

明鉴漏洞扫描系统

10.43预约体检

Web应用漏洞评估报告



**目 录**

1 任务信息 3

2 风险分布 3

2.1 漏洞风险分布 3

2.2 漏洞名称分布 4

2.3 OWASP漏洞类型分布 5

2.4 WASC风险分布 6

3 网站统计列表 7

4 漏洞统计列表 7

4.1 漏洞概况 7

4.2 漏洞详情 8

4.2.1 低危 8

4.2.2 信息 16

附录1 漏洞等级评估标准 17

# 任务信息

本报告共扫描评估了1个IP，发现紧急漏洞数0个，高危漏洞数0个，中危漏洞数0个，低危漏洞数9个，信息漏洞数2个，为了您的资产安全，请及时修复。

|  |  |
| --- | --- |
| **任务名称** | 网站扫描-20240924-26636预约体检 |
| **执行方式** | 立即执行 |
| **扫描模板** | 快速漏洞扫描 |
| **扫描范围** | 扫描当前页 |
| **时间统计** | 开始时间：2024-09-24 15:06:37  结束时间：2024-09-24 15:11:37  扫描耗时：5分 |
| **创建者** | admin |

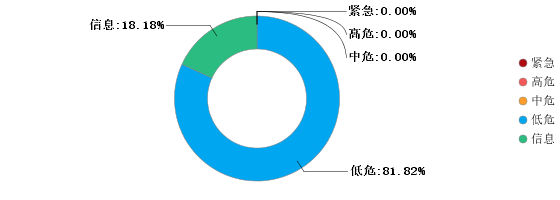
# 风险分布

## 漏洞风险分布

分布列表：

|  |  |  |
| --- | --- | --- |
| **安全级别** | **漏洞数量** | **百分比** |
| 紧急 | 0 | 0.00% |
| 高危 | 0 | 0.00% |
| 中危 | 0 | 0.00% |
| 低危 | 9 | 81.82% |
| 信息 | 2 | 18.18% |
| 漏洞数量总计 | 11 | |

分布占比：



## 漏洞名称分布

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **数量** | **是否加V** |
| GeneratedX-Frame-Options Header未配置 | 1 | 是 |
| GeneratedHTTP Content-Security-Policy缺失 | 1 | 是 |
| Generated敏感目录 | 1 | 是 |
| GeneratedMicrosoft IIS 版本信息泄露 | 1 | 是 |
| GeneratedHTTP Referrer-Policy缺失 | 1 | 是 |
| GeneratedHTTP X-Content-Type-Options缺失 | 1 | 是 |
| GeneratedHTTP X-Download-Options缺失 | 1 | 是 |
| GeneratedHTTP X-Permitted-Cross-Domain-Policies缺失 | 1 | 是 |
| GeneratedHTTP X-XSS-Protection缺失 | 1 | 是 |
| Generated无HTTP重定向 | 1 | 是 |
| Generated未加密的连接 | 1 | 是 |

注：通过对大量网站的历史的扫描结果分析，漏洞加V代表漏洞准确性比较可靠，误报几率较小。

## OWASP漏洞类型分布

OWASP漏洞类型列表：

|  |  |
| --- | --- |
| **OWASP类型（2017）** | **漏洞个数** |
| A1:注入 | 0 |
| A2:失效的认证和会话管理 | 0 |
| A3:敏感数据泄露 | 1 |
| A4:XML外部实体 | 0 |
| A5:失效的访问控制 | 0 |
| A6:安全配置错误 | 7 |
| A7:跨站脚本 | 0 |
| A8:不安全的反序列化 | 0 |
| A9:使用含有已知漏洞的组件 | 3 |
| A10:不足的日志记录和监控 | 0 |
| 其他未分类 | 0 |

OWASP漏洞类型分布图：

## WASC风险分布

WASC风险分布列表：

|  |  |
| --- | --- |
| **WASC分类** | **漏洞个数** |
| 服务错误配置 | 1 |
| 信息泄露 | 4 |
| 错误配置 | 6 |

WASC风险分布图：

# 网站统计列表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **网站URL** | **紧急** | **高危** | **中危** | **低危** | **信息** | **状态** |
| http://10.10.10.43:8001 | 0 | 0 | 0 | 9 | 2 | 可访问 |

注：网络因素问题，可能会影响被扫描网站扫描结果的准确性。

# 漏洞统计列表

## 漏洞概况

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **漏洞名称** | **漏洞数量/漏洞总数** | **影响页面数** |
| 1 | GeneratedMicrosoft IIS 版本信息泄露 | 1/11 | 1 |
| 2 | GeneratedHTTP Content-Security-Policy缺失 | 1/11 | 1 |
| 3 | GeneratedHTTP Referrer-Policy缺失 | 1/11 | 1 |
| 4 | GeneratedHTTP X-Content-Type-Options缺失 | 1/11 | 1 |
| 5 | GeneratedHTTP X-Download-Options缺失 | 1/11 | 1 |
| 6 | GeneratedHTTP X-Permitted-Cross-Domain-Policies缺失 | 1/11 | 1 |
| 7 | GeneratedHTTP X-XSS-Protection缺失 | 1/11 | 1 |
| 8 | Generated敏感目录 | 1/11 | 1 |
| 9 | GeneratedX-Frame-Options Header未配置 | 1/11 | 1 |
| 10 | Generated无HTTP重定向 | 1/11 | 1 |
| 11 | Generated未加密的连接 | 1/11 | 1 |

## 漏洞详情

### 低危

#### HTTP Referrer-Policy缺失

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | HTTP Referrer-Policy缺失 |
| **漏洞描述** | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 |
| **修复建议** | 1）修改服务端程序，给 HTTP 响应头加上 Referrer-Policy 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader("Referrer-Policy", "value") 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header("Referrer-Policy:value") 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头Response.AddHeader "Referrer-Policy", "value" 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse()response["Referrer-Policy"] = "value" 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make\_response()response.headers["Referrer-Policy"] = "value"；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 Referrer-Policy 如果使用Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add\_header Referrer-Policy value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header addReferrer-Policy "value"。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### Microsoft IIS 版本信息泄露

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | Microsoft IIS 版本信息泄露 |
| **漏洞描述** | 此 Web 应用程序返回的 HTTP 响应包括名为 Server 的响应头。响应头的值包含Microsoft IIS服务器的版本信息。 |
| **修复建议** | Microsoft IIS 应配置为从响应中删除不需要的 HTTP 响应头。 |
| **CVSS 评分** | 0.0 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | IIS版本:10.0 |

#### HTTP X-XSS-Protection缺失

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | HTTP X-XSS-Protection缺失 |
| **漏洞描述** | HTTP X-XSS-Protection 响应头是 Internet Explorer，Chrome 和 Safari 的一个特性，当检测到跨站脚本攻击 (XSS)时，浏览器将停止加载页面。若网站设置了良好的 Content-Security-Policy 来禁用内联 JavaScript ('unsafe-inline')，现代浏览器不太需要这些保护， 但其仍然可以为尚不支持 CSP 的旧版浏览器的用户提供保护。 |
| **修复建议** | 将您的服务器配置X-XSS-Protection头。  X-XSS-Protection值为：  0 禁止XSS过滤。  1 启用XSS过滤（通常浏览器是默认的）。 如果检测到跨站脚本攻击，浏览器将清除页面（删除不安全的部分）。  1;mode=block 启用XSS过滤。 如果检测到攻击，浏览器将不会清除页面，而是阻止页面加载。  1; report=<reporting-URI> (Chromium only) 启用XSS过滤。 如果检测到跨站脚本攻击，浏览器将清除页面并使用CSP report-uri指令的功能发送违规报告。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### HTTP X-Content-Type-Options缺失

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | HTTP X-Content-Type-Options缺失 |
| **漏洞描述** | 通过设置"X-Content-Type-Options: nosniff"响应标头，对 script 和 styleSheet 在执行是通过MIME 类型来过滤掉不安全的文件。设置X-Content-Type-Options，可能导致IE9、IE11拒绝加载没有返回Content-Type的相关资源。 |
| **修复建议** | 响应中添加X-Content-Type-Options: nosniff。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### HTTP X-Permitted-Cross-Domain-Policies缺失

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | HTTP X-Permitted-Cross-Domain-Policies缺失 |
| **漏洞描述** | Web 服务器对于 HTTP 请求的响应头中缺少 X-Permitted-Cross-Domain-Policies，这将导致浏览器提供的安全特性失效。 当一些在线的 Web Flash 需要加载其他域的内容时，很多 Web 会通过设置一个 crossdomain.xml 文件的方式来控制其跨域方式。很有可能有些开发者并没有修改 crossdomain.xml 文件的权限，但是又有和跨域的 Flash 共享数据的需求，这时候可以通过设置 X-Permitted-Cross-Domain-Policies 头的方式来替代 crossdomain.xml 文件，其可选的值有： none master-only by-content-type by-ftp-filename all。Web 服务器对于 HTTP 请求的响应头中缺少 X-Permitted-Cross-Domain-Policies，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 |
| **修复建议** | 1）修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader("X-Permitted-Cross-Domain-Policies", "value") 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header("X-Permitted-Cross-Domain-Policies: value") 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader "X-Permitted-Cross-Domain-Policies", "value" 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response["X-Permitted-Cross-Domain-Policies"] = "value" 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make\_response() response.headers["X-Permitted-Cross-Domain-Policies"] = "value"； 2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add\_header X-Permitted-Cross-Domain-Policies value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add X-Permitted-Cross-Domain-Policies "value"。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### HTTP Content-Security-Policy缺失

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | HTTP Content-Security-Policy缺失 |
| **漏洞描述** | 内容安全策略 (CSP) 是一个额外的安全层，用于检测并削弱某些特定类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击等。无论是数据盗取、网站内容污染还是散发恶意软件，这些攻击都是主要的手段。CSP 的实质就是白名单制度，开发者明确告诉客户端，哪些外部资源可以加载和执行，等同于提供白名单。它的实现和执行全部由浏览器完成，开发者只需提供配置。CSP 大大增强了网页的安全性。攻击者即使发现了漏洞，也没法注入脚本，除非还控制了一台列入了白名单的可信主机。CSP开启可能会导致js、css出现报错。 |
| **修复建议** | 启用 CSP方法：一种是通过 HTTP 头信息的Content-Security-Policy的字段，另一种是通过网页的meta标签。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### HTTP X-Download-Options缺失

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | HTTP X-Download-Options缺失 |
| **漏洞描述** | Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，这将导致浏览器提供的安全特性失效。Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 |
| **修复建议** | 1）修改服务端程序，给 HTTP 响应头加上 X-Download-Options 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader("X-Download-Options", "value") 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header("X-Download-Options: value") 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader "X-Download-Options", "value" 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response["X-Download-Options"] = "value" 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make\_response() response.headers["X-Download-Options"] = "value"； 2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 X-Download-Options 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add\_header X-Download-Options value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add X-Download-Options "value"。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### X-Frame-Options Header未配置

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | X-Frame-Options Header未配置 |
| **漏洞描述** | 弱点描述： X-Frame-Options HTTP响应头可以指示浏览器是否允许当前网页在“frame”或“iframe”标签中显示，以此使网站内容不被其他站点引用和免于点击劫持攻击。 |
| **修复建议** | 一般性的建议： 给您的网站添加X-Frame-Options响应头，赋值有如下三种，1、DENY：无论如何不在框架中显示；2、SAMEORIGIN：仅在同源域名下的框架中显示；3、ALLOW-FROM uri：仅在指定域名下的框架中显示。如Apache修改配置文件添加“Header always append X-Frame-Options SAMEORIGIN”；Nginx修改配置文件“add\_header X-Frame-Options SAMEORIGIN;”。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### 敏感目录

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | 敏感目录 |
| **漏洞描述** | 弱点描述： Web应用程序显露了某些目录名称，此信息可以帮助攻击者对站点进一步的攻击。例如，知道目录之后，攻击者便可能获得目录下边的文件名，也许还能猜出其它的文件名或目录名，并尝试访问它们。这些可能包含敏感信息。攻击者通过搜集信息，以便进一步攻击目标站点。 |
| **修复建议** | 一般性的建议： [1]使用非常规的目录名称。 [2]特定的目录设置合理的权限。 |
| **CVSS 评分** | 3.7 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | upload/ |

### 信息

#### 未加密的连接

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | 未加密的连接 |
| **漏洞描述** | 此扫描目标是通过未加密的连接连接到的。 潜在的攻击者可以拦截和修改从该站点发送和接收的数据。 |
| **修复建议** | 该站点应通过安全 (HTTPS) 连接发送和接收数据。 |
| **CVSS 评分** | 0.0 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

#### 无HTTP重定向

参考信息：

|  |  |
| --- | --- |
| **漏洞名称** | 无HTTP重定向 |
| **漏洞描述** | 检测到您的 Web 应用程序使用 HTTP 协议，但未自动将用户重定向到 HTTPS。 |
| **修复建议** | 建议在您的 Web 应用程序中实施 HTTP 重定向。 |
| **CVSS 评分** | 0.0 |

URL信息：

|  |  |
| --- | --- |
| **漏洞URL** | http://10.10.10.43:8001/ |
| **参考POC** | http://10.10.10.43:8001/ |

1. 漏洞等级评估标准

目前定义有五类风险等级，具体定义依据评分系统CVSS V3.0结合实际可能造成的影响评估：

|  |  |
| --- | --- |
| 风险等级 | 说明 |
| 紧急 | 可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。 |
| 高危 | 被利用之后，造成的影响较大，但直接利用难度较高的漏洞，或本身无法直接攻击，但能为进一步攻击造成极大便利的漏洞 |
| 中危 | 利用难度较高，或满足严格要求才能实现攻击的漏洞，或漏洞本身无法被直接攻击，但能为进一步攻击起较大帮助作用的漏洞 |
| 低危 | 无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞。 |
| 信息 | 本身对网站安全没有直接影响，提供的信息可能为攻击者提供少量帮助，或可用于其他手段的攻击。 |