



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 9.0.3.5, 规则: 8804
扫描开始时间: 2017/11/29 15:43:04

目录

介绍

- 常规信息
- 登陆设置

摘要

- 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

- 使用 HTTP 动词篡改的认证旁路 8
- 查询中接受的主体参数 7
- 检测到隐藏目录 2
- 缺少“Content-Security-Policy”头 5
- 缺少“X-Content-Type-Options”头 5
- 缺少“X-XSS-Protection”头 5
- 发现电子邮件地址模式 1

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。

中等严重性问题:	8
低严重性问题:	24
参考严重性问题:	1
报告中包含的严重性问题总数:	33
扫描中发现的严重性问题总数:	33

常规信息

扫描文件名称: test
扫描开始时间: 2017/11/29 15:43:04
测试策略: Default

主机: redtiger.labs.overthewire.org
端口: 0
操作系统: 未知
Web 服务器: Apache
应用程序服务器: 任何








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: <http://redtiger.labs.overthewire.org/>
<http://redtiger.labs.overthewire.org/level1.php>

摘要










问题类型 7

TOC

问题类型	问题的数量
中 使用 HTTP 动词篡改的认证旁路	8 
低 查询中接受的主体参数	7 
低 检测到隐藏目录	2 
低 缺少“Content-Security-Policy”头	5 
低 缺少“X-Content-Type-Options”头	5 
低 缺少“X-XSS-Protection”头	5 
参 发现电子邮件地址模式	1 

有漏洞的 URL 10

TOC

URL	问题的数量
中 http://redtiger.labs.overthewire.org/	2 
中 http://redtiger.labs.overthewire.org/level1.php	5 
中 http://redtiger.labs.overthewire.org/level2.php	5 
中 http://redtiger.labs.overthewire.org/level3.php	2 
中 http://redtiger.labs.overthewire.org/level5.php	5 
中 http://redtiger.labs.overthewire.org/level6.php	5 
中 http://redtiger.labs.overthewire.org/level8.php	2 
中 http://redtiger.labs.overthewire.org/special1.php	5 
低 http://redtiger.labs.overthewire.org/icons/	1 
低 http://redtiger.labs.overthewire.org/icons/small/	1 

修订建议 7

TOC

修复任务		问题的数量
中	将您的服务器配置为仅允许所需 HTTP 方法	8
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	2
低	将您的服务器配置为使用“Content-Security-Policy”头	5
低	将您的服务器配置为使用“X-Content-Type-Options”头	5
低	将您的服务器配置为使用“X-XSS-Protection”头	5
低	请勿接受在查询字符串中发送的主体参数	7
低	除去 Web 站点中的电子邮件地址	1

安全风险 4

TOC

风险		问题的数量
中	可能会升级用户特权并通过 Web 应用程序获取管理许可权	8
中	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	31
低	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	22
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	2

原因 2

TOC

原因		问题的数量
中	Web 应用程序编程或配置不安全	31
低	Web 服务器或应用程序服务器是以不安全的方式配置的	2

WASC 威胁分类

TOC

威胁		问题的数量
信息泄露	25	
认证不充分	8	

按问题类型分类的问题

问题 1 / 8

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://redtiger.labs.overthewire.org/>

实体: (Page)

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应

```
RedTiger's Hackit
Welcome to my 1st hackit. Visitors: 100995.
This hackit is for people who want to test their knowledge in PHP / SQL security.
It has some similarities to h0y3r's and shadowleer's sql-injection hackits but it will also test you in some logical ways of
thinking.
All levels are based on real vulnerabilities I found in the wild.
Be honest. Dont bruteforce the passwords and dont make any solutions public!!!
Well I am not a friend of long speeches so just start now.

Special challenge
You can see my contact information when level2 is solved
--> Start <-- here

Notice: Level4 is the only level you need to exploit blindly to get the value
I know that my anti-blind-checks are not very consistent. So find the right way to exploit the levels. Anyway, have fun!

Start here -->
Level 1 Simple SQL-Injection solved by 6780 hackers
Level 2 Simple login-bypass solved by 5170 hackers
Level 3 Get an error solved by 1758 hackers
Level 4 Blind Injection solved by 1207 hackers
Level 5 Advanced login-bypass solved by 1048 hackers
Level 6 SQL-Injection solved by 753 hackers
Level 7 CSRF Injections solved by 604 hackers
```

测试响应

```
RedTiger's Hackit
Welcome to my 1st hackit. Visitors: 100995.
This hackit is for people who want to test their knowledge in PHP / SQL security.
It has some similarities to h0y3r's and shadowleer's sql-injection hackits but it will also test you in some logical ways of
thinking.
All levels are based on real vulnerabilities I found in the wild.
Be honest. Dont bruteforce the passwords and dont make any solutions public!!!
Well I am not a friend of long speeches so just start now.

Special challenge
You can see my contact information when level2 is solved
--> Start <-- here

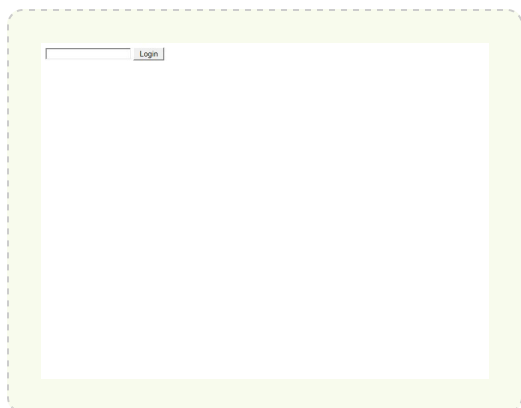
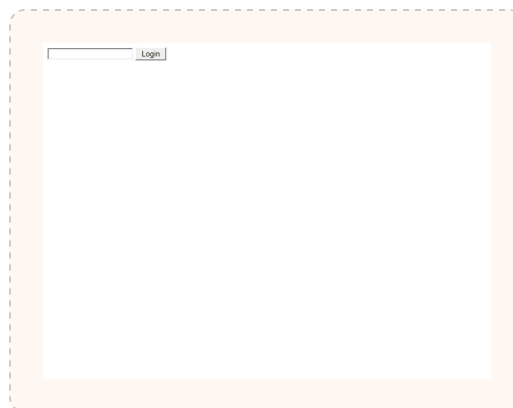
Notice: Level4 is the only level you need to exploit blindly to get the value
I know that my anti-blind-checks are not very consistent. So find the right way to exploit the levels. Anyway, have fun!

Start here -->
Level 1 Simple SQL-Injection solved by 6780 hackers
Level 2 Simple login-bypass solved by 5170 hackers
Level 3 Get an error solved by 1758 hackers
Level 4 Blind Injection solved by 1207 hackers
Level 5 Advanced login-bypass solved by 1048 hackers
Level 6 SQL-Injection solved by 753 hackers
Level 7 CSRF Injections solved by 604 hackers
```



使用 HTTP 动词篡改的认证旁路**严重性:** 中**CVSS 分数:** 6.4**URL:** <http://redtiger.labs.overthewire.org/level6.php>**实体:** level6.php (Page)**风险:** 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置**原因:** Web 应用程序编程或配置不安全**固定值:** 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应**测试响应**

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://redtiger.labs.overthewire.org/special1.php>

实体: special1.php (Page)

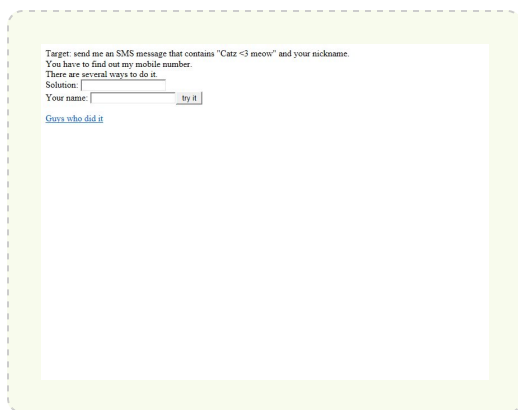
风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

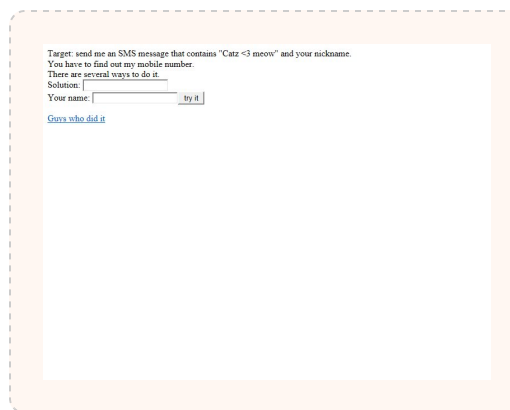
固定值: 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应



测试响应



问题 4 / 8

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://redtiger.labs.overthewire.org/level3.php>

实体: level3.php (Page)

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应



测试响应



问题 5 / 8

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://redtiger.labs.overthewire.org/level2.php>

实体: level2.php (Page)

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应



测试响应



使用 HTTP 动词篡改的认证旁路**严重性:** 中**CVSS 分数:** 6.4**URL:** <http://redtiger.labs.overthewire.org/level5.php>**实体:** level5.php (Page)**风险:** 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置**原因:** Web 应用程序编程或配置不安全**固定值:** 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应



测试响应



使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://redtiger.labs.overthewire.org/level8.php>

实体: level8.php (Page)

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应



测试响应



问题 8 / 8

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://redtiger.labs.overthewire.org/level1.php>

实体: level1.php (Page)

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为仅允许所需 HTTP 方法

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”完全相同, 这表明动词篡改能够绕过站点认证。

原始响应

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Horroxoxe
Hint: You really need one? omg _-'
TableName: level1_users

Category: 1
This category does not exist!

Username:
Password:



测试响应

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Horroxoxe
Hint: You really need one? omg _-'
TableName: level1_users

Category: 1
This category does not exist!

Username:
Password:

问题 1 / 7

TOC

查询中接受的主体参数

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level6.php>

实体: level6.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
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 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

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

原始响应



测试响应



问题 2 / 7

TOC

查询中接受的主体参数

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/special1.php>

实体: special1.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
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 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

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

原始响应

```
the solution not correct
Target: send me an SMS message that contains "Catz <3 meow" and your nickname.
You have to find out my mobile number.
There are several ways to do it.
Solution: [
Your name: [ ] try it
Guys who did it
```

测试响应

```
Target: send me an SMS message that contains "Catz <3 meow" and your nickname.
You have to find out my mobile number.
There are several ways to do it.
Solution: [
Your name: [ ] try it
Guys who did it
```

问题 3 / 7

TOC

查询中接受的主体参数

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level3.php>

实体: level3.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
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 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

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

原始响应



测试响应



问题 4 / 7

TOC

查询中接受的主体参数

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level2.php>

实体: level2.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
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 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

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

原始响应



测试响应



查询中接受的主体参数	
严重性:	低
CVSS 分数:	5.0
URL:	http://redtiger.labs.overthewire.org/level5.php
实体:	level5.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 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 应用程序编程或配置不安全
固定值:	请勿接受在查询字符串中发送的主体参数

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

原始响应



测试响应



查询中接受的主体参数

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level8.php>

实体: level8.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
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 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

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

原始响应



测试响应



问题 7 / 7

TOC

查询中接受的主体参数

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level1.php>

实体: level1.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
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 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

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

原始响应

Welcome to level 1
Lets start with a simple injection.
Target: Get the login for the user Horrox
Hint: You really need one! omg _-_
Tablename: level1_users

Category: 1
This category does not exist!

Username:
Password:

Login incorrect!

测试响应

Welcome to level 1
Lets start with a simple injection.
Target: Get the login for the user Horrox
Hint: You really need one! omg _-_
Tablename: level1_users

Category: 1
This category does not exist!

Username:
Password:



低

检测到隐藏目录 2

TOC

问题 1 / 2

TOC

检测到隐藏目录

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/icons/>

实体: icons/ (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

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录, 即使不允许对其进行访问。

未经处理的测试响应:

```
...
GET /icons/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 403 Forbidden
Server: Apache
Content-Length: 215
Date: Wed, 29 Nov 2017 07:47:42 GMT
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
...
```

检测到隐藏目录

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/icons/small/>

实体: small/ (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

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录, 即使不允许对其进行访问。

未经处理的测试响应:

```
...
GET /icons/small/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 403 Forbidden
Server: Apache
Content-Length: 221
Date: Wed, 29 Nov 2017 07:47:42 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
...
```

缺少“Content-Security-Policy”头严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level6.php>

实体: level6.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

推理: AppScan 检测到 Content-Security-Policy 响应头缺失，这可能会更大程度得暴露于各种跨站点注入攻击下之

未经处理的测试响应:

```
...
GET /level6.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

缺少“Content-Security-Policy”头严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/special1.php>

实体: special1.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

未经处理的测试响应:

```
...
GET /special1.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache
Content-Length: 362
Vary: Accept-Encoding
Date: Wed, 29 Nov 2017 07:46:35 GMT
Content-Type: text/html; charset=UTF-8

Target: send me an SMS message that contains "Catz &lt;3 meow" and your nickname.<br>You have to
find out my mobile number.<br>There are several ways to do it. <br><form method="POST">Solution:
<input type="text" name="solution"><br>Your name: <input type="text" name="name"><input
type="submit" value="try it"></form>
<a href="special1.txt">Guys who did it</a>

...
```

问题 3 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level2.php>

实体: level2.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

未经处理的测试响应:

```
...
GET /level2.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
```

```
Server: Apache
```

```
...
```

问题 4 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level5.php>

实体: level5.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

推理: AppScan 检测到 Content-Security-Policy 响应头缺失，这可能会更大程度得暴露于各种跨站点注入攻击下之

未经处理的测试响应:

```
...
GET /level5.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

问题 5 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level1.php>

实体: level1.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

未经处理的测试响应:

```
...
GET /level1.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

低

缺少“X-Content-Type-Options”头 5

TOC

问题 1 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level6.php>

实体: level6.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-Content-Type-Options”头

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失, 这可能会更大程度得暴露于偷渡式下载攻击之下

未经处理的测试响应:

```
...
GET /level6.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

问题 2 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/special1.php>

实体: special1.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-Content-Type-Options”头

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失, 这可能会更大程度得暴露于偷渡式下载攻击之下

未经处理的测试响应:


```

...
GET /special1.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache
Content-Length: 362
Vary: Accept-Encoding
Date: Wed, 29 Nov 2017 07:46:35 GMT
Content-Type: text/html; charset=UTF-8

Target: send me an SMS message that contains "Catz &lt;3 meow" and your nickname.<br>You have to
find out my mobile number.<br>There are several ways to do it. <br><form method="POST">Solution:
<input type="text" name="solution"><br>Your name: <input type="text" name="name"><input
type="submit" value="try it"></form>
<a href="special1.txt">Guys who did it</a>

...

```

问题 3 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level2.php>

实体: level2.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-Content-Type-Options”头

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下

未经处理的测试响应:

```

...
GET /level2.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...

```

缺少“X-Content-Type-Options”头严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level5.php>

实体: level5.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
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 应用程序编程或配置不安全**固定值:** 将您的服务器配置为使用“X-Content-Type-Options”头

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下

未经处理的测试响应:

```
...
GET /level5.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level1.php>

实体: level1.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-Content-Type-Options”头

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失, 这可能会更大程度得暴露于偷渡式下载攻击之下

未经处理的测试响应:

```
...
GET /level1.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

低

缺少“X-XSS-Protection”头 5

TOC

问题 1 / 5

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level6.php>

实体: level6.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

推理: AppScan 检测到 X-XSS-Protection 响应头缺失, 这可能会造成跨站点脚本编制攻击
未经处理的测试响应:

```
...
GET /level6.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

问题 2 / 5

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/special1.php>

实体: special1.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

推理: AppScan 检测到 X-XSS-Protection 响应头缺失, 这可能会造成跨站点脚本编制攻击
未经处理的测试响应:

```
...
GET /special1.php HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Apache
Content-Length: 362
Vary: Accept-Encoding
Date: Wed, 29 Nov 2017 07:46:35 GMT
Content-Type: text/html; charset=UTF-8
```

```
Target: send me an SMS message that contains "Catz &lt;3 meow" and your nickname.<br>You have to
find out my mobile number.<br>There are several ways to do it. <br><form method="POST">Solution:
<input type="text" name="solution"><br>Your name: <input type="text" name="name"><input
type="submit" value="try it"></form>
<a href="special1.txt">Guys who did it</a>
```

...

问题 3 / 5

TOC

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level2.php>

实体: level2.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

推理: AppScan 检测到 X-XSS-Protection 响应头缺失，这可能会造成跨站点脚本编制攻击
未经处理的测试响应:

```
...
GET /level2.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Apache
```

...

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level5.php>

实体: level5.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

推理: AppScan 检测到 X-XSS-Protection 响应头缺失，这可能会造成跨站点脚本编制攻击
未经处理的测试响应:

```

...
GET /level5.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...

```

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://redtiger.labs.overthewire.org/level1.php>

实体: level1.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

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

未经处理的测试响应:

```
...
GET /level1.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://redtiger.labs.overthewire.org/
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Apache

...
```

问题 1 / 1

TOC

发现电子邮件地址模式

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://redtiger.labs.overthewire.org/>

实体: (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的电子邮件地址

推理: 响应包含可能是专用的电子邮件地址。

未经处理的测试响应:

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: redtiger.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache

...
```