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 HCL AppScan Standard 创建 10.0.0, 规则： 0
扫描开始时间： 2022/3/2 9:17:07

目录

- 发现电子邮件地址模式 4
- 发现可能的服务器路径泄露模式 3
- 客户端（JavaScript）Cookie 引用 1
- 未分类站点的链接 2
- 应用程序错误 6
- 整数溢出 2

介绍

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

高严重性问题：	15
中等严重性问题：	22
低严重性问题：	29
参考严重性问题：	24
报告中包含的严重性问题总数：	90
扫描中发现的严重性问题总数：	90

常规信息

扫描文件名称： test

扫描开始时间： 2022/3/2 9:17:07

测试策略： Default

主机	demo.testfire.net
端口	80
操作系统：	未知
Web 服务器：	Apache
应用程序服务器：	Tomcat

登陆设置

登陆方法：	记录的登录
并发登陆：	已启用
会话中检测：	已启用
会话中模式：	`>Sign Off<`
跟踪或会话 ID cookie：	`JSESSIONID`
跟踪或会话 ID 参数：	
登陆序列：	`http://demo.testfire.net/bank/login.aspx` `http://demo.testfire.net/login.jsp`

```
http://demo.testfire.net/doLogin
http://demo.testfire.net/bank/main.jsp
```

摘要

问题类型 25

TOC

	问题类型	问题的数量
高	SQL 注入	4
高	发现不存在的域的链接	1
高	跨站点脚本编制	9
高	通过 URL 重定向钓鱼	1
中	phpPgAdmin redirect.php URL 重定向	2
中	不充分帐户封锁	1
中	跨站点请求伪造	6
中	链接注入（便于跨站请求伪造）	6
中	通过框架钓鱼	7
低	“Content-Security-Policy”头缺失或不安全	3
低	“X-Content-Type-Options”头缺失或不安全	3
低	“X-XSS-Protection”头缺失或不安全	3
低	查询中接受的主体参数	3
低	发现数据库错误模式	6
低	跨帧脚本编制防御缺失或不安全	4
低	在未加密连接中发现信用卡号模式 (Visa)	3
低	直接访问管理页面	1
低	自动填写未对密码字段禁用的 HTML 属性	3
参	HTML 注释敏感信息泄露	6
参	发现电子邮件地址模式	4
参	发现可能的服务器路径泄露模式	3
参	客户端（JavaScript）Cookie 引用	1
参	未分类站点的链接	2
参	应用程序错误	6
参	整数溢出	2

有漏洞的 URL 23

TOC

	URL	问题的数量
高	http://demo.testfire.net/bank/showTransactions	10
高	http://demo.testfire.net/doLogin	6
高	http://demo.testfire.net/index.jsp	9
高	http://demo.testfire.net/bank/customize.jsp	7
高	http://demo.testfire.net/bank/queryxpath.jsp	6
高	http://demo.testfire.net/search.jsp	6
高	http://demo.testfire.net/sendFeedback	6
高	http://demo.testfire.net/util/serverStatusCheckService.jsp	3
中	http://demo.testfire.net/	1
中	http://demo.testfire.net/bank/	1
中	http://demo.testfire.net/admin/admin.jsp	5
中	http://demo.testfire.net/bank/doTransfer	6
中	http://demo.testfire.net/bank/showAccount	6
低	http://demo.testfire.net/login.jsp	6
低	http://demo.testfire.net/bank/transfer.jsp	1
低	http://demo.testfire.net/admin/	1
低	http://demo.testfire.net/bank/apply.jsp	1
参	http://demo.testfire.net/bank/main.jsp	1
参	http://demo.testfire.net/doSubscribe	1
参	http://demo.testfire.net/swagger/properties.json	1
参	http://demo.testfire.net/swagger/swagger-ui-bundle.js	3
参	http://demo.testfire.net/swagger/swagger-ui-standalone-preset.js	2
参	http://demo.testfire.net/feedback.jsp	1

修订建议 20

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	32
高	从 web 站点除去不存在的域	1
高	禁用基于参数值指向外部站点的重定向	1
中	多次登录尝试失败后实施帐户封锁	1
中	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
中	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	6
低	除去 HTML 注释中的敏感信息	6
低	除去 Web 站点中的电子邮件地址	4

低	除去 Web 站点中的信用卡号	3
低	除去客户端中的业务逻辑和安全逻辑	1
低	检查链接，确定它是否确实本应包含在 Web 应用程序中	2
低	将“autocomplete”属性正确设置为“off”	3
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	3
低	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头	4
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	3
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	3
低	将适当的授权应用到管理脚本	1
低	请勿接受在查询字符串中发送的主体参数	3
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	3
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	8

安全风险 11

TOC

	风险	问题的数量
高	可能会查看、修改或删除数据库条目和表	10
高	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	33
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	21
中	可能会升级用户特权并通过 Web 应用程序获取管理许可权	2
中	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件	6
低	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	29
低	可能会绕开 Web 应用程序的认证机制	3
参	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	3
参	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色	1
参	不适用	2
参	可能会收集敏感的调试信息	8

原因 13

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	32
高	Web 应用程序包含了不存在的域的链接	1

高	Web 应用程序执行指向外部站点的重定向	1	
中	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	
中	Web 应用程序编程或配置不安全	27	
中	应用程序使用的认证方法不充分	6	
低	Web 服务器或应用程序服务器是以不安全的方式配置的	1	
参	程序员在 Web 页面上留下调试信息	6	
参	未安装第三方产品的最新补丁或最新修补程序	3	
参	Cookie 是在客户端创建的	1	
参	不适用	2	
参	未对入局参数值执行适当的边界检查	8	
参	未执行验证以确保用户输入与预期的数据类型匹配	8	

WASC 威胁分类

TOC

威胁	问题的数量
SQL 注入	10
URL 重定向滥用	2
恶意内容测试	2
可预测资源位置	1
跨站点脚本编制	9
跨站点请求伪造	6
蛮力	1
内容电子欺骗	15
信息泄露	42
整数溢出	2

按问题类型分类的问题

高 SQL 注入 4 TOC

问题 1 / 4 TOC

SQL 注入	
严重性：	高
CVSS 分数：	9.7
URL：	http://demo.testfire.net/bank/showTransactions
实体：	startDate (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:
78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered
&amp;quot;;&amp;quot; at line 1, column 139.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedConnection.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.ConnectionChild.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.execute(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.executeQuery(Unknown Source)
```

```
 com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:403)
...
```

问题 2 / 4

TOC

SQL 注入	
严重性：	高
CVSS 分数：	9.7
URL：	http://demo.testfire.net/bank/showTransactions
实体：	endDate (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:
78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered
&amp;quot;;&amp;quot; at line 1, column 165.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedConnection.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.ConnectionChild.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.execute(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.executeQuery(Unknown Source)
 com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:403)
...
```

问题 3 / 4

TOC

SQL 注入

严重性：	高
CVSS 分数：	9.7
URL：	http://demo.testfire.net/doLogin
实体：	passw (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">
  Syntax error: Encountered ";" at line 1, column 76.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return
(confirminput(login));">
    <table>
      <tr>
        <td>
          Username:
        </td>
        <td>

...
```

问题 4 / 4

TOC

SQL 注入

严重性：	高
CVSS 分数：	9.7
URL：	http://demo.testfire.net/doLogin
实体：	uid (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">
  Syntax error: Encountered ";" at line 1, column 52.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return
(confirminput(login));">
    <table>
      <tr>
        <td>
          Username:
        </td>
        <td>

...
```

高 发现不存在的域的链接 1

TOC

问题 1 / 1

TOC

发现不存在的域的链接

严重性：	高
CVSS 分数：	8.5
URL：	http://demo.testfire.net/index.jsp
实体：	http://www.exampledomainnotinuse.org/mybeacon.gif (Link)
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
原因：	Web 应用程序包含了不存在的域的链接
固定值：	从 web 站点除去不存在的域

推理： AppScan 找到外部站点的链接，但无法解析该链接

未经处理的测试响应：

```
...

<div class="fl" style="width: 99%;">

<h1>Benefits</h1>

<p>Altoro Mutual offers a wide array of benefits for both full and part time employees including:

<ul>
    <li><b>Work/Life:</b>
        <ul>
          <li>On-site Child Care<img src="http://www.exampledomainnotinuse.org/mybeacon.gif"
alt="We are setting a beacon" height="30" witdth="30"></li>
          <li>Flexible Time</li>
          <li>Health Club Membership Discounts</li>
          <li>Company Discount Program</li>
          <li>Paid Vacations</li>
          <li>Paid Holidays (10 per year)</li>
        </ul>
    </li>

    <li><b>Health Plans: </b>

...
```

高 跨站点脚本编制 9

TOC

问题 1 / 9

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/sendFeedback
实体：	sendFeedback (Page)
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。

测试响应

未经处理的测试响应：

```
...

Content-Type: application/x-www-form-urlencoded

cfile=%3E%22%27%3E%3Cscript%3Ealert%28138%29%3C%2Fscript%3E&name=%3E%22%27%3E%3Cscript%3Ealert%28
138%29%3C%2Fscript%3E&email_addr=%3E%22%27%3E%3Cscript%3Ealert%28138%29%3C%2Fscript%3E&subject=%3
E%22%27%3E%3Cscript%3Ealert%28138%29%3C%2Fscript%3E&comments=%3E%22%27%3E%3Cscript%3Ealert%28138%
29%3C%2Fscript%3E&submit=%3E%22%27%3E%3Cscript%3Ealert%28138%29%3C%2Fscript%3E

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7182
Date: Wed, 02 Mar 2022 01:36:23 GMT
Content-Type: text/html;charset=ISO-8859-1









...

...


    <td valign="top" colspan="3" class="bb">


  <div class="fl" style="width: 99%;">

   <h1>Thank You</h1>

   <p>Thank you for your comments, >"'><script>alert(138)</script>.  They will be reviewed by our
Customer Service staff and given the full attention that they deserve.

   However, the email you gave is incorrect () and you will not receive a response.

  </p>

  </div>
    </td>
</div>


...
```

问题 2 / 9

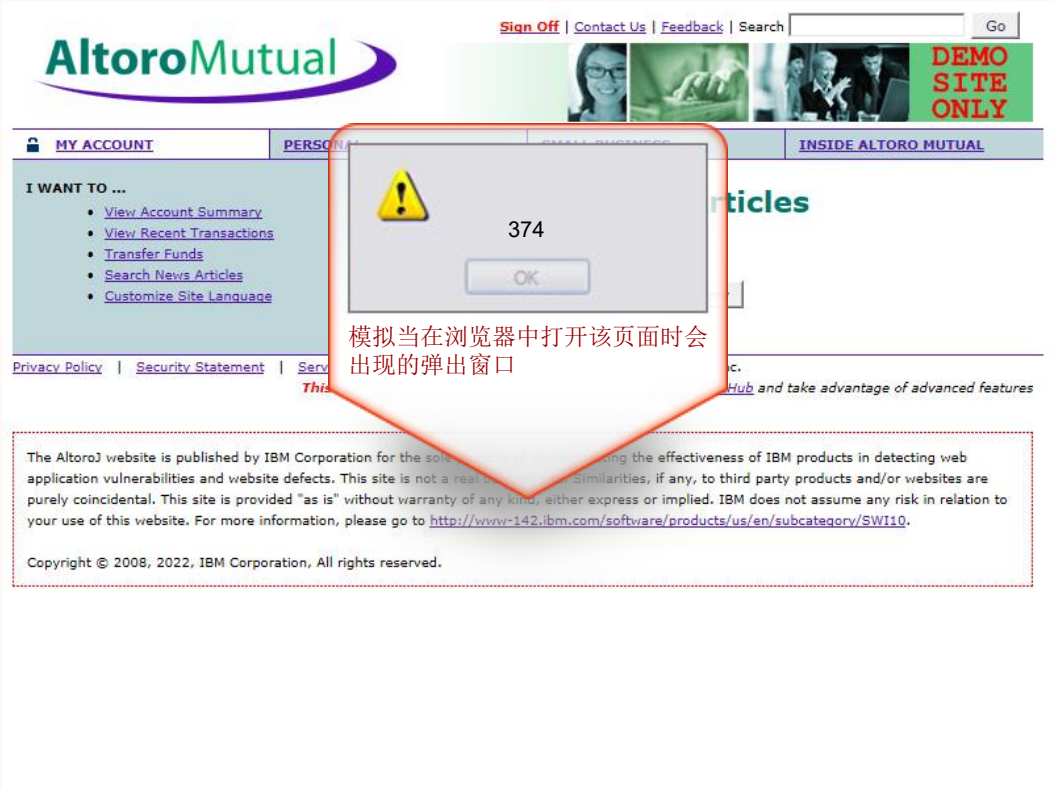
TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/bank/queryxpath.jsp
实体：	queryxpath.jsp (Page)
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。

测试响应



未经处理的测试响应：

```
...

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 5633
Date: Wed, 02 Mar 2022 01:36:55 GMT
Content-Type: text/html;charset=ISO-8859-1









<!-- BEGIN HEADER -->

...

...

<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="http://demo.testfire.net/bank/queryxpath.jsp">
     Search our news articles database
     <br /><br />
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value=">"'>
<script>alert(374)</script>"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />
   News title not found, try again


   </form>
  </div>
    </td>
</div>

...
```

问题 3 / 9

TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/bank/customize.jsp
实体：	customize.jsp (Page)
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。

测试响应

未经处理的测试响应：

```
...

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 5584
Date: Wed, 02 Mar 2022 01:36:55 GMT
Content-Type: text/html;charset=ISO-8859-1









<!-- BEGIN HEADER -->

...

...

    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">


  <h1>Customize Site Language</h1>
```

```
  <form method="post">
    <p>
    Current Language: >"'><script>alert(377)</script>
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?
content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>

...
```

问题 4 / 9

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/search.jsp
实体：	query (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。

测试响应

未经处理的测试响应：

```
...

Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6996
Date: Wed, 02 Mar 2022 01:38:20 GMT
Content-Type: text/html;charset=ISO-8859-1




<!-- BEGIN HEADER -->
```

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


...

...



  <div class="fl" style="width: 99%;">

  <h1>Search Results</h1>

  <p>No results were found for the query:<br /><br />

  1234<script>alert(510)</script>

  </div>
    </td>
</div>


<!-- BEGIN FOOTER -->


...
```

问题 5 / 9

TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/index.jsp
实体：	content (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。

测试响应

未经处理的测试响应：

```
...

        </ul>
    </td>
<!-- TOC END -->

    <td valign="top" colspan="3" class="bb">



   <p>Failed due to The requested resource (/static/inside_contact.htm<script
>eval('ale'+'rt'+'('64')')</script>) is not available</p>

    </td>

</div>


<!-- BEGIN FOOTER -->


...
```

问题 6 / 9

TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/sendFeedback
实体：	name (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。

测试响应

未经处理的测试响应：

```
...

Content-Length: 131
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

cfile=comments.txt&name=John+Smith<script>alert(942)
</script>&email_addr=753+Main+Street&subject=1234&comments=1234&submit=+Submit+

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7203
Date: Wed, 02 Mar 2022 01:39:18 GMT
Content-Type: text/html;charset=ISO-8859-1









...

...


    <td valign="top" colspan="3" class="bb">


  <div class="fl" style="width: 99%;">

   <h1>Thank You</h1>

   <p>Thank you for your comments, John Smith<script>alert(942)</script>.  They will be reviewed
by our Customer Service staff and given the full attention that they deserve.

   However, the email you gave is incorrect (753 main street) and you will not receive a
response.

  </p>

  </div>
    </td>
</div>


...
```

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/util/serverStatusCheckService.jsp
实体：	HostName (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。

测试响应

```
{ "HostName": "AltoroMutual", "HostStatus": "OK" }
```

未经处理的测试响应：

```
...

Referer: http://demo.testfire.net/status_check.jsp
Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0; td_cookie=6882800
```

```
Connection: keep-alive
Host: demo.testfire.net
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 87
Date: Wed, 02 Mar 2022 01:41:18 GMT
Content-Type: text/html;charset=ISO-8859-1



{
 "HostName": "AltoroMutual<script>alert(1290)</script>",
 "HostStatus": "OK"
}
...
```

问题 8 / 9

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/bank/queryxpath.jsp
实体：	query (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： 测试在响应中成功嵌入脚本，一旦用户激活 OnMouseOver 功能（即将鼠标光标悬浮在易受攻击的控件上方），就会执行此脚本。这意味着应用程序易受到跨站点脚本编制攻击。

测试响应

未经处理的测试响应：

```
...

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 5657
Date: Wed, 02 Mar 2022 01:45:31 GMT
Content-Type: text/html;charset=ISO-8859-1









<!-- BEGIN HEADER -->

...

...

<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">

  <div class="fl" style="width: 99%;">
   <h1>Search News Articles</h1>
   <form id="QueryXpath" method="get" action="http://demo.testfire.net/bank/queryxpath.jsp">
     Search our news articles database
     <br /><br />
```

```
    <input type="hidden" id=content" name="content" value="queryxpath.jsp"/>
    <input type="text" id="query" name="query" width=450 value="Enter title (e.g. Watchfire)"
onMouseOver=alert(1764)//"/>
    <input type="submit" width=75 id="Button1" value="Query">
     <br /><br />
   News title not found, try again


   </form>
  </div>
    </td>
</div>

...
```

问题 9 / 9

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://demo.testfire.net/bank/customize.jsp
实体：	lang (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。

测试响应

未经处理的测试响应：

```
...
DY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyNzIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2
FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";  JSESSIONID=2CCED4734DD36781F533493051CEAFC0;
td_cookie=6882800
Connection: Keep-Alive
Host: demo.testfire.net
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 5594
Date: Wed, 02 Mar 2022 01:45:59 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...

...
```

```
    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">



  <h1>Customize Site Language</h1>

  <form method="post">
    <p>
    Current Language: international<script>alert(1961)</script>
    </p>

    <p>
    You can change the language setting by choosing:
    </p>
    <p>
    <a id="HyperLink1" href="./customize.jsp?
content=customize.jsp&lang=international">International</a>
    <a id="HyperLink2" href="./customize.jsp?content=customize.jsp&lang=english">English</a>
    </p>

...
```

高 通过 URL 重定向钓鱼 1

TOC

问题 1 / 1

TOC

通过 URL 重定向钓鱼	
严重性:	高
CVSS 分数:	8.5
URL:	http://demo.testfire.net/bank/customize.jsp
实体:	content (Parameter)
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
原因:	Web 应用程序执行指向外部站点的重定向
固定值:	禁用基于参数值指向外部站点的重定向

推理: 测试结果似乎指示存在脆弱性，因为响应包含指向 demo.testfire.net 的重定向，这显示应用程序允许重定向到外部站点，这是网络钓鱼攻击可利用的弱点。

中 phpPgAdmin redirect.php URL 重定向 2 TOC

问题 1 / 2 TOC

phpPgAdmin redirect.php URL 重定向

严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/
实体：	redirect.php (Page)
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
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： 测试结果似乎指示存在脆弱性，因为响应包含指向 demo.testfire.net 的重定向，这显示应用程序允许重定向到外部站点，这是网络钓鱼攻击可利用的弱点。

问题 2 / 2 TOC

phpPgAdmin redirect.php URL 重定向

严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/
实体：	redirect.php (Page)
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
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： 测试结果似乎指示存在脆弱性，因为响应包含指向 demo.testfire.net 的重定向，这显示应用程序允许重定向到外部站点，这是网络钓鱼攻击可利用的弱点。

中 不充分帐户封锁 1 TOC

问题 1 / 1 TOC

不充分帐户封锁	
严重性:	中
CVSS 分数:	6.4
URL:	http://demo.testfire.net/doLogin
实体:	passw (Parameter)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因:	Web 应用程序编程或配置不安全
固定值:	多次登录尝试失败后实施帐户封锁

推理: 发送了两次合法的登录尝试，并且在其间发送了几次错误的登录尝试。最后一个响应与第一个响应相同。这表明存在未充分实施帐户封锁的情况，从而使登录页面可能受到蛮力攻击。（即使第一个响应不是成功的登录页面，也是如此。）

中 跨站点请求伪造 6 TOC

问题 1 / 6 TOC

跨站点请求伪造	
严重性:	中
CVSS 分数:	6.4
URL:	http://demo.testfire.net/bank/showAccount
实体:	showAccount (Page)
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:	应用程序使用的认证方法不充分
固定值:	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理: 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

问题 2 / 6

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/showTransactions
实体：	showTransactions (Page)
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：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

问题 3 / 6

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/doTransfer
实体：	doTransfer (Page)
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：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应 **测试响应**

问题 4 / 6

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/queryxpath.jsp
实体：	queryxpath.jsp (Page)
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：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应

测试响应

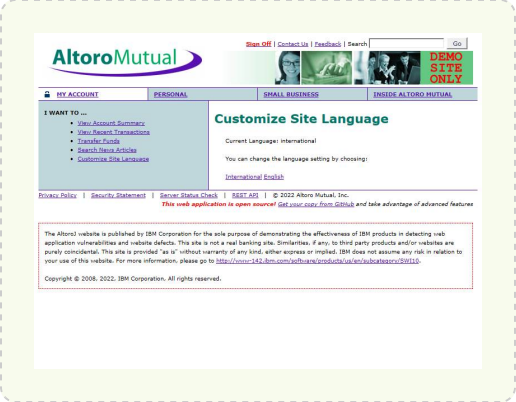
问题 5 / 6

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/customize.jsp
实体：	customize.jsp (Page)
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：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

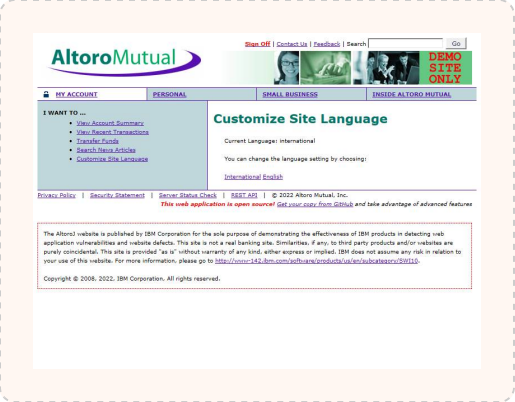
推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应



≈

测试响应



问题 6 / 6

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/admin/admin.jsp
实体：	admin.jsp (Page)
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：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

中 链接注入（便于跨站请求伪造） 6

TOC

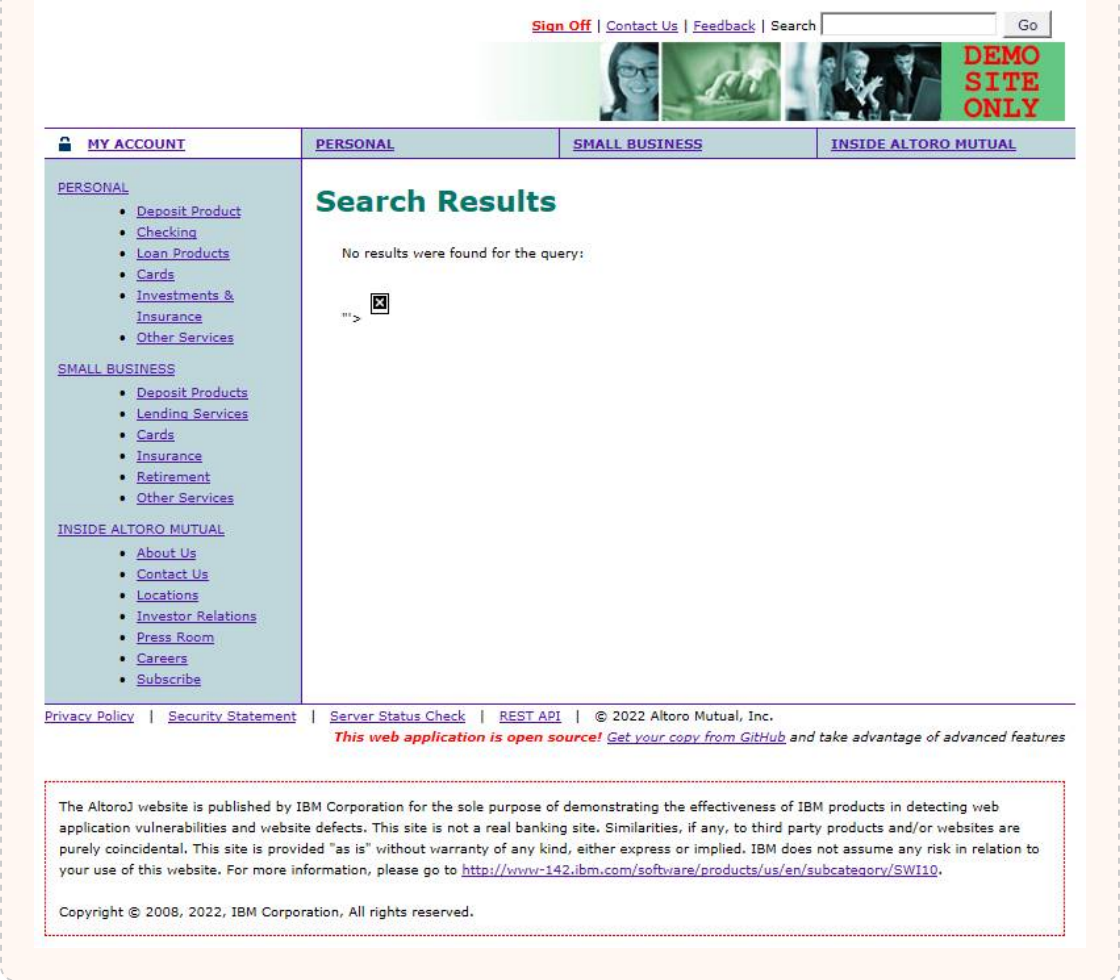
问题 1 / 6

TOC

链接注入（便于跨站请求伪造）	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/search.jsp
实体：	query (Parameter)
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
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，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应



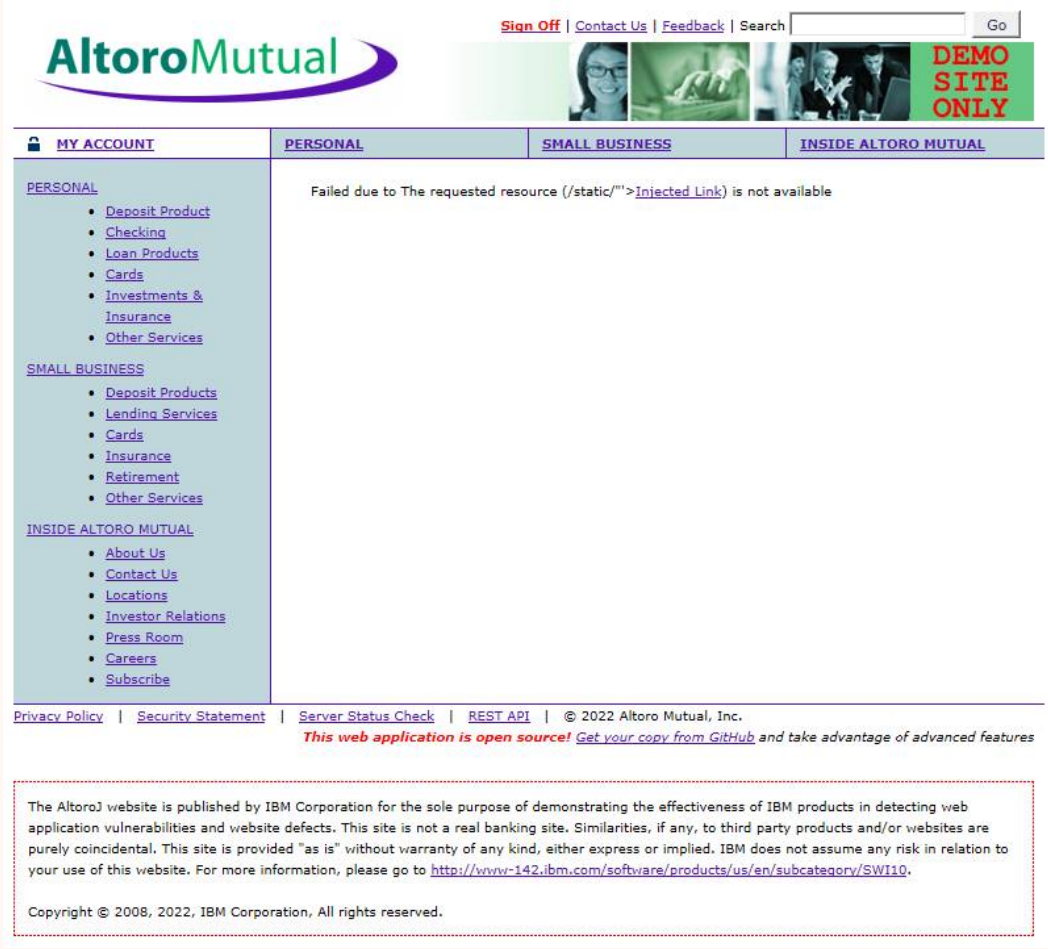
问题 2 / 6

TOC

链接注入（便于跨站请求伪造）	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/index.jsp
实体：	content (Parameter)
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
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，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应



问题 3 / 6

TOC

链接注入（便于跨站请求伪造）

严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/sendFeedback
实体：	name (Parameter)
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
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，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应

问题 4 / 6

TOC

链接注入（便于跨站请求伪造）	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/util/serverStatusCheckService.jsp
实体：	HostName (Parameter)
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
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，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应

{ "HostName": """> ", "HostStatus": "OK" }

问题 5 / 6

TOC

链接注入（便于跨站请求伪造）

严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/queryxpath.jsp
实体：	query (Parameter)
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
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

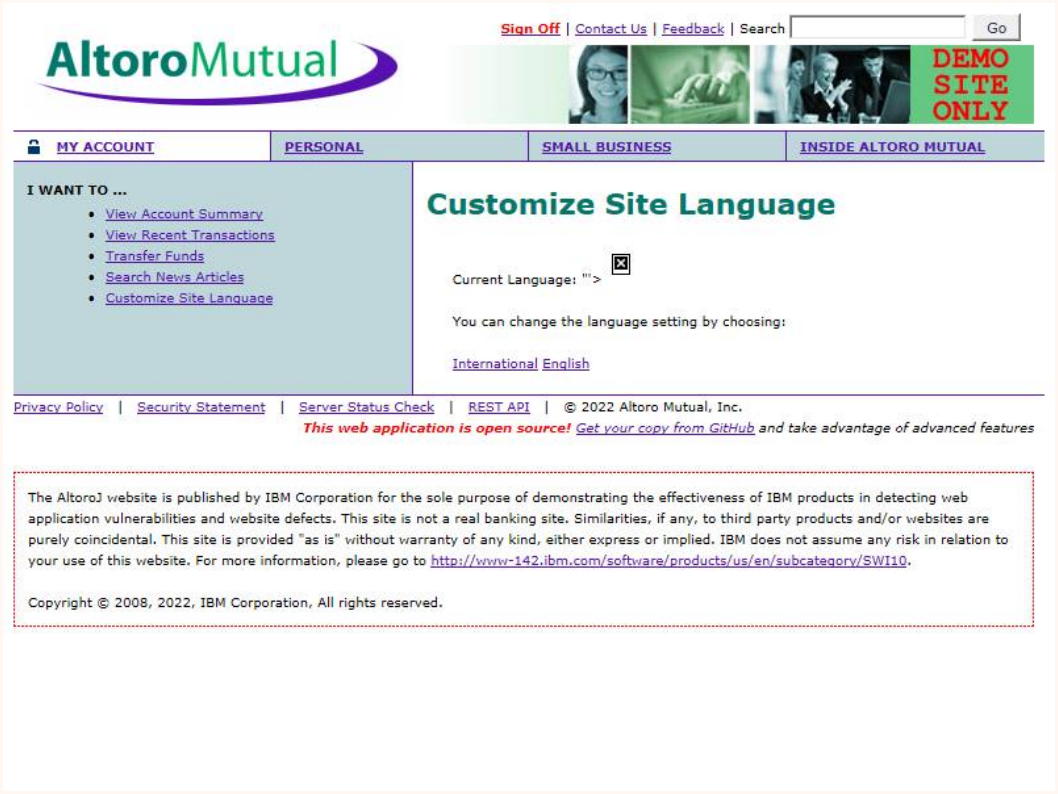
推理： 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应

链接注入（便于跨站请求伪造）	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/customize.jsp
实体：	lang (Parameter)
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
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，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应



中 通过框架钓鱼 7 TOC

问题 1 / 7

TOC

通过框架钓鱼	
严重性:	中
CVSS 分数:	6.4
URL:	http://demo.testfire.net/search.jsp
实体:	query (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

问题 2 / 7

TOC

通过框架钓鱼	
严重性:	中
CVSS 分数:	6.4
URL:	http://demo.testfire.net/index.jsp
实体:	content (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

问题 3 / 7

TOC

通过框架钓鱼	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/sendFeedback
实体：	email_addr (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

问题 4 / 7

TOC

通过框架钓鱼	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/sendFeedback
实体：	name (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

问题 5 / 7

TOC

通过框架钓鱼	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/util/serverStatusCheckService.jsp
实体：	HostName (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

问题 6 / 7

TOC

通过框架钓鱼	
严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/queryxpath.jsp
实体：	query (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

问题 7 / 7

TOC

通过框架钓鱼

严重性：	中
CVSS 分数：	6.4
URL：	http://demo.testfire.net/bank/customize.jsp
实体：	lang (Parameter)
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
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，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

低 “Content-Security-Policy”头缺失或不安全 3 TOC

问题 1 / 3 TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/index.jsp
实体：	index.jsp (Page)
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：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Referer: http://demo.testfire.net/logout.jsp
Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0; td_cookie=6882800
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:32:55 GMT
Content-Type: text/html;charset=ISO-8859-1









...
```

问题 2 / 3

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/login.jsp
实体：	login.jsp (Page)
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：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:36:10 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...
```

问题 3 / 3

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/search.jsp
实体：	search.jsp (Page)
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：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6969
Date: Wed, 02 Mar 2022 01:36:13 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...
```

低 “X-Content-Type-Options”头缺失或不安全 3

TOC

问题 1 / 3

TOC

“X-Content-Type-Options”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/index.jsp
实体：	index.jsp (Page)
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：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Referer: http://demo.testfire.net/logout.jsp
Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0; td_cookie=6882800
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:32:55 GMT
Content-Type: text/html;charset=ISO-8859-1









...
```

问题 2 / 3

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/login.jsp
实体：	login.jsp (Page)
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：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:36:10 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...
```

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/search.jsp
实体：	search.jsp (Page)
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：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6969
Date: Wed, 02 Mar 2022 01:36:13 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...
```

低 “X-XSS-Protection”头缺失或不安全 3

TOC

问题 1 / 3

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/index.jsp
实体：	index.jsp (Page)
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：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Referer: http://demo.testfire.net/logout.jsp
Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTklNDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0; td_cookie=6882800
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:32:55 GMT
Content-Type: text/html;charset=ISO-8859-1









...
```

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/login.jsp
实体：	login.jsp (Page)
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：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:36:10 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...
```

问题 3 / 3

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/search.jsp
实体：	search.jsp (Page)
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：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6969
Date: Wed, 02 Mar 2022 01:36:13 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...
```

低 查询中接受的主体参数 3

TOC

问题 1 / 3

TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	showTransactions (Page)
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：	请勿接受在查询字符串中发送的主体参数

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

问题 2 / 3

TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/doTransfer
实体：	doTransfer (Page)
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：	请勿接受在查询字符串中发送的主体参数

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

原始响应 **测试响应**

问题 3 / 3 TOC

查询中接受的主体参数

严重性:	低
CVSS 分数:	5.0
URL:	http://demo.testfire.net/admin/admin.jsp
实体:	admin.jsp (Page)
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:	请勿接受在查询字符串中发送的主体参数

推理: 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

低 发现数据库错误模式 6 TOC

问题 1 / 6 TOC

发现数据库错误模式

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	showTransactions (Global)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:
78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered
&amp;quot;&amp;gt;&amp;quot; at line 1, column 131.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedConnection.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.ConnectionChild.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.execute(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.executeQuery(Unknown Source)
 com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:403)
...
```

问题 2 / 6

TOC

发现数据库错误模式

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	startDate (Global)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:
78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered
&amp;quot;\&amp;quot;&amp;quot; at line 1, column 149.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedConnection.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.ConnectionChild.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.execute(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.executeQuery(Unknown Source)
 com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:403)
...
```

问题 3 / 6

TOC

发现数据库错误模式

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	endDate (Global)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

 org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
 com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet.doPost(AccountViewServlet.java:
78)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
 javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
 org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
 com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
</pre></p><p><b>Root Cause</b> <pre>java.sql.SQLSyntaxErrorException: Syntax error: Encountered
&amp;quot;\&amp;quot;&amp;quot; at line 1, column 175.
 org.apache.derby.impl.jdbc.SQLExceptionFactory40.getSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.Util.generateCsSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.wrapInSQLException(Unknown Source)
 org.apache.derby.impl.jdbc.TransactionResourceImpl.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedConnection.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.ConnectionChild.handleException(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.execute(Unknown Source)
 org.apache.derby.impl.jdbc.EmbedStatement.executeQuery(Unknown Source)
 com.ibm.security.appscan.altoromutual.util.DBUtil.getTransactions(DBUtil.java:403)
...
```

发现数据库错误模式

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/doLogin
实体：	doLogin (Global)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://demo.testfire.net/doLogin
Cookie: JSESSIONID=3FE5FB4852F4B479E641122A66AF09AA
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:53:39 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...

...

<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">
  Syntax error: Encountered "<" at line 1, column 49.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return
(confirminput(login));">
    <table>
      <tr>
        <td>
          Username:
```

```
        </td>
        <td>

...
```

问题 5 / 6

TOC

发现数据库错误模式	
严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/doLogin
实体：	passw (Global)
风险：	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://demo.testfire.net/doLogin
Cookie: JSESSIONID=0C6E91A1CB899108F5AED4C11B0FFABB
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:54:01 GMT
Content-Type: text/html;charset=ISO-8859-1









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


...

...

<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
```

```
  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">
  Syntax error: Encountered "|" at line 1, column 69.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return
(confirminput(login));">
    <table>
      <tr>
        <td>
          Username:
        </td>
        <td>

...
```

问题 6 / 6

TOC

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://demo.testfire.net/doLogin
实体:	uid (Global)
风险:	可能会查看、修改或删除数据库条目和表
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，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应:

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://demo.testfire.net/doLogin
Cookie: JSESSIONID=BD47183C9C26228698AB0344807684DA
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:54:09 GMT
Content-Type: text/html;charset=ISO-8859-1
```

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


...

...

<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">
  Syntax error: Encountered "|" at line 1, column 47.
  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return
(confirminput(login));">
    <table>
      <tr>
        <td>
          Username:
        </td>
        <td>

...
```

低 跨帧脚本编制防御缺失或不安全 4 TOC

问题 1 / 4 TOC

跨帧脚本编制防御缺失或不安全	
严重性:	低
CVSS 分数:	5.0
URL:	http://demo.testfire.net/bank/showAccount
实体:	showAccount (Page)
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:	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:36:25 GMT
Content-Type: text/html;charset=ISO-8859-1









...
```

问题 2 / 4

TOC

跨帧脚本编制防御缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	showTransactions (Page)
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：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

startDate=2019-01-01&endDate=2019-01-01

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:36:50 GMT
Content-Type: text/html;charset=ISO-8859-1
```

```
...
```

问题 3 / 4

TOC

跨帧脚本编制防御缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/customize.jsp
实体：	customize.jsp (Page)
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：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 5566
Date: Wed, 02 Mar 2022 01:36:54 GMT
Content-Type: text/html;charset=ISO-8859-1









<!-- BEGIN HEADER -->

...
```

问题 4 / 4

TOC

跨帧脚本编制防御缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/queryxpath.jsp
实体：	queryxpath.jsp (Page)
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：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 5630
Date: Wed, 02 Mar 2022 01:36:53 GMT
Content-Type: text/html;charset=ISO-8859-1









<!-- BEGIN HEADER -->

...
```

低 在未加密连接中发现信用卡号模式 (Visa) 3

TOC

问题 1 / 3

TOC

在未加密连接中发现信用卡号模式 (Visa)

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/showAccount
实体：	showAccount (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 站点中的信用卡号

推理： 响应包含完整的 Visa 信用卡号。
未经处理的测试响应：

```
...

          <tr>
          <th colSpan="2">
          Balance Detail</th></tr>
          <tr>
          <th align="left" width="80%" height="26">
          <form id="Form1" method="get" action="showAccount">
          <select size="1" name="listAccounts" id="listAccounts">
       <option value="800003">800003 Checking</option>
<option value="800002">800002 Savings</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

      </select>
          <input type="submit" id="btnGetAccount" Value="Select Account">
          </FORM>
          </th>
          <th align="middle" height="26">
          Amount
          </th>
          </tr>

...
```

问题 2 / 3

TOC

在未加密连接中发现信用卡号模式 (Visa)

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/transfer.jsp
实体：	transfer.jsp (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 站点中的信用卡号

推理： 响应包含完整的 Visa 信用卡号。
未经处理的测试响应：

```
...


  <table cellSpacing="0" cellPadding="1" width="100%" border="0">
    <tr>
      <td><strong>From Account:</strong>
      </td>
      <td>
     <select size="1" id="fromAccount" name="fromAccount">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

     </select>
      </td>
    </tr>
    <tr>
      <td><strong>To Account:</strong></td>
      <td>
     <select size="1" id="toAccount" name="toAccount">
    <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

     </select>
      </td>
    </tr>
    <tr>
      <td><strong> Amount to Transfer:</strong>
      </td>
      <td><input type="text" id="transferAmount" name="transferAmount"></td>
    </tr>

...
```

问题 3 / 3

TOC

在未加密连接中发现信用卡号模式 (Visa)

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/doTransfer
实体：	doTransfer (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 站点中的信用卡号

推理： 响应包含完整的 Visa 信用卡号。
未经处理的测试响应：

```
...
```

```
  <table cellSpacing="0" cellPadding="1" width="100%" border="0">
    <tr>
      <td><strong>From Account:</strong>
      </td>
      <td>
     <select size="1" id="fromAccount" name="fromAccount">
    <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

     </select>
      </td>
    </tr>
    <tr>
      <td><strong>To Account:</strong></td>
      <td>
     <select size="1" id="toAccount" name="toAccount">
    <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

     </select>
      </td>
    </tr>
    <tr>
      <td><strong> Amount to Transfer:</strong>
      </td>
      <td><input type="text" id="transferAmount" name="transferAmount"></td>
    </tr>

...
```

低 直接访问管理页面 1 TOC

问题 1 / 1 TOC

直接访问管理页面	
严重性:	低
CVSS 分数:	5.0
URL:	http://demo.testfire.net/admin/
实体:	admin.jsp (Page)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权
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:	将适当的授权应用到管理脚本

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求: **测试响应**

```
...

Referer: http://demo.testfire.net/index.jsp?content=personal_other.htm
Cookie: AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyNzIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==; JSESSIONID=2CCED4734DD36781F533493051CEAFC0; td_cookie=6882800
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:48:53 GMT
Content-Type: text/html;charset=ISO-8859-1




...

...

  }
  </script>

  <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
  <div class="fl" style="width: 99%;">
  <p><span style="color:#FF0066; font-size:12pt;font-weight:bold; ">

  </span></p>

  <h1>Edit User Information</h1>

  <table width="100%" border="0" >
  <!-- action="addAccount" -->
  <form id="addAccount" name="addAccount" action="" method="post
```

```
GET /admin/admin.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: http://demo.testfire.ne
t/index.jsp?content=personal_oth
er.htm
Cookie: AltoroAccounts="ODAwMDAy
flNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1
MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+
OC4yOTEyNzIwODU1MTc5MjRFMjB8NDUz
OTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2Fy
ZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIw
fA==";  JSESSIONID=2CCED4734DD367
81F533493051CEAFC0; td_cookie=68
82800
Connection: Keep-Alive
Host: demo.testfire.net
Accept: text/html,application/xh
tml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: en-US
```

```
">
    <tr>
      <td colspan="4">
        <h2>Add an account to an
existing user</h2>
      </td>
    </tr>
    <tr>
      <th>
        Users:
      </th>
      <th>
        Account Types:
      </th>

...

...

    </select>
      </td>
      <td>
        <Select name="accttypes"
>
          <option Value="Checkin
g">Checking</option>
          <option Value="Savings
" Selected>Savings</option>
          <option Value="IRA">IR
A</option>
        </Select></td>
      <td></td>
      <td><input type="submit" v
alue="Add Account"></td>
    </tr>
    </form>

   <!-- action="changePassword"
-->
    <form id="changePass" name="
changePass" action="" method="po
st" onsubmit="return confirmpass
(this);">
    <tr>
      <td colspan="4"><h2><br><b
r>Change user's password</h2></t
d>
    </tr>
    <tr>
      <th>
        Users:
      </th>
      <th>
        Password:
      </th>
      <th>

...

...
```

```
    </select>
      </td>
      <td>
        <input type="password" n
ame="password1">
      </td>
      <td>
        <input type="password" n
ame="password2">
      </td>
      <td>
        <input type="submit" nam
e="change" value="Change Passwor
d">
      </td>
    </tr>
    </form>
    <!-- action="addUser" -->
    <form method="post" name="ad
dUser" action="" id="addUser" on
submit="return confirmpass(this)
;">
    <tr>
      <td colspan="4"><h2><br><b
r>Add an new user</h2></td>
    </tr>
    <tr>
      <th>
        First Name:
        <br>
        Last Name:
      </th>
      <th>
        Username:

...

...

      <td>
        <input type="text" name=
"username">
      </td>
      <td>
        <input type="password" n
ame="password1">
        <br>
        <input type="password" n
ame="password2">
      </td>
      <td>
        <input type="submit" nam
e="add" value="Add User">
      </td>
    </tr>
    <tr>
      <td colspan="4">It is high
ly recommended that you leave th
e username as first
        initial last name.
      </td>
```

```
    </tr>
  </form>


...
```

低 自动填写未对密码字段禁用的 HTML 属性 3 TOC

问题 1 / 3 TOC

自动填写未对密码字段禁用的 HTML 属性	
严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/login.jsp
实体：	login.jsp (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

推理： AppScan 发现密码字段没有强制禁用自动填写功能。

未经处理的测试响应：

```
...

        </td>
        <td>
        </td>
      </tr>
      <tr>
        <td>
          Password:
        </td>
        <td>
          <input type="password" id="passw" name="passw" style="width: 150px;">
        </td>
      </tr>
      <tr>
          <td></td>
          <td>
          <input type="submit" name="btnSubmit" value="Login">
          </td>
        </tr>
    </table>

...
```

问题 2 / 3

TOC

自动填写未对密码字段禁用的 HTML 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/bank/apply.jsp
实体：	apply.jsp (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

推理： AppScan 发现密码字段没有强制禁用自动填写功能。

未经处理的测试响应：

```
...

    </td>
<!-- MEMBER TOC END -->
    <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">
   <h1>Altoro Mutual Gold Visa Application</h1>
   <span><p><b>No application is needed.</b>To approve your new $10000 Altoro Mutual Gold Visa<br
/>with an 7.9% APR simply enter your password below.</p>
   <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">

   </span></p>
   <form method="post" name="Credit" action="ccApply"><table border=0><tr><td>Password:</td>
<td><input type="password" name="passwd"></td></tr><tr><td></td><td><input type="submit"
name="Submit" value="Submit"></td></tr></table></form></span>
  </div>
    </td>
</div>


<!-- BEGIN FOOTER -->


</tr>

...
```

问题 3 / 3

TOC

自动填写未对密码字段禁用的 HTML 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://demo.testfire.net/admin/admin.jsp
实体：	admin.jsp (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

推理： AppScan 发现密码字段没有强制禁用自动填写功能。

未经处理的测试响应：

```
...

     <option value="jsmith">jsmith</option>

     <option value="sspeed">sspeed</option>

     <option value="tuser">tuser</option>

    </select>
      </td>
      <td>
        <input type="password" name="password1">
      </td>
      <td>
        <input type="password" name="password2">
      </td>
      <td>
        <input type="submit" name="change" value="Change Password">
      </td>
    </tr>
    </form>
    <!-- action="addUser" -->
    <form method="post" name="addUser" action="" id="addUser" onsubmit="return
confirmpass(this);">
    <tr>

...

...

      <td>
        <input type="text" name="firstname">
        <br>
        <input type="text" name="lastname">
      </td>
      <td>
        <input type="text" name="username">
      </td>
      <td>
        <input type="password" name="password1">
        <br>
        <input type="password" name="password2">
      </td>
      <td>
        <input type="submit" name="add" value="Add User">
      </td>
    </tr>
    <tr>
      <td colspan="4">It is highly recommended that you leave the username as first
        initial last name.
      </td>

...
```

参 HTML 注释敏感信息泄露 6 TOC

问题 1 / 6 TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/login.jsp
实体：	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtm... (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Date: Wed, 02 Mar 2022 01:36:10 GMT
Content-Type: text/html;charset=ISO-8859-1









<!-- BEGIN HEADER -->
<!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" xml:lang="en" >



...
```

问题 2 / 6 TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/login.jsp
实体：	To get the latest admin login, please contact SiteOps at 415-555-6159 (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...

        </ul>
    </td>
<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
  <div class="fl" style="width: 99%;">

  <h1>Online Banking Login</h1>

  <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
  <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-
weight:bold;">

  </span></p>

  <form action="doLogin" method="post" name="login" id="login" onsubmit="return
(confirminput(login));">
    <table>
      <tr>
        <td>
          Username:

...
```

问题 3 / 6

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/main.jsp
实体：	Trade Stocks (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...


    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a></li>
          <li><a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a>
</li>
          <li><a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
    <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

          <li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a></li>
          <li><a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
        </ul>

    </td>
<!-- MEMBER TOC END -->
 <td valign="top" colspan="3" class="bb">


...
```

问题 4 / 6

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/showAccount
实体：	To modify account information do not connect to SQL source directly. Make all changes (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...
    <td valign="top" colspan="3" class="bb">



  <div class="fl" style="width: 99%;">


  <!-- To modify account information do not connect to SQL source directly.  Make all changes
  through the admin page. -->

  <h1>Account History - 800003 Checking</h1>

  <table width="590" border="0">
    <tr>
      <td colspan=2>
        <table cellSpacing="0" cellPadding="1" width="100%" border="1">
          <tr>
          <th colSpan="2">

...
```

问题 5 / 6

TOC

HTML 注释敏感信息泄露	
严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/admin/admin.jsp
实体：	Be careful what you change. All changes are made directly to AltoroJ database. (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...
      myform.password2.value="";
      myform.password1.focus();
      alert ("Passwords do not match");
      return false;
    }

  }
  </script>
```

```
  <!-- Be careful what you change.  All changes are made directly to AltoroJ database. -->
  <div class="fl" style="width: 99%;">
  <p><span style="color:#FF0066;font-size:12pt;font-weight:bold;">

  </span></p>

  <h1>Edit User Information</h1>

  <table width="100%" border="0">
  <!-- action="addAccount" -->

...
```

问题 6 / 6

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/admin/admin.jsp
实体：	action="changePassword" (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...

          <option Value="Checking">Checking</option>
          <option Value="Savings" Selected>Savings</option>
          <option Value="IRA">IRA</option>
        </Select></td>
      <td></td>
      <td><input type="submit" value="Add Account"></td>
    </tr>
    </form>

   <!-- action="changePassword" -->
    <form id="changePass" name="changePass" action="" method="post" onsubmit="return
confirmpass(this);">
    <tr>
      <td colspan="4"><h2><br><br>Change user's password</h2></td>
    </tr>
    <tr>
      <th>
        Users:
      </th>
      <th>

...
```

参 发现电子邮件地址模式 4 TOC

问题 1 / 4 TOC

发现电子邮件地址模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/doSubscribe
实体：	doSubscribe (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：

```
...

   <h1>Subscribe</h1>

   <p>We recognize that things are always evolving and changing here at Altoro Mutual.
   Please enter your email below and we will automatically notify of noteworthy events.</p>

   <form action="doSubscribe" method="post" name="subscribe" id="subscribe" onsubmit="return
confirmEmail(txtEmail.value);">
     <table>
       <tr>
         <td colspan="2">
          <div style="font-weight: bold; font-size: 12px; color: red;" id="message">Thank you.
Your email test@altoromutual.com has been accepted.</div>
         </td>
       </tr>
       <tr>
         <td>
          Email:
         </td>
         <td>
          <input type="text" id="txtEmail" name="txtEmail" value="" style="width: 150px;">
         </td>

...
```

问题 2 / 4 TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/swagger/properties.json
实体：	properties.json (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：

```
...

   ],
   "properties": {
    "name": {
     "type": "string",
     "example": "J Smith"
    },
    "email": {
     "type": "string",
     "format": "email",
     "example": "jsmtih@altoromutual.com"
    },
    "subject": {
     "type": "string",
     "example": "Amazing web design"
    },
    "message": {
     "type": "string",
     "example": "I like the new look of your applicaiton"
    }

...
```

问题 3 / 4

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
实体：	swagger-ui-standalone-preset.js (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：

```
...
...on(t){
/*!
 * The buffer module from node.js, for the browser.
 *
 * @author   Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
 * @license  MIT
 */
var r=n(325),i=n(326),o=n(167);function u(){return s.TYPE...

...

...
...&t.__esModule?t:{default:t}}var a={string:function(){return"string"},string_email:function()
{return"user@example.com"},"string_date-time":function(){return(new
Date).toISOString()},number:function(){return 0},number_...

...
```

问题 4 / 4

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/swagger/swagger-ui-bundle.js
实体：	swagger-ui-bundle.js (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：

```
...
...on(e){
/*!
 * The buffer module from node.js, for the browser.
 *
 * @author   Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
 * @license  MIT
 */
var r=n(529),o=n(530),i=n(261);function a(){return s.TYPE...

...

...
&&"function"==typeof t.callee?"Arguments":a}},function(e,t){var
n=0,r=Math.random();e.exports=function(e){return"Symbol(".concat(void 0===e?"":e,")_",
(++n+r).toString(36))}},function(e,t,n){var
r=n(74),o=n(33).document,i=r(o)&&r(o.createElement);e.exports=function(e){return i?
o.createElement(e):{}}},function(e,t,n){var r=n(242)("keys"),o=n(167);e.exports=function(e)
```

{return r[e]||(r[e]=o(e))}},function(e,t,n){var r=n(117).f,o=n(118),i=n(17)
("toStringTag");e.exports=function(e,t,n){e&&!o(e=n?e:e.prototype,i)&&r(e,i,
{configurable:!0,value:t})}},function(e,t,n){"use strict";var r=n(121);e.exports.f=function(e)
{return new function(e){var t,n;this.promise=new e(function(e,r){if(void 0!==t||void 0!==n)throw
TypeError("Bad Promise constructor");t=e,n=r}),this.resolve=r(t),this.reject=r(n)}
(e)}},function(e,t,n){var r=n(256),o=n(53);e.exports=function(e,t,n){if(r(t))throw
TypeError("String#"+n+" doesn't accept regex!");return String(o(e))}},function(e,t,n){var r=n(17)
("match");e.exports=function(e){var t=/./;try{"/./"[e](t)}catch(n){try{return t[r]=!1,!"/./"[e]
(t)}catch(e){}}return!0}},function(e,t,n){t.f=n(19)},function(e,t,n){var
r=n(21),o=n(15),i=n(114),a=n(174),u=n(40).f;e.exports=function(e){var t=o.Symbol||(o.Symbol=i?
{}:r.Symbol||{});"_"==e.charAt(0)||e in t||u(t,e,{value:a.f(e)})}},function(e,t)
{t.f=Object.getOwnPropertySymbols},function(e,t){},function(e,t,n){"use strict";(function(t){
/*!
 * @description Recursive object extending
 * @author Viacheslav Lotsmanov <lotsmanov89@gmail.com>
 * @license MIT
 *
 * The MIT License (MIT)
 *
 * Copyright (c) 2013-2018 Viacheslav Lotsmanov
 *
 * Permission is hereby granted, free of charge, to any person obtaining a copy of
 * this software and associated documentation files (the "Software"), to deal in
 * the Software without restriction, including without limitation the rights to
...

...
...&e.__esModule?e:{default:e}}var u={string:function(){return"string"},string_email:function()
{return"user@example.com"},"string_date-time":function(){return(new
Date).toISOString()},number:function(){return 0},number_...

...

...
...r r,o,i;o=this,i=function(){
/*!
 * Autolinker.js
 * 0.15.3
 *
 * Copyright(c) 2015 Gregory Jacobs <greg@greg-jacobs.com>
 * MIT Licensed. http://www.opensource.org/licenses/mit-license.php
 *
 * https://github.com/gregj...

...

参 发现可能的服务器路径泄露模式 3 TOC

问题 1 / 3 TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/feedback.jsp
实体：	feedback.jsp (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补程序
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：

```
...

  <p>Our Frequently Asked Questions area will help you with many of your inquiries.<br />
  If you can't find your question, return to this page and use the e-mail form below.</p>

  <p><b>IMPORTANT!</b> This feedback facility is not secure.  Please do not send any <br />
  account information in a message sent from here.</p>

  <form name="cmt" method="post" action="sendFeedback">

  <!--- Dave- Hard code this into the final script - Possible security problem.
    Re-generated every Tuesday and old files are saved to .bak format at
L:\backup\website\oldfiles    --->
  <input type="hidden" name="cfile" value="comments.txt">

  <table border=0>
    <tr>
      <td align=right>To:</td>
      <td valign=top><b>Online Banking</b> </td>
    </tr>
    <tr>
      <td align=right>Your Name:</td>

...
```

问题 2 / 3

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
实体：	swagger-ui-standalone-preset.js (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补程序
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：

```
...
...call(e,n(11))},function(t,e,n){var r=n(347)("toUpperCase");t.exports=r},function(t,e){var
n=RegExp("[\\u200d\\ud800-\\udfff\\u0300-\\u036f--e...

...

...
...turn i(t)?o(t):r(t)}},function(t,e){t.exports=function(t){return t.split("")}},function(t,e)
{var n="--begin_highlight_tag--[\\ud800-\\udfff]",r="
```

问题 3 / 3

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/swagger/swagger-ui-bundle.js
实体：	swagger-ui-bundle.js (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补程序
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：

```
...
...pertyName=l[f]),c.hasOwnProperty(f)&&(h.mutationMethod=c[f]),u.properties[f]=h}}},a=":A-Z_a-
z\\u00C0-\\u00D6\\u00D8-\\u00F6\\u00F8-\\u02FF--e...

...

...
```

```
...o=t>n?0:n-t>>>0,t>>>=0;for(var i=Array(o);++r<o;)i[r]=e[r+t];return i}},function(e,t){var
n=RegExp("--begin_highlight_tag--[\\u200d\\ud800-\\udfff\\u0300-\\u036f--e...

...

...
...turn o(e)?i(e):r(e)}},function(e,t){e.exports=function(e){return e.split("")}},function(e,t)
{var n="--begin_highlight_tag--[\\ud800-\\udfff]",r="
```

参 客户端（JavaScript）Cookie 引用 1

TOC

问题 1 / 1

TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/swagger/swagger-ui-bundle.js
实体：	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==type... (Page)
风险：	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因：	Cookie 是在客户端创建的
固定值：	除去客户端中的业务逻辑和安全逻辑

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

原始响应

```
...
....reduce(function(e,t){var n=P.cookies[t];return e+
(e?"&":"")+v.default.serialize(t,n)},"");P.headers.Cookie=U}return P.cookies&&delete P.cookies,
(0,m.mergeInQueryOrForm)(P),P}function i(e){return(0,x.isOAS3)(e...

...

...
...ult)(r);if("undefined"!==o){var
u="object"===o&&!Array.isArray(r)&&n.explode?"":n.name+"=";t.headers.Cookie=u+(0,a.default)
({key:n.name,value:r,escape:!1,style:n.style||"form",explode:void 0!==n.explode&&n.exp...

...
```

参 未分类站点的链接 2

TOC

问题 1 / 2

TOC

未分类站点的链接	
严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/index.jsp
实体：	http://www.exampledomainnotinuse.org/mybeacon.gif (Link)
风险：	不适用
原因：	不适用
固定值：	检查链接，确定它是否确实本应包含在 Web 应用程序中

推理： 未列在 IBM X-Force Exchange URL 过滤数据库的链接，安全或非安全都有。

The Malware Link Analysis module could not classify this link

问题 2 / 2

TOC

未分类站点的链接	
严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/index.jsp
实体：	http://192.105.92.101/flash.js (Link)
风险：	不适用
原因：	不适用
固定值：	检查链接，确定它是否确实本应包含在 Web 应用程序中

推理： 未列在 IBM X-Force Exchange URL 过滤数据库的链接，安全或非安全都有。

The Malware Link Analysis module could not classify this link

参 应用程序错误 6

TOC

问题 1 / 6

TOC

应用程序错误	
严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/showAccount
实体：	listAccounts (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 500 Internal Server Error
Connection: close
Server: Apache-Coyote/1.1
Content-Length: 3585
Content-Language: en
Date: Wed, 02 Mar 2022 01:39:24 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```

问题 2 / 6

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/sendFeedback
实体：	email_addr (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Content-Length: 105
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

cfile=comments.txt&name=John+Smith&email_addr.=753+Main+Street&subject=1234&comments=1234&submit=
+Submit+

HTTP/1.1 500 Internal Server Error
Connection: close
Server: Apache-Coyote/1.1
Content-Length: 6898
Date: Wed, 02 Mar 2022 01:39:37 GMT
Content-Type: text/html;charset=ISO-8859-1




...
```

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	endDate (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Content-Length: 32
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

startDate=2019-01-01&endDate=%27

HTTP/1.1 500 Internal Server Error
Transfer-Encoding: chunked
Connection: close
Server: Apache-Coyote/1.1
Content-Language: en
Date: Wed, 02 Mar 2022 01:44:59 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/doTransfer
实体：	toAccount (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Connection: Keep-Alive
Host: demo.testfire.net
Content-Length: 76
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

fromAccount=800003&toAccount=%27&transferAmount=1234&transfer=Transfer+Money

HTTP/1.1 500 Internal Server Error
Connection: close
Server: Apache-Coyote/1.1
Content-Length: 1775
Content-Language: en
Date: Wed, 02 Mar 2022 01:44:59 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/doTransfer
实体：	transferAmount (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Connection: Keep-Alive
Host: demo.testfire.net
Content-Length: 59
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

fromAccount=800003&toAccount=800003&transfer=Transfer+Money

HTTP/1.1 500 Internal Server Error
Connection: close
Server: Apache-Coyote/1.1
Content-Length: 1163
Content-Language: en
Date: Wed, 02 Mar 2022 01:45:03 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/showTransactions
实体：	startDate (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Content-Length: 32
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

startDate=%27&endDate=2019-01-01

HTTP/1.1 500 Internal Server Error
Transfer-Encoding: chunked
Connection: close
Server: Apache-Coyote/1.1
Content-Language: en
Date: Wed, 02 Mar 2022 01:45:27 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```

参 整数溢出 2

TOC

问题 1 / 2

TOC

整数溢出	
严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/showAccount
实体：	listAccounts (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTEuMDE5OTk1NDM0MDY1MjIyMkUyMHw4MDAwMDN+Q2hlY2tpbmd+OC4yOTEyN
zIwODU1MTc5MjRFMjB8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4zODg5MzAzMTU1NzMxNDg0RTIwfA==";
JSESSIONID=2CCED4734DD36781F533493051CEAFC0
Connection: keep-alive
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 500 Internal Server Error
Connection: close
Server: Apache-Coyote/1.1
Content-Length: 3642
Content-Language: en
Date: Wed, 02 Mar 2022 01:39:27 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```

问题 2 / 2

TOC

整数溢出

严重性：	参考
CVSS 分数：	0.0
URL：	http://demo.testfire.net/bank/doTransfer
实体：	toAccount (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Connection: Keep-Alive
Host: demo.testfire.net
Content-Length: 93
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

fromAccount=800003&toAccount=9999999999999999999&transferAmount=1234&transfer=Transfer+Money

HTTP/1.1 500 Internal Server Error
Connection: close
Server: Apache-Coyote/1.1
Content-Length: 1813
Content-Language: en
Date: Wed, 02 Mar 2022 01:45:04 GMT
Content-Type: text/html;charset=utf-8

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY
...
```