安恒信息 DAS-SECURITY 安全中国

明鉴®网络安全等级保护检查工具箱

Web 应用漏洞评估报告

目　录

1 任务信息

本报告共扫描评估了 29 个 IP，发现紧急漏洞数 0 个，高危漏洞数 1 个，中危漏洞数 3 个，低危漏洞数 38 个，信息漏洞数 23 个，为了您的资产安全，请及时修复。

任务名称	网站扫描_生态环境
执行方式	立即执行
扫描模板	全部漏洞扫描
扫描范围	扫描当前域
时间统计	开始时间：2024-09-25 13:53:03 结束时间：2024-09-25 14:04:13 扫描耗时：11 分 10 秒
创建者	admin

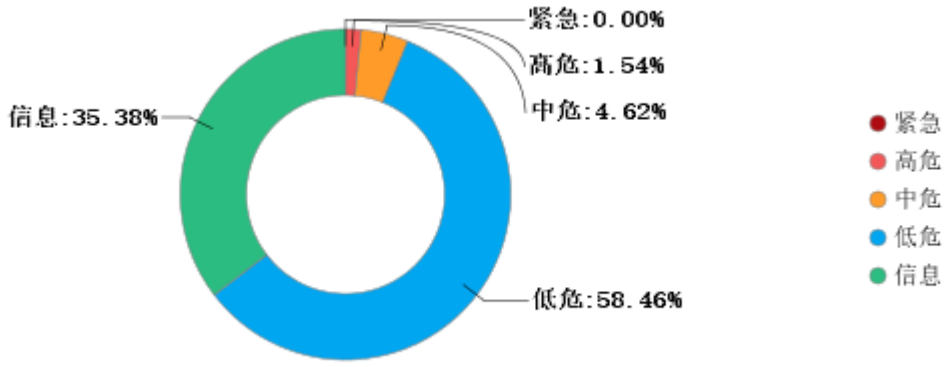
2 风险分布

2.1 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	1	1.54%
中危	3	4.62%
低危	38	58.46%
信息	23	35.38%
漏洞数量总计	65	

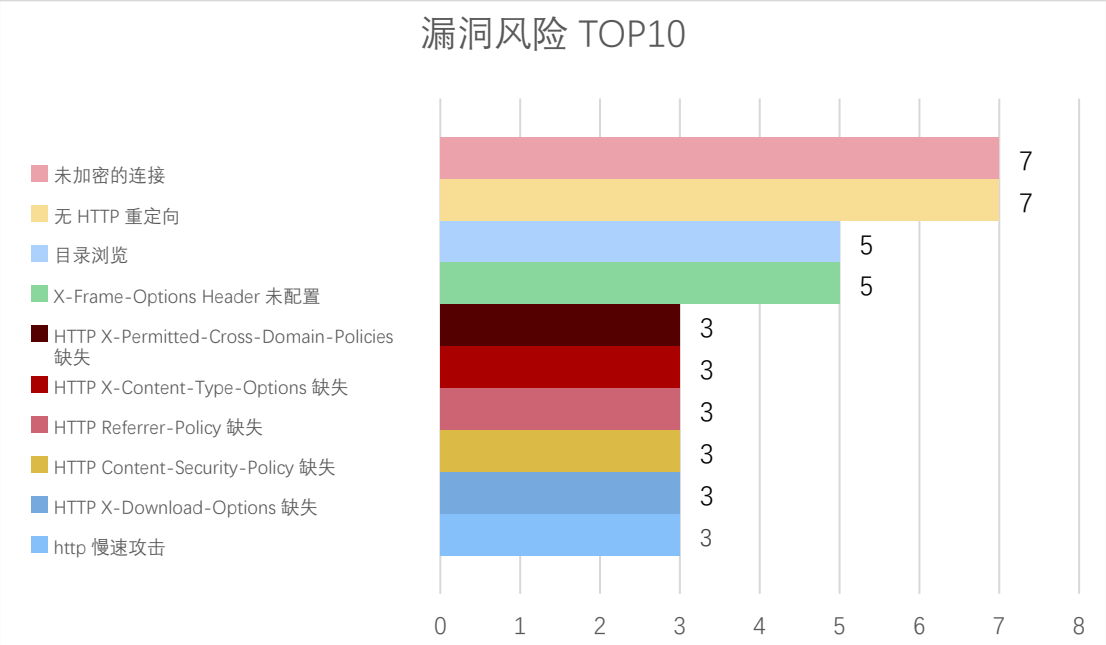
分布占比：



2.2 漏洞名称分布

漏洞名称	数量	是否加 V
跨站脚本	1	否
Web 应用程序错误	1	是
存在漏洞的 JavaScript 库	1	是
会话 Cookie 中缺少 secure 属性	1	是
具有缺失、不一致或矛盾属性的 Cookie	1	是
检测到 Javascript 源码映射文件	1	是
相对路径覆盖(RPO)漏洞	1	是
开启 options 方法	1	是
敏感目录	1	否
内网 IP	1	否
客户端(javascript)cookie 引用	1	否
错误页面 Web 应用服务器版本泄露	2	是
过时的 JavaScript 库	2	否
Content Type 未设置	2	是
http 慢速攻击	3	是
HTTP X-Download-Options 缺失	3	是
HTTP Content-Security-Policy 缺	3	是

失		
HTTP Referrer-Policy 缺失	3	是
HTTP X-Content-Type-Options 缺失	3	是
HTTP X-Permitted-Cross-Domain-Policies 缺失	3	是
HTTP X-XSS-Protection 缺失	3	是
子资源完整性（SRI)未实施	3	是
X-Frame-Options Header 未配置	5	是
目录浏览	5	是
无 HTTP 重定向	7	否
未加密的连接	7	否



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。

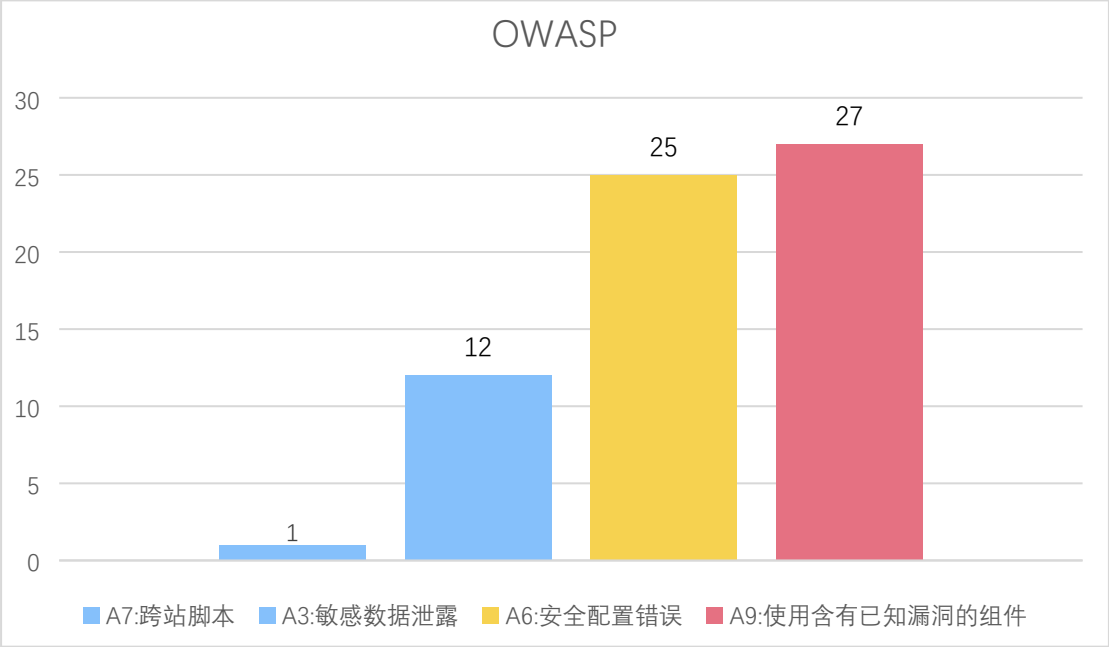
2.3 OWASP 漏洞类型分布

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	12
A4:XML 外部实体	0
A5:失效的访问控制	0
A6:安全配置错误	25
A7:跨站脚本	1
A8:不安全的反序列化	0
A9:使用含有已知漏洞的组件	27
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:



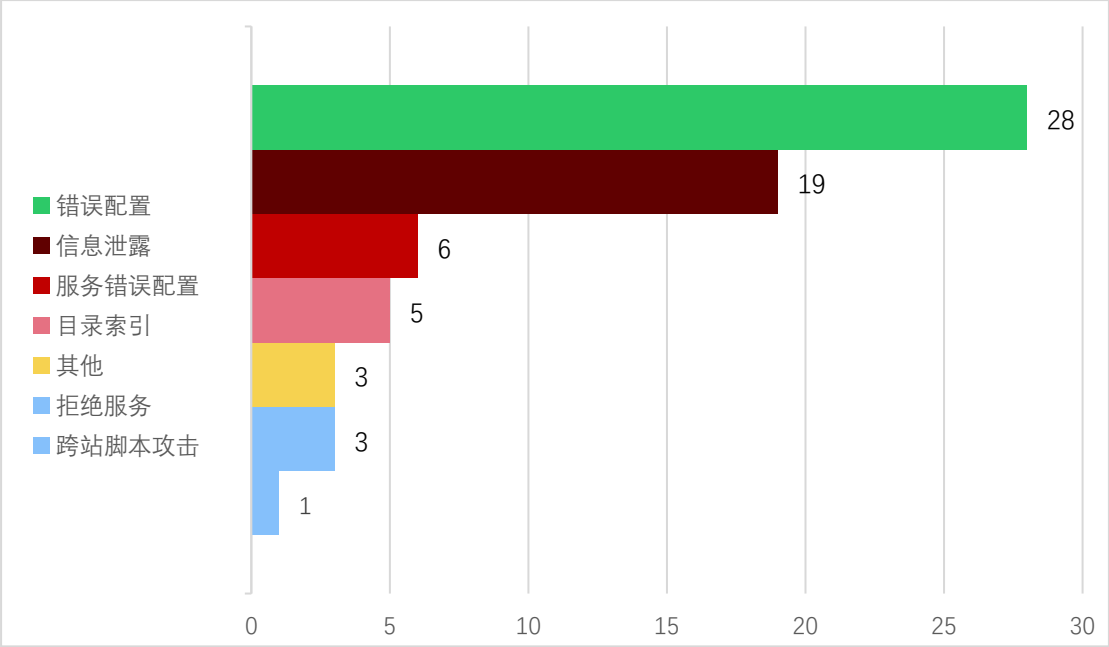
2.4 WASC 风险分布

WASC 风险分布列表:

WASC 分类	漏洞个数
跨站脚本攻击	1

拒绝服务	3
其他	3
目录索引	5
服务错误配置	6
信息泄露	19
错误配置	28

WASC 风险分布图:



3 网站统计列表

网站 URL	紧急	高危	中危	低危	信息	状态
http://124.119.31.167:57801	0	1	0	12	9	可访问
http://124.119.31.167:18080	0	0	1	0	2	可访问
http://124.119.31.167:18666	0	0	1	8	2	可访问
http://124.119.31.167:32769	0	0	1	0	2	可访问
http://124.119.31.167:44011	0	0	0	17	6	可访问

http://124.119.31.167:8888	0	0	0	1	2	可访问
http://124.119.31.167:18081	0	0	0	0	0	不可访问
http://124.119.31.167:32768	0	0	0	0	0	--
http://124.119.31.167:35000	0	0	0	0	0	不可访问
http://124.119.31.167:5003	0	0	0	0	0	不可访问
http://124.119.31.167:57802	0	0	0	0	0	不可访问
http://124.119.31.167:57803	0	0	0	0	0	不可访问
http://124.119.31.167:57804	0	0	0	0	0	不可访问
http://124.119.31.167:57805	0	0	0	0	0	不可访问
http://124.119.31.167:57806	0	0	0	0	0	不可访问
http://124.119.31.167:57807	0	0	0	0	0	不可访问
http://124.119.31.167:57808	0	0	0	0	0	不可访问
http://124.119.31.167:57809	0	0	0	0	0	不可访问
http://124.119.31.167:57810	0	0	0	0	0	不可访问
http://124.119.31.167:57811	0	0	0	0	0	不可访问
http://124.119.31.167:57812	0	0	0	0	0	不可访问
http://124.119.31.167:57813	0	0	0	0	0	不可访问
http://124.119.31.167:57814	0	0	0	0	0	不可访问
http://124.119.31.167:57815	0	0	0	0	0	--
http://124.119.31.167:57816	0	0	0	0	0	不可访问
http://124.119.31.167:57817	0	0	0	0	0	不可访问

http://124.119.31.167:57818	0	0	0	0	0	不可访问
http://124.119.31.167:57819	0	0	0	0	0	不可访问
http://124.119.31.167:57820	0	0	0	0	0	不可访问

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。

4 漏洞统计列表

4.1 漏洞概况

序号	漏洞名称	漏洞数量/漏洞总数	影响页面数
1	跨站脚本	1/65	1
2	http 慢速攻击	3/65	3
3	具有缺失、不一致或矛盾属性的 Cookie	1/65	1
4	会话 Cookie 中缺少 secure 属性	1/65	1
5	目录浏览	5/65	5
6	开启 options 方法	1/65	1
7	检测到 Javascript 源码映射文件	1/65	1
8	HTTP Content-Security-Policy 缺失	3/65	3
9	HTTP Referrer-Policy 缺失	3/65	3
10	HTTP X-Content-Type-Options 缺失	3/65	3
11	HTTP X-Download-Options 缺失	3/65	3
12	HTTP X-Permitted-Cross-Domain-Policies 缺失	3/65	3
13	HTTP X-XSS-Protection 缺失	3/65	3
14	相对路径覆盖(RPO)漏洞	1/65	1

15	敏感目录	1/65	1
16	存在漏洞的 JavaScript 库	1/65	1
17	Web 应用程序错误	1/65	1
18	错误页面 Web 应用服务器版本泄露	2/65	2
19	X-Frame-Options Header 未配置	5/65	5
20	Content Type 未设置	2/65	2
21	内网 IP	1/65	1
22	客户端(javascript)cookie 引用	1/65	1
23	无 HTTP 重定向	7/65	7
24	未加密的连接	7/65	7
25	过时的 JavaScript 库	2/65	2
26	子资源完整性（SRI)未实施	3/65	3

4.2 漏洞详情

4.2.1 高危

4.2.1.1 跨站脚本

参考信息:

漏洞名称	跨站脚本
漏洞描述	跨站脚本（cross-site scripting，XSS）是一种安全攻击，其中，攻击者在看上去来源可靠的链接中恶意嵌入译码。当有人点击链接，嵌入程序作为客户网络要求的一部分提交并且会在用户电脑上执行，一般来说会被攻击者盗取信息。 动态回复包括用户输入数据在内的错误信息这种网络形式使得攻击者可能改变控制结构和/或页面的行为。攻击者用多种方式进行攻击，如通过在论坛信息或垃圾邮件信息链接中嵌入密码。攻击者可能用电邮诈骗假装可信来

	源。 像其它网络攻击一样，如 SQL injection，很多对跨站脚本（cross-site scripting, XSS）的指责都指向引起可能性的不安全应用。动态产生页面的网络服务器应用如果不能确认用户输入并确保产生的页面都正确编码了，他们会易受跨站脚本攻击。能造成跨站脚本的攻击有时候指得是跨站脚本漏洞。 主要危害： [1]获取其他用户 Cookie 中的敏感数据。 [2]屏蔽页面特定信息。 [3]伪造页面信息。 [4]拒绝服务攻击。 [5]突破外网内网不同安全设置。 [6]与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。 参考链接： [1]http://baike.baidu.com/view/2633667.htm
修复建议	一般性的建议：过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User-Agent、Referer、Accept-Language 等，其中危险字符如下： [1] | [2] & [3] ; [4] $ [5] % [6] @ [7] ' [8] " [9] [10] () [11] + [12] CR [13] LF [14] , [15] . [16] script [17] document [18] eval 开发语言的建议：

	[1]严格控制输入： Asp：request Aspx：Request.QueryString、Form、Cookies、SeverVaiables 等 Php：$_GET、$_POST、$_COOKIE、$_SERVER、$_GlOBAL、$_REQUEST 等 Jsp：request.getParameter、request.getCookies 等 客户端提交的变量一般从以上函数获得，严格限制提交的数据长度、类型、字符集。 [2]严格控制输出： HtmlEncode：对一段指定的字符串应用 HTML 编码。 UrlEncode：对一段指定的字符串 URL 编码。 XmlEncode：将在 XML 中使用的输入字符串编码。 XmlAttributeEncode：将在 XML 属性中使用的输入字符串编码。 escape：函数可对字符串进行编码。 decodeURIComponent：返回统一资源标识符的一个已编码组件的非编码形式。 encodeURI：将文本字符串编码为一个有效的统一资源标识符（URI)。
CVSS 评分	8.6

URL 信息：

漏洞 URL	http://124.119.31.167:57801/previewUrl/onlinePreview?url=
参考 POC	注入方式:param ,参数:url ,Payload 值:<iframe src=javascript:alert`77707`>

4.2.2 中危

4.2.2.1 http 慢速攻击

参考信息:

漏洞名称	http 慢速攻击
漏洞描述	Slow HTTP DOS 是一种应用层拒绝服务攻击，主要针对 HTTP 协议，攻击的成本很低，并且能够消耗服务器端资源，占用客户端连接数，导致正常用户无法连接服务器。
修复建议	1.设置适当的超时时间（Apache 默认启用了 reqtimeout 模块），规定请求头和请求体发送的时间以及频率 2.增加 MaxClient （MaxRequestWorkers）：增加最大连接数
CVSS 评分	5.3

URL 信息:

漏洞 URL	http://124.119.31.167:18080/
参考 POC	: 187s

URL 信息:

漏洞 URL	http://124.119.31.167:32769/
参考 POC	: 176s

URL 信息:

漏洞 URL	http://124.119.31.167:18666/
参考 POC	: 194s

4.2.3 低危

4.2.3.1 会话 Cookie 中缺少 secure 属性

参考信息:

漏洞名称	会话 Cookie 中缺少 secure 属性
漏洞描述	弱点描述： 在应用程序测试过程中，检测到所测试的 Web 应用程序设置了不含“secure”属性的会话 cookie。由于此会话 cookie 不包含“secure”属性，所以用户可以通过未加密的 http 协议传输 Cookie,可能造成用户信息被窃听。
修复建议	一般性的建议： [1]基本上，cookie 的唯一必需属性是“name”字段，建议设置“secure”属性，以保证 cookie 的安全。
CVSS 评分	3.7

URL 信息：

漏洞 URL	http://124.119.31.167:44011/vemApi/
参考 POC	http://124.119.31.167:44011/vemApi/

4.2.3.2 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://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

URL 信息：

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息：

漏洞 URL	http://124.119.31.167:57801/

参考 POC	http://124.119.31.167:57801/

4.2.3.3 存在漏洞的 JavaScript 库

参考信息:

漏洞名称	存在漏洞的 JavaScript 库
漏洞描述	您正在使用易受攻击的 JavaScript 库。此版本的库存在一个或多个漏洞。
修复建议	建议升级到最新版本
CVSS 评分	3.7

URL 信息:

漏洞 URL	http://124.119.31.167:44011/static/js/vendor.e480f04d4b67372d0d95.js
参考 POC	组件名称:YUI, :2.9.0，参考链接:http://www.cvedetails.com/cve/CVE-2013-4940/, http://www.cvedetails.com/cve/CVE-2012-5883/, http://www.cvedetails.com/cve/CVE-2012-5882/, http://www.cvedetails.com/cve/CVE-2012-5881/, 漏洞概要:Cross-site scripting (XSS) vulnerability in io.swf / Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.8.0 through 2.9.0 / Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.5.0 through 2.9.0 / TCross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.4.0 through 2.9.0 , CVE 编号:CVE-2013-4940, CVE-2012-5883, CVE-2012-5882, CVE-2012-5881

4.2.3.4 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://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息：

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息：

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

4.2.3.5 开启 options 方法

参考信息：

漏洞名称	开启 options 方法
漏洞描述	弱点描述： Web 服务器配置为允许使用危险的 HTTP 方法，如 PUT、MOVE、COPY、DELETE、PROPFIND、SEARCH、MKCOL、LOCK、UNLOCK、PROPPATCH，该配置可能允许未授权的用户对 Web 服务器进行敏感操作。
修复建议	一般性的建议： [1]如果服务器不需要支持 WebDAV 请禁用 WebDAV，或禁用掉不安全的 HTTP 方法，IIS 在 IIS 服务中的"Web 服务扩展"中关闭 WebDav。
CVSS 评分	3.7

URL 信息：

漏洞 URL	http://124.119.31.167:57801/api/
参考 POC	method_unsafe:GET,HEAD,OPTIONS

4.2.3.6 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://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息:

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

4.2.3.7 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://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息：

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

4.2.3.8 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://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

URL 信息：

漏洞 URL	http://124.119.31.167:8888/error/

参考 POC	http://124.119.31.167:8888/error/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/api/
参考 POC	http://124.119.31.167:57801/api/

4.2.3.9 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://124.119.31.167:57801/preview/
参考 POC	data/

4.2.3.10 目录浏览

参考信息：

漏洞名称	目录浏览
漏洞描述	弱点描述： Web 服务器通常配置成不允许目录列表含有文件名以及目录名。倘若 Web 服务器配置不当，便有可能发送对含有目录名的请求来获得目录列表。比如名称为“files”的目录，那么它的目录列表的访问请求示例如下：http://Website/files/。 攻击者读取上述内容，以便进一步攻击目标站点。 参考链接： [1]http://technet.microsoft.com/zh-cn/library/hh831557.aspx
修复建议	一般性的建议： 在所有 Web 目录中查找目录列表。如有可能，在一个控制整个服务器的配置中禁用目录列表。还可以确保每个目录包含服务器默认提供的 index.html 文件。 [1]Apache 禁止浏览网站目录内容 默认情况下，如果你的网站下有一个文件夹，如果些文件夹下没有默认页面，当用户 http://你的网址/a/即 apache 会把此文件夹中的内容全列出来。如果想禁止此功能，可以有 2 个方法: 1.编译时增加参数–disable-autoindex: ./configure –prefix=/usr/local/httpd2.0.53 \ –disable-autoindex \ –enable-so \ –datadir=/usr/local/Web 2.修改 httpd.conf 找到下面这一句把它注释掉即可 Options Indexes FollowSymLinks 建议默认情况下，设置 APACHE 禁止用户浏览目录内容。 [2]TomCat 禁止浏览网站目录内容 conf/Web.xml 文件:

	<servlet> <servlet-name>default</servlet-name> <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class> <init-param> <param-name>debug</param-name> <param-value>0</param-value> </init-param> <init-param> <param-name>listings</param-name> <param-value>false</param-value> </init-param> <load-on-startup>1</load-on-startup> </servlet> [3]IIS 禁用目录浏览 您可以通过以下方法执行此过程：使用用户界面 (UI)、在命令行窗口中运行 Appcmd.exe 命令、直接编辑配置文件或编写 WMI 脚本。 用户界面 使用 UI: 打开 IIS 管理器，然后导航至您要管理的级别。 在“功能视图”中，双击“目录浏览”。 在“操作”窗格中，如果“目录浏览”功能已启用而您要禁用它，请单击“禁用”。
CVSS 评分	3.7

URL 信息：

漏洞 URL	http://124.119.31.167:44011/file/
参考 POC	http://124.119.31.167:44011/file/

URL 信息：

漏洞 URL	http://124.119.31.167:44011/file/B659004001/2023/05/

参考 POC	http://124.119.31.167:44011/file/B659004001/2023/05/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/file/B659004001/2023/05/01/
参考 POC	http://124.119.31.167:44011/file/B659004001/2023/05/01/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/file/B659004001/
参考 POC	http://124.119.31.167:44011/file/B659004001/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/file/B659004001/2023/
参考 POC	http://124.119.31.167:44011/file/B659004001/2023/

4.2.3.11 相对路径覆盖(RPO)漏洞

参考信息:

漏洞名称	相对路径覆盖(RPO)漏洞
漏洞描述	RPO（Relative Path Overwrite）相对路径覆盖，主要是利用浏览器的一些特性和部分服务端的配置差异导致的漏洞， 攻击者可以利用前端代码中加载的 css/js 的相对路径来加载其他文件，最终浏览器将服务器返回的不是 css/js 的文件当做 css/js 来解析，从而导致 XSS，信息泄露等漏洞产生。
修复建议	建议对静态文件导入使用绝对路径，将 Web 服务器配置为在所有页面上包括 X-Frame-Options：deny 的响应头。
CVSS 评分	3.7

URL 信息:

漏洞 URL	http://124.119.31.167:18666/

参考 POC	http://124.119.31.167:18666/

4.2.3.12 检测到 Javascript 源码映射文件

参考信息:

漏洞名称	检测到 Javascript 源码映射文件
漏洞描述	客户端 Javascript 源代码可以组合、压缩或编译。源码映射文件(source map)是从转换后的源码映射到原始源码的文件，可以帮助攻击者阅读和调试 Javascript。
修复建议	不应允许攻击者访问源码映射文件。
CVSS 评分	3.7

URL 信息:

漏洞 URL	http://124.119.31.167:44011/static/js/manifest.2ae2e69a05c33dfc65f8.js
参考 POC	http://124.119.31.167:44011/static/js/manifest.2ae2e69a05c33dfc65f8.js.map

4.2.3.13 Web 应用程序错误

参考信息:

漏洞名称	Web 应用程序错误
漏洞描述	弱点描述：Web 应用程序在处理访问者的请求时，如果符合 Web 应用程序的逻辑或者 Web 应用程序本身没有异常，那么将结果直接反馈给访问者。如果提交不符合 Web 应用程序逻辑的数据，Web 应用程序在处理这些请求的时候未做相应的处理，直接把 Web 服务器的错误反馈给访问者。
修复建议	一般性的建议: 过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User-Agent、Referer、Accept-Language 等，其中危险字符如下: [1] | [2] & [3] ;

	[4] $ [5] % [6] @ [7] ' [8] " [9] [10] () [11] + [12] CR [13] LF [14] , [15] . 开发语言的建议: [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，那么就该确保该值确实是数字，且在 10..99 范围内。 [4] 验证数据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。
CVSS 评分	3.7

URL 信息:

漏洞 URL	http://124.119.31.167:44011/vemApi/getVerifyCode?rnd=
参考 POC	HTTP CODE : 500

4.2.3.14 错误页面 Web 应用服务器版本泄露

参考信息:

漏洞名称	错误页面 Web 应用服务器版本泄露

漏洞描述	弱点描述： Web 服务器未能正确处理异常请求导致 Web 服务器版本信息泄露，攻击者收集到服务器信息后可进行进一步针对性攻击。
修复建议	一般性的建议： [1]关闭 Web 服务器错误提示。 [2]关闭运行平台的错误提示。 [3]建立错误机制，不要把真实的错误反馈给访问者。
CVSS 评分	3.7

URL 信息：

漏洞 URL	http://124.119.31.167:44011/
参考 POC	Server: nginx/1.16.1

URL 信息：

漏洞 URL	http://124.119.31.167:57801/
参考 POC	Server: nginx/1.10.2

4.2.3.15 具有缺失、不一致或矛盾属性的 Cookie

参考信息：

漏洞名称	具有缺失、不一致或矛盾属性的 Cookie
漏洞描述	cookie 的至少一个属性导致此 cookie 无效、或与此 cookie 的其他属性不兼容、或与此 cookie 的使用环境不兼容。虽然这本身不是漏洞，但它可能会导致应用程序的意外行为，这可能会导致安全问题。
修复建议	确保 cookie 配置符合适用标准。
CVSS 评分	3.1

URL 信息：

漏洞 URL	http://124.119.31.167:57801/api/auth/getVcode?vcodeId=

参考 POC	:1.Cookie without SameSite attribute.

4.2.3.16 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://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息:

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

4.2.3.17 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://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息：

漏洞 URL	http://124.119.31.167:44011/

参考 POC	http://124.119.31.167:44011/

URL 信息:

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

4.2.4 信息

4.2.4.1 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://124.119.31.167:32769/
参考 POC	http://124.119.31.167:32769/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/extendConfig/
参考 POC	http://124.119.31.167:57801/extendConfig/

URL 信息:

漏洞 URL	http://124.119.31.167:8888/
参考 POC	http://124.119.31.167:8888/

URL 信息:

漏洞 URL	http://124.119.31.167:18080/
参考 POC	http://124.119.31.167:18080/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息:

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

4.2.4.2 客户端(javascript)cookie 引用

参考信息:

漏洞名称	客户端(javascript)cookie 引用
漏洞描述	在应用程序测试过程中，检测到 JavaScript 中对 cookie 的引用。
修复建议	项目中尽量不要有 cookie 的操作。
CVSS 评分	0.0

URL 信息:

漏洞 URL	http://124.119.31.167:57801/api/static/js/chunk-libs.561210c3.js
参考 POC	http://124.119.31.167:57801/api/static/js/chunk-libs.561210c3.js

4.2.4.3 Content Type 未设置

参考信息:

漏洞名称	Content Type 未设置
漏洞描述	此页面未设置 Content-Type 标头值。这个值通知浏览器期望什么样的数据。如果缺少此标头，浏览器可能会错误地处理数据。这可能会导致安全问题。

修复建议	为此页面设置 Content-Type 标头值。
CVSS 评分	0.0

URL 信息:

漏洞 URL	http://124.119.31.167:44011/vemApi/getVerifyCode
参考 POC	http://124.119.31.167:44011/vemApi/getVerifyCode

URL 信息:

漏洞 URL	http://124.119.31.167:44011/vemApi/getVerifyCode?rnd=
参考 POC	http://124.119.31.167:44011/vemApi/getVerifyCode?rnd=

4.2.4.4 子资源完整性（SRI)未实施

参考信息:

漏洞名称	子资源完整性（SRI)未实施
漏洞描述	子资源完整性（SRI）是一项安全功能，使浏览器能够验证它们获取的第三方资源（例如，从 CDN）是否在没有意外操作的情况下交付。它的工作原理是允许开发人员提供获取的文件必须匹配的加密哈希，可以操作第三方资源（例如脚本和样式表）。有权访问或入侵托管 CDN 的攻击者可以操纵或替换文件。 SRI 允许开发人员指定要加载的资源的 base64 编码的加密哈希。然后将包含散列的完整性属性添加到 <script> HTML 元素标签。完整性字符串由 base64 编码的哈希组成，后跟取决于哈希算法的前缀。此前缀可以是 sha256、sha384 或 sha512。建议为从外部主机加载的所有脚本实施子资源完整性（SRI)。
修复建议	使用 SRI Hash Generator 链接生成实现子资源完整性(SRI) 的 <script> 元素。例如，您可以使用以下 <script> 元素告诉浏览器在执行 https://example.com/example-framework.js 脚本之前，浏

	览器必须首先将脚本与预期的哈希值进行比较，并验证是否匹配。 <script src="https://example.com/example-framework.js"integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>
CVSS 评分	0.0

URL 信息:

漏洞 URL	http://124.119.31.167:57801/index.html
参考 POC	http://124.119.31.167:57801/index.html

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

4.2.4.5 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://124.119.31.167:32769/
参考 POC	http://124.119.31.167:32769/

URL 信息:

漏洞 URL	http://124.119.31.167:8888/
参考 POC	http://124.119.31.167:8888/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/
参考 POC	http://124.119.31.167:57801/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/extendConfig/
参考 POC	http://124.119.31.167:57801/extendConfig/

URL 信息:

漏洞 URL	http://124.119.31.167:18080/
参考 POC	http://124.119.31.167:18080/

URL 信息:

漏洞 URL	http://124.119.31.167:18666/
参考 POC	http://124.119.31.167:18666/

URL 信息:

漏洞 URL	http://124.119.31.167:44011/
参考 POC	http://124.119.31.167:44011/

4.2.4.6 过时的 JavaScript 库

参考信息:

漏洞名称	过时的 JavaScript 库
漏洞描述	您使用的是过时版本的 JavaScript 库，该库已有最新版本。尽管未发现您的版本受到任何安全漏洞的影响，但建议使库保持最新。
修复建议	建议升级到最新版本
CVSS 评分	0.0

URL 信息:

漏洞 URL	http://124.119.31.167:44011/static/js/vendor.e480f04d4b67372d0d95.js
参考 POC	组件名称:jQuery, :3.5.1，参考链接:https://code.jquery.com/

URL 信息:

漏洞 URL	http://124.119.31.167:57801/api/static/js/chunk-libs.561210c3.js
参考 POC	组件名称:Vue.js, :2.6.12，参考链接:https://github.com/vuejs/vue/releases

4.2.4.7 内网 IP

参考信息:

漏洞名称	内网 IP
漏洞描述	弱点描述: Web 应用程序中错误消息或者代码注释中含有内部 IP 地址，它可能反映了内部网络的 IP 地址规划方案。可以辅助攻击者策划出对内部网络进一步的攻击。
修复建议	一般性的建议: [1]关闭 Web 服务器错误提示。 [2]确保代码注释中不含有 ip 地址。
CVSS 评分	0.0

URL 信息:

漏洞 URL	http://124.119.31.167:57801/js/app.3abf7338.js
参考 POC	192.168.9.82,

附录 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。