိုမတူညီမှုတွေကိုလည်း Lab တစ်ခုချင်းအလိုက်အကောင်းဆုံး အကိုးအကားတွေနဲ့ ရှင်းပြသွားမှာဖြစ်ပါတယ်။

တတိယပိုင်းကဖတော့ SQL Injection Note လို့ပြောရပါလိမ့်မယ်။ SQL Injection နဲ့ပတ်သက်သော လိုအပ်သော DIOS တွေ Query တွေကို တတိယပိုင်းမှာဖြည့်တင်း ရေးသားထားမှာဖြစ်ပြီးတော့၊ SQL Injection မဖြစ်အောင်အတတ်နိုင်ဆုံး ဘယ်လိုကာကွယ်ရမလဲဆိုတဲ့ နည်းလမ်းတွေကိုပါဖော်ပြပေးသွား မှာဖြစ်ပါတယ်။

ဒါကြောင့် ဒီသုံးပိုင်းလုံးမှာပါဝင်တဲ့ SQL Injection နဲ့ပတ်သက်သော Knowledge တွေကို စာဖတ်သူတို့ရဲ့ Education နယ်ပယ်ထဲမှာအပြည့်အဝပြန်လည် အသုံးချနိုင်မယ်လို့ယုံကြည်ပါတယ်။ ဒီစာအုပ်သည် Attacking Purpose မဟုတ်တဲ့အတွက် Deface ရေးနည်း။ Deface အုပ်နည်းတွေတော့ ပါဝင်မှာမဟုတ်ပါဘူး။ စာဖတ်သူတို့အတွက် SQL Injection Lab Site တွေနဲ့ Real World ကြားက ကွာဟမှုကို တတ်နိုင်သမျှကျဉ်းမြောင်းသွားစေဖို့ကိုပဲ ရည်ရွယ်ထားခြင်းဖြစ်တယ်ဆိုတာကို ကြိုတင်အသိပေးချင်ပါတယ်။ ဒါဆိုရင် ဒီစာအုပ်မှာပါဝင်မယ့် အပိုင်းကဏ္ဍတွေနဲ့ အကြောင်းအရာတွေကိုသိပြီဖြစ်တဲ့အတွက် ဆက်လက်ပြီး တစ်ပိုင်းချင်း အစဉ်အတိုင်းဖလှယ်လာကြည့်ကြရအောင်။