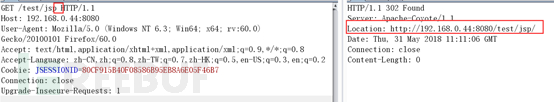
**在Web服务器防止Host头攻击**

前言

访问网站时如果访问路径中缺少/，大多数中间件都会自动将路径补全，返回302或301跳转如下图，Location位置的域名会使用Host头的值。

这种情况实际上风险较低，难以构成Host头攻击。但是由于大多漏洞扫描器会将这种情况检测为Host头攻击，为了通过上级检查或各种审核，大多数甲方单位会要求修复漏洞，彻底解决问题。

[](http://image.3001.net/images/20180718/15319086626129.png)

该跳转路径不是web项目定义的，是中间件自动跳转的，所以不能用编写静态变量的方法修复，web项目中的全局过滤器也无法拦截。需要在web服务器层面配置才能修复。下面给出几种常见服务器的参考修复方法，其中如有错误或不妥的地方欢迎指正。

Apache：

方法一：

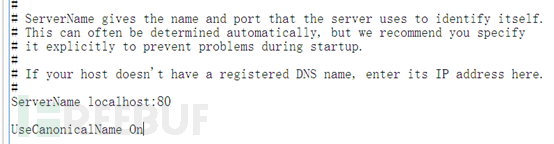
修改\conf\httpd.conf文件

修改ServerName为应用的域名，例如

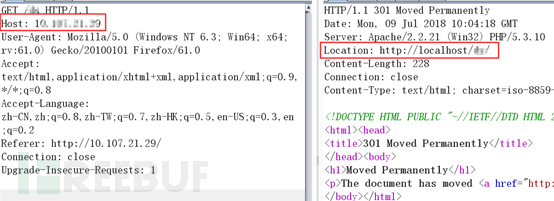
**ServerName** **www**.domain.com:80

添加下列行

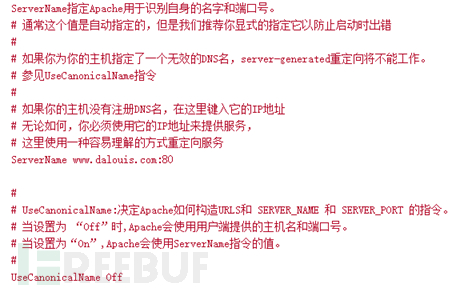
**UseCanonicalName** On

[](http://image.3001.net/images/20180718/1531910129762.png)重启Apache即可。

修复成功的话会看到，服务器端将会使用设定好的ServerName。

[](http://image.3001.net/images/20180718/15319101377214.png)

参数解释：

[](http://image.3001.net/images/20180718/15319101586584.png)

方法二：

修改\conf\httpd.conf文件

参考以下配置添加：

NameVirtualHost 192.168.0.16

<VirtualHost 192.168.0.16>

ServerName 192.168.0.16

<Location />

Order Allow,Deny

Deny from all

</Location>

</VirtualHost>

<VirtualHost 192.168.0.16>

DocumentRoot "C:\www"

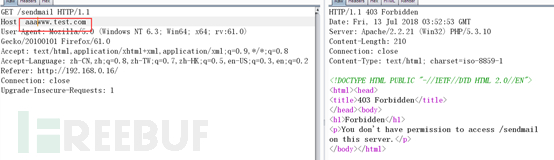
ServerName [www.test.com](http://www.test.com/)

</VirtualHost>

重启Apache即可。

作用：

拒绝直接通过192.168.0.16这个IP的任何访问请求，这时如果你用192.168.0.16访问，会提示拒绝访问。仅允许通过[www.test.com](http://www.test.com/)这个域名访问，主目录指向C:\www

[](http://image.3001.net/images/20180718/1531910565923.png)方法三：

修改\conf\httpd.conf文件

找到”#LoadModule rewrite\_module modules/mod\_rewrite.so”去除前面的”#”号

添加类似以下配置：

RewriteEngine on

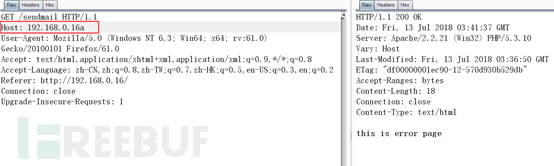
RewriteCond %{HTTP\_HOST} !^192.168.0.16$ [NC]

RewriteRule ^(.\*)$ /error.html

重启Apache即可。

作用：

当HOST头不是192.168.0.16时，重定向到错误页面。

[](http://image.3001.net/images/20180718/15319106672602.png)Nginx：

方法一：

修改nginx.conf

添加一个默认server，当host头被修改匹配不到server时会跳到该默认server，该默认server直接返回403错误。

例子如下：

**server** {

**listen** 8888 default;

**server\_name** \_;

**location** / {

**return** 403;

       }

       }

重启nginx即可。

方法二：

修改nginx.conf

在目标server添加检测规则，参考以下标红配置：

**server** {

**server\_name**  192.168.0.171;

**listen**       8888;

**if** ($http\_Host !~\*^192.168.0.171:8888$)

        {

**return** 403;

        }

**include** /etc/nginx/default.d/\*.conf;

**location** / {

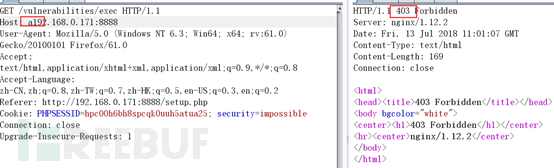
**root** /www/dvwa;

**index** index.php index.html index.htm;

       }

       }

重启nginx即可。

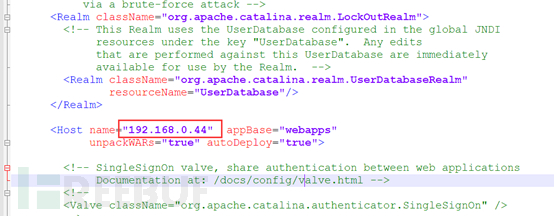
[](http://image.3001.net/images/20180721/15321558068198.png)

Tomcat：

修改tomcat\conf\server.xml

找到如下位置：

[](http://image.3001.net/images/20180721/15321558643364.png)将Host里的name修改为静态的域名，如下：

[](http://image.3001.net/images/20180721/15321558812062.png)重启tomcat即完成修复。

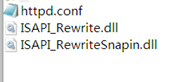
IIS6.0：

使用ISAPI\_Rewrite插件对请求包内容进行检测并重写URL。

插件安装包和破解工具下载地址：<https://pan.baidu.com/s/1hZVfCm7FraQWHlKMKyItFQ>

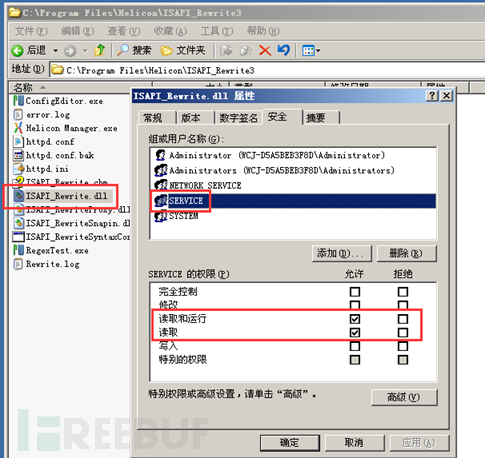
下载完成后双击程序一直点击下一步安装即可。

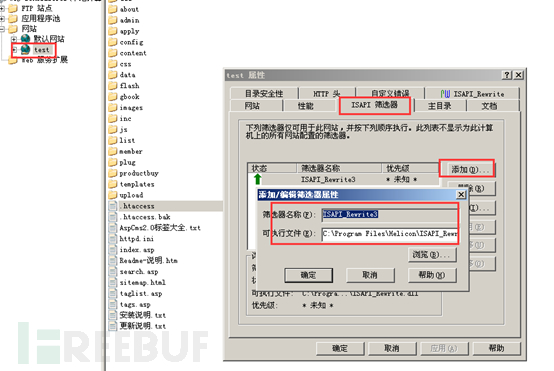
[](http://image.3001.net/images/20180721/15321559463282.png)破解工具解压后如图三个文件

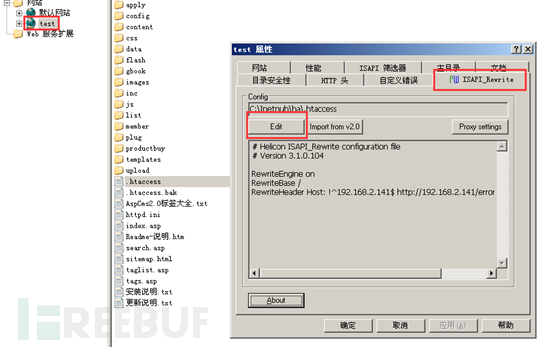
[](http://image.3001.net/images/20180721/15321559607539.png)

将破解的这三个文件直接复制粘贴到ISAPI\_Rewrite的安装目录，也就是覆盖掉官方的原文件, 如果提示不能覆盖,你可以先将官方的这个三个文件重命名其它的名字,再将这个三个破解文件复制过来。

替换完成后，必须为ISAPI\_Rewrite.dll添加SERVICE用户组，并授予读取、读取和运行权限。（该步非常重要，否则后续ISAPI\_Rewrite将无法工作）。

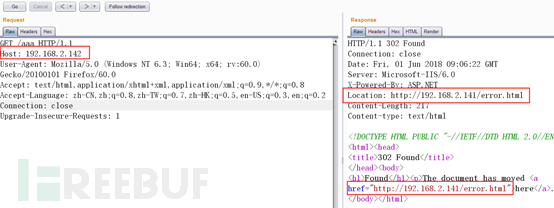
[](http://image.3001.net/images/20180721/15321559827881.png)打开IIS管理工具，选择目标项目->属性->ISAPI筛选器->添加->选择你安装的ISAPI\_Rewrite.dll文件的路径->确定

[](http://image.3001.net/images/20180721/15321559979900.png)重启IIS和重新打开IIS管理工具，在目标项目->属性中可以看到新增的ISAPI\_Rewrite标签，在这里可以根据需求直接写.htaccess规则进行重定向。

[](http://image.3001.net/images/20180721/15321560123718.png)

配置Host头白名单，可参考以下规则。

配置完成点击应用后，当请求包中Host字段不为设定好的192.168.2.141时，会自动跳转到报错页面。

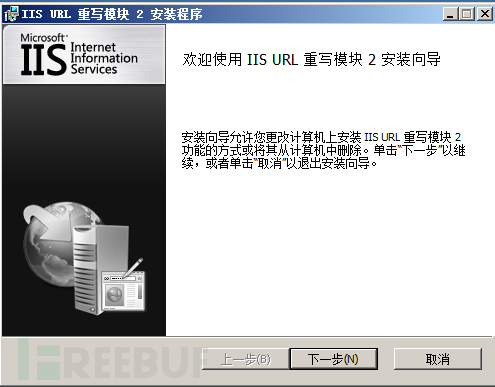
[](http://image.3001.net/images/20180721/15321561331981.png)IIS7.0/7.5/8.0：

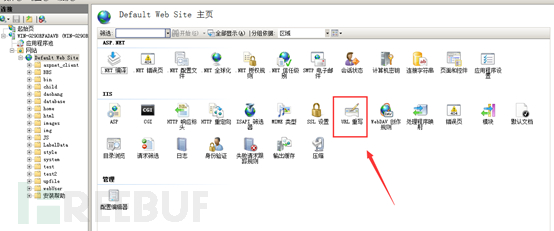
微软推出了一款URL 重写模块工具，可对请求URL进行过滤处理，此工具需要自行安装，下面提供工具下载地址：

微软下载地址(64位)： <http://www.microsoft.com/zh-cn/download/details.aspx?id=7435>

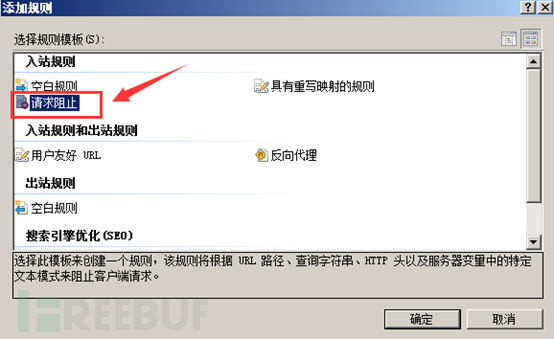
微软下载地址(32位)： <http://www.microsoft.com/zh-cn/download/details.aspx?id=5747>

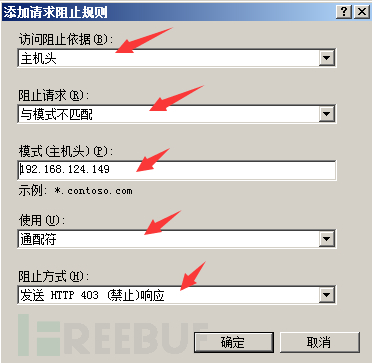
下载完成后双击程序一直点击下一步安装即可。

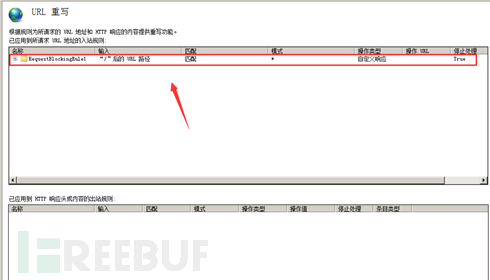
[](http://image.3001.net/images/20180721/15321561715080.png)然后重新启动iis管理工具，此时可以看到IIS栏下有一个URL重写工具。

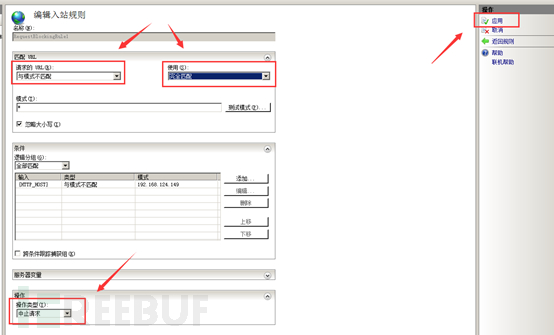
[](http://image.3001.net/images/20180721/15321561867010.png)双击URL重写功能，然后在URL地址入站规则栏上添加规则。

[](http://image.3001.net/images/20180721/15321561989318.png)选择请求阻止。

[](http://image.3001.net/images/20180721/15321562109070.png)参照下图进行配置规则，主机头那填写好网站域名或ip即可，然后点击确定。

[](http://image.3001.net/images/20180721/1532156222814.png)此时双击刚创建的规则。

[](http://image.3001.net/images/20180721/15321562334867.png)在请求的URL选择项选择“与模式不匹配”，在使用项那选择“完成匹配”，在操作类型那选择“中止请求”，然后点击右上角的应用按钮。

[](http://image.3001.net/images/20180721/15321562461517.png)然后重新启动网站，此时重新测试就会发现当host不是192.168.124.149时，服务器会中止请求，从而起到防范host头部的作用。

[](http://image.3001.net/images/20180721/15321562627893.png)

原文链接：

http://www.freebuf.com/articles/web/178315.html