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 Security AppScan Standard 创建 9.0.0.0, 规则： 1699
扫描开始时间： 2018/12/4 17:27:00

目录

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题：	3
低严重性问题：	6
参考严重性问题：	3
报告中包含的严重性问题总数：	12
扫描中发现的严重性问题总数：	12

一般信息

扫描文件名称：	1
扫描开始时间：	2018/12/4 17:27:00
测试策略：	Default
主机	www.ged.com.cn
操作系统：	Win32
Web 服务器：	IIS
应用程序服务器：	Any

登陆设置

登陆方法：	记录的登录
并发登陆：	已启用
JavaScript 执行文件：	已禁用
会话中检测：	已启用
会话中模式：	
跟踪或会话标识 cookie：	
跟踪或会话标识参数：	
登陆序列：	

管理综合报告

问题类型 7

TOC

	问题类型	问题的数量
高	跨站点脚本编制	1
高	已解密的登录请求	2
低	Allaire ColdFusion 路径泄露	2
低	ASP.NET 定制错误路径泄露	2
低	ColdFusion MX Probe.cfm 路径泄露	2
参	发现电子邮件地址模式	1
参	发现可能的服务器路径泄露模式	2

有漏洞的 URL 6

TOC

	URL	问题的数量
高	http://www.ged.com.cn/index.php	2
高	http://www.ged.com.cn/cn/index.php	2
低	http://www.ged.com.cn/cn/guanyuwomen/fazhanqianjing/	3
低	http://www.ged.com.cn/cn/jingyingguanli/	3
参	http://www.ged.com.cn/cn/touzizheguanxi/touzizhezixun/	1
参	http://www.ged.com.cn/a	1

修订建议 7

TOC

	修复任务	问题的数量
高	查看危险字符注入的可能解决方案	1
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	2

低	除去 Web 站点中的电子邮件地址	1
低	请联系您的产品供应商，以了解最近是否推出了补丁或修订程序	2
低	升级至 Macromedia ColdFusion 的最新版本	2
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	2
低	在生产环境中禁用 Robust Exception Information 功能	2

安全风险 4

TOC

	风险	问题的数量
高	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	1
高	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	2
低	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	8
参	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	1

原因 6

TOC

	原因	问题的数量
高	未对用户输入正确执行危险字符清理	1
高	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	2
低	未安装第三方产品的最新补丁或最新修订程序	4
低	Web 站点上安装了没有已知补丁且易受攻击的第三方软件	2
低	Web 服务器或应用程序服务器是以不安全的方式配置的	2
参	Web 应用程序编程或配置不安全	1

WASC 威胁分类

TOC

威胁	问题的数量
传输层保护不足	2
跨站点脚本编制	1
信息泄露	9

按问题类型分类的问题

高 跨站点脚本编制 1 TOC

问题 1 / 1 TOC

跨站点脚本编制	
严重性：	高
URL：	http://www.ged.com.cn/index.php
实体：	countnum (Parameter)
风险：	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
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应：

```
...

  </li>
   </ul>

 <div class="uwebcms_page_center_line"></div>
 <div class="uwebcms_page_botton">
  <div id="pagelist">共有 281 条记录 当前第 1 页/共有 15 页 每页显示 20 条</div>
 </div>
 <div class="uwebcms_page_botton">
  <div id="pagination" class="pagination">
   <span class="current disabled">首页</span><span class="current disabled">上一页</span><span
class="current disabled">1</span><a title="2" href="http://www.ged.com.cn/index.php?
page=2&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">2</a>
<a title="3" href="http://www.ged.com.cn/index.php?
page=3&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">3</a>
<a title="4" href="http://www.ged.com.cn/index.php?
page=4&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">4</a>
<a title="5" href="http://www.ged.com.cn/index.php?
page=5&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">5</a>
<a title="6" href="http://www.ged.com.cn/index.php?
page=6&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">6</a>
<a href="">...</a><a title="15" href="http://www.ged.com.cn/index.php?
```

```
page=15&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+
{toString:alert}`">15</a><a class="p1" title="下一页" href="http://www.ged.com.cn/index.php?
page=2&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">下一页
</a><a class="p1" title="尾页" href="http://www.ged.com.cn/index.php?
page=15&ac=search&at=result&lng=cn&keyword=&countnum=281"onmouseover=`24+{toString:alert}`">尾页
</a>  </div>
 </div>
 </div>

<div class="footer clearfloat">
            <div class="footWarp wp1200 clearfloat">
                <div class="targetWrap">
                    Copyright © 广东电力发展股份有限公司版权所有
                    <a target="
" href="http://www.miitbeian.gov.cn">粤ICP备05071253号-1</a>

...
```

高 已解密的登录请求 2 TOC

问题 1 / 2 TOC

已解密的登录请求	
严重性：	高
URL：	http://www.ged.com.cn/index.php
实体：	index.php (Page)
风险：	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因：	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值：	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

推理： AppScan 识别了不是通过 SSL 发送的登录请求。

原始请求

```
lng=cn&mid=0&keyword=
```

问题 2 / 2 TOC

已解密的登录请求

严重性：	高
URL：	http://www.ged.com.cn/cn/index.php
实体：	index.php (Page)
风险：	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因：	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值：	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

推理： AppScan 识别了不是通过 SSL 发送的登录请求。

原始请求

```
lng=cn&keyword=&keyname=summary
```

低 Allaire ColdFusion 路径泄露 2 TOC

问题 1 / 2 TOC

Allaire ColdFusion 路径泄露

严重性：	低
URL：	http://www.ged.com.cn/cn/guanyuwomen/fazhanqianjing/
实体：	application.cfm (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	升级至 Macromedia ColdFusion 的最新版本

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>MapRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>StaticFile</td></tr>
    <tr><th>错误代码</th><td>0x80070002</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th>
<td>http://www.ged.com.cn:80/cfdocs/exampleapp/email/application.cfm</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\cfdocs\exampleapp\email\application.cfm</td>
</tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

问题 2 / 2 TOC

Allaire ColdFusion 路径泄露

严重性：	低
URL：	http://www.ged.com.cn/cn/jingyingguanli/
实体：	application.cfm (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	升级至 Macromedia ColdFusion 的最新版本

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>MapRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>StaticFile</td></tr>
    <tr><th>错误代码</th><td>0x80070002</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th>
<td>http://www.ged.com.cn:80/cfdocs/exampleapp/email/application.cfm</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\cfdocs\exampleapp\email\application.cfm</td>
</tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

低 ASP.NET 定制错误路径泄露 2

TOC

问题 1 / 2

TOC

ASP.NET 定制错误路径泄露

严重性：	低
URL：	http://www.ged.com.cn/cn/guanyuwomen/fazhanqianjing/
实体：	~AppScan.aspx (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	Web 站点上安装了没有已知补丁且易受攻击的第三方软件
固定值：	请联系您的产品供应商，以了解最近是否推出了补丁或修订程序

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>ExecuteRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>AboMapperCustom-837005425</td></tr>
    <tr><th>错误代码</th><td>0x800704ec</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th>
<td>http://www.ged.com.cn:80/cn/guanyuwomen/fazhanqianjing/~AppScan.aspx</td></tr>
    <tr><th>物理路径</th>
<td>d:\freehost\gedcomcn\web\cn\guanyuwomen\fazhanqianjing\~AppScan.aspx</td></tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

问题 2 / 2

TOC

ASP.NET 定制错误路径泄露

严重性：	低
URL：	http://www.ged.com.cn/cn/jingyingguanli/
实体：	~AppScan.aspx (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	Web 站点上安装了没有已知补丁且易受攻击的第三方软件
固定值：	请联系您的产品供应商，以了解最近是否推出了补丁或修订程序

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>ExecuteRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>AboMapperCustom-837005425</td></tr>
    <tr><th>错误代码</th><td>0x800704ec</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th>
<td>http://www.ged.com.cn:80/cn/jingyingguanli/~AppScan.aspx</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\cn\jingyingguanli\~AppScan.aspx</td></tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

低 ColdFusion MX Probe.cfm 路径泄露 2

TOC

问题 1 / 2

TOC

ColdFusion MX Probe.cfm 路径泄露

严重性：	低
URL：	http://www.ged.com.cn/cn/jingyingguanli/
实体：	probe.cfm (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
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
固定值：	在生产环境中禁用 Robust Exception Information 功能

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>MapRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>StaticFile</td></tr>
    <tr><th>错误代码</th><td>0x80070002</td></tr>
```

```
   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th><td>http://www.ged.com.cn:80/cfide/probe.cfm</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\cfide\probe.cfm</td></tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

问题 2 / 2

TOC

ColdFusion MX Probe.cfm 路径泄露

严重性：	低
URL：	http://www.ged.com.cn/cn/guanyuwomen/fazhanqianjing/
实体：	probe.cfm (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
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
固定值：	在生产环境中禁用 Robust Exception Information 功能

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>MapRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>StaticFile</td></tr>
    <tr><th>错误代码</th><td>0x80070002</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th><td>http://www.ged.com.cn:80/cfide/probe.cfm</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\cfide\probe.cfm</td></tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

参 发现电子邮件地址模式 1 TOC

问题 1 / 1 TOC

发现电子邮件地址模式

严重性：	参考信息
URL：	http://www.ged.com.cn/cn/touzizheguanxi/touzizhezixun/
实体：	(Page)
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
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

推理： 响应包含可能是专用的电子邮件地址。

未经处理的测试响应：

```
...

        <div class="investorBox clearfloat">
            <div class="investorWrap clearfloat">
                <div class="investorName clearfloat">
                    <div class="introName secretary">
                        <h6>董事会秘书：刘维</h6>
<ul>
<li>联系地址：广州市天河东路2号粤电广场南塔36楼</li>
<li>联系电话：（020）87570276</li>
<li>传真号码：（020）85138084</li>
<li>电子信箱：<a href="mailto:qinxiao@ged.com.cn">liuw@ged.com.cn</a></li>
</ul>                    </div>
                    <div class="introName represent">
                        <h6>证券事务代表：秦晓</h6>
<ul>
<li>联系地址：广州市天河东路2号粤电广场南塔36楼</li>
<li>联系电话：（020）87570251</li>
<li>传真号码：（020）85138084</li>
<li>电子信箱：<a href="mailto:qinxiao@ged.com.cn">qinxiao@ged.com.cn</a></li>
</ul>                    </div>
                </div>
                <div class="message clearfloat">
                    <div class="Img"><img
src="http://ged.com.cn/templates/specialty/images/investor_01.jpg"></div>
                    <div class="messageForm">

                        <script type="text/javascript"
src="http://ged.com.cn/js/My97DatePicker/WdatePicker.js"></script>
<script type="text/javascript">
 var seccode_empty = "验证码输入错误或为空，请重新输入！";

...
```

参 发现可能的服务器路径泄露模式 2 TOC

问题 1 / 2 TOC

发现可能的服务器路径泄露模式

严重性：	参考信息
URL：	http://www.ged.com.cn/cn/index.php
实体：	index.php (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>MapRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>AboMapperCustom-7519</td></tr>
    <tr><th>错误代码</th><td>0x80070002</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th><td>http://www.ged.com.cn:80/cn/index.php?
ac=search&amp;at=list</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\cn\index.php</td></tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```

问题 2 / 2 TOC

发现可能的服务器路径泄露模式

严重性：	参考信息
URL：	http://www.ged.com.cn/a
实体：	a (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

    <tr><th>通知</th><td>MapRequestHandler</td></tr>
    <tr class="alt"><th>处理程序</th><td>StaticFile</td></tr>
    <tr><th>错误代码</th><td>0x80070002</td></tr>

   </table>
  </div>
  <div id="details-right">
   <table border="0" cellpadding="0" cellspacing="0">
    <tr class="alt"><th>请求的 URL</th><td>http://www.ged.com.cn:80/a</td></tr>
    <tr><th>物理路径</th><td>d:\freehost\gedcomcn\web\a</td></tr>
    <tr class="alt"><th>登录方法</th><td>匿名</td></tr>
    <tr><th>登录用户</th><td>匿名</td></tr>

   </table>
   <div class="clear"></div>
  </div>
 </fieldset>
</div>
<div class="content-container">
...
```