Web 应用程序报告

该报告包含有关 **Web** 应用程序的重要安全信息。

安全报告

该报告由 IBM Rational AppScan 8.0.0.0 创建
2014-4-29 8:21:28

报告信息

Web 应用程序报告

扫描名称：F_上海方心健康科技发展有限公司--安全测试

已扫描的主机

主机	操作系统	Web 服务器	应用程序服务器
www.zgska.cn	Win32	IIS, IIS6	ASP.NET

内容

该报告包含以下部分：

- 管理摘要报告
- 详细的安全性问题
- 修复任务
- 咨询和修订建议

管理摘要报告

测试策略

- Default

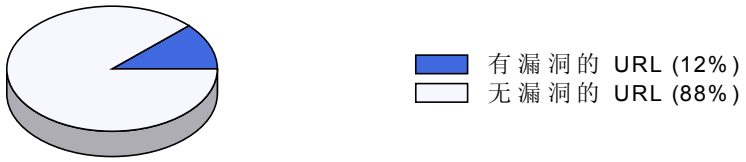
安全风险

以下是在应用程序中最常出现的安全风险。如果要探索哪些问题中包含这些风险，请参阅该报告中的“详细的安全性问题”部分。

- 可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
- 可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

有漏洞的 URL

12% 的 URL 具有包含安全性问题的测试结果。



已扫描的 URL

AppScan 已扫描 233 个 URL。

安全性问题可能原因

以下是应用程序中找到的安全性问题最常见的原因。以下的原因是问题中重复最多的原因。如果要探索哪些问题中包含这些原因，请参阅该报告中的“详细的安全性问题”部分。

- Web 服务器或应用程序服务器是以不安全的方式配置的
- 程序员在 Web 页面上留下调试信息
- Web 应用程序编程或配置不安全
- 未对用户输入正确执行危险字符清理

具有“最多安全问题”（数量问题）的 URL

- http://www.zgska.cn/ (1)

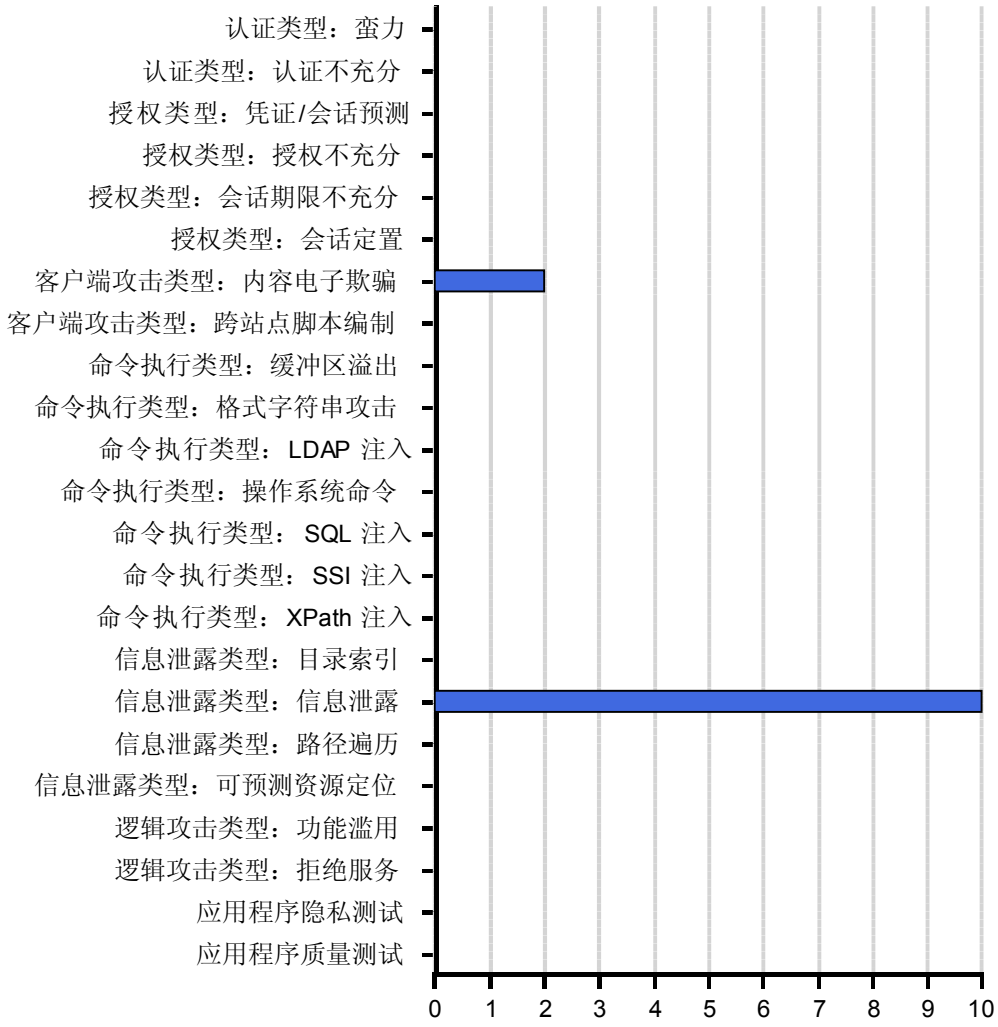
- http://www.zgska.cn/case/index_43.aspx（1）
- http://www.zgska.cn/config/（1）
- http://www.zgska.cn/information/（1）
- http://www.zgska.cn/member/（1）

每台主机的安全性问题

主机	高	中	低	参考信息	总计
http://www.zgska.cn/	0	2	8	2	12
总计	**0**	**2**	**8**	**2**	**12**

每个“威胁类”安全性问题分发

以下是由“威胁类”分发的安全性问题列表。



安全性问题原因分发

58% 与应用程序相关的安全性问题（总计 12 个问题中的 7 个）。
通常，可以由应用程序开发者修订与应用程序相关的“安全性问题”，因为它们是由应用程序代码中的缺陷造成的。
42% 基础结构和平台安全性问题（总计 12 个问题中的 5 个）。
通常，可以由系统或网络管理员来修订“基础结构和平台安全性问题”，因为这些安全性问题是由第三方产品中的错误配置或缺陷造成的。

详细的安全性问题

有漏洞的 URL：http://www.zgska.cn/

此 URL 共有 1 个安全性问题

[1 / 1] HTML 注释敏感信息泄露

严重性：	低
测试类型：	应用程序
有漏洞的 URL：	http://www.zgska.cn/
CVE 标识：	不适用
CWE 标识：	615
修复任务：	除去 HTML 注释中的敏感信息

8 的变体 1 [ID=10639]

用户可能需要注意以下事项：

```
GET / HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 200 OK
Content-Length: 29670
Connection: close
Date: Mon, 28 Apr 2014 09:57:03 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="/cn/css/css_whir.css" rel="stylesheet" type="text/css" />
<meta name="Author" content="万户网络设计制作" />
<title>中国式抗癌，防治癌症转移与复发，防治肿瘤转移与复发、松友饮，汤钊猷
</title>
<meta name="keywords" content="中国式抗癌、防治癌症转移与复发，汤钊猷、肿瘤
```

```
转移与复发、癌症康复、松友饮、松友饮颗粒、、汤钊猷，松友饮" />
<meta name="Description" content="传播中国式抗癌的科学理念，防治肿瘤转移与复发，防治癌症转移与复发，松友饮为癌症患者提供在线交流平台，提供防治癌症的一些方法88" />

<script type="text/javascript" src="/cn/Script/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="/cn/Script/MSClass.js"></script>

<script type="text/javascript">
var syspath='/';
</script>



<script type="text/javascript">
    var menu=1;
</script>
<SCRIPT type=text/javascript><!--

document.onselectstart = function () { return false; }

var nI  = 0;
var kI  = 0;
var run = false;

function setOpacity(obj,o) {
    if (o<0) o=0; else if (o>100) o = 100;
    if (obj.filters)obj.filters.alpha.opacity=o; else obj.style.opacity = o/100;
}
function TPR__(p) {
    P1.style.left  = 50-(2.5*p)+"%";
    P1.style.width = (2.5*p)+"%";
    setOpacity(P1i, .5*p*p);
    if (p == 20) run = false;
}
function TPR_(p) {
    P2.style.width = 50-(2.5*p)+"%";
    setOpacity(P2i, 100-.5*(p*p));
    if (p == 20) {
        P2i.src = IMGSRC[kI].src;
        setOpacity(P2i, 100);
        P2.style.width = "50%";
        for(var i=1; i<=20; i++) setTimeout("TPR__("+i+")", i*32);
    }
}
function TPR() {
    if (!run) {
        run = true;
        P01i.src = IMGSRC[kI].src;
        P1.style.width = 0;
        kI++;
        if (kI>=nI) kI = 0;
        titLe(kI);
```

```
            P02i.src = IMGSRC[kI].src;
            P1i.src  = IMGSRC[kI].src;
            for (var i=1; i<=20; i++) setTimeout("TPR_("+i+")", i*32);
      } else setTimeout("TPR()", 100);
}

function TPL__(p) {
      P2.style.width = (2.5*p)+"%";
      setOpacity(P2i, .5*p*p);
      if (p == 20) run = false;
}
function TPL_(p) {
      P1.style.left  = (2.5*p)+"%";
      P1.style.width = 40+(10-2.5*p)+"%";
      setOpacity(P1i, 100-.5*(p*p));
      if (p == 20) {
            P1i.src = IMGSRC[kI].src;
            setOpacity(P1i, 100);
            P1.style.left  = 0;
            P1.style.width = "50%";
            for(var i=1; i<=20; i++) setTimeout("TPL__("+i+")", i*32);
      }
}
function TPL() {
      if (!run) {
            run = true;
            P02i.src = IMGSRC[kI].src;
            P2.style.width = 0;
            kI--;
            if (kI < 0) kI = nI-1;
            titLe(kI);
            P01i.src = IMGSRC[kI].src;
            P2i.src  = IMGSRC[kI].src;
            for(var i=1; i<=20; i++) setTimeout("TPL_("+i+")", i*32);
      } else setTimeout("TPL()", 100);
}
function titLe(p) {
      document.getElementById("TXTBOX").innerHTML = IMGSRC[p].alt;
}
onload = function() {
      IMGSRC  = document.getElementById("imgsrc").getElementsByTagName("img");
      DB      = document.getElementById("DHTMLBOOK");
      P01     = DB.getElementsByTagName("span")[0];
      P01i    = P01.getElementsByTagName("img")[0];
      P02     = DB.getElementsByTagName("span")[1];
      P02i    = P02.getElementsByTagName("img")[0];
      P1      = DB.getElementsByTagName("span")[2];
      P1i     = P1.getElementsByTagName("img")[0];
      P2      = DB.getElementsByTagName("span")[3];
      P2i     = P2.getElementsByTagName("img")[0];
      nI      = IMGSRC.length;
      P1i.src = IMGSRC[kI].src;
      P2i.src = IMGSRC[kI].src;
```

```
        titLe(kl);
        DB.style.visibility = "visible";
    }
    //-->
    </SCRIPT>
    </head>

    <body>



    <!---头部开始-->
    <script src="/cn/Script/JsHelper.js" type="text/javascript" id="syspath" syspath='/'></script>
    <div class="head">
       <a class="logo" href='#'></a>
       <div class="right">
          <span><a href="#" onclick="javascript:addfavor('http://www.zgska.cn/','中国式抗癌');">
    加入收藏</a> | <a href="#" onclick="this.style.behavior='url
    (#default#homepage)';this.setHomePage('http://www.zgska.cn/');">设为首页
    </a></span><font class="time"></font>  欢迎您来到中国式抗癌网!

       </div>
       <div class="search">
       <div class="tel">关爱热线：021-64370629</div>
       <div id="notLogined" style="float: left; padding:0px 0px 0px 5px;"><input type="text"
    id="txtUname" name="username" class="inputstyle" value="用户名" onblur="if
    (this.value=='')this.value='用户名';" onfocus="this.value='';" /> <input type="password"
    name="password" id="txtPwd" onblur="if(this.value=='')this.value='000';"
    onfocus="this.value='';" value="000" class="inputstyle" /> <input type="button" class="login"
    value="登录" id="btnLogin" /><input type="button" class="reg" value="注册"
    id="btnReg" /></div>

       <d...
```

响应中的验证：

- `<!-- <div class="hover"><a href='/research/list_61.aspx'>最新前沿</a></div>-->`

推理：

AppScan 发现了包含看似为敏感信息的 HTML 注释。

CWE 标识：

615

有漏洞的 URL：http://www.zgska.cn/case/index_43.aspx

此 URL 共有 1 个安全性问题

[1 / 1] 链接注入（便于跨站请求伪造）

严重性： 中

测试类型： 应用程序

有漏洞的 URL： http://www.zgska.cn/case/index_43.aspx (参数 = lcid)

CVE 标识： 不适用

CWE 标识： 74

修复任务： 过滤掉用户输入中的危险字符

1 的变体 1 [ID=10006]

以下更改已应用到原始请求：

• 已将参数“lcid”的值设置为“http://demo.testfire.net”

请求/响应：

```
GET /case/index_43.aspx?lcid=http://demo.testfire.net HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn
Referer: http://www.zgska.cn/


HTTP/1.1 200 OK
Content-Length: 16822
Connection: close
Date: Mon, 28 Apr 2014 10:10:20 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="/cn/css/css_whir.css" rel="stylesheet" type="text/css" />
<meta name="Author" content="万户网络设计制作" />
<title>中国式抗癌，防治癌症转移与复发，防治肿瘤转移与复发、松友饮，汤钊猷</title>
<meta name="keywords" content="中国式抗癌、防治癌症转移与复发，汤钊猷、肿瘤转移与复发、癌症康
复、松友饮、松友饮颗粒、、汤钊猷，松友饮" />
<meta name="Description" content="传播中国式抗癌的科学理念，防治肿瘤转移与复发，防治癌症转移与
复发，松友饮为癌症患者提供在线交流平台，提供防治癌症的一些方法88" />

<script type="text/javascript" src="/cn/Script/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="/cn/Script/MSClass.js"></script>

<script type="text/javascript">
var syspath='/';
</script>



    <script src="/cn/Script/JsHelper.js" type="text/javascript" id="syspath"
syspath='/'></script>
    <script type="text/javascript">
        var menu = 7;
        var columnId ='http://demo.testfire.net';
```

```
    </script>
</head>
<body>


<!---头部开始-->
<script src="/cn/Script/JsHelper.js" type="text/javascript" id="syspath"
syspath='/'></script>
<div class="head">
    <a class="logo" href='#'></a>
    <div class="right">
       <span><a href="#" onclick="javascript:addfavor('http://www.zgska.cn/',' 中国式
抗癌');">加入收藏</a> | <a href="#" onclick="this.style.behavior='url
(#default#homepage)';this.setHomePage('http://www.zgska.cn/');"> 设为首页
</a></span><font class="time"></font>  欢迎您来到中国式抗癌网!

    </div>
    <div class="search">
    <div class="tel">关爱热线：021-64370629</div>
    <div id="notLogined" style="float: left; padding:0px 0px 0px 5px;"><input
type="text" id="txtUname" name="username" class="inputstyle" value=" 用户名"
onblur="if(this.value=='')this.value=' 用户名';" onfocus="this.value='';" /> <input
type="password" name="password" id="txtPwd" onblur="if(this.value=='')
this.value='000';" onfocus="this.value='';" value="000" class="inputstyle" /> <input
type="button" class="login" value=" 登录" id="btnLogin" /><input type="button"
class="reg" value="注册" id="btnReg" /></div>

    <div class="searchbg"><input type="text" id="txtSearch" class="searchbg_input"
value="输入您所查找内容" onblur="if(this.value=='')this.value=' 输入您所查找内容';"
onfocus="this.value='';" /><input type="button" class="searchbg_btn"
id="btnSearch" /></div>

    </div>
</div>

<div class="mainnavwrap">
    <div class="mainnav">
        <ul>
            <li><a href='/index.aspx' id="mainnav1"><em> 首页</em></a></li>
            <li><a href='/inter/index_13.aspx' id="mainnav2"><em> 走近汤钊猷院士
</em></a></li>
            <li><a href='/speak/index_21.aspx' id="mainnav3"><em> 国际交流
</em></a></li>
            <li><a href='/research/list_28.aspx' id="mainnav4"><em> 肿瘤防治研究
</em></a></li>
            <li><a href='/question/index_36.aspx' id="mainnav5"><em> 专家解疑
</em></a></li>
            <li><a href='/knowledge/list_70.aspx' id="mainnav6"><em> 肿瘤知识库
</em></a></li>

            <li><a href="/case/index_43.aspx?lcid=19" id="mainnav7"><em> 临床案例
</em></a></li>

            <li><a href='/house/list_47.aspx' id="mainnav8"><em> 患友家园
</em></a></li>
            <li><a href='/Information/list_74.aspx' id="mainnav9"><em> 最新活动
</em></a></li>
        </ul>
    </div>
</div>
<!---头部结束-->
<script type="text/javascript">
    jQuery("#btnSearch").click(function () {

          var searchinput = jQuery("#txtSearch").val();
           if (searchinput == "" || searchinput == " 输入您所查找内容") {
               alert("请输入关键字!");
               return false;
           }
           if (searchinput.length > 50) {
               alert("输入的关键字字数不要过多!");
               return false;
```

```
            }
            window.location = "/search/search.aspx?key=" + escape(searchinput);
            return true;
        });
    function addfavor(url, title) {
        if (confirm("网站名称：" + title + "\n网址：" + url + "\n确定添加收藏?")) {
            var ua = navigator.userAgent.toLowerCase();
            if (ua.indexOf("msie 8") > -1) {
                external.AddToFavoritesBar(url, title, '中国式抗癌'); //IE8
            } else {
                try {
                    window.external.addFavorite(url, title);
                } catch (e) {
                    try {
                        window.sidebar.addP...
```

响应中的验证：

- var columnId ='**http://demo.testfire.net**';
- var columnId ='http://**demo.testfire.net**';

推理：

测试响应包含指向文件“WF_XSRF.html”的链接，证明跨站点请求伪造尝试已成功。

CWE 标识：

74

有漏洞的 URL：http://www.zgska.cn/config/

此 URL 共有 1 个安全性问题

[1 / 1] 检测到隐藏目录

严重性：	低
测试类型：	基础结构
有漏洞的 URL：	http://www.zgska.cn/config/
CVE 标识：	不适用
CWE 标识：	不适用
修复任务：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

1 的变体 1 [ID=3340]

以下更改已应用到原始请求：

- 已将路径设置为“/config/”

请求/响应：

```
GET /config/ HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
```

```
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:07:06 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

响应中的验证：

- HTTP/1.1 **403** Forbidden

推理：

测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应泄露了存在此目录，即使不允许对其进行访问。

CWE 标识：

不适用

有漏洞的 URL：http://www.zgska.cn/information/

此 URL 共有 1 个安全性问题

[1 / 1] 检测到隐藏目录

严重性：	低
测试类型：	基础结构
有漏洞的 URL：	http://www.zgska.cn/information/
CVE 标识：	不适用
CWE 标识：	不适用
修复任务：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

1 的变体 1 [ID=3448]

以下更改已应用到原始请求：

- 已将路径设置为“/information/”

请求/响应：

```
GET /information/ HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:07:08 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing
```

```
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

响应中的验证：

- HTTP/1.1 **403** Forbidden

推理：

测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应泄露了存在此目录，即使不允许对其进行访问。

CWE 标识：

不适用

有漏洞的 URL：http://www.zgska.cn/member/

此 URL 共有 1 个安全性问题

[1 / 1] 检测到隐藏目录

严重性：	低
测试类型：	基础结构
有漏洞的 URL：	http://www.zgska.cn/member/
CVE 标识：	不适用
CWE 标识：	不适用
修复任务：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

1 的变体 1 [ID=4034]

以下更改已应用到原始请求：

- 已将路径设置为“/member/”

请求/响应：

```
GET /member/ HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:07:19 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

响应中的验证：

- HTTP/1.1 **403** Forbidden

推理：
测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应泄露了存在此目录，即使不允许对其进行访问。

CWE 标识：
不适用

有漏洞的 URL：http://www.zgska.cn/question/index_36.aspx

此 URL 共有 1 个安全性问题

[1 / 1] HTML 注释敏感信息泄露

严重性：	低
测试类型：	应用程序
有漏洞的 URL：	http://www.zgska.cn/question/index_36.aspx
CVE 标识：	不适用
CWE 标识：	615
修复任务：	除去 HTML 注释中的敏感信息

6 的变体 1 [ID=10647]

用户可能需要注意以下事项：

```
GET /question/index_36.aspx HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn
Referer: http://www.zgska.cn/


HTTP/1.1 200 OK
Content-Length: 17447
Connection: close
Date: Mon, 28 Apr 2014 09:57:28 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="/cn/css/css_whir.css" rel="stylesheet" type="text/css" />
<meta name="Author" content="万户网络设计制作" />
<title>中国式抗癌，防治癌症转移与复发，防治肿瘤转移与复发、松友饮，汤钊猷
</title>
<meta name="keywords" content="中国式抗癌、防治癌症转移与复发，汤钊猷、肿瘤
转移与复发、癌症康复、松友饮、松友饮颗粒、、汤钊猷，松友饮" />
<meta name="Description" content="传播中国式抗癌的科学理念，防治肿瘤转移与复
发，防治癌症转移与复发，松友饮为癌症患者提供在线交流平台，提供防治癌症的
一些方法88" />

<script type="text/javascript" src="/cn/Script/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="/cn/Script/MSClass.js"></script>

<script type="text/javascript">
var syspath='/';
</script>



<script type="text/javascript">
      var menu=5;
      var columnId='36';
</script>


</head>

<body>


<!---头部开始-->
<script src="/cn/Script/JsHelper.js" type="text/javascript" id="syspath" syspath='/'></script>
<div class="head">
   <a class="logo" href='#'></a>
   <div class="right">
      <span><a href="#" onclick="javascript:addfavor('http://www.zgska.cn/','中国式抗癌');">
加入收藏</a> | <a href="#" onclick="this.style.behavior='url
(#default#homepage)';this.setHomePage('http://www.zgska.cn/');">设为首页
</a></span><font class="time"></font>  欢迎您来到中国式抗癌网!

   </div>
   <div class="search">
   <div class="tel">关爱热线：021-64370629</div>
   <div id="notLogined" style="float: left; padding:0px 0px 0px 5px;"><input type="text"
id="txtUname" name="username" class="inputstyle" value="用户名" onblur="if
(this.value=='')this.value='用户名';" onfocus="this.value='';" /> <input type="password"
name="password" id="txtPwd" onblur="if(this.value=='')this.value='000';"
```

```
onfocus="this.value='';" value="000" class="inputstyle" /> <input type="button" class="login"
value="登录" id="btnLogin" /><input type="button" class="reg" value="注册"
id="btnReg" /></div>

    <div class="searchbg"><input type="text" id="txtSearch" class="searchbg_input"
value="输入您所查找内容" onblur="if(this.value=='')this.value='输入您所查找内容';"
onfocus="this.value='';" /><input type="button" class="searchbg_btn"
id="btnSearch" /></div>

    </div>
</div>

<div class="mainnavwrap">
    <div class="mainnav">
        <ul>
            <li><a href='/index.aspx' id="mainnav1"><em>首页</em></a></li>
            <li><a href='/inter/index_13.aspx' id="mainnav2"><em>走近汤钊猷院士
</em></a></li>
            <li><a href='/speak/index_21.aspx' id="mainnav3"><em>国际交流</em></a></li>
            <li><a href='/research/list_28.aspx' id="mainnav4"><em>肿瘤防治研究
</em></a></li>
            <li><a href='/question/index_36.aspx' id="mainnav5"><em>专家解疑
</em></a></li>
            <li><a href='/knowledge/list_70.aspx' id="mainnav6"><em>肿瘤知识库
</em></a></li>

            <li><a href="/case/index_43.aspx?lcid=19" id="mainnav7"><em>临床案例
</em></a></li>

            <li><a href='/house/list_47.aspx' id="mainnav8"><em>患友家园</em></a></li>
            <li><a href='/Information/list_74.aspx' id="mainnav9"><em>最新活动
</em></a></li>
        </ul>
    </div>
</div>
<!---头部结束-->
<script type="text/javascript">
      jQuery("#btnSearch").click(function () {

                var searchinput = jQuery("#txtSearch").val();
            if (searchinput == "" || searchinput == "输入您所查找内容") {
                alert("请输入关键字!");
                return false;
            }
            if (searchinput.length > 50) {
                alert("输入的关键字字数不要过多!");
                return false;
            }
                window.location = "/search/search.aspx?key=" + escape(searchinput);
                return true;
      });
    function addfavor(url, title) {
        if (confirm("网站名称：" + title + "\n网址：" + url + "\n确定添加收藏?")) {
```

```
var ua = navigator.userAgent.toLowerCase();
if (ua.indexOf("msie 8") > -1) {
    external.AddToFavoritesBar(url, title, '中国式抗癌'); //IE8
} else {
    try {
        window.external.addFavorite(url, title);
    } catch (e) {
        try {
            window.sidebar.addPanel(title, url, ""); //firefox
        } catch (e) {
            alert("加入收藏失败，请使用Ctrl+D进行添加");
        }
    }
}...
```

响应中的验证：

• <!-- 查看详细>> -->

推理：

AppScan 发现了包含看似为敏感信息的 HTML 注释。

CWE 标识：

615

有漏洞的 URL：http://www.zgska.cn/research/

此 URL 共有 1 个安全性问题

[1 / 1] 检测到隐藏目录

严重性：	低
测试类型：	基础结构
有漏洞的 URL：	http://www.zgska.cn/research/
CVE 标识：	不适用
CWE 标识：	不适用
修复任务：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

1 的变体 1 [ID=4135]

以下更改已应用到原始请求：

• 已将路径设置为“/research/”

请求/响应：

```
GET /research/ HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn
```

```
HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:07:21 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

响应中的验证：

- HTTP/1.1 **403** Forbidden

推理：

测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应泄露了存在此目录，即使不允许对其进行访问。

CWE 标识：

不适用

有漏洞的 URL：http://www.zgska.cn/research/list_81.aspx

此 URL 共有 1 个安全性问题

[1 / 1] 链接注入（便于跨站请求伪造）

严重性：	中
测试类型：	应用程序
有漏洞的 URL：	http://www.zgska.cn/research/list_81.aspx (参数 = pid)
CVE 标识：	不适用
CWE 标识：	74
修复任务：	过滤掉用户输入中的危险字符

1 的变体 1 [ID=21108]

以下更改已应用到原始请求：

- 已将参数“pid”的值设置为“http://demo.testfire.net”

请求/响应：

```
GET /research/list_81.aspx?pid=http://demo.testfire.net HTTP/1.0
Cookie: ASP.NET_SessionId=po442zeoqarm4xynttwkx245
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn
Referer: http://www.zgska.cn/research/list_31.aspx


HTTP/1.1 200 OK
Content-Length: 12754
Connection: close
Date: Mon, 28 Apr 2014 10:23:15 GMT
Server: Microsoft-IIS/6.0
```

```
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="/cn/css/css_whir.css" rel="stylesheet" type="text/css" />
<meta name="Author" content="万户网络设计制作" />
<title>中国式抗癌，防治癌症转移与复发，防治肿瘤转移与复发、松友饮，汤钊猷</title>
<meta name="keywords" content="中国式抗癌、防治癌症转移与复发，汤钊猷、肿瘤转移与复发、癌症康复、松友饮、松友饮颗粒、、汤钊猷，松友饮" />
<meta name="Description" content="传播中国式抗癌的科学理念，防治肿瘤转移与复发，防治癌症转移与复发，松友饮为癌症患者提供在线交流平台，提供防治癌症的一些方法88" />

<script type="text/javascript" src="/cn/Script/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="/cn/Script/MSClass.js"></script>

<script type="text/javascript">
var syspath='/';
</script>


<script type="text/javascript">
    var menu=4;
    var columnId='http://demo.testfire.net';
</script>


</head>

<body>


<!---头部开始-->
<script src="/cn/Script/JsHelper.js" type="text/javascript" id="syspath"
syspath='/'></script>
<div class="head">
    <a class="logo" href='#'></a>
    <div class="right">
        <span><a href="#" onclick="javascript:addfavor('http://www.zgska.cn/',' 中国式
抗癌');">加入收藏</a> | <a href="#" onclick="this.style.behavior='url
(#default#homepage)';this.setHomePage('http://www.zgska.cn/');"> 设为首页
</a></span><font class="time"></font>  欢迎您来到中国式抗癌网!

    </div>
    <div class="search">
    <div class="tel">关爱热线：021-64370629</div>
    <div id="notLogined" style="float: left; padding:0px 0px 0px 5px;"><input
type="text" id="txtUname" name="username" class="inputstyle" value="用户名"
onblur="if(this.value=='')this.value='用户名';" onfocus="this.value='';" /> <input
type="password" name="password" id="txtPwd" onblur="if(this.value=='')
this.value='000';" onfocus="this.value='';" value="000" class="inputstyle" /> <input
type="button" class="login" value="登录" id="btnLogin" /><input type="button"
class="reg" value="注册" id="btnReg" /></div>

    <div class="searchbg"><input type="text" id="txtSearch" class="searchbg_input"
value="输入您所查找内容" onblur="if(this.value=='')this.value='输入您所查找内容';"
onfocus="this.value='';" /><input type="button" class="searchbg_btn"
id="btnSearch" /></div>

    </div>
</div>

<div class="mainnavwrap">
    <div class="mainnav">
```

```
        <ul>
            <li><a href='/index.aspx' id="mainnav1"><em> 首页</em></a></li>
            <li><a href='/inter/index_13.aspx' id="mainnav2"><em> 走近汤钊猷院士
</em></a></li>
            <li><a href='/speak/index_21.aspx' id="mainnav3"><em> 国际交流
</em></a></li>
            <li><a href='/research/list_28.aspx' id="mainnav4"><em> 肿瘤防治研究
</em></a></li>
            <li><a href='/question/index_36.aspx' id="mainnav5"><em> 专家解疑
</em></a></li>
            <li><a href='/knowledge/list_70.aspx' id="mainnav6"><em> 肿瘤知识库
</em></a></li>

            <li><a href="/case/index_43.aspx?lcid=19" id="mainnav7"><em> 临床案例
</em></a></li>

            <li><a href='/house/list_47.aspx' id="mainnav8"><em> 患友家园
</em></a></li>
            <li><a href='/Information/list_74.aspx' id="mainnav9"><em> 最新活动
</em></a></li>
        </ul>
    </div>
</div>
<!---头部结束-->
<script type="text/javascript">
    jQuery("#btnSearch").click(function () {

            var searchinput = jQuery("#txtSearch").val();
             if (searchinput == "" || searchinput == " 输入您所查找内容") {
                 alert("请输入关键字!");
                 return false;
             }
             if (searchinput.length > 50) {
                 alert("输入的关键字字数不要过多!");
                 return false;
             }
            window.location = "/search/search.aspx?key=" + escape(searchinput);
            return true;
        });
    function addfavor(url, title) {
        if (confirm("网站名称：" + title + "\n网址：" + url + "\n确定添加收藏?")) {
            var ua = navigator.userAgent.toLowerCase();
            if (ua.indexOf("msie 8") > -1) {
                external.AddToFavoritesBar(url, title, ' 中国式抗癌'); //IE8
            } else {
                try {
                    window.external.addFavorite(url, title);
                } catch (e) {
                    try {
                        window.sidebar.addPanel(title, url, ""); //firefox
                    } catch (e) {
                        alert(" 加入收藏失败，请使用C...
```

响应中的验证：

- var columnId='**http://demo.testfire.net**';
- var columnId='http://**demo.testfire.net**';

推理：

测试响应包含指向文件“WF_XSRF.html”的链接，证明跨站点请求伪造尝试已成功。

CWE 标识：

74

有漏洞的 URL：http://www.zgska.cn/search/

此 URL 共有 1 个安全性问题

[1 / 1] 检测到隐藏目录

严重性： 低

测试类型： 基础结构

有漏洞的 URL： http://www.zgska.cn/search/

CVE 标识： 不适用

CWE 标识： 不适用

修复任务： 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

1 的变体 1 [ID=3564]

以下更改已应用到原始请求：

• 已将路径设置为“/search/”

请求/响应：

```
GET /search/ HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:07:10 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

响应中的验证：

• HTTP/1.1 **403** Forbidden

推理：

测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应泄露了存在此目录，即使不允许对其进行访问。

CWE 标识：

不适用

有漏洞的 URL：http://www.zgska.cn/speak/index_21.aspx

此 URL 共有 1 个安全性问题

[1 / 1] HTML 注释敏感信息泄露

严重性：	低
测试类型：	应用程序
有漏洞的 URL：	http://www.zgska.cn/speak/index_21.aspx
CVE 标识：	不适用
CWE 标识：	615
修复任务：	除去 HTML 注释中的敏感信息

1 的变体 1 [ID=12514]

用户可能需要注意以下事项：

```
GET /speak/index_21.aspx HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn
Referer: http://www.zgska.cn/


HTTP/1.1 200 OK
Content-Length: 18147
Connection: close
Date: Mon, 28 Apr 2014 09:57:52 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="/cn/css/css_whir.css" rel="stylesheet" type="text/css" />
<meta name="Author" content="万户网络设计制作" />
<title>中国式抗癌，防治癌症转移与复发，防治肿瘤转移与复发、松友饮，汤钊猷
</title>
<meta name="keywords" content="中国式抗癌、防治癌症转移与复发，汤钊猷、肿瘤
转移与复发、癌症康复、松友饮、松友饮颗粒、、汤钊猷，松友饮" />
<meta name="Description" content="传播中国式抗癌的科学理念，防治肿瘤转移与复
发，防治癌症转移与复发，松友饮为癌症患者提供在线交流平台，提供防治癌症的
一些方法88" />

<script type="text/javascript" src="/cn/Script/jquery-1.4.2.min.js"></script>
```

```
<script type="text/javascript" src="/cn/Script/MSClass.js"></script>

<script type="text/javascript">
var syspath='/';
</script>



<script type="text/javascript">
      var menu=3;
      var columnId='21';
</script>


</head>

<body>


<!---头部开始-->
<script src="/cn/Script/JsHelper.js" type="text/javascript" id="syspath" syspath='/'></script>
<div class="head">
    <a class="logo" href='#'></a>
    <div class="right">
       <span><a href="#" onclick="javascript:addfavor('http://www.zgska.cn/','中国式抗癌');">
加入收藏</a> | <a href="#" onclick="this.style.behavior='url
(#default#homepage)';this.setHomePage('http://www.zgska.cn/');">设为首页
</a></span><font class="time"></font>  欢迎您来到中国式抗癌网!

    </div>
    <div class="search">
    <div class="tel">关爱热线：021-64370629</div>
    <div id="notLogined" style="float: left; padding:0px 0px 0px 5px;"><input type="text"
id="txtUname" name="username" class="inputstyle" value="用户名" onblur="if
(this.value=='')this.value='用户名';" onfocus="this.value='';" /> <input type="password"
name="password" id="txtPwd" onblur="if(this.value=='')this.value='000';"
onfocus="this.value='';" value="000" class="inputstyle" /> <input type="button" class="login"
value="登录" id="btnLogin" /><input type="button" class="reg" value="注册"
id="btnReg" /></div>

    <div class="searchbg"><input type="text" id="txtSearch" class="searchbg_input"
value="输入您所查找内容" onblur="if(this.value=='')this.value='输入您所查找内容';"
onfocus="this.value='';" /><input type="button" class="searchbg_btn"
id="btnSearch" /></div>

    </div>
</div>

<div class="mainnavwrap">
    <div class="mainnav">
        <ul>
            <li><a href='/index.aspx' id="mainnav1"><em>首页</em></a></li>
            <li><a href='/inter/index_13.aspx' id="mainnav2"><em>走近汤钊猷院士
```

```
</em></a></li>
        <li><a href='/speak/index_21.aspx' id="mainnav3"><em>国际交流</em></a></li>
        <li><a href='/research/list_28.aspx' id="mainnav4"><em>肿瘤防治研究
</em></a></li>
        <li><a href='/question/index_36.aspx' id="mainnav5"><em>专家解疑
</em></a></li>
        <li><a href='/knowledge/list_70.aspx' id="mainnav6"><em>肿瘤知识库
</em></a></li>

        <li><a href="/case/index_43.aspx?lcid=19" id="mainnav7"><em>临床案例
</em></a></li>

        <li><a href='/house/list_47.aspx' id="mainnav8"><em>患友家园</em></a></li>
        <li><a href='/Information/list_74.aspx' id="mainnav9"><em>最新活动
</em></a></li>
      </ul>
   </div>
</div>
<!---头部结束-->
<script type="text/javascript">
     jQuery("#btnSearch").click(function () {

            var searchinput = jQuery("#txtSearch").val();
        if (searchinput == "" || searchinput == "输入您所查找内容") {
            alert("请输入关键字!");
            return false;
        }
        if (searchinput.length > 50) {
            alert("输入的关键字字数不要过多!");
            return false;
        }
            window.location = "/search/search.aspx?key=" + escape(searchinput);
            return true;
     });
   function addfavor(url, title) {
     if (confirm("网站名称：" + title + "\n网址：" + url + "\n确定添加收藏?")) {
        var ua = navigator.userAgent.toLowerCase();
        if (ua.indexOf("msie 8") > -1) {
            external.AddToFavoritesBar(url, title, '中国式抗癌'); //IE8
        } else {
            try {
                window.external.addFavorite(url, title);
            } catch (e) {
                try {
                    window.sidebar.addPanel(title, url, ""); //firefox
                } catch (e) {
                    alert("加入收藏失败，请使用Ctrl+D进行添加");
                }
            }
        }
...
```

响应中的验证：

-
-

推理：

AppScan 发现了包含看似为敏感信息的 HTML 注释。

CWE 标识：

615

有漏洞的 URL：http://www.zgska.cn/cn/Script/MSClass.js

此 URL 共有 1 个安全性问题

[1 / 1] 发现电子邮件地址模式

严重性：	参考信息
测试类型：	应用程序
有漏洞的 URL：	http://www.zgska.cn/cn/Script/MSClass.js
CVE 标识：	不适用
CWE 标识：	359
修复任务：	除去 Web 站点中的电子邮件地址

1 的变体 1 [ID=10652]

请求/响应：

```
GET /cn/Script/MSClass.js HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 200 OK
Content-Length: 16533
Cache-Control: max-age=432000
Content-Type: application/x-javascript
Last-Modified: Thu, 17 Apr 2014 07:48:50 GMT
Accept-Ranges: bytes
ETag: "42bcb178115acf1:934e1"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:11:10 GMT
Connection: close

<!--
/*MSClass (Class Of Marquee Scroll - General Uninterrupted Scrolling(JS)) Ver 2.9*\

@ Code By : Yongxiang Cui(333) E-Mail:zhadan007@21cn.com http://www.popub.net
@ Update  : 2012-01-08 (Ver 2.9.120108)
@ Examples: http://www.popub.net/script/MSClass.html

\***============== Please keep the above copyright information ==============***/
```

```
eval(function(MSClass){var d=MSClass,p=d[0],k=d[1],c=k.length,a=62,e=function(c)
{return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString
(36))};if(!''.replace(/^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e)
{return d[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}(['17 1V(){1c c=1W,b=1K,a;13(!(c 71
b.47)){18(1v b[0]=="2F"&&b[0].1j&&b.1j<5)||(1v b[0]!="2F"&&b.1j<5)?2z("70 6Z 6Y 6X
6W!"):6v 1V(b[0],b[1],b[2],b[3],b[4],b[5],b[6],b[7],b[8],b[9],b[1O],b[11],b[12])}
c.$=17(d){18 1R.6U(d)};c.t=(c.F=["3G 2.9.6T","6S 6R 1V 6Q","6P 6O 6N
(6M)","6L://6K.6J.6I/6H/3G.6G","6F 6E(4K) 6D@6C.6B"]).6A("\\n");13(!((c.c=1v(c.a=b
[0]["3G"]||b[0]||b[0][0])=="2F"?c.$(c.a[0])||c.$(c.a.4J):c.$(c.a))&&c.6z.1Y().2X
(6y>>4K,6x>>>4)==c.F[1].2X(6w>>>6v,14>>6u))){18 2z("4f ["+(c.a.4J||c.a[0]||c.a)+"]
6t 6s!")||(c.c=-1)}13(c.c.3F=="3q"||c.c.3F=="4p"||c.c.3F=="6r"){c.a=
[0,c.c.4e];c.c=c.c.3B}c.1a=b[1]||b[0]["1a"]||0;c.1g=b[2]||b[0]["1g"]||1;c.1E=c.W=
(a=b[3]||b[0]["1E"]||0)==0?1s(c.c.16.1P):a;c.1D=c.H=(a=b[4]||b[0]["1D"]||0)==0?1s
(c.c.16.1S):a;c.1X=(a=b[5]||b[0]["1X"]||0)<2O?(a*1O||2O):a;c.2g=(a=b[6]||b[0]["2g"]
||0)<=4I?a*2K:a;c.2k=(a=b[7]||b[0]["2k"]||0)<=4I?(a*2K||38):a;c.1e=b[8]||b[0]["1e"]
||0;c.2r=b[9]||b[0]["2r"]||0;c.2q=b[1O]||b[0]["2q"];c.3i=c.$(b[11]||b[0]["6q"])
||0;c.3h=c.$(b[12]||b[0]["6p"])||0;c.c.16.3m=c.c.16.4a=c.c.16.49="2C";13(b.1j>=5||b
[0]["6o"]){c.3e()}}1V.3P.3e=17(){13(1W.c==-1||1W.i>=0){13(1W.i==2){1W.2v()}18 1x}1c
k=1W,M=k.c,b,w,Z,1b,1u,1H,z,n,T=0,g="6n",1f=1V,R=0,s=[],h=0,O=0,d=0,r={6m:-2,6l:-
1,6k:-1,28:0,6j:0,6i:1,6h:1,2Q:2,6g:3,6f:4,6e:5},S=
[],1q=0,V=0,v=0,1O=0,I=0,B=0,a=0,F=0,X=0,l=0,J=0,2j=0,D=0,x=0,u=0,W=0,1A=0,c=
[],1G=1C,1h=1C,t=0,o=0,Y=k.1e,P=k.2g,C=0,U=0,A=[],2l=0,N=0,Q=0;k.I=k.j=1+(k.i=k.2i=-
1);13(!1f.H){1p.$?0:1p.$=k.$;1f.m=(1R.3A)?1:0;1f.4j=6d.6c.6b("6a")>0;1f.H=17(m,j,i)
{i?0:i=0;18 1f.m?(m.2e[j]!="4H"&&m.2e[j]!="4G"&&m.2e[j]!="4F"&&m.2e[j]!="69"&&m.2e
[j]!="68"&&m.2e[j]!="3y")?m.2e[j]:i:(1p.2u(m,1C)[j]!="4H"&&1p.2u(m,1C)[j]!
="4G"&&1p.2u(m,1C)[j]!="4F"&&1p.2u(m,1C)[j]!="4g"&&1p.2u(m,1C)[j]!="3y")?1p.2u(m,1C)
[j]:i};(1f.K=17(m,j,i){1f.m?m.67("4E"+j,i):m.66(j,i,1x)})(28.1R,"65",17(i){13
((i||1p.1J).64==63){2z(k.t)}});1f.L=17(m,j,i){1f.m?m.62("4E"+j,i):m.61
(j,i,1x)};1f.1Z={4q:17(i,m,j){18 m},6O:17(i,m,j){18 m*(i/=j)*i},5Z:17(i,m,j){18-m*
(i/=j)*(i-2)},5Y:17(i,m,j){18(i/=j/2)<1?m/2*i*i:-m/2*((--i)*(i-2)-1)},5X:17(i,m,j)
{18 m*(i/=j)*i*i},5W:17(i,m,j){18 m*((i=i/j-1)*i*i+1)},5V:17(i,m,j){18(i/=j/2)<1?
m/2*i*i*i:m/2*((i-=2)*i*i+2)},5U:17(i,m,j){18 m*(i/=j)*i*i*i},5T:17(i,m,j){18-m*
((i=i/j-1)*i*i*i-1)},5S:17(i,m,j){18(i/=j/2)<1?m/2*i*i*i*i:-m/2*((i-=2)*i*i*i-
2)},5R:17(i,m,j){18 m*(i/=j)*i*i*i*i},5Q:17(i,m,j){18 m*((i=i/j-1)*i*i*i*i+1)},5P:17
(i,m,j){18(i/=j/2)<1?m/2*i*i*i*i*i:m/2*((i-=2)*i*i*i*i+2)},5O:17(i,m,j){18-m*1d.4D
(i/j*(1d.1I/2))+m},5N:17(i,m,j){18 m*1d.2H(i/j*(1d.1I/2))},5M:17(i,m,j){18-m/2*
(1d.4D(1d.1I*i/j)-1)},5L:17(i,m,j){18 i==0?0:m*1d.1U(2,1O*(i/j-1))},5K:17(i,m,j){18
i==j?m:m*(-1d.1U(2,-1O*i/j)+1)},5J:17(i,m,j){18 i==0?0:i==j?m:(i/=j/2)<1?m/2*1d.1U
(2,1O*(i-1)):m/2*(-1d.1U(2,-1O*--i)+2)},5I:17(i,m,j){18-m*(1d.3O(1-(i/=j)*i)-
1)},5H:17(i,m,j){18 m*1d.3O(1-(i=i/j-1)*i)},5G:17(i,m,j){18(i/=j/2)<1?-m/2*(1d.3O(1-
i*i)-1):m/2*(1d.3O(1-(i-=2)*i)+1)},2P:17(j,1m,1o){1c m=1.2t,19=0,i=1m;13(j==0){18 0}
13((j/=1o)==1){18 1m}13(!19){19=1o*0.3}13(i<1d.3E(1m)){i=1m;m=19/4}1r{m=19/(2*1d.1I)
*1d.3D(1m/i)}18-(i*1d.1U(2,1O*(j-=1))*1d.2H((j*1o-m)*(2*1d.1I)/19))},43:17(j,1m,1o)
{1c m=1.2t,19=0,i=1m;13(j==0){18 0}13((j/=1o)==1){18 1m}13(!19){19=1o*0.3}13(i<1d.3E
(1m)){i=1m;m=19/4}1r{m=19/(2*1d.1I)*1d.3D(1m/i)}18 i*1d.1U(2,-1O*j)*1d.2H((j*1o-m)*
(2*1d.1I)/19)+1m},5F:17(j,1m,1o){1c m=1.2t,19=0,i=1m;13(j==0){18 0}13((j/=1o/2)==2)
{18 1m}13(!19){19=1o*(0.3*1.5)}13(i<1d.3E(1m)){i=1m;m=19/4}1r{m=19/(2*1d.1I)*1d.3D
(1m/i)}13(j<1){18-0.5*(i*1d.1U(2,1O*(j-=1))*1d.2H((j*1o-m)*(2*1d.1I)/19))}18 i*1d.1U
(2,-1O*(j-=1))*1d.2H((j*1o-m)*(2*1d.1I)/19)*0.5+1m},3k:17(i,19,m){1c j=1.2t;18 19*
(i/=m)*i*((j+1)*i-j)},42:17(i,19,m){1c j=1.2t;18 19*((i=i/m-1)*i*((j+1)*i+j)
+1)},5E:17(i,19,m){1c j=1.2t;18(i/=m/2)<1?1...
```

响应中的验证：

• @ Code By : Yongxiang Cui(333) E-Mail:**zhadan007@21cn.com** http://www.popub.net

推理：

响应包含可能是专用的电子邮件地址。

CWE 标识：

359

有漏洞的 URL：http://www.zgska.cn/cn/Script/prototype.js

此 URL 共有 1 个安全性问题

[1 / 1] 发现电子邮件地址模式

严重性：	参考信息
测试类型：	应用程序
有漏洞的 URL：	http://www.zgska.cn/cn/Script/prototype.js
CVE 标识：	不适用
CWE 标识：	359
修复任务：	除去 Web 站点中的电子邮件地址

1 的变体 1 [ID=17351]

请求/响应：

```
GET /cn/Script/prototype.js HTTP/1.0
Cookie: ASP.NET_SessionId=zncn4a2hc0f3ci55bedkkgyf
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.zgska.cn


HTTP/1.1 200 OK
Content-Length: 47603
Cache-Control: max-age=432000
Content-Type: application/x-javascript
Last-Modified: Thu, 17 Apr 2014 07:48:51 GMT
Accept-Ranges: bytes
ETag: "16a62d79115acf1:934e1"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 28 Apr 2014 10:19:19 GMT
Connection: close

/*  Prototype JavaScript framework, version 1.4.0
 *  (c) 2005 Sam Stephenson <sam@conio.net>
 *
 *  THIS FILE IS AUTOMATICALLY GENERATED. When sending patches, please diff
 *  against the source tree, available from the Prototype darcs repository.
 *
 *  Prototype is freely distributable under the terms of an MIT-style license.
 *
 *  For details, see the Prototype web site: http://prototype.conio.net/
 *
/*--------------------------------------------------------------------------*/

var Prototype = {
  Version: '1.4.0',
  ScriptFragment: '(?:<script.*?>)((\n|\r|.)*?)(?:<\/script>)',

  emptyFunction: function() {},
  K: function(x) {return x}
}

var Class = {
  create: function() {
    return function() {
      this.initialize.apply(this, arguments);
    }
  }
}

var Abstract = new Object();
```

```
Object.extend = function(destination, source) {
  for (property in source) {
    destination[property] = source[property];
  }
  return destination;
}

Object.inspect = function(object) {
  try {
    if (object == undefined) return 'undefined';
    if (object == null) return 'null';
    return object.inspect ? object.inspect() : object.toString();
  } catch (e) {
    if (e instanceof RangeError) return '...';
    throw e;
  }
}

Function.prototype.bind = function() {
  var __method = this, args = $A(arguments), object = args.shift();
  return function() {
    return __method.apply(object, args.concat($A(arguments)));
  }
}

Function.prototype.bindAsEventListener = function(object) {
  var __method = this;
  return function(event) {
    return __method.call(object, event || window.event);
  }
}

Object.extend(Number.prototype, {
  toColorPart: function() {
    var digits = this.toString(16);
    if (this < 16) return '0' + digits;
    return digits;
  },

  succ: function() {
    return this + 1;
  },

  times: function(iterator) {
    $R(0, this, true).each(iterator);
    return this;
  }
});

var Try = {
  these: function() {
    var returnValue;

    for (var i = 0; i < arguments.length; i++) {
      var lambda = arguments[i];
      try {
        returnValue = lambda();
        break;
      } catch (e) {}
    }

    return returnValue;
  }
}

/*--------------------------------------------------------------------------*/

var PeriodicalExecuter = Class.create();
PeriodicalExecuter.prototype = {
  initialize: function(callback, frequency) {
    this.callback = callback;
    this.frequency = frequency;
```

```
    this.currentlyExecuting = false;

    this.registerCallback();
  },

  registerCallback: function() {
    setInterval(this.onTimerEvent.bind(this), this.frequency * 1000);
  },

  onTimerEvent: function() {
    if (!this.currentlyExecuting) {
      try {
        this.currentlyExecuting = true;
        this.callback();
      } finally {
        this.currentlyExecuting = false;
      }
    }
  }
}

/*--------------------------------------------------------------------------*/

function $() {
  var elements = new Array();

  for (var i = 0; i < arguments.length; i++) {
    var element = arguments[i];
    if (typeof element == 'string')
      element = document.getElementById(element);

    if (arguments.length == 1)
      return element;

    elements.push(element);
  }

  return elements;
}
Object.extend(String.prototype, {
  stripTags: function() {
    return this.replace(/<\/?[^>]+>/gi, '');
  },

  stripScripts: function() {
    return this.replace(new RegExp(Prototype.ScriptFragment, 'img'), '');
  },

  extractScripts: function() {
    var matchAll = new RegExp(Prototype.ScriptFragment, 'img');
    var matchOne = new RegExp(Prototype.ScriptFragment, 'im');
    return (this.match(matchAll) || []).map(function(scriptTag) {
      return (scriptTag.match(matchOne) || ['', ''])[1];
    });
  },

  evalScripts: function() {
    return this.extractScripts().map(eval);
  },

  escapeHTML: function() {
    var div = document.createElement('div');
    var text = document.createTextNode(this);
    div.appendChild(text);
    return div.innerHTML;
  },

  unescapeHTML: function() {
    var div = document.createElement('div');
    div.innerHTML = this.stripTags();
    return div.childNodes[0] ? div.childNodes[0].nodeValue : '';
  },
```

```
  toQueryParams: function() {
    var pairs = this.match(/^\??(.*)$/)[1].split('&');
    return pairs.inject({}, function(params, pairString) {
      var pair = pairString.split('=');
      params[pair[0]] = pair[1];
      return params;
    });
  },

  toArray: function() {
    retu...
```

响应中的验证：

```
• /*  Prototype JavaScript framework, version 1.4.0
 *  (c) 2005 Sam Stephenson <sam@conio.net>
 *
 *  THIS FILE IS AUTOMATICALLY GENERATED. When sending patches, please diff
 *  against the sou
```

推理：

响应包含可能是专用的电子邮件地址。

CWE 标识：

359

修复任务

URL	修复任务	已解决的安全性问题
http://www.zgska.cn/ (1)		
	除去 HTML 注释中的敏感信息 (低)	HTML 注释敏感信息泄露
http://www.zgska.cn/case/index_43.aspx (1)		
	过滤掉用户输入中的危险字符 (中) 参数: lcid	链接注入（便于跨站请求伪造）
http://www.zgska.cn/config/ (1)		
	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 (低)	检测到隐藏目录
http://www.zgska.cn/information/ (1)		
	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 (低)	检测到隐藏目录
http://www.zgska.cn/member/ (1)		
	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 (低)	检测到隐藏目录
http://www.zgska.cn/question/index_36.aspx (1)		
	除去 HTML 注释中的敏感信息 (低)	HTML 注释敏感信息泄露
http://www.zgska.cn/research/ (1)		
	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 (低)	检测到隐藏目录
http://www.zgska.cn/research/list_81.aspx (1)		
	过滤掉用户输入中的危险字符 (中) 参数: pid	链接注入（便于跨站请求伪造）
http://www.zgska.cn/search/ (1)		
	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 (低)	检测到隐藏目录

http://www.zgska.cn/speak/index_21.aspx (1)

除去 HTML 注释中的敏感信息 (低)	HTML 注释敏感信息泄露

http://www.zgska.cn/cn/Script/MSClass.js (1)

除去 Web 站点中的电子邮件地址 (低)	发现电子邮件地址模式

http://www.zgska.cn/cn/Script/prototype.js (1)

除去 Web 站点中的电子邮件地址 (低)	发现电子邮件地址模式

咨询和修订建议

链接注入（便于跨站请求伪造）

应用程序

WASC 威胁分类

客户端攻击类型：内容电子欺骗

http://www.webappsec.org/projects/threat/classes/content_spoofing.shtml

CVE 标识

不适用

CWE 标识

74

安全风险

可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

可能原因

未对用户输入正确执行危险字符清理

技术描述

“链接注入”是修改站点内容的行为，其方式为将外部站点的 URL 嵌入其中，或将有易受攻击的站点中的脚本 的 URL 嵌入其中。将 URL 嵌入易受攻击的站点中，攻击者便能够以它为平台来启动对其他站点的攻击，以及攻击这个易受攻击的站点本身。
在这些可能的攻击中，有些需要用户在攻击期间登录站点。攻击者从这一易受攻击的站点本身启动这些攻击，成功的机会比较大，因为用户登录的可能性更大。
“链接注入”漏洞是用户输入清理不充分的结果，清理结果会在稍后的站点响应中返回给用户。攻击者能够将危险字符注入响应中，便能够嵌入 URL 及其他可能的内容修改。
以下是“链接注入”的示例（我们假设“www.vulnerable.com”站点有一个用来问候用户的参数，称为“name”）。
下列请求：HTTP://www.vulnerable.com/greet.asp?name=John Smith
会生成下列响应：

```
<HTML>
<BODY>
    Hello, John Smith.
</BODY>
</HTML>
```

然而，恶意的用户可以发送下列请求：
HTTP://www.vulnerable.com/greet.asp?name=<IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">
这会返回下列响应：

```
<HTML>
<BODY>
```

```
    Hello, <IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">.
 </BODY>
 </HTML>
```

如该示例所示，这有可能导致用户浏览器向几乎是攻击者所期待的任何站点发出自动请求。因此，他可能利用这个“链接注入”漏洞来启动若干类型的攻击：
跨站点伪造请求：攻击者可以让用户的浏览器向用户目前登录的站点发送请求，以及执行用户并不想执行的操作。
这些操作可能包括从站点中注销，或修改用户的概要文件、电子邮件地址，甚至是修改密码，结果造成彻底的帐户接管。
跨站点脚本编制：任何“跨站点脚本编制”攻击都开始自诱惑用户单击精心制作的 URL，以便利用受害者站点中的漏洞。
发送含有恶意链接的电子邮件，或创建一个 Web 站点来包含指向易受攻击的站点的链接，通常可以做到这一点。
当采用“链接注入”漏洞时，有可能在 A 站点中嵌入一个恶意的 URL，当单击这个链接时，便启动对 B 站点的“跨站点脚本编制”攻击。
网络钓鱼：攻击者有可能注入指向类似受攻击站点的恶意站点的链接。
不小心的用户可能单击这个链接，但并不知道自己即将离开原始站点而浏览到恶意站点。之后，攻击者便可以诱惑用户重新登录，然后获取他的登录凭证。

一般修订建议

若干问题的补救方法在于对用户输入进行清理。
通过验证用户输入未包含危险字符，便可能防止恶意的用户导致应用程序执行计划外的任务，例如：启动任意 SQL 查询、嵌入将在客户端执行的 Javascript 代码、运行各种操作系统命令，等等。
建议过滤出所有以下字符：

[1] |（竖线符号）
[2] & （& 符号）
[3];（分号）
[4] $（美元符号）
[5] %（百分比符号）
[6] @（at 符号）
[7] '（单引号）
[8] "（引号）
[9] \'（反斜杠转义单引号）
[10] \"（反斜杠转义引号）
[11] <>（尖括号）
[12] ()（括号）
[13] +（加号）
[14] CR（回车符，ASCII 0x0d）
[15] LF（换行，ASCII 0x0a）
[16] ,（逗号）
[17] \（反斜杠）

以下部分描述各种问题、问题的修订建议以及可能触发这些问题的危险字符：
SQL 注入和 SQL 盲注：
A. 确保用户输入的值和类型（如 Integer、Date 等）有效，且符合应用程序预期。
B. 利用存储过程，将数据访问抽象化，让用户不直接访问表或视图。当使用存储过程时，请利用 ADO 命令对象来实施它们，以强化变量类型。
C. 清理输入以排除上下文更改符号，例如：

[1] '（单引号）
[2] "（引号）
[3] \'（反斜线转义单引号）
[4] \"（反斜杠转义引号）

[5])（结束括号）
[6] ;（分号）
跨站点脚本编制：
A. 清理用户输入，并过滤出 JavaScript 代码。我们建议您过滤下列字符：
[1] <>（尖括号）
[2] "（引号）
[3] '（单引号）
[4] %（百分比符号）
[5] ;（分号）
[6] ()（括号）
[7] &（& 符号）
[8] +（加号）
B. 如果要修订 <%00script> 变体，请参阅 MS 文章 821349
C. 对于 UTF-7 攻击： [-] 可能的话，建议您施行特定字符集编码（使用 'Content-Type' 头或 <meta> 标记）。
HTTP 响应分割：清理用户输入（至少是稍后嵌入在 HTTP 响应中的输入）。
请确保输入未包含恶意的字符，例如：
[1] CR（回车符，ASCII 0x0d）
[2] LF（换行，ASCII 0x0a）远程命令执行：清理输入以排除对执行操作系统命令有意义的符号，例如：
[1] |（竖线符号）
[2] & （& 符号）
[3];（分号）
执行 shell 命令：
A. 绝不将未检查的用户输入传递给 eval()、open()、sysopen()、system() 之类的 Perl 命令。
B. 确保输入未包含恶意的字符，例如：
[1] $（美元符号）
[2] %（百分比符号）
[3] @（at 符号）
XPath 注入：清理输入以排除上下文更改符号，例如：
[1] '（单引号）
[2] "（引号） 等
LDAP 注入：
A. 使用正面验证。字母数字过滤（A..Z,a..z,0..9）适合大部分 LDAP 查询。
B. 应该过滤出或进行转义的特殊 LDAP 字符：
[1] 在字符串开头的空格或“#”字符
[2] 在字符串结尾的空格字符
[3] ,（逗号）
[4] +（加号）
[5] "（引号）
[6] \（反斜杠）
[7] <>（尖括号）
[8] ;（分号）
[9] ()（括号）
MX 注入：
应该过滤出特殊 MX 字符：
[1] CR（回车符，ASCII 0x0d）
[2] LF（换行，ASCII 0x0a）记录伪造：
应该过滤出特殊记录字符：
[1] CR（回车符，ASCII 0x0d）
[2] LF（换行，ASCII 0x0a）
[3] BS（退格，ASCII 0x08）

ORM 注入：
A. 确保用户输入的值和类型（如 Integer、Date 等）有效，且符合应用程序预期。
B. 利用存储过程，将数据访问抽象化，让用户不直接访问表或视图。
C. 使用参数化查询 API
D. 清理输入以排除上下文更改符号，例如： (*)：
[1] '（单引号）
[2] "（引号）
[3] \'（反斜线转义单引号）
[4] \"（反斜杠转义引号）
[5])（结束括号）
[6] ；（分号）
(*) 这适用于 SQL。高级查询语言可能需要不同的清理机制。

引用和相关链接

OWASP 文章
跨站点请求伪造常见问题（FAQ）
跨站点请求伪造培训模块
CWE-74：将数据清理到其他平面失败（“注入”）

HTML 注释敏感信息泄露

应用程序

WASC 威胁分类

信息泄露类型：信息泄露

http://www.webappsec.org/projects/threat/classes/information_leakage.shtml

CVE 标识

不适用

CWE 标识

615

安全风险

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

可能原因

程序员在 Web 页面上留下调试信息

技术描述

很多 Web 应用程序程序员使用 HTML 注释，以在需要时帮助调试应用程序。尽管添加常规注释有助于调试应用程序，但一些程序员往往会遗留重要数据（例如：与 Web 应用程序相关的文件名、旧的链接或原非供用户浏览的链接、旧的代码片段等）。

一般修订建议

[1] 请勿在 HTML 注释中遗留任何重要信息（如文件名或文件路径）。
[2] 从生产站点注释中除去以前（或未来）站点链接的跟踪信息。
[3] 避免在 HTML 注释中放置敏感信息。
[4] 确保 HTML 注释不包括源代码片段。
[5] 确保程序员没有遗留重要信息。

引用和相关链接

WASC 威胁分类：信息泄露
CWE-615：通过注释泄露信息

检测到隐藏目录

基础结构

WASC 威胁分类

信息泄露类型：信息泄露

http://www.webappsec.org/projects/threat/classes/information_leakage.shtml

CVE 标识

不适用

CWE 标识

不适用

安全风险

可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点

可能原因

Web 服务器或应用程序服务器是以不安全的方式配置的

技术描述

Web 应用程序显现了站点中的目录。虽然目录并没有列出其内容，但此信息可以帮助攻击者发展对站点进一步的攻击。例如，知道目录名称之后，攻击者便可以猜测它的内容类型，也许还能猜出其中的文件名或子目录，并尝试访问它们。
内容的敏感度越高，此问题也可能越严重。

一般修订建议

如果不需要禁止的资源，请将其从站点中除去。
可能的话，请发出改用“404 — 找不到”响应状态代码，而不是“403 — 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

引用和相关链接

不适用

发现电子邮件地址模式

应用程序

WASC 威胁分类

信息泄露类型：信息泄露

http://www.webappsec.org/projects/threat/classes/information_leakage.shtml

CVE 标识

不适用

CWE 标识

359

安全风险

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

可能原因

Web 应用程序编程或配置不安全

技术描述

Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。
AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。
而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

一般修订建议

从 Web 站点中除去任何电子邮件地址，使恶意的用户无从利用。

引用和相关链接

Spambot 的定义（维基百科）
CWE-359：隐私违例