浙江大学 360 校园版定期安全简报（2015 年 4 月）

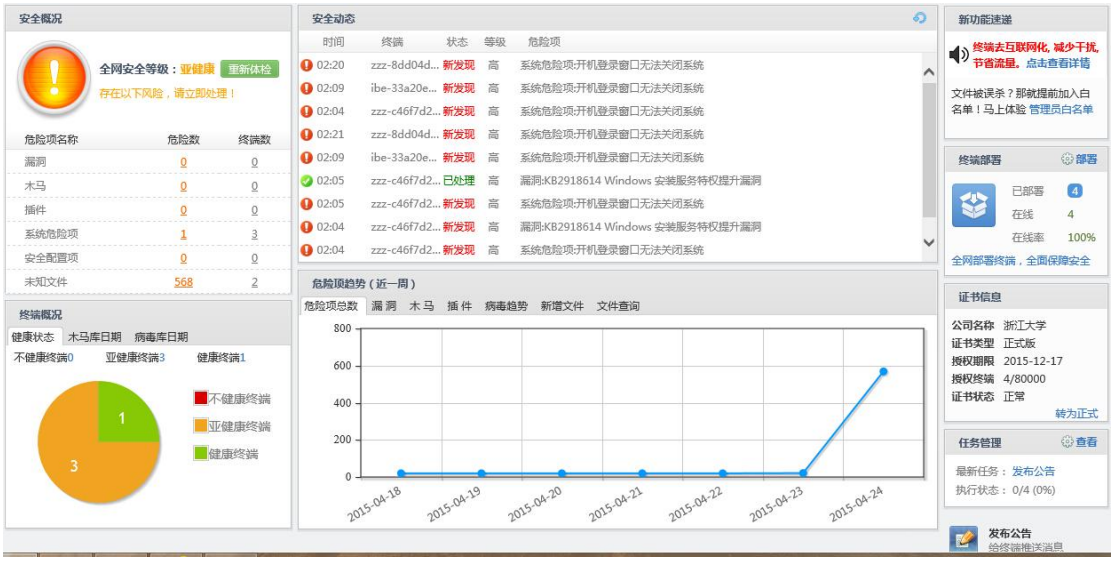
一、 360 虚拟服务器全网等级情况

目前，浙大使用了 2 台服务器为 360 天擎校园版的服务器，一台总控中心，一台分控中心。

1.1 服务器安全等级概况：

1) 10.203.2.93

2) 10.203.2.92



截止至 2015 年 4 月 25 日 15 点止，10.203.2.92 为 360 的总控中心，只负责分发漏洞补丁事宜，安装客户端 4 台，10.203.2.93 服务器安装客户端 250 台。

1.2 受感染用户前 10 名（总排行 2015 年）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名
1	zju	10.15.83.72	2784	玉泉-图书馆
2	PC-201309181536	10.189.253.139	1136	紫金港-无线网
3	PC2013101815TCN	10.75.0.128	1004	紫金港农生环大楼
4	mayanning-PC	192.168.1.106	454	VPN
5	DELL-PC	10.78.49.49	302	紫金港生科院
6	xugangjiang-PC	10.189.251.190	228	紫金港-无线网
7	YeZhiguo	10.71.123.36	90	紫金港-医学院综合楼
8	zju-HP	10.51.120.163	64	之江-主楼
9	violin-lcl	192.168.1.100	46	VPN
10	ZhenyiNi-PC	10.18.3.98	44	玉泉硅材料实验室 3

1.3 受感染用户前 10 名（本月排行）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名	处理措施
1	PC2013101815TCN	10.75.0.128	976	紫金港农生环大楼	清除成功
2	mayanning-PC	192.168.1.106	157	VPN	清除成功
3	LENOVO-PC	10.189.106.164	29	紫金港-无线网	清除成功
4	maox	10.180.53.193	20	玉泉-无线网	清除成功
5	2012-03261653	10.189.127.153	18	紫金港-无线网	清除成功
6	wangfei-PC	10.15.42.87	16	玉泉-热能所	清除成功
7	chenxin	222.205.99.126	16	VPN	清除成功
8	YeZhiguo	10.71.123.36	13	紫金港-医学院综合楼	清除成功
9	PC-201309181536	10.189.253.139	13	紫金港-无线网	清除成功

10	zju-HP	10.51.120.163	10	之江-主楼	清除成功

二、 安全简讯

2.1 11 月检测统计

360 天擎自 10 月初部署以来，随着每天的人数的增多，漏洞补丁、木马、系统危险项日益增多，本月所有统计如下表所示：

日期	终端总数	活跃终端	体检分数	漏洞	木马	插件	系统危险项	安全配置项
2015-04-24	250	122	89	24	13	7	45	9
2015-04-23	245	171	64	176	17	5	35	8
2015-04-22	242	170	61	117	18	5	36	8
2015-04-21	241	167	57	141	8	3	34	8
2015-04-20	241	167	50	29	9	3	33	8
2015-04-19	239	112	45	20	2	2	23	8
2015-04-18	239	113	47	7	2	2	15	8
2015-04-17	237	168	51	200	5	3	26	8
2015-04-16	236	161	51	34	6	2	26	8
2015-04-15	238	176	63	77	6	2	33	9
2015-04-14	229	169	66	1	9	3	38	8
2015-04-13	227	165	65	1	9	2	30	8
2015-04-12	225	109	53	1	2	1	13	8
2015-04-11	226	100	56	1	4	1	14	8
2015-04-10	227	157	66	20	11	4	30	8
2015-04-09	227	160	63	0	8	4	23	7
2015-04-08	225	161	65	22	6	3	25	8
2015-04-07	223	156	65	0	9	5	53	7
2015-04-06	222	97	60	0	6	3	10	9
2015-04-05	223	80	57	3	3	3	10	9
2015-04-04	223	88	53	3	3	4	10	9

2015-04-03	225	159	64	71	7	3	26	8
2015-04-02	224	166	62	0	8	4	33	9
2015-04-01	221	163	64	11	7	4	26	8
2015-03-31	223	160	67	8	7	7	39	6
2015-03-30	215	165	67	133	8	8	29	1
2015-03-29	215	113	61	2	4	2	13	7
2015-03-28	214	111	65	0	1	3	15	7
2015-03-27	212	153	64	70	5	6	26	7
2015-03-26	207	161	66	137	7	4	23	7
2015-03-25	206	157	66	0	7	3	22	8

● 2.2 XP 加固日志数据

2014 年 4 月 8 日微软对 XP 系统停止服务以来，360 盾甲对 XP 的安全，防护，系统加固产生了至关重要的作用。

360 天擎校园版自 2015 年以来，3 月 25 日至 4 月 24 日累计修复 14566 条。


分组 全网 开始日期 2015-03-25 结束日期 2015-04-24 查询

日期	终端名称	IP地址	操作类型	操作说明	详细说明
2015-04-24 10:17:29	DRwang	10.11.111.49	自动允许	驱动加载	进程：C:\WINDOWS\system32\svchost.exe 动作：驱动加载 路径：C:\WINDOWS\syste
2015-04-24 10:17:29	DRwang	10.11.111.49	自动允许	驱动加载	进程：C:\WINDOWS\system32\svchost.exe 动作：驱动加载 路径：C:\WINDOWS\syste
2015-04-24 10:09:48	CHINA-9F846D022321455	10.15.101.166	自动允许	进程创建	进程：H:\Program Files\PLSQL Developer\plsqldev.exe 动作：进程创建 路径：D:\Progr
2015-04-24 09:58:38	Turkey	10.13.72.131	自动允许	驱动加载	进程：D:\Program Files\Tencent\QQ\QQProtect\Bin\QQProtect.exe 动作：驱动加载 路
2015-04-24 09:54:26	DRwang	10.11.111.49	自动允许	驱动加载	进程：D:\qq\QQProtect\Bin\QQProtect.exe 动作：驱动加载 路径：D:\qq\QQProtect\Bi
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 右键菜单	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5E19C0CE-C02C-46
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 右键菜单	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5E19C0CE-C02C-46
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 右键菜单	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5E19C0CE-C02C-46
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 文件关联	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\shellex\ContextMenu
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 右键菜单	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5E19C0CE-C02C-46
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 右键菜单	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\shellex\ContextMenuHan
2015-04-24 09:53:02	15F5EAEDC99A404	10.73.7.237	自动允许	修改 右键菜单	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\Background\shell
2015-04-24 09:51:17	DRwang	10.11.111.49	自动允许	驱动加载	进程：C:\WINDOWS\system32\svchost.exe 动作：驱动加载 路径：C:\WINDOWS\syste
2015-04-24 09:51:17	DRwang	10.11.111.49	自动允许	驱动加载	进程：C:\WINDOWS\system32\svchost.exe 动作：驱动加载 路径：C:\WINDOWS\syste
2015-04-24 09:45:20	lab3211	192.168.1.101	自动允许	修改 系统敏感启动项	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

共14566条记录 1 2 3 ... 972 下一页 跳转

2.3 本月终端插件情况统计

本月来累计统计的插件情况如下：

插件名称	危险级别	终端数量	上报日期
百度地址栏搜索插件	高	12	2015-04-23 11:39:10
腾讯应用宝附带功能组件	高	4	2015-04-23 10:44:49
百度杀毒所附带的浏览器插件	高	3	2015-04-23 18:16:55
捆绑安装的工具栏按钮	高	2	2015-04-19 23:03:15

潜在风险的浏览器插件	高	2	2015-04-23 11:08:21
恶意的篡改程序	高	1	2015-03-30 16:26:30
Lockbat 快捷方式篡改广告程序	高	1	2015-03-31 08:39:15
恶意的文件关联项	高	1	2015-04-23 22:23:26
百度工具栏	高	1	2015-04-04 17:23:47
腾讯搜索插件	高	1	2015-04-10 15:13:39
木马残留文件	高	1	2015-03-31 08:39:15
Qvod 播放器相关插件	高	1	2015-04-09 11:10:14

2.4 Microsoft 2015 年 4 月安全更新

安全公告编号:CNTA-2015-0008

4 月 14 日，微软发布了 2015 年 4 月份的月度例行安全公告，共含 11 项更新，修复了 Microsoft Windows、Internet Explorer、Office、.NET Framework、Server 软件、Office Services 和 Web Apps 中存在的 26 个安全漏洞。

其中，4 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制，获得敏感信息，或进行拒绝服务攻击。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

下表所示为了微软本月安全公告详情（按严重性排序），更多情况请参阅微软的官方网站。

公告 ID	公告标题和摘要	最高严重等级和漏洞影响	重新启动要求	受影响的软件
MS15-032	**Internet Explorer 的累积性安全更新 (3038314)** 此安全更新可解决 Internet Explorer 中的漏洞。 最严重的漏洞可能在用户使用 Internet Explorer 查看经特殊设计的网页时允许远程执行代码。 成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。 与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限	严重 远程执行代码	需要重启	Microsoft Windows、Internet Explorer

	的客户受到的影响更小。			
MS15-033	**Microsoft Office 中的漏洞可能允许远程执行代码（3048019）** 此安全更新可修复 Microsoft Office 中的漏洞。 最严重的漏洞可能在用户打开经特殊设计的 Microsoft Office 文件时允许远程执行代码。 成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。 与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	严重 远程执行代码	可能要求重新启动	Microsoft Office
MS15-034	**HTTP.sys 中的漏洞可能允许远程执行代码（3042553）** 此安全更新可修复 Microsoft Windows 中的漏洞。 如果攻击者向受影响的 Windows 系统发送经特殊设计的的 HTTP 请求，此漏洞可能允许远程执行代码。	严重 远程执行代码	需要重启	Microsoft Windows
MS15-035	**Microsoft Graphics 组件中的漏洞可能允许远程执行代码（3046306）** 此安全更新可修复 Microsoft Windows 中的漏洞。 如果攻击者成功诱使用户浏览经特殊设计的网站、打开经特殊设计的文件或浏览包含经特殊设计的增强型图元文件 (EMF) 图像文件的工作目录，则漏洞可能会允许远程执行代码。 但是在所有情况下，攻击者无法强迫用户执行此类操作；攻击者必须说服用户执行此类操作，通常方式为通过电子邮件或 Instant Messenger 消息进行诱骗。	严重 远程执行代码	可能要求重新启动	Microsoft Windows
MS15-036	**Microsoft SharePoint Server 中的漏洞可能允许特权提升（3052044）** 此安全更新可解决 Microsoft Office 服务器和效率软件中的漏洞。 如果攻击者向受影响的 SharePoint server 发送经特殊设计的请求，则该	重要 特权提升	可能要求重新启动	Microsoft 服务器软件, 效率软件

	漏洞可能允许特权提升。 成功利用此漏洞的攻击者可以阅读攻击者未授权阅读的内容、使用受害者的身份代表受害者在 SharePoint 网站上执行操作（例如，更改权限和删除内容）以及在受害者的浏览器中注入恶意内容。			
MS15-037	**Windows 任务计划程序中的漏洞可能允许特权提升 (3046269)** 此安全更新可修复 Microsoft Windows 中的漏洞。 成功利用此漏洞的攻击者可以利用已知的无效任务来引发任务计划程序，以在系统帐户的上下文中运行经特殊设计的应用程序。 攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。	重要 特权提升	无需重新启动	Microsoft Windows
MS15-038	**Microsoft Windows 中的漏洞可能允许特权提升 (3049576)** 此安全更新可修复 Microsoft Windows 中的漏洞。 这些漏洞在攻击者登录系统并运行特制应用程序时允许提升特权。 要利用这些漏洞，攻击者必须先登录到系统。	重要 特权提升	需要重启	Microsoft Windows
MS15-039	**XML Core Services 中的漏洞可能允许绕过安全功能 (3046482)** 此安全更新可修复 Microsoft Windows 中的漏洞。 如果用户打开经特殊设计的文件，此漏洞可能允许绕过安全功能。 但是在所有情况下，攻击者无法强迫用户打开经特殊设计的文件；攻击者必须说服用户打开此文件，通常方式为通过电子邮件或 Instant Messenger 消息进行诱骗。	重要 安全功能规避	可能要求重新启动	Microsoft Windows
MS15-040	**Active Directory 联合身份验证服务中的漏洞可能允许信息泄漏 (3045711)** 此安全更新可解决 Active Directory 联合身份验证服务 (AD FS) 中的一个漏洞。 如果用户从应用程序注销后未关闭其浏览器，攻击者在该用户注销后立即在浏览器中重新打开应用程序，则该漏洞可能允许信息泄漏。	重要 信息泄露	可能要求重新启动	Microsoft Windows

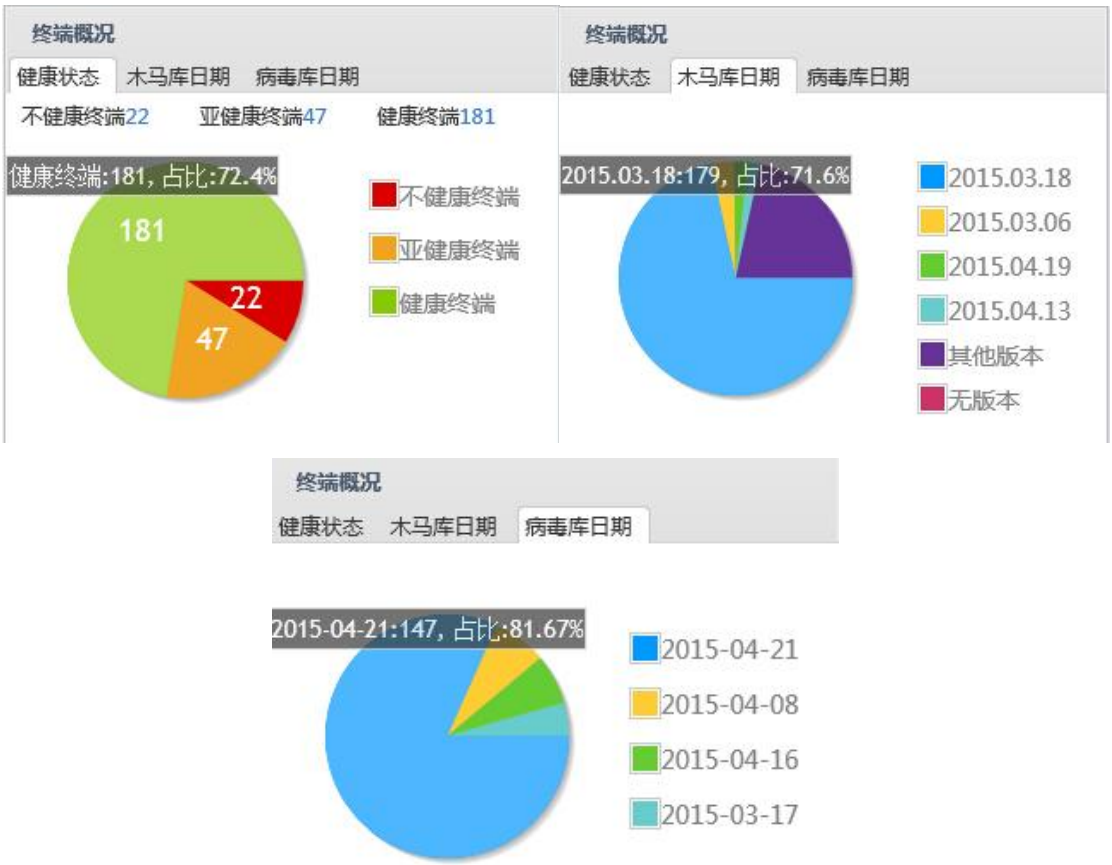
MS15-041	**.NET Framework 中的漏洞可能允许信息泄漏（3048010）** 此安全更新可解决 Microsoft .NET Framework 中的一个漏洞。如果攻击者向已禁用自定义错误信息的受影响服务器发送经过特殊设计的 Web 请求，则此漏洞可能允许信息泄漏。成功利用此漏洞的攻击者可以查看部分 web 配置文件，这可能会暴露敏感信息。	重要 信息泄露	可能要求重新启动	Microsoft Windows、Microsoft .NET Framework
MS15-042	**Windows Hyper-V 中的漏洞可能允许拒绝服务（3047234）** 此安全更新可修复 Microsoft Windows 中的漏洞。如果经过身份验证的攻击者在虚拟机 (VM) 会话中运行经特殊设计的应用程序，则此漏洞可能允许拒绝服务。请注意，拒绝服务不允许攻击者在运行 Hyper-V 主机的其他 VM 上执行代码或提升用户权限，但可能会导致该主机上的其他 VM 在虚拟机管理器中无法管理。	重要 拒绝服务	需要重启	Microsoft Windows

2.5 截止至本月月底的全网安全状况如下：

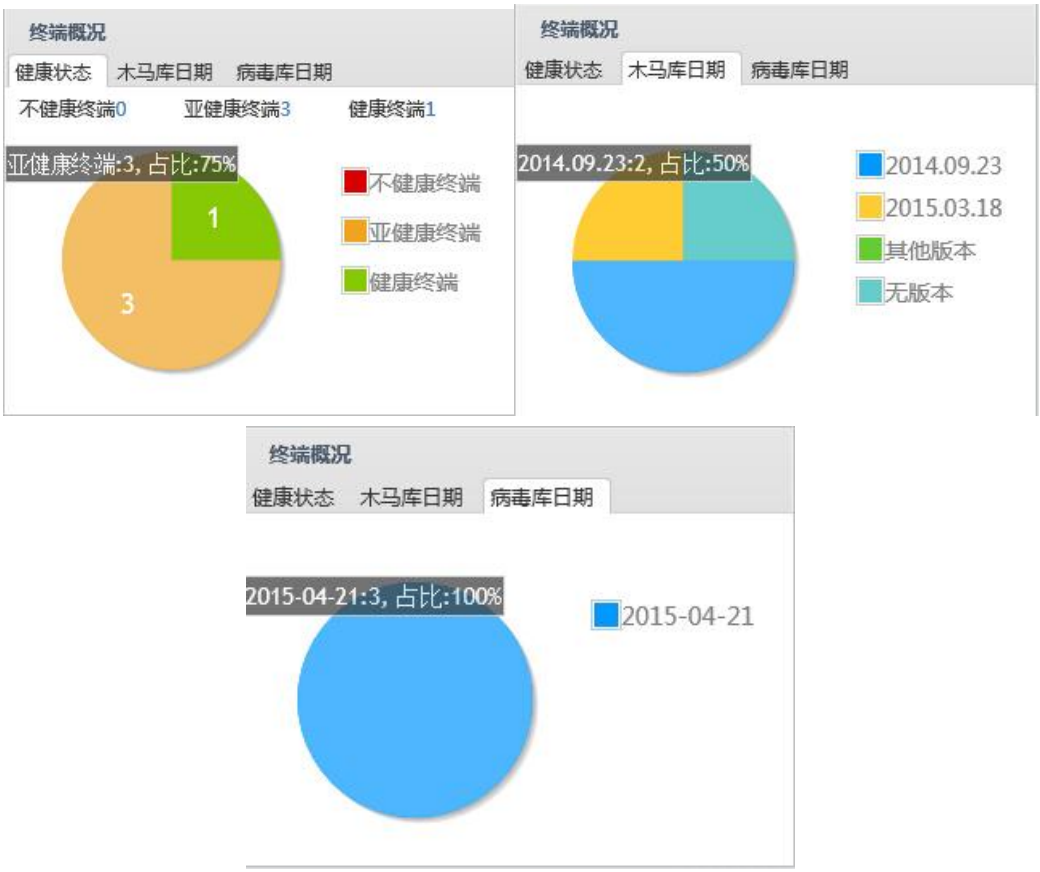
10.203.2.93　　10.203.2.92

2．6 终端概况如下

1）10.203.2.93


终端概况
健康状态
木马库日期
病毒库日期
不健康终端22
亚健康终端47
健康终端181
健康终端:181, 占比:72.4%
181
22
47
不健康终端
亚健康终端
健康终端
2015.03.18:179, 占比:71.6%
2015.03.18
2015.03.06
2015.04.19
2015.04.13
其他版本
无版本
2015-04-21:147, 占比:81.67%
2015-04-21
2015-04-08
2015-04-16
2015-03-17

2）10.203.2.92


终端概况
健康状态
木马库日期
病毒库日期
不健康终端0
亚健康终端3
健康终端1
亚健康终端:3, 占比:75%
1
3
不健康终端
亚健康终端
健康终端
2014.09.23:2, 占比:50%
2014.09.23
2015.03.18
其他版本
无版本
2015-04-21:3, 占比:100%
2015-04-21

三、 程序员 Web 面试之 JQuery

以下摘自 powertoolsteam 的 BLOG

jQuery 是什么？

jQuery 是 javascript 编写一个可重用的 JavaScript 库。

不使用 JQuery 设置 UI 文本的 JavaScript 代码如下：

```
1. document.getElementById("txt1").value = "hello";
```

用 JQuery 类库后的的 JavaScript 代码如下：

```
1. $("#txt1").val("Hello");
```

可见，在使用 JQuery 类库后的 JavaScript 代码明显简洁了很多，也更符合 IT 行业特点：短、平、快。

jquery 与 JavaScript 的关系，JQuery 会取代 JavaScript 吗？

JavaScript：是一门 Web 最流行的脚本语言。

JQuery： 是一个优秀的 Javascript 框架。它是轻量级的 js 库 ，它兼容 CSS3，还兼容各种浏览器（IE 6.0+, FF 1.5+, Safari 2.0+, Opera 9.0+）。

故，jQuery 是并不是要取代的 JavaScript；使用 JQuery 使 Web 开发变得简单。

如何使用 jQuery 库？

从 jquery.com 下载的 jquery.js 文件(最新的 JQuery 版本 V1.11.1 或 V2.1.1)。jQuery 的文件规则，如“jquery-1.4.1.j s”，其中 1.4.1 是 JS 文件的版本的版本号。

在开发 Web 程序前，需要包含的 JavaScript，如图下面的代码：

```
1. <script src="file:///C:/jquery-1.11.1.min.js" type="text/ja
   vascript"></script>
```

CDN（内容分发网络）是什么？

在开发 Web 页面，考虑最多的问题之一是页面在客户端电脑的响应：时间越短，用户体验越好。

而制约用户体验的关键因素之一是浏览器下载 Web 文件大小，包括*.html、图片、*.js、*.css 等文件。

为了最大化复用和节约带宽，故 CDN 应运而生：其基本思路是尽可能避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使内容传输的更快、更稳定。其目的是使用户可就近取得所需内容，解决 Internet 网络拥挤的状况，提高用户访问网站的响应速度。

如何使用 JQuery CDN?

推荐使用官方的 CDN 节点，使用代码如下：

```
<script src="//code.jquery.com/jquery-1.11.0.min.js"></scri
pt>
<script src="//code.jquery.com/jquery-migrate-1.2.1.min.js"
></script>
```

还有 Google 提供的 JQuery CDN：

```
<script type="text/javascript" src="http://ajax.googleapis.
com/ajax/libs/jquery/1.9.1/jquery.min.js">
</script>
```

同时微软也提供了 JQuery CDN 的节点：

```
<script type="text/javascript" src="http://ajax.microsoft.c
om/ajax/jquery/jquery-1.9.1.min.js">
</script>
```

如何在 CDN 网络不可访问情况下，能自动访问网站的 JQuery 文件？

一般情况下，CDN 网络节点是可靠的。

但是偶尔也有失灵的时候，故为了提供双保险，可进行判断网络加载 CDN 失败，则自动加载网站上的 JQuery

，示例代码如下：

```
<script type="text/javascript" src="http:/ajax.microsoft.co
m/ajax/jquery/jquery-1.9.1.min.js"></script>
<script type="text/javascript">if (typeof jQuery == 'undefi
ned')
{
  document.write(unescape("%3Cscript src='Scripts/jquery.1.
9.1.min.js' type='text/javascript'%3E%3C/script%3E"));
}</script>
```

同版本的 JQuery.js 文件和 JQuery.min.js 有何不同？

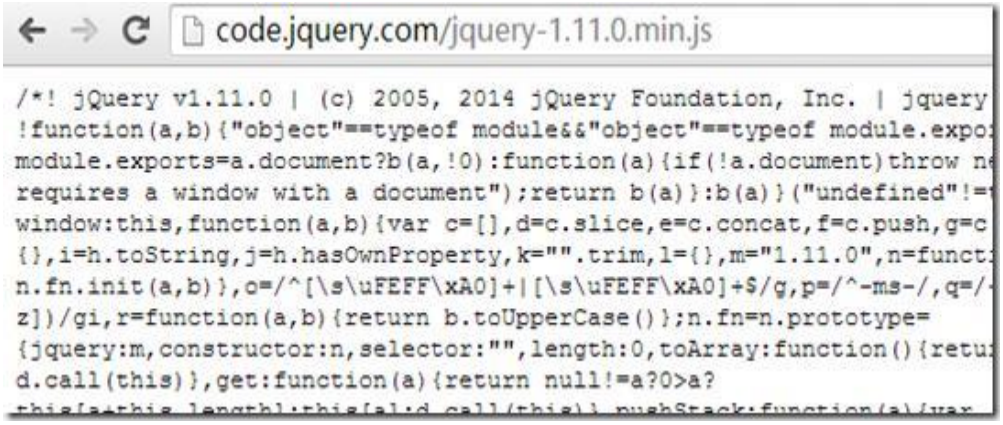
相同：

这两个文件提供相同的 jQuery 的功能，即在函数调用上没有区别。

不同：

JQuery.js 文件，适合让程序员阅读，如下图所示：

JQuery.min.js 文件，通过压缩和删除所有的空格，以节省带宽和空间，使得文件更小，用于网络传输，不适合程序员阅读。



何时使用 jquery.js，何时使用 jquery.min.js？

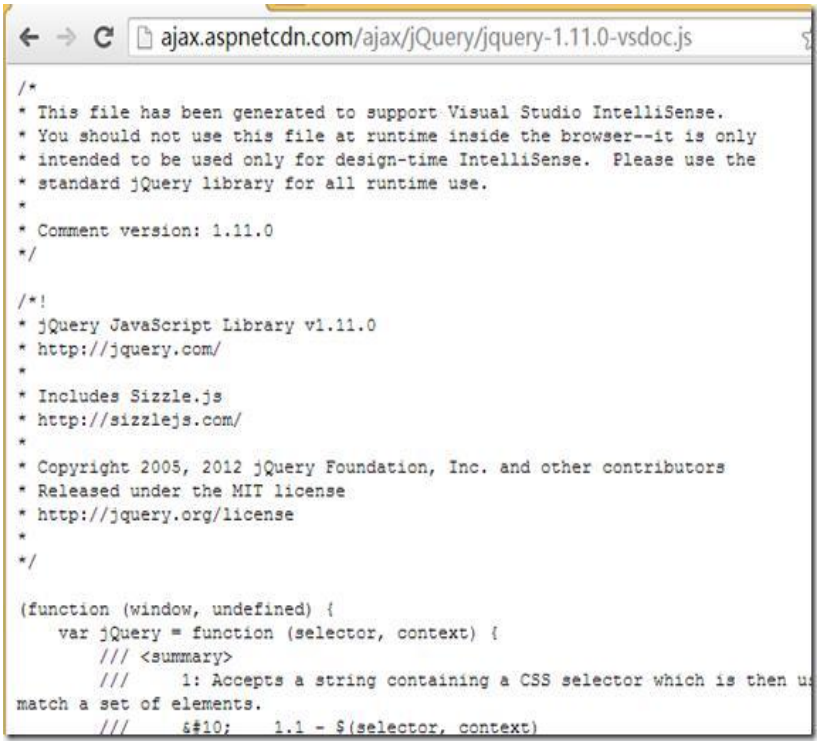
开发调试场景下：用 JQuery.js 文件，因为你想调试，能够看到 javascript 代码。

生产部署环境下：用 JQuery.min.js 文件，可减少网络宽度，加快网页加载速度。

JQuery.vsdoc.js 文件是什么？

*.vsdoc.js 文件是用来在微软的开发环境 Visual Studio 下使用的，方便得获得 JQuery 的智能感知，当你输入 JQuery 函授后，会自动提示函数的类型、函数使用说明、函数参数等等。

如果在 VS 下用 JQuery 开发 Web 程序，则 vsdoc.js 文件会大大的提高开发效率。

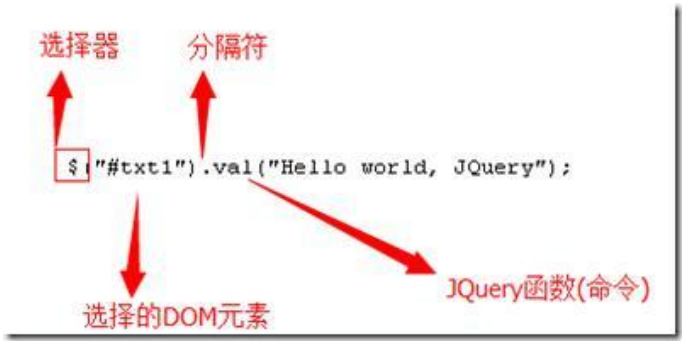


JQuery 的基本语法如何解释？

jQuery 的语法结构可以分为四部分：

1. 默认情况下，所有 Jquery 的命令开始以一个“$”符号。
2. 其次是 HTML 元素的选择。例如下面是我们通过 ID“txt1”选择一个 HTML 文本框。
3. 接着由点（.）分隔。这个操作者将分离的元素和该元素的动作(函数)。
4. 最后什么样的函数(动作)。

例如在下面的 jQuery 代码，我们正在设置的文本值为“Hello world, jQuery”。



在 jQuery 中，“$”符号代表什么？

在 JQuery 中，“$”符号是一个 jQuery 的别名，默认的 JQuery 类库以$开头。

为何要使用 JQuery.noConflict（）

有很多类似 JQuery 一样的类库，如 MooTools, Backbone, Sammy, Cappuccino, Knockout 。这些类库中，有的也使用了$符号，如果同时使用，则会导致命名冲突。

为了解决这个冲突，需要用到 JQuery.noConflict()，这样就不依赖$这个默认符号了。例如：

```
1. $.noConflict();
2. jQuery("p").text("I am jquery and I am working&hellip;");
```

或者使用别名代替：

```
1. var jq = $.noConflict();
2. jq("p").text("I am invoked using jquery shortcut&hellip;");
```

请举例说明 JQuery 的选择器

选择所有 HTML 的 p 元素，并隐藏

```
1. $("p").hide();
```

选择 ID 为 Text1 的 HTML 元素，并赋值

```
1. $("#Text1").val("Hello");
```

选择 Class 为 Text1dHTML 元素，并赋值

```
1. $(".Text1").val("Hello");
```

在 JQuery 中，如何使用 document.ready?

一次完整的 HTML DOM 加载完成，会触发 HTML 的“document.ready”事件，而要通过 JQuery 访问 HTML 元素，则需要页面的 HTML 元素加载完成。

例如：

```
1. <script>
2.     $("#text1").val("Sometext"); // 报错。因为 text1 此刻未加载完成，无法访问</script>
3. </head>
4. <body>
5. <input type="text" id="text1" />
6. </body>
```

而在 Ready 事件中的可访问 HTML 元素，例子如下：

```
1. <script>
2.         $(document).ready(function(){
```

```
3.              $("#text1").val("Sometext");
4.         });</script>
```

同一个页面中，能否加载多个个 document.ready 事件？

可以。

如何用 JQuery 对 HTML 元素事件进行附加？

下面通过 2 个例子来说明

例子 1，选择所有的 button 元素，在其 click 事件中，对所有 p 元素进行 toggle。

```
1. $("button").click(function(){
2. $("p").toggle();
3. });
```

例子 2，选择 ID 为 p1 的元素，在 mouseenter 事件中，进行 alert。

```
1. $("#p1").mouseenter(function(){
2.   alert("You entered p1!");
3. });
```

如何使用 JQuery 添加样式(style)？

使用例子如下：

```
1. $("li").filter(".middle").addClass("selected");
```

css 样式内容如下：

```
1. <style>
2.       .selected { color:red; }</style>
```

四、 技术交流

欢迎老师和同学们前来交流问题，多提建议，希望下期简报内容更加接近大家的需求。

咨询服务电话：87951669
邮箱: netsafe@zju.edu.cn

工程师联系方式：
13588277982 章荣伟