[《精通脚本黑客》](file:///F:\Doc\精通脚本黑客.pdf)

# 常识了解：

1. asp、aspx一般会与windows和IIS搭配
2. PHP、JSP会解释perl文件，所以可以上传pl文件
3. 先收集信息分析信息，然后根据信息扫描漏洞，然后测试漏洞是否可行，最后解决漏洞
4. access数据库是在每个网站目录下，mysql数据库是放在一起
5. [HTML响应机制（Response mechanism）](HTML%20Response%20Mechanism.docx)
6. 语言：[PHP](PHP.docx)、[VBScript](VBScript.docx)、[JavaScript](JavaScript%20Language.docx)、[HTML语言](HTML%20Language.docx)、python、C
7. [数据库](Database.docx)：Oracle、[MySQL](MySQL.docx)、[SQL Server](SQL%20Server.docx)、access
8. 环境：[ASP](ASP.docx)、[PHP](file:///F:\Experience\About《精通脚本黑客》\PHP.docx)、[JSP](JSP.docx)
9. DOS命令(获取shell后使用)
10. 后台登陆界面网页源代码用户名和密码所指向的变量名可能为数据库列名
11. **\*\*\*网络安全中的重要知识点**：**①**[**Cookie**](file:///F:\Experience\About《精通脚本黑客》\Cookie.docx) **②**[**正则表达式（Regular expression）**](file:///F:\Experience\About《精通脚本黑客》\Regular%20expression.docx) **③**[**XSS**](file:///F:\Experience\About《精通脚本黑客》\XSS.docx)④[脚本病毒](Script%20Virus.docx)
12. **UNIX/Linux权限**：权限分为所有者权限、同组用户权限、其他组用户权限，r只读、w只写、x执行

**例**：rwxrwxr-x，第一个rwx表示文件目录的所有者权限为读、写、执行，第二个为同组用户，第三为其他组用户

**常见数据库组合：**

*ASP+IIS+ACCESS/MSSQL*

*PHP+Apache+MySQL*

*JSP+Tomcat+MySQL/MSSQL*

**Linux命令查询**：<http://man.linuxde.net/>

一、FootPrinting（踩点）——使用[Google高级搜索](Google%20advanced%20search.doc)

A、 网站注册信息（[域名后缀](Domain%20suffix.txt)等）

B、 网管资料

C、 共享资料

D、 端口信息

E、 FTP资源

F、 网站拓扑结构

G、 网站URL地址结构

H、 网站系统版本

I、 后台地址（[常用后台文件名](Common%20background%20file%20name.txt)）

J、 弱口令

二、初步测试（Google Hack）

**1.查找别人留下的Webshell**

搜索引擎：*某些木马关键字 inurl:文件名*

**2.利用搜索引擎批量注入**

inurl:asp?id=

inurl:php?id=

site:网站 inurl:asp?id= \php?id=

intext(网页中含有的字样)

inurl(网址中含有的字样)

**3.测试是否存在简单注入漏洞（构造语句）**

例如网址后加上and 1=1和and 1=2，如果返回页面不同即为存在漏洞

参考[常用的语句](Google%20Hacking%20statement.doc)

三、使用已有漏洞渗透（[burpsuite](Burpsuite%20detailed.doc)）

**1）查找别人留下的Webshell**

① 搜索引擎：*某些木马关键字 inurl:文件名*

② 工具爬取：木马关键字，木马文件名

**2）爬取目录与文件（数据库文件，网站体系结构）**

数据库（需要了解目标数据库，可以试装一遍）

自定义字典，用工具爬取

参考<robots.txt>

**3）暴库**

1.寻找conn.asp等数据库连接文件，直接访问出错暴库（相对路径出错）

2.在该网站的最后一个“/”改成“%5c”就能够暴出它的数据库来（虚拟目录绝对路径出错）

**4）突破后台登陆**

根据登陆文件名，如login.asp、admin.asp、denglu.asp、manager.asp、guanli.asp

社工猜测\字典撞库\绕过登陆

**5）漏洞攻击**

1.注入漏洞（获取数据）

1）判断是否存注入漏洞：

需要自己总结构造，关注最新漏洞平台报告，常用的有asp?id=、asp?newsid=、asp?page=、asp?Article=、php?id=、’、

and 1=1、and 1=2

2）判断数据库类型(根据注入报错判断)：

Access：小数据库，url后加and user>0，若返回错误含有Microsoft JET Database则为Access

MySQL：支持/\*注释，url后面加/\*，若没有出错即为MySQL，或者加/\*%20s\*/，若返回错误则为MySQL

MSSQL：同Access，若含有SQL Server则为MSSQL/用’、and 1=1、and 1=2报错

3）注入方法：

[Access+asp手工注入](SQL%20manual%20injection-access.docx)

[MySQL+asp手工注入](SQL%20manual%20injection-mysql.docx)

[MSSQL+asp手工注入](SQL%20manual%20injection-mssql.docx)

其他方法参考[常用SQL注入语句](Common%20SQL%20injection%20statements.doc)

2.旁注攻击

网站虚拟主机服务器绑定多个域名，可以从其他薄弱网站入手

第三方插件——默认密码\获取第三方插件数据库——攻击

3.cookie欺骗

心情网络投票：

1.function touvote(){window.open

2.formvote.submit();}"

3.formvote.action=

4.document.write (vote)

Google hack后修改admin和qx值为admin=admin和qx=qx，cookie欺骗

4.跨站漏洞（输入的字符能够被其他人看到）（获取权限）

**①**在有**输入框**的地方输入并保存

**<script>alert("test")</script>**

在重新打开时弹窗则说明有漏洞

**②**若script字符被过滤则使用

<img src=javascript:alert("test") >

**③**若javasrcipt:字符被过滤则使用ASCII 码来替换，把被过滤字符转换为16进制字符替换

<img src="javascrip&#116&#58alert(/xss/)">

或者添加空格，tab，比如

<img src="javas????cript:alert(/xss/)" width=100>

还可以用事件和属性避免关键字，绕过监测，比如

<img src="#" onerror=alert(/xss/)>

<img src="#" style="Xss:expression(alert(/xss/));">

值得一提的是，yahoo mail 的跨站漏洞，是由如下的语句造成的。

<STYLE onload=alert('cookes exploit!');alert(document.cookie)">

总结来说，输入script语句提交测试HTML编码后的结果，并根据（浏览器网页源码）改变的字符进行猜测修改，

也可以用超链接，或者别的编码方式侧类旁通寻找<a href => </a>的语法格式代码

5.其他漏洞

查看具体漏洞报告网站

链接渗透师导航<https://www.shentoushi.top/index>

**6）其他技术**

社会工程学：自定义字典，邮件，网页钓鱼等等

**7）攻击类型**

①信息泄露

注入——获取数据库

获取账号——获取权限——获取数据库

获取权限——上传木马——获取[webshell（注意免杀）](WebShell.docx)

②DDos攻击

③拒绝服务

④XSS