网站安全检测报告—漏洞检测 (www.scicpa.org.cn)

本报告有三零卫士安全平台（30SOC）自动生成，如需帮助，请和三零卫士安全服务人员取得联系（见报告底部）

检测时间： 2017/10/9 9:02
检测用时： 0天0小时24分20秒
链接深度： 3
目录深度： 7
检测广度： 5000

发现页面：181 个
发现高危：2 个

目录

1 指纹信息

应用模板	—	操作系统版本	Windows
应用程序版本	IIS	应用程序语言	ASP.NET
开放端口			

2 风险级别

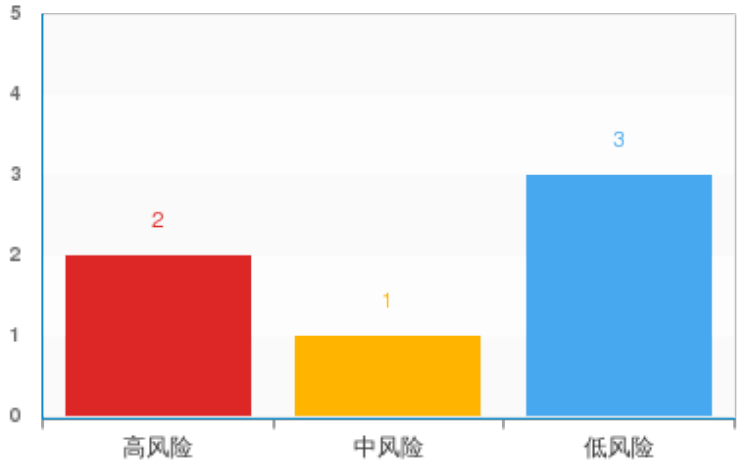
风险等级说明

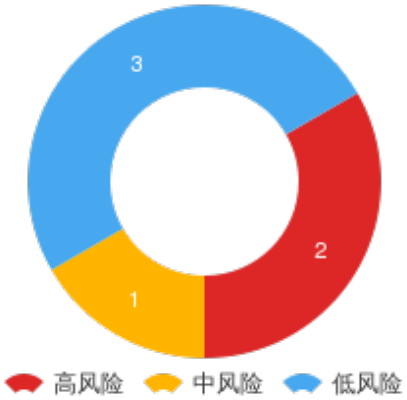
高 存在一个或多个高等级风险的漏洞。请及时确认这些漏洞，建议立即予以修复，以确保不会造成严重后果。

中 存在一个或多个中等级风险的漏洞。请及时确认这些漏洞，以确保不会升级成更严重的问题。

低 存在一个或多个低等级风险的漏洞或信息泄露风险。请及时确认这些漏洞或风险，以确保不会升级成更严重的问题。

3 风险汇总





4 漏洞汇总

4.1 漏洞类型列表

风险名称	风险级别	影响页面数量
跨站脚本漏洞	高	1
Http.sys 远程代码可执行	高	1
HTML表单没有CSRF保护	中	1
ASP.NET版本泄露	低	1
按键劫持: 缺少跨框架头部Options方法定义	低	1
OPTIONS方法启用	低	1

4.2 漏洞类型排名(数量Top10)

5 详细信息

高风险

1 跨站脚本漏洞

[Cross site scripting]

漏洞编号： CWE-79,CWE-79,

影响页面：/search.php

涉及参数：search

技术细节：

请求信息

```
GET /search.php?search=the%22%20HQ0F%3d3Xl5(%5b%21%2b%21%5d)%207jg%3d%22 HTTP/1.1
Referer: http://www.scicpa.org.cn/
Cookie: UM_distinctid=15efeb6921112-02003b924-1e1c7f57-c0000-15efeb6921211; CNZZDATA1261420401=1295877388-1507510697-htt
p%253A%252F%252Fwww.acunetix-referrer.com%252F%7C1507510697
Host: www.scicpa.org.cn
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

应答信息

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-Powered-By: PHP/5.4.8
Set-Cookie: PHPSESSID=0isc6nppj3dqeh9nimg70i7pf4; path=/
X-Powered-By: ASP.NET
Date: Mon, 09 Oct 2017 01:23:31 GMT
Content-Length: 8033
Original-Content-Encoding: gzip
```

1 Http.sys 远程代码可执行

[HTTP.sys remote code execution vulnerability]

漏洞编号： CVE-2015-1635,CWE-119

影响页面：/template/sckjsxh/css/style.css

涉及参数：

技术细节：

请求信息

GET /template/sckjsxh/css/style.css HTTP/1.1

Range: bytes=0-18446744073709551615

Cookie: UM_distinctid=15efeb6921112-02003b924-1e1c7f57-c0000-15efeb6921211; CNZZDATA1261420401=1295877388-1507510697-http%253A%252F%252Fwww.acunetix-referrer.com%252F%7C1507510697

Host: www.scicpa.org.cn

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Accept: */*

应答信息

HTTP/1.1 416 Requested Range Not Satisfiable

Content-Type: text/html; charset=us-ascii

Content-Range: bytes: */5994

Server: Microsoft-HTTPAPI/2.0

Date: Mon, 09 Oct 2017 01:35:25 GMT

Connection: close

Content-Length: 362

中风险

1 HTML表单没有CSRF保护

[HTML form without CSRF protection]

漏洞编号： CWE-352

影响页面：/

涉及参数：

技术细节：

请求信息

GET / HTTP/1.1

Pragma: no-cache

Cache-Control: no-cache

Host: www.scicpa.org.cn

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Accept: */*

应答信息

HTTP/1.1 200 OK

Content-Type: text/html

Last-Modified: Sat, 30 Sep 2017 07:21:16 GMT

Accept-Ranges: bytes

ETag: "0bef9b3bc39d31:0"

Vary: Accept-Encoding

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Date: Mon, 09 Oct 2017 01:19:12 GMT

Content-Length: 124406

Original-Content-Encoding: gzip

低风险

1 ASP.NET版本泄露

[ASP.NET version disclosure]

漏洞编号： CWE-200

影响页面：/

涉及参数：

技术细节：

请求信息

GET /|~.aspx HTTP/1.1

Host: www.scicpa.org.cn

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Accept: */*

应答信息

HTTP/1.1 500 Internal Server Error

Cache-Control: private

Content-Length: 3297

Content-Type: text/html; charset=utf-8

Server: Microsoft-IIS/8.5

X-AspNet-Version: 4.0.30319

X-Powered-By: ASP.NET

Date: Mon, 09 Oct 2017 01:21:36 GMT

1 按键劫持: 缺少跨框架头部Options方法定义

[Clickjacking: X-Frame-Options header missing]

漏洞编号： CWE-693

影响页面：Web Server

涉及参数：

技术细节：

请求信息

```
GET / HTTP/1.1
Cookie: UM_distinctid=15efeb6921112-02003b924-1e1c7f57-c0000-15efeb6921211; CNZZDATA1261420401=1295877388-1507510697-
http%253A%252F%252Fwww.acunetix-referrer.com%252F%7C1507510697
Host: www.scicpa.org.cn
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

应答信息

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 30 Sep 2017 07:21:16 GMT
Accept-Ranges: bytes
ETag: "0bef9b3bc39d31:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Mon, 09 Oct 2017 01:21:36 GMT
Content-Length: 124406
Original-Content-Encoding: gzip
```

1 OPTIONS方法启用

[OPTIONS method is enabled]

漏洞编号： CWE-200

影响页面：Web Server

涉及参数：

技术细节：

请求信息

```
OPTIONS / HTTP/1.1
Host: www.scicpa.org.cn
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

应答信息

```
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Server: Microsoft-IIS/8.5
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Mon, 09 Oct 2017 01:21:59 GMT
Content-Length: 0
```

6 威胁分析

跨站脚本漏洞

描述： 网站页面存在跨站脚本漏洞，这可能导致攻击者利用该漏洞，创建出嵌入了恶意脚本代码的超级链接，管理员或用户点击这个看起来指向可信任域的链接，被执行了攻击者所提供的代码，从而窃取管理员口令或窃取用户会话cookie。

影响分析： 恶意用户可能会注入JavaScript、VBScript、ActiveX控件、HTML或Flash为来欺骗用户，为了收集数据，攻击者可以窃取cookie会话和接管帐户，模拟用户，也有可能修改页面的内容提交给用户。

解决方案：过滤用户输入的特殊字符，例如script iframe src window.open and or onmouseover > < = " % / \ ' 等。

Http.sys 远程代码可执行

描述： 使用Microsoft IIS 6.0以上版本的Microsoft Windows的HTTP协议堆栈(HTTP.sys)中存在远程执行代码漏洞，该漏洞源于HTTP.sys文件没有正确分析经特殊设计的HTTP请求。成功利用此漏洞的攻击者可以在系统帐户的上下文中执行任意代码。影响的系统包括：Microsoft Windows 7 SP1，Windows Server 2008 R2 SP1，Windows 8，Windows8.1，Windows Server 2012 和Windows Server 2012 R2。

影响分析： 黑客可以通过系统账户发送特殊制作的HTTP请求远程执行代码，从而影响操作系统

解决方案：目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms15-034

HTML表单没有CSRF保护

描述： CSRF（Cross-site request forgery跨站请求伪造，也被称成为"one click attack"或者session riding，通常缩写为CSRF或者XSRF，是一种对网站的恶意利用。尽管听起来像跨站脚本（XSS），但它与XSS非常不同，并且攻击方式几乎相左。XSS利用站点内的信任用户，而CSRF则通过伪装来自受信任用户的请求来利用受信任的网站。与XSS攻击相比，CSRF攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比XSS更具危险性。

影响分析： 攻击者可能会强制Web应用程序的用户执行攻击者选择的动作，一个成功的CSRF漏洞使最终用户正常操作的数据处于危险中，如果最终用户是管理员帐户，这可能会危及整个Web应用程序。

解决方案：对于web站点，将持久化的授权方法（例如cookie或者HTTP授权）切换为瞬时的授权方法（在每个form中提供隐藏field），这将帮助网站防止这些攻击。一种类似的方式是在form中包含秘密信息、用户指定的代号作为cookie之外的验证。 另一个可选的方法是"双提交"cookie。此方法只工作于Ajax请求，但它能够作为无需改变大量form的全局修正方法。如果某个授权的cookie在form post之前正被JavaScript代码读取，那么限制跨域规则将被应用。如果服务器需要在Post请求体或者URL中包含授权cookie的请求，那么这个请求必须来自于受信任的域，因为其它域是不能从信任域读取cookie的。 与通常的信任想法相反，使用Post代替Get方法并不能提供卓有成效

的保护。因为JavaScript能使用伪造的POST请求。尽管如此，那些导致对安全产生“副作用”的请求应该总使用Post方式发送。Post方式不会在web服务器和代理服务器日志中留下数据尾巴，然而Get方式却会留下数据尾巴。
尽管CSRF是web应用的基本问题，而不是用户的问题，但用户能够在缺乏安全设计的网站上保护他们的帐户：通过在浏览其它站点前登出站点或者在浏览器会话结束后清理浏览器的cookie。

ASP.NET版本泄露

描述： 从返回的HTTP响应包获取X-ASPNET-Version，这个值由Visual Studio，以确定哪些ASP.NET的版本是在使用中，应被禁用。

影响分析： The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

解决方案：更改web.config文件以防止ASP.NET版本泄露：

按键劫持: 缺少跨框架头部Options方法定义

描述： 按键劫持: 缺少跨框架头部Options方法定义，导致无法完成页面点击动作。

影响分析： 影响相应的Web应用程序

解决方案：检测源代码，补全头部信息。（该漏洞可能是传输过程中的加载丢失导致的误报）

OPTIONS方法启用

描述： 攻击者可能利用此功能获取网站敏感信息，导致重要内容泄露。

影响分析： The OPTIONS method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

解决方案：禁用或删除WebDAV，如果你不需要在此服务器上。

7 联系我们

总部

地址：上海市徐汇区宜山路810号贝岭大厦11楼
电话：（86）021-55313030
传真：（86）021-54363095

上海服务中心

地址：上海市徐汇区宜山路810号贝岭大厦11楼
电话：（86）021-54363010
传真：（86）021-54363095

北京服务中心

地址：北京市丰台区南四环西路188号18区6栋
电话：（86）010-57533163
传真：（86）010-57533163

广州服务中心

地址：广州市天河区天河直街30号金中环大厦A座3604-3606
电话：（86）020-38288430
传真：（86）020-38550652

成都服务中心

地址：成都市高新区创业路16号
电话：（86）028-86082220
传真：（86）028-85325800

武汉服务中心

地址：武汉市武昌区徐东路7号
电话：（86）027-88612165
传真：（86）027-86705880

杭州服务中心

地址：杭州市文三路477号
电话：（86）0571-28913098
传真：（86）0571-28939029

南京服务中心

地址：南京市草场门大街96号
电话：（86）025-86222703
传真：（86）025-86210976