



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。

International Standard - ISO 27002 报告

该报告由 HCL AppScan Standard 创建 10.0.0, 规则: 0
扫描开始时间: 2023/12/22 17:50:40

条例

International Standard - ISO 27002

Summary Description

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization.

National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

ISO 27002 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Information security is achieved by implementing a suitable set of controls, such as: policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed, improved and reported on to ensure that the specific security and business objectives of the organization are met.

ISO 27002 is intended to serve as a single reference point for identifying a range of controls required for industry and commerce systems and for developing organizational security standards, effective security management practices and to help build confidence in inter-organizational activities.

Covered Information

ISO27002 is organized into eleven major sections, each covering a different topic or area:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance

- 9.Information Security Incident Management
- 10.Business Continuity Management
- 11.Compliance

HCL AppScan's ISO 27002 Solution

HCL AppScan's ISO 27002 solution helps detect existing web application vulnerabilities that violate this standard's control objectives and which existence in the web application can mean inappropriate implementation of the controls set out in this standard.

Covered Entities

All companies and other entities are encouraged to adopt the standard and start the process of improving information security management within the organization.

Effective Date

Latest version - June 2005

For more information on securing web applications, please visit <https://www.hcltechsw.com/wps/portal/products/appscan/offerings/websecurity/>

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. HCL customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

违反部分

在规则的 24/28 个部分中检测到问题:

部分	问题的数量
6.2.1 - The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.	321

6.2.2 d)1) - The Access control policy should cover the permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;	10
6.2.2 d)2) - The Access control policy should include an authorization process for user access and privileges.	8
8.3.3 - The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement or adjusted upon change.	7
10.3.1 - The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	5
10.8.1 a) - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: procedures designed to protect exchanged information from interception, copying, modification, misrouting, and destruction.	32 3
10.8.1 b) - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications.	17
10.8.1 g) - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: use of cryptographic techniques to protect the confidentiality, integrity and authenticity of information.	7
10.9.1 a) - Security considerations for electronic commerce should include the level of confidence each party requires in each others claimed identity, e.g. through authentication.	7
10.9.1 h) - Security considerations for electronic commerce should include the degree of verification appropriate to check payment information supplied by a customer	10
10.9.2 c) - Security considerations for online transactions should include encrypted communications path between all involved parties	0
10.9.3 - The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification	11
11.2.2 - The allocation and use of privileges should be restricted and controlled.	8
11.2.3 - The allocation of passwords should be controlled through a formal management process.	1
11.2.4 - Management should review user's access rights at regular intervals using a formal process.	7
11.4.2 - Appropriate authentication methods should be used to control access by remote users.	7
11.5.2 - All users should have a unique identifier for their personal use only, and suitable authentication technique should be chosen to substantiate the claimed identity of a user.	7
11.5.5 - Inactive sessions should shut down after a defined period of inactivity.	0
11.5.6 - Restriction on connection times should be used to provide additional security for high-risk applications.	0
11.6.1 - Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.	8
12.2.1 - Data input to applications should be validated to ensure that this data is correct and appropriate.	41
12.2.2 - Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	41
12.2.3 - Requirements for ensuring authenticity and protecting message integrity in applications should be identified and appropriate controls identified and implemented.	8
12.3.1 - A policy on the use of cryptographic controls for protection of information should be developed and implemented.	0
12.4.3 - Access to program source code should be restricted.	31 3
12.5.4 - Opportunities for information leakage should be prevented.	31 3
15.1.3 - Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	22 9
15.1.4 - Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	7

部分违例（按问题）

在规则的 24/28 个部分中检测到 326 个唯一问题：

URL	实体	问题类型	部分
http://192.168.13.3.196/home/login/lock.html	lock.html	“Content-Security-Policy”头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/login/index.html	index.html	“X-Content-Type-Options”头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/login/index.html	index.html	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/home/index/main.html	main.html	不安全的第三方链接 (target="_blank")	6.2.1
http://192.168.13.3.196/home/login/lock.html	lock.html	“X-Content-Type-Options”头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/login/lock.html	lock.html	“X-XSS-Protection”头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/login/lock.html	lock.html	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/home/login/index.html	layui.use(['form'], function() {var form = layui.form,\$ = layui.\$,layer = layui.layer;// {U i...	客户端（JavaScript）Cookie 引用	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/login/index.html	index.html	“Content-Security-Policy”头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/		“X-XSS-Protection”头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/index	limit	整数溢出	10.3.1, 10.8.1 a), 10.8.1 b), 12.2.1, 12.2.2, 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/oa/plan/calendar	calendar	查询中接受的主体参数	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/login	index.html	“X-XSS-Protection”头缺失	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

/index.html		或不安全	
http://192.168.13.196/home/login/lock.html	lock_password	查询中的密码参数	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/flow_type	flow_type	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.196/		不安全的第三方链接 (target="_blank")	6.2.1
http://192.168.13.196/		"Content-Security-Policy"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/personal/leave	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/list	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/		"X-Content-Type-Options"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/user/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/		发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.196/home/api/get_article_list	get_article_list	"Content-Security-Policy"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/api/get_article_list	get_article_list	"X-Content-Type-Options"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/api/get_article_list	get_article_list	"X-XSS-Protection"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/personal/change	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/static/assets/gougou/module/admin.js	layui.define(['element'], function (exports) {	客户端 (JavaScript) Cookie 引用	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/home/api/get_view_log	get_view_log	"Content-Security-Policy"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/user/index	limit	整数溢出	10.3.1, 10.8.1 a), 10.8.1 b), 12.2.1, 12.2.2, 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/api/get_view_log	get_view_log	"X-Content-Type-Options"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/api/get_view_log	get_view_log	"X-XSS-Protection"头缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

http://192.168.13.3.196/home/api/get_article_list	get_article_list	跨站点请求伪造	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.3.196/home/cate/expense_cate_check	expense_cate_check	查询中接受的主体参数	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/api/log_list	log_list	发现内部 IP 泄露模式	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/calendar	calendar	查询中接受的主体参数	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/api/log_list	log_list	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/home/index/index	index	跨帧脚本编制防御缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/api/get_note_list	get_note_list	跨站点请求伪造	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.3.196/home/index/main.html	main.html	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/api/index/get_department_select	get_department_select	跨站点请求伪造	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.3.196/home/flow/add	add	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_check	expense_cate_check	跨站点请求伪造	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.3.196/oa/plan/calendar	uid	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/user/user/index	index	发现电子邮件地址模式	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/copy	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/user/user/index	index	发现内部 IP 泄露模式	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/calendar	calendar	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/home/api/log_list	log_list	JSON 中反映的未清理用户输入	6.2.1, 6.2.2 d)1), 10.8.1 a), 10.8.1 b), 10.9.1 h), 10.9.3, 12.2.1, 12.2.2, 15.1.3

http://192.168.13.3.196/static/assets/layui/layui.js	layui.js	发现可能的服务器路径泄露模式	6.2.1, 10.8.1 a), 10.8.1 b), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/flow_type_check	id	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/flow_type_check	status	整数溢出	10.3.1, 10.8.1 a), 10.8.1 b), 12.2.1, 12.2.2, 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/flow_type_check	status	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/api/index/get_department_select	keyword	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_added	title	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_check	status	整数溢出	10.3.1, 10.8.1 a), 10.8.1 b), 12.2.1, 12.2.2, 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/expense_cate_added	id	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_check	id	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_check	status	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/finance/invoice/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/oa/work/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/oa/schedule/calendar	uid	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/oa/schedule/calendar	end	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/oa/plan/calendar	end	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.3.196/oa/plan/calendar	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4

3.196/oa/schedule/index			12.5.4
http://192.168.13.196/oa/plan/calendar	start	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/oa/schedule/calendar	start	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/oa/work/index	send	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/finance/income/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/finance/expense/index	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/home/login/lock.html	lock.html	跨站点请求伪造	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.196/home/api/log_list	limit	整数溢出	10.3.1, 10.8.1 a), 10.8.1 b), 12.2.1, 12.2.2, 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/api/log_list	limit	JSON 中反映的未清理用户输入	6.2.1, 6.2.2 d)1), 10.8.1 a), 10.8.1 b), 10.9.1 h), 10.9.3, 12.2.1, 12.2.2, 15.1.3
http://192.168.13.196/home/api/log_list	limit	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/user/department/	department.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/adm/seal/	seal.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/schedule/	schedule.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/cate/	cate.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/approve/	approve.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/keywords/	keywords.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/department/	department.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/flow/	flow.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/department/	department.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

http://192.168.13.3.196/home/keywords/	keywords.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/	home.ar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	department.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/	home.ear	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	keywords.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	department.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	keywords.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	keywords.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	department.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/customer/	customer/	检测到隐藏目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/	home.tar.lzma	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/	home.war	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/	home.wim	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	keywords.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

3.196/home/keyw ords/			
http://192.168.13.3.196/home/cate/	cate.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
<a href="http://192.168.13.3.196/home/keyw
ords/">http://192.168.13.3.196/home/keyw ords/	keywords.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	department.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
<a href="http://192.168.13.3.196/home/keyw
ords/">http://192.168.13.3.196/home/keyw ords/	keywords.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	department.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keyw	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

ords/			
http://192.168.13.3.196/user/user/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	user.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	keywords.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/department/	department.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	user.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/flow/	flow.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/keywords/	keywords.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/cate/	cate.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

http://192.168.13.196/user/department/	department.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/flow/	flow.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/schedule/	schedule.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/user/	user.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/position/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/personal/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/position/	position.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/position/	position.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/personal/	personal.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/work/	work.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/user/	user.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/plan/	plan.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/personal/	personal.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/user/	user.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/personal/	personal.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/user/position/	position.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/schedule/	schedule.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/approve/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/schedule/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/adm/meeting/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

http://192.168.13.3.196/user/user/	user.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	user.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	user.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	income.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	user.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/user/	user.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

http://192.168.13.3.196/oa/approve/	approve.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/personal/	personal.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/approve/	approve.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

3.196/oa/approve/			
http://192.168.13.3.196/oa/schedule/	schedule.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/seal/	seal.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/adm/meeting/	meeting.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/user/position/	position.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/	/	启用了不安全的“OPTIONS”HTTP方法	6.2.1, 10.8.1 a), 10.8.1 b), 10.9.3, 12.2.1, 12.2.2, 15.1.3
http://192.168.13.3.196/adm/seal/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/install/	install/	检测到隐藏目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/home/	home/	检测到隐藏目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	sqlnet.log	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	sqlnet.trc	Oracle 日志文件信息泄露	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/	schedule.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/	schedule.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

http://192.168.13.3.196/oa/work/	work.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/	schedule.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	expense.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	income.zip	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/	schedule.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/plan/	plan.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	expense.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	income.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/schedule/	schedule.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	expense.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/oa/work/	work.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	income.rar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	expense.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/income/	income.ace	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	expense.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.3.196/finance/expense/	expense.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

ense/			
http://192.168.13.196/finance/income/	income.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/expense/	expense.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/income/	income.tar	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/expense/	expense.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/income/	income.arj	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/expense/	expense.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/income/	income.arc	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/income/	income.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/finance/expense/	expense.tar.gz	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/work/	work.lha	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/oa/schedule/	schedule.lzh	发现压缩目录	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/cate/flow_type	flow_type	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/flow_type	flow_type	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/expense_cate_check	expense_cate_check	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/expense_cate	expense_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/expense_cate	expense_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/flow_type_check	flow_type_check	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/cate/flow_type_check	flow_type_check	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4

http://192.168.13.3.196/home/flow/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/flow/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_add	expense_cate_add	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_add	expense_cate_add	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/work_cate	work_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/cost_cate	cost_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/expense_cate_check	expense_cate_check	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/cost_cate	cost_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/subject	subject	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/work_cate	work_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/industry_cate	industry_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/subject	subject	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/user/department/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/user/personal/change	change	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/industry_cate	industry_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/services_cate	services_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/services_cate	services_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.3.196/home/cate/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4

http://192.168.13.196/home/keywords/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/keywords/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/adm/seal/seal_cate	seal_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/department/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/position/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/personal/leave	leave	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/position/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/user/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/schedule/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/adm/meeting/meeting_cate	meeting_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/copy	copy	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/user/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/personal/change	change	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/list	list	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/user/personal/leave	leave	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/adm/seal/seal_cate	seal_cate	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/adm/meeting	meeting_cate	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4

ng/meeting_cate			
http://192.168.13.196/oa/work/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/list	list	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/approve/copy	copy	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/plan/calendar	calendar	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/plan/calendar	calendar	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/work/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/oa/schedule/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/finance/expense/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/finance/expense/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/login/login_submit	login_submit	跨站点请求伪造	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.196/finance/income/index	index	归档文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/finance/income/index	index	临时文件下载	6.2.1, 10.8.1 a), 12.4.3, 12.5.4
http://192.168.13.196/home/login/login_submit	login_submit	查询中接受的主体参数	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3
http://192.168.13.196/home/login/login_submit	password	不充分帐户封锁	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 10.9.1 h), 10.9.3, 11.2.2, 11.6.1, 12.2.1, 12.2.2, 12.2.3, 15.1.3
http://192.168.13.196/home/login/login_submit	password	应用程序错误	6.2.1, 10.8.1 a), 12.2.1, 12.2.2, 12.4.3, 12.5.4
http://192.168.13.196/home/login/lock.html	lock.html	使用 HTTP 动词篡改的认证旁路	6.2.1, 6.2.2 d)1), 6.2.2 d)2), 8.3.3, 10.8.1 a), 10.8.1 g), 10.9.1 a), 10.9.1 h), 10.9.3, 11.2.2, 11.2.3, 11.2.4, 11.4.2, 11.5.2, 11.6.1, 12.2.1, 12.2.2, 12.2.3, 15.1.3, 15.1.4
http://192.168.13.196/home/login/lock.html	lock.html	跨帧脚本编制防御缺失或不安全	6.2.1, 10.8.1 a), 12.4.3, 12.5.4, 15.1.3

详细的安全性问题（按部分）

高

6.2.1 - The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. 321

查询中的密码参数

风险: 可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

原因: 查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

固定值: 发送敏感信息时，始终使用 **SSL** 和 **POST**（主体）参数。

CVSS 分数: 8.5

严重性

URL

实体

高

<http://192.168.133.196/home/login/lock.htm>

lock_password

不充分帐户封锁

风险: 可能会升级用户特权并通过 **Web** 应用程序获取管理许可权

原因: **Web** 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性

URL

实体

中

http://192.168.133.196/home/login/login_sbmit

password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

“Content-Security-Policy”头缺失或不安全

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: 将服务器配置为使用安全策略的“Content-Security-Policy”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-Content-Type-Options”头缺失或不安全

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: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-XSS-Protection”头缺失或不安全

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: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

Oracle 日志文件信息泄露

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 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: 关闭跟踪，限制对日志文件的访问，或者将其除去

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/finance/expense/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.log
低	http://192.168.133.196/adm/seal/	sqlnet.log
低	http://192.168.133.196/adm/meeting/	sqlnet.log
低	http://192.168.133.196/oa/approve/	sqlnet.trc
低	http://192.168.133.196/oa/work/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.log
低	http://192.168.133.196/home/flow/	sqlnet.log
低	http://192.168.133.196/user/position/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.trc
低	http://192.168.133.196/home/flow/	sqlnet.trc
低	http://192.168.133.196/user/personal/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.trc
低	http://192.168.133.196/finance/expense/	sqlnet.trc
低	http://192.168.133.196/user/position/	sqlnet.log
低	http://192.168.133.196/user/personal/	sqlnet.trc
低	http://192.168.133.196/oa/approve/	sqlnet.log
低	http://192.168.133.196/oa/schedule/	sqlnet.trc
低	http://192.168.133.196/adm/meeting/	sqlnet.trc
低	http://192.168.133.196/adm/seal/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.trc

低	http://192.168.133.196/oa/schedule/	sqlnet.log
低	http://192.168.133.196/oa/work/	sqlnet.trc
低	http://192.168.133.196/finance/income/	sqlnet.log
低	http://192.168.133.196/finance/income/	sqlnet.trc

不安全的第三方链接 (target="_blank")

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: 链接元素中的 rel 属性未设置为“noopener noreferrer”。

固定值: 将属性 rel = "noopener noreferrer" 添加到带有 target="_blank" 的每个元素

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/index/main.html	main.html
低	http://192.168.133.196/	

查询中接受的主体参数

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/oa/schedule/calendar	calendar
低	http://192.168.133.196/home/login/login_submit	login_submit

发现压缩目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/user/department/	department.arc
低	http://192.168.133.196/adm/seal/	seal.rar
低	http://192.168.133.196/oa/schedule/	schedule.zip
低	http://192.168.133.196/home/cate/	cate.tar.gz
低	http://192.168.133.196/oa/approve/	approve.tar
低	http://192.168.133.196/home/keywords/	keywords.lzh
低	http://192.168.133.196/user/department/	department.lha
低	http://192.168.133.196/home/flow/	flow.tar.gz
低	http://192.168.133.196/user/department/	department.lzh
低	http://192.168.133.196/home/keywords/	keywords.tar
低	http://192.168.133.196/home/	home.ar
低	http://192.168.133.196/user/department/	department.tar
低	http://192.168.133.196/home/	home.ear
低	http://192.168.133.196/home/keywords/	keywords.arj
低	http://192.168.133.196/user/department/	department.arj
低	http://192.168.133.196/home/keywords/	keywords.arc
低	http://192.168.133.196/home/keywords/	keywords.tar.gz
低	http://192.168.133.196/user/department/	department.tar.gz
低	http://192.168.133.196/user/position/	position.zip
低	http://192.168.133.196/home/	home.tar.lzma
低	http://192.168.133.196/home/	home.war
低	http://192.168.133.196/home/	home.wim
低	http://192.168.133.196/home/cate/	cate.zip
低	http://192.168.133.196/user/position/	position.gz
低	http://192.168.133.196/home/flow/	flow.zip

低	http://192.168.133.196/user/position/	position.rar
低	http://192.168.133.196/home/keywords/	keywords.zip
低	http://192.168.133.196/home/cate/	cate.gz
低	http://192.168.133.196/home/flow/	flow.gz
低	http://192.168.133.196/home/cate/	cate.rar
低	http://192.168.133.196/home/flow/	flow.rar
低	http://192.168.133.196/home/cate/	cate.ace
低	http://192.168.133.196/home/flow/	flow.ace
低	http://192.168.133.196/home/cate/	cate.lha
低	http://192.168.133.196/home/flow/	flow.lha
低	http://192.168.133.196/home/cate/	cate.lzh
低	http://192.168.133.196/oa/plan/	plan.gz
低	http://192.168.133.196/home/keywords/	keywords.gz
低	http://192.168.133.196/user/position/	position.lzh
低	http://192.168.133.196/home/flow/	flow.lzh
低	http://192.168.133.196/user/department/	department.zip
低	http://192.168.133.196/home/keywords/	keywords.rar
低	http://192.168.133.196/home/cate/	cate.tar
低	http://192.168.133.196/user/department/	department.gz
低	http://192.168.133.196/user/user/	user.zip
低	http://192.168.133.196/home/flow/	flow.tar
低	http://192.168.133.196/home/keywords/	keywords.ace
低	http://192.168.133.196/home/cate/	cate.arj
低	http://192.168.133.196/user/position/	position.tar
低	http://192.168.133.196/user/department/	department.rar
低	http://192.168.133.196/user/user/	user.gz
低	http://192.168.133.196/home/flow/	flow.arj
低	http://192.168.133.196/home/keywords/	keywords.lha
低	http://192.168.133.196/home/cate/	cate.arc
低	http://192.168.133.196/user/department/	department.ace
低	http://192.168.133.196/home/flow/	flow.arc
低	http://192.168.133.196/oa/schedule/	schedule.gz

低	http://192.168.133.196/user/user/	user.rar
低	http://192.168.133.196/user/position/	position.lha
低	http://192.168.133.196/user/position/	position.arj
低	http://192.168.133.196/user/personal/	personal.zip
低	http://192.168.133.196/oa/work/	work.zip
低	http://192.168.133.196/user/user/	user.ace
低	http://192.168.133.196/oa/plan/	plan.rar
低	http://192.168.133.196/user/personal/	personal.gz
低	http://192.168.133.196/user/user/	user.lha
低	http://192.168.133.196/user/personal/	personal.rar
低	http://192.168.133.196/user/position/	position.arc
低	http://192.168.133.196/oa/schedule/	schedule.rar
低	http://192.168.133.196/user/user/	user.lzh
低	http://192.168.133.196/adm/seal/	seal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.lha
低	http://192.168.133.196/oa/approve/	approve.arj
低	http://192.168.133.196/oa/work/	work.gz
低	http://192.168.133.196/user/personal/	personal.ace
低	http://192.168.133.196/oa/plan/	plan.ace
低	http://192.168.133.196/user/position/	position.tar.gz
低	http://192.168.133.196/user/user/	user.tar
低	http://192.168.133.196/user/personal/	personal.lha
低	http://192.168.133.196/user/user/	user.arj
低	http://192.168.133.196/user/personal/	personal.lzh
低	http://192.168.133.196/finance/income/	income.lha
低	http://192.168.133.196/user/personal/	personal.tar
低	http://192.168.133.196/oa/approve/	approve.arc
低	http://192.168.133.196/user/user/	user.arc
低	http://192.168.133.196/user/user/	user.tar.gz
低	http://192.168.133.196/user/personal/	personal.arj
低	http://192.168.133.196/adm/seal/	seal.zip
低	http://192.168.133.196/adm/meeting/	meeting.tar

低	http://192.168.133.196/user/personal/	personal.arc
低	http://192.168.133.196/oa/approve/	approve.tar.gz
低	http://192.168.133.196/adm/seal/	seal.gz
低	http://192.168.133.196/user/personal/	personal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.zip
低	http://192.168.133.196/oa/approve/	approve.zip
低	http://192.168.133.196/adm/meeting/	meeting.gz
低	http://192.168.133.196/adm/meeting/	meeting.arj
低	http://192.168.133.196/adm/seal/	seal.ace
低	http://192.168.133.196/adm/meeting/	meeting.arc
低	http://192.168.133.196/oa/approve/	approve.gz
低	http://192.168.133.196/adm/meeting/	meeting.rar
低	http://192.168.133.196/adm/seal/	seal.lha
低	http://192.168.133.196/oa/approve/	approve.rar
低	http://192.168.133.196/adm/meeting/	meeting.tar.gz
低	http://192.168.133.196/oa/approve/	approve.ace
低	http://192.168.133.196/adm/seal/	seal.lzh
低	http://192.168.133.196/oa/work/	work.rar
低	http://192.168.133.196/adm/seal/	seal.tar
低	http://192.168.133.196/oa/approve/	approve.lha
低	http://192.168.133.196/adm/seal/	seal.arj
低	http://192.168.133.196/oa/approve/	approve.lzh
低	http://192.168.133.196/oa/schedule/	schedule.ace
低	http://192.168.133.196/adm/seal/	seal.arc
低	http://192.168.133.196/oa/plan/	plan.lha
低	http://192.168.133.196/adm/meeting/	meeting.ace
低	http://192.168.133.196/adm/meeting/	meeting.lzh
低	http://192.168.133.196/user/position/	position.ace
低	http://192.168.133.196/oa/plan/	plan.zip
低	http://192.168.133.196/oa/work/	work.ace
低	http://192.168.133.196/oa/schedule/	schedule.lha
低	http://192.168.133.196/oa/plan/	plan.lzh

低	http://192.168.133.196/oa/plan/	plan.tar
低	http://192.168.133.196/oa/schedule/	schedule.tar
低	http://192.168.133.196/oa/work/	work.lzh
低	http://192.168.133.196/oa/plan/	plan.arj
低	http://192.168.133.196/oa/work/	work.tar
低	http://192.168.133.196/oa/schedule/	schedule.arj
低	http://192.168.133.196/oa/plan/	plan.arc
低	http://192.168.133.196/finance/expense/	expense.zip
低	http://192.168.133.196/finance/income/	income.zip
低	http://192.168.133.196/oa/schedule/	schedule.arc
低	http://192.168.133.196/oa/work/	work.arj
低	http://192.168.133.196/oa/plan/	plan.tar.gz
低	http://192.168.133.196/finance/expense/	expense.gz
低	http://192.168.133.196/finance/income/	income.gz
低	http://192.168.133.196/oa/work/	work.arc
低	http://192.168.133.196/oa/schedule/	schedule.tar.gz
低	http://192.168.133.196/finance/expense/	expense.rar
低	http://192.168.133.196/oa/work/	work.tar.gz
低	http://192.168.133.196/finance/income/	income.rar
低	http://192.168.133.196/finance/expense/	expense.ace
低	http://192.168.133.196/finance/income/	income.ace
低	http://192.168.133.196/finance/expense/	expense.lha
低	http://192.168.133.196/finance/expense/	expense.lzh
低	http://192.168.133.196/finance/income/	income.lzh
低	http://192.168.133.196/finance/expense/	expense.tar
低	http://192.168.133.196/finance/income/	income.tar
低	http://192.168.133.196/finance/expense/	expense.arj
低	http://192.168.133.196/finance/income/	income.arj
低	http://192.168.133.196/finance/expense/	expense.arc
低	http://192.168.133.196/finance/income/	income.arc
低	http://192.168.133.196/finance/income/	income.tar.gz
低	http://192.168.133.196/finance/expense/	expense.tar.gz

低	http://192.168.133.196/oa/work/	work.lha
低	http://192.168.133.196/oa/schedule/	schedule.lzh

归档文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/user/personal/leave	leave
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate

低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

检测到隐藏目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/customer/	customer/
低	http://192.168.133.196/install/	install/
低	http://192.168.133.196/home/	home/

跨帧脚本编制防御缺失或不安全

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: 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/index/index	index
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/	

临时文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/user/personal/leave	leave

低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: 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: 禁用 WebDAV，或者禁止不需要的 HTTP 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

发现电子邮件地址模式

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/user/user/index	index

发现可能的服务器路径泄露模式

风险: 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修补程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	index.html
参考	http://192.168.133.196/home/login/lock.html	lock.html
参考	http://192.168.133.196/home/cate/flow_type	flow_type
参考	http://192.168.133.196/	
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/index/main.html	main.html
参考	http://192.168.133.196/home/flow/add	add
参考	http://192.168.133.196/oa/plan/calendar	calendar
参考	http://192.168.133.196/static/assets/layui/layui.js	layui.js

发现内部 IP 泄露模式

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 站点中的内部 IP 地址

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/user/user/index	index

客户端（JavaScript）Cookie 引用

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

CVSS 分数: 0.0

严重性

URL

实体

参考

<http://192.168.133.196/home/login/index.html>

layui.use(['form'], function() {var form = layui.
i.form,\$ = layui.\$,layer = layui.layer;// {U
i...

参考

<http://192.168.133.196/static/assets/gougu/module/admin.js>

layui.define(['element'], function (exports) {

应用程序错误		
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	
CVSS 分数:	0.0	
严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/oa/approve/index	limit
参考	http://192.168.133.196/user/personal/leave	limit
参考	http://192.168.133.196/oa/approve/list	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/user/personal/change	limit
参考	http://192.168.133.196/oa/plan/calendar	uid
参考	http://192.168.133.196/oa/approve/copy	limit
参考	http://192.168.133.196/home/cate/flow_type_check	id
参考	http://192.168.133.196/oa/plan/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/api/index/get_department_select	keyword
参考	http://192.168.133.196/home/cate/expense_cate_add	title
参考	http://192.168.133.196/home/cate/expense_cate_add	id
参考	http://192.168.133.196/home/cate/expense_cate_check	id
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/finance/invoice/index	limit
参考	http://192.168.133.196/oa/work/index	limit
参考	http://192.168.133.196/oa/schedule/calendar	uid
参考	http://192.168.133.196/oa/schedule/calendar	end
参考	http://192.168.133.196/oa/plan/calendar	end

参考	http://192.168.133.196/oa/schedule/index	limit
参考	http://192.168.133.196/oa/plan/calendar	start
参考	http://192.168.133.196/oa/schedule/calendar	start
参考	http://192.168.133.196/oa/work/index	send
参考	http://192.168.133.196/finance/income/index	limit
参考	http://192.168.133.196/finance/expense/index	limit
参考	http://192.168.133.196/home/api/log_list	limit
参考	http://192.168.133.196/home/login/login_sbmit	password

中

6.2.2 d)1) - The Access control policy should cover the permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; 10

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性

URL

实体

中

http://192.168.133.196/home/login/login_sbmit

password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

中

6.2.2 d)2) - The Access control policy should include an authorization process for user access and privileges. ⑧

不充分帐户封锁

风险: 可能会升级用户特权并通过 **Web** 应用程序获取管理许可权

原因: **Web** 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_su_bmit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

8.3.3 - The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement or adjusted upon change. ⑦

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

参

10.3.1 - The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. ⑤

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

高

10.8.1 a) - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: procedures designed to protect exchanged information from interception, copying, modification, misrouting, and destruction. 323

查询中的密码参数

风险: 可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

原因: 查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

固定值: 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

CVSS 分数: 8.5

严重性	URL	实体
高	http://192.168.133.196/home/login/lock.html	lock_password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

“Content-Security-Policy”头缺失或不安全

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: 将服务器配置为使用安全策略的“Content-Security-Policy”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-Content-Type-Options”头缺失或不安全

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: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-XSS-Protection”头缺失或不安全

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: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

Oracle 日志文件信息泄露

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 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: 关闭跟踪，限制对日志文件的访问，或者将其除去

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/finance/expense/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.log
低	http://192.168.133.196/adm/seal/	sqlnet.log
低	http://192.168.133.196/adm/meeting/	sqlnet.log
低	http://192.168.133.196/oa/approve/	sqlnet.trc
低	http://192.168.133.196/oa/work/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.log
低	http://192.168.133.196/home/flow/	sqlnet.log
低	http://192.168.133.196/user/position/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.trc
低	http://192.168.133.196/home/flow/	sqlnet.trc
低	http://192.168.133.196/user/personal/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.trc
低	http://192.168.133.196/finance/expense/	sqlnet.trc
低	http://192.168.133.196/user/position/	sqlnet.log
低	http://192.168.133.196/user/personal/	sqlnet.trc
低	http://192.168.133.196/oa/approve/	sqlnet.log
低	http://192.168.133.196/oa/schedule/	sqlnet.trc
低	http://192.168.133.196/adm/meeting/	sqlnet.trc
低	http://192.168.133.196/adm/seal/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.trc

低	http://192.168.133.196/oa/schedule/	sqlnet.log
低	http://192.168.133.196/oa/work/	sqlnet.trc
低	http://192.168.133.196/finance/income/	sqlnet.log
低	http://192.168.133.196/finance/income/	sqlnet.trc

查询中接受的主体参数

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/oa/schedule/calendar	calendar
低	http://192.168.133.196/home/login/login_submit	login_submit

发现压缩目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/user/department/	department.arc
低	http://192.168.133.196/adm/seal/	seal.rar
低	http://192.168.133.196/oa/schedule/	schedule.zip
低	http://192.168.133.196/home/cate/	cate.tar.gz
低	http://192.168.133.196/oa/approve/	approve.tar
低	http://192.168.133.196/home/keywords/	keywords.lzh
低	http://192.168.133.196/user/department/	department.lha
低	http://192.168.133.196/home/flow/	flow.tar.gz
低	http://192.168.133.196/user/department/	department.lzh
低	http://192.168.133.196/home/keywords/	keywords.tar
低	http://192.168.133.196/home/	home.ar
低	http://192.168.133.196/user/department/	department.tar
低	http://192.168.133.196/home/	home.ear
低	http://192.168.133.196/home/keywords/	keywords.arj
低	http://192.168.133.196/user/department/	department.arj
低	http://192.168.133.196/home/keywords/	keywords.arc
低	http://192.168.133.196/home/keywords/	keywords.tar.gz
低	http://192.168.133.196/user/department/	department.tar.gz
低	http://192.168.133.196/user/position/	position.zip
低	http://192.168.133.196/home/	home.tar.lzma
低	http://192.168.133.196/home/	home.war
低	http://192.168.133.196/home/	home.wim
低	http://192.168.133.196/home/cate/	cate.zip
低	http://192.168.133.196/user/position/	position.gz
低	http://192.168.133.196/home/flow/	flow.zip

低	http://192.168.133.196/user/position/	position.rar
低	http://192.168.133.196/home/keywords/	keywords.zip
低	http://192.168.133.196/home/cate/	cate.gz
低	http://192.168.133.196/home/flow/	flow.gz
低	http://192.168.133.196/home/cate/	cate.rar
低	http://192.168.133.196/home/flow/	flow.rar
低	http://192.168.133.196/home/cate/	cate.ace
低	http://192.168.133.196/home/flow/	flow.ace
低	http://192.168.133.196/home/cate/	cate.lha
低	http://192.168.133.196/home/flow/	flow.lha
低	http://192.168.133.196/home/cate/	cate.lzh
低	http://192.168.133.196/oa/plan/	plan.gz
低	http://192.168.133.196/home/keywords/	keywords.gz
低	http://192.168.133.196/user/position/	position.lzh
低	http://192.168.133.196/home/flow/	flow.lzh
低	http://192.168.133.196/user/department/	department.zip
低	http://192.168.133.196/home/keywords/	keywords.rar
低	http://192.168.133.196/home/cate/	cate.tar
低	http://192.168.133.196/user/department/	department.gz
低	http://192.168.133.196/user/user/	user.zip
低	http://192.168.133.196/home/flow/	flow.tar
低	http://192.168.133.196/home/keywords/	keywords.ace
低	http://192.168.133.196/home/cate/	cate.arj
低	http://192.168.133.196/user/position/	position.tar
低	http://192.168.133.196/user/department/	department.rar
低	http://192.168.133.196/user/user/	user.gz
低	http://192.168.133.196/home/flow/	flow.arj
低	http://192.168.133.196/home/keywords/	keywords.lha
低	http://192.168.133.196/home/cate/	cate.arc
低	http://192.168.133.196/user/department/	department.ace
低	http://192.168.133.196/home/flow/	flow.arc
低	http://192.168.133.196/oa/schedule/	schedule.gz

低	http://192.168.133.196/user/user/	user.rar
低	http://192.168.133.196/user/position/	position.lha
低	http://192.168.133.196/user/position/	position.arj
低	http://192.168.133.196/user/personal/	personal.zip
低	http://192.168.133.196/oa/work/	work.zip
低	http://192.168.133.196/user/user/	user.ace
低	http://192.168.133.196/oa/plan/	plan.rar
低	http://192.168.133.196/user/personal/	personal.gz
低	http://192.168.133.196/user/user/	user.lha
低	http://192.168.133.196/user/personal/	personal.rar
低	http://192.168.133.196/user/position/	position.arc
低	http://192.168.133.196/oa/schedule/	schedule.rar
低	http://192.168.133.196/user/user/	user.lzh
低	http://192.168.133.196/adm/seal/	seal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.lha
低	http://192.168.133.196/oa/approve/	approve.arj
低	http://192.168.133.196/oa/work/	work.gz
低	http://192.168.133.196/user/personal/	personal.ace
低	http://192.168.133.196/oa/plan/	plan.ace
低	http://192.168.133.196/user/position/	position.tar.gz
低	http://192.168.133.196/user/user/	user.tar
低	http://192.168.133.196/user/personal/	personal.lha
低	http://192.168.133.196/user/user/	user.arj
低	http://192.168.133.196/user/personal/	personal.lzh
低	http://192.168.133.196/finance/income/	income.lha
低	http://192.168.133.196/user/personal/	personal.tar
低	http://192.168.133.196/oa/approve/	approve.arc
低	http://192.168.133.196/user/user/	user.arc
低	http://192.168.133.196/user/user/	user.tar.gz
低	http://192.168.133.196/user/personal/	personal.arj
低	http://192.168.133.196/adm/seal/	seal.zip
低	http://192.168.133.196/adm/meeting/	meeting.tar

低	http://192.168.133.196/user/personal/	personal.arc
低	http://192.168.133.196/oa/approve/	approve.tar.gz
低	http://192.168.133.196/adm/seal/	seal.gz
低	http://192.168.133.196/user/personal/	personal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.zip
低	http://192.168.133.196/oa/approve/	approve.zip
低	http://192.168.133.196/adm/meeting/	meeting.gz
低	http://192.168.133.196/adm/meeting/	meeting.arj
低	http://192.168.133.196/adm/seal/	seal.ace
低	http://192.168.133.196/adm/meeting/	meeting.arc
低	http://192.168.133.196/oa/approve/	approve.gz
低	http://192.168.133.196/adm/meeting/	meeting.rar
低	http://192.168.133.196/adm/seal/	seal.lha
低	http://192.168.133.196/oa/approve/	approve.rar
低	http://192.168.133.196/adm/meeting/	meeting.tar.gz
低	http://192.168.133.196/oa/approve/	approve.ace
低	http://192.168.133.196/adm/seal/	seal.lzh
低	http://192.168.133.196/oa/work/	work.rar
低	http://192.168.133.196/adm/seal/	seal.tar
低	http://192.168.133.196/oa/approve/	approve.lha
低	http://192.168.133.196/adm/seal/	seal.arj
低	http://192.168.133.196/oa/approve/	approve.lzh
低	http://192.168.133.196/oa/schedule/	schedule.ace
低	http://192.168.133.196/adm/seal/	seal.arc
低	http://192.168.133.196/oa/plan/	plan.lha
低	http://192.168.133.196/adm/meeting/	meeting.ace
低	http://192.168.133.196/adm/meeting/	meeting.lzh
低	http://192.168.133.196/user/position/	position.ace
低	http://192.168.133.196/oa/plan/	plan.zip
低	http://192.168.133.196/oa/work/	work.ace
低	http://192.168.133.196/oa/schedule/	schedule.lha
低	http://192.168.133.196/oa/plan/	plan.lzh

低	http://192.168.133.196/oa/plan/	plan.tar
低	http://192.168.133.196/oa/schedule/	schedule.tar
低	http://192.168.133.196/oa/work/	work.lzh
低	http://192.168.133.196/oa/plan/	plan.arj
低	http://192.168.133.196/oa/work/	work.tar
低	http://192.168.133.196/oa/schedule/	schedule.arj
低	http://192.168.133.196/oa/plan/	plan.arc
低	http://192.168.133.196/finance/expense/	expense.zip
低	http://192.168.133.196/finance/income/	income.zip
低	http://192.168.133.196/oa/schedule/	schedule.arc
低	http://192.168.133.196/oa/work/	work.arj
低	http://192.168.133.196/oa/plan/	plan.tar.gz
低	http://192.168.133.196/finance/expense/	expense.gz
低	http://192.168.133.196/finance/income/	income.gz
低	http://192.168.133.196/oa/work/	work.arc
低	http://192.168.133.196/oa/schedule/	schedule.tar.gz
低	http://192.168.133.196/finance/expense/	expense.rar
低	http://192.168.133.196/oa/work/	work.tar.gz
低	http://192.168.133.196/finance/income/	income.rar
低	http://192.168.133.196/finance/expense/	expense.ace
低	http://192.168.133.196/finance/income/	income.ace
低	http://192.168.133.196/finance/expense/	expense.lha
低	http://192.168.133.196/finance/expense/	expense.lzh
低	http://192.168.133.196/finance/income/	income.lzh
低	http://192.168.133.196/finance/expense/	expense.tar
低	http://192.168.133.196/finance/income/	income.tar
低	http://192.168.133.196/finance/expense/	expense.arj
低	http://192.168.133.196/finance/income/	income.arj
低	http://192.168.133.196/finance/expense/	expense.arc
低	http://192.168.133.196/finance/income/	income.arc
低	http://192.168.133.196/finance/income/	income.tar.gz
低	http://192.168.133.196/finance/expense/	expense.tar.gz

低	http://192.168.133.196/oa/work/	work.lha
低	http://192.168.133.196/oa/schedule/	schedule.lzh

归档文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/user/personal/leave	leave
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate

低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

检测到隐藏目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/customer/	customer/
低	http://192.168.133.196/install/	install/
低	http://192.168.133.196/home/	home/

跨帧脚本编制防御缺失或不安全

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: 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/index/index	index
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/	

临时文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/user/personal/leave	leave

低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: 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: 禁用 WebDAV，或者禁止不需要的 HTTP 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

发现电子邮件地址模式

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/user/user/index	index

发现可能的服务器路径泄露模式

风险: 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修补程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	index.html
参考	http://192.168.133.196/home/login/lock.html	lock.html
参考	http://192.168.133.196/home/cate/flow_type	flow_type
参考	http://192.168.133.196/	
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/index/main.html	main.html
参考	http://192.168.133.196/home/flow/add	add
参考	http://192.168.133.196/oa/plan/calendar	calendar
参考	http://192.168.133.196/static/assets/layui/layui.js	layui.js

发现内部 IP 泄露模式

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 站点中的内部 IP 地址

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/user/user/index	index

客户端（JavaScript）Cookie 引用

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

CVSS 分数： 0.0

严重性

URL

实体

参考

<http://192.168.133.196/home/login/index.html>

layui.use(['form'], function() {var form = layui.
i.form,\$ = layui.\$,layer = layui.layer;// {U
◆◆◆◆i...

参考

<http://192.168.133.196/static/assets/gougu/module/admin.js>

layui.define(['element'], function (exports) {

应用程序错误		
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	
CVSS 分数:	0.0	
严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/oa/approve/index	limit
参考	http://192.168.133.196/user/personal/leave	limit
参考	http://192.168.133.196/oa/approve/list	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/user/personal/change	limit
参考	http://192.168.133.196/oa/plan/calendar	uid
参考	http://192.168.133.196/oa/approve/copy	limit
参考	http://192.168.133.196/home/cate/flow_type_check	id
参考	http://192.168.133.196/oa/plan/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/api/index/get_department_select	keyword
参考	http://192.168.133.196/home/cate/expense_cate_add	title
参考	http://192.168.133.196/home/cate/expense_cate_add	id
参考	http://192.168.133.196/home/cate/expense_cate_check	id
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/finance/invoice/index	limit
参考	http://192.168.133.196/oa/work/index	limit
参考	http://192.168.133.196/oa/schedule/calendar	uid
参考	http://192.168.133.196/oa/schedule/calendar	end
参考	http://192.168.133.196/oa/plan/calendar	end

参考	http://192.168.133.196/oa/schedule/index	limit
参考	http://192.168.133.196/oa/plan/calendar	start
参考	http://192.168.133.196/oa/schedule/calendar	start
参考	http://192.168.133.196/oa/work/index	send
参考	http://192.168.133.196/finance/income/index	limit
参考	http://192.168.133.196/finance/expense/index	limit
参考	http://192.168.133.196/home/api/log_list	limit
参考	http://192.168.133.196/home/login/login_submit	password

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

低

10.8.1 b) - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications. 17

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: 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: 禁用 WebDAV，或者禁止不需要的 HTTP 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

发现可能的服务器路径泄露模式

风险: 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修补程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	index.html
参考	http://192.168.133.196/home/login/lock.html	lock.html
参考	http://192.168.133.196/home/cate/flow_type	flow_type
参考	http://192.168.133.196/	
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/index/main.html	main.html
参考	http://192.168.133.196/home/flow/add	add
参考	http://192.168.133.196/oa/plan/calendar	calendar
参考	http://192.168.133.196/static/assets/layui/layui.js	layui.js

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

中

10.8.1 g) - Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: use of cryptographic techniques to protect the confidentiality, integrity and authenticity of information. 7

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

10.9.1 a) - Security considerations for electronic commerce should include the level of confidence each party requires in each others claimed identity, e.g. through authentication. 7

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

10.9.1 h) - Security considerations for electronic commerce should include the degree of verification appropriate to check payment information supplied by a customer 10

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_submit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

10.9.2 c) - Security considerations for online transactions should include encrypted communications path between all involved parties 0

中

10.9.3 - The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification

11

不充分帐户封锁

风险: 可能会升级用户特权并通过 **Web** 应用程序获取管理许可权

原因: **Web** 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_sbmit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: **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: 禁用 **WebDAV**，或者禁止不需要的 **HTTP** 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/



JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
	http://192.168.133.196/home/api/log_list	log_list
	http://192.168.133.196/home/api/log_list	limit

中

11.2.2 - The allocation and use of privileges should be restricted and controlled. 


不充分帐户封锁

风险: 可能会升级用户特权并通过 **Web** 应用程序获取管理许可权

原因: **Web** 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
	http://192.168.133.196/home/login/login_sbmit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

11.2.3 - The allocation of passwords should be controlled through a formal management process. ①

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

11.2.4 - Management should review user's access rights at regular intervals using a formal process. 7

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

11.4.2 - Appropriate authentication methods should be used to control access by remote users. 7

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

11.5.2 - All users should have a unique identifier for their personal use only, and suitable authentication technique should be chosen to substantiate the claimed identity of a user. 7

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.htm	lock.html

11.5.5 - Inactive sessions should shut down after a defined period of inactivity. 0

11.5.6 - Restriction on connection times should be used to provide additional security for high-risk applications. 0

中 11.6.1 - Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. 8

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_smbmit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

中

12.2.1 - Data input to applications should be validated to ensure that this data is correct and appropriate. 41

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_submit	password

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: 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: 禁用 WebDAV，或者禁止不需要的 HTTP 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

客户端（JavaScript）Cookie 引用

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	layui.use(['form'], function() {var form = layui.form,\$ = layui.\$,layer = layui.layer;// {U💎💎💎💎i...
参考	http://192.168.133.196/static/assets/gougou/module/admin.js	layui.define(['element'], function (exports) {

应用程序错误

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/oa/approve/index	limit
参考	http://192.168.133.196/user/personal/leave	limit
参考	http://192.168.133.196/oa/approve/list	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/user/personal/change	limit
参考	http://192.168.133.196/oa/plan/calendar	uid
参考	http://192.168.133.196/oa/approve/copy	limit
参考	http://192.168.133.196/home/cate/flow_type_check	id
参考	http://192.168.133.196/oa/plan/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/api/index/get_department_select	keyword
参考	http://192.168.133.196/home/cate/expense_cate_add	title
参考	http://192.168.133.196/home/cate/expense_cate_add	id
参考	http://192.168.133.196/home/cate/expense_cate_check	id
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/finance/invoice/index	limit
参考	http://192.168.133.196/oa/work/index	limit
参考	http://192.168.133.196/oa/schedule/calendar	uid
参考	http://192.168.133.196/oa/schedule/calendar	end
参考	http://192.168.133.196/oa/plan/calendar	end

参考	http://192.168.133.196/oa/schedule/index	limit
参考	http://192.168.133.196/oa/plan/calendar	start
参考	http://192.168.133.196/oa/schedule/calendar	start
参考	http://192.168.133.196/oa/work/index	send
参考	http://192.168.133.196/finance/income/index	limit
参考	http://192.168.133.196/finance/expense/index	limit
参考	http://192.168.133.196/home/api/log_list	limit
参考	http://192.168.133.196/home/login/login_submit	password

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

中

12.2.2 - Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

41

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_submit	password

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: 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: 禁用 WebDAV，或者禁止不需要的 HTTP 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/

JSON 中反映的未清理用户输入

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
CVSS 分数:	0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

客户端 (JavaScript) Cookie 引用

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
CVSS 分数:	0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	layui.use(['form'], function() {var form = layui. i.form,\$ = layui.\$,layer = layui.layer;// {U {U {U {U...
参考	http://192.168.133.196/static/assets/gougul/module/admin.js	layui.define(['element'], function (exports) {

应用程序错误

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/oa/approve/index	limit
参考	http://192.168.133.196/user/personal/leave	limit
参考	http://192.168.133.196/oa/approve/list	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/user/personal/change	limit
参考	http://192.168.133.196/oa/plan/calendar	uid
参考	http://192.168.133.196/oa/approve/copy	limit
参考	http://192.168.133.196/home/cate/flow_type_check	id
参考	http://192.168.133.196/oa/plan/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/api/index/get_department_select	keyword
参考	http://192.168.133.196/home/cate/expense_cate_add	title
参考	http://192.168.133.196/home/cate/expense_cate_add	id
参考	http://192.168.133.196/home/cate/expense_cate_check	id
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/finance/invoice/index	limit
参考	http://192.168.133.196/oa/work/index	limit
参考	http://192.168.133.196/oa/schedule/calendar	uid
参考	http://192.168.133.196/oa/schedule/calendar	end
参考	http://192.168.133.196/oa/plan/calendar	end

参考	http://192.168.133.196/oa/schedule/index	limit
参考	http://192.168.133.196/oa/plan/calendar	start
参考	http://192.168.133.196/oa/schedule/calendar	start
参考	http://192.168.133.196/oa/work/index	send
参考	http://192.168.133.196/finance/income/index	limit
参考	http://192.168.133.196/finance/expense/index	limit
参考	http://192.168.133.196/home/api/log_list	limit
参考	http://192.168.133.196/home/login/login_submit	password

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

中

12.2.3 - Requirements for ensuring authenticity and protecting message integrity in applications should be identified and appropriate controls identified and implemented. ⑧

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_smbmit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_smbmit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

12.3.1 - A policy on the use of cryptographic controls for protection of information should be developed and implemented. 0

高 12.4.3 - Access to program source code should be restricted. 313

查询中的密码参数

风险: 可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

原因: 查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

固定值: 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

CVSS 分数: 8.5

严重性	URL	实体
高	http://192.168.133.196/home/login/lock.htm	lock_password

“Content-Security-Policy”头缺失或不安全

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: 将服务器配置为使用安全策略的“Content-Security-Policy”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.htm	lock.html
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-Content-Type-Options”头缺失或不安全

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: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-XSS-Protection”头缺失或不安全

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: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

Oracle 日志文件信息泄露

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 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: 关闭跟踪，限制对日志文件的访问，或者将其除去

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/finance/expense/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.log
低	http://192.168.133.196/adm/seal/	sqlnet.log
低	http://192.168.133.196/adm/meeting/	sqlnet.log
低	http://192.168.133.196/oa/approve/	sqlnet.trc
低	http://192.168.133.196/oa/work/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.log
低	http://192.168.133.196/home/flow/	sqlnet.log
低	http://192.168.133.196/user/position/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.trc
低	http://192.168.133.196/home/flow/	sqlnet.trc
低	http://192.168.133.196/user/personal/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.trc
低	http://192.168.133.196/finance/expense/	sqlnet.trc
低	http://192.168.133.196/user/position/	sqlnet.log
低	http://192.168.133.196/user/personal/	sqlnet.trc
低	http://192.168.133.196/oa/approve/	sqlnet.log
低	http://192.168.133.196/oa/schedule/	sqlnet.trc
低	http://192.168.133.196/adm/meeting/	sqlnet.trc
低	http://192.168.133.196/adm/seal/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.trc

低	http://192.168.133.196/oa/schedule/	sqlnet.log
低	http://192.168.133.196/oa/work/	sqlnet.trc
低	http://192.168.133.196/finance/income/	sqlnet.log
低	http://192.168.133.196/finance/income/	sqlnet.trc

查询中接受的主体参数

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/oa/schedule/calendar	calendar
低	http://192.168.133.196/home/login/login_submit	login_submit

发现压缩目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/user/department/	department.arc
低	http://192.168.133.196/adm/seal/	seal.rar
低	http://192.168.133.196/oa/schedule/	schedule.zip
低	http://192.168.133.196/home/cate/	cate.tar.gz
低	http://192.168.133.196/oa/approve/	approve.tar
低	http://192.168.133.196/home/keywords/	keywords.lzh
低	http://192.168.133.196/user/department/	department.lha
低	http://192.168.133.196/home/flow/	flow.tar.gz
低	http://192.168.133.196/user/department/	department.lzh
低	http://192.168.133.196/home/keywords/	keywords.tar
低	http://192.168.133.196/home/	home.ar
低	http://192.168.133.196/user/department/	department.tar
低	http://192.168.133.196/home/	home.ear
低	http://192.168.133.196/home/keywords/	keywords.arj
低	http://192.168.133.196/user/department/	department.arj
低	http://192.168.133.196/home/keywords/	keywords.arc
低	http://192.168.133.196/home/keywords/	keywords.tar.gz
低	http://192.168.133.196/user/department/	department.tar.gz
低	http://192.168.133.196/user/position/	position.zip
低	http://192.168.133.196/home/	home.tar.lzma
低	http://192.168.133.196/home/	home.war
低	http://192.168.133.196/home/	home.wim
低	http://192.168.133.196/home/cate/	cate.zip
低	http://192.168.133.196/user/position/	position.gz
低	http://192.168.133.196/home/flow/	flow.zip

低	http://192.168.133.196/user/position/	position.rar
低	http://192.168.133.196/home/keywords/	keywords.zip
低	http://192.168.133.196/home/cate/	cate.gz
低	http://192.168.133.196/home/flow/	flow.gz
低	http://192.168.133.196/home/cate/	cate.rar
低	http://192.168.133.196/home/flow/	flow.rar
低	http://192.168.133.196/home/cate/	cate.ace
低	http://192.168.133.196/home/flow/	flow.ace
低	http://192.168.133.196/home/cate/	cate.lha
低	http://192.168.133.196/home/flow/	flow.lha
低	http://192.168.133.196/home/cate/	cate.lzh
低	http://192.168.133.196/oa/plan/	plan.gz
低	http://192.168.133.196/home/keywords/	keywords.gz
低	http://192.168.133.196/user/position/	position.lzh
低	http://192.168.133.196/home/flow/	flow.lzh
低	http://192.168.133.196/user/department/	department.zip
低	http://192.168.133.196/home/keywords/	keywords.rar
低	http://192.168.133.196/home/cate/	cate.tar
低	http://192.168.133.196/user/department/	department.gz
低	http://192.168.133.196/user/user/	user.zip
低	http://192.168.133.196/home/flow/	flow.tar
低	http://192.168.133.196/home/keywords/	keywords.ace
低	http://192.168.133.196/home/cate/	cate.arj
低	http://192.168.133.196/user/position/	position.tar
低	http://192.168.133.196/user/department/	department.rar
低	http://192.168.133.196/user/user/	user.gz
低	http://192.168.133.196/home/flow/	flow.arj
低	http://192.168.133.196/home/keywords/	keywords.lha
低	http://192.168.133.196/home/cate/	cate.arc
低	http://192.168.133.196/user/department/	department.ace
低	http://192.168.133.196/home/flow/	flow.arc
低	http://192.168.133.196/oa/schedule/	schedule.gz

低	http://192.168.133.196/user/user/	user.rar
低	http://192.168.133.196/user/position/	position.lha
低	http://192.168.133.196/user/position/	position.arj
低	http://192.168.133.196/user/personal/	personal.zip
低	http://192.168.133.196/oa/work/	work.zip
低	http://192.168.133.196/user/user/	user.ace
低	http://192.168.133.196/oa/plan/	plan.rar
低	http://192.168.133.196/user/personal/	personal.gz
低	http://192.168.133.196/user/user/	user.lha
低	http://192.168.133.196/user/personal/	personal.rar
低	http://192.168.133.196/user/position/	position.arc
低	http://192.168.133.196/oa/schedule/	schedule.rar
低	http://192.168.133.196/user/user/	user.lzh
低	http://192.168.133.196/adm/seal/	seal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.lha
低	http://192.168.133.196/oa/approve/	approve.arj
低	http://192.168.133.196/oa/work/	work.gz
低	http://192.168.133.196/user/personal/	personal.ace
低	http://192.168.133.196/oa/plan/	plan.ace
低	http://192.168.133.196/user/position/	position.tar.gz
低	http://192.168.133.196/user/user/	user.tar
低	http://192.168.133.196/user/personal/	personal.lha
低	http://192.168.133.196/user/user/	user.arj
低	http://192.168.133.196/user/personal/	personal.lzh
低	http://192.168.133.196/finance/income/	income.lha
低	http://192.168.133.196/user/personal/	personal.tar
低	http://192.168.133.196/oa/approve/	approve.arc
低	http://192.168.133.196/user/user/	user.arc
低	http://192.168.133.196/user/user/	user.tar.gz
低	http://192.168.133.196/user/personal/	personal.arj
低	http://192.168.133.196/adm/seal/	seal.zip
低	http://192.168.133.196/adm/meeting/	meeting.tar

低	http://192.168.133.196/user/personal/	personal.arc
低	http://192.168.133.196/oa/approve/	approve.tar.gz
低	http://192.168.133.196/adm/seal/	seal.gz
低	http://192.168.133.196/user/personal/	personal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.zip
低	http://192.168.133.196/oa/approve/	approve.zip
低	http://192.168.133.196/adm/meeting/	meeting.gz
低	http://192.168.133.196/adm/meeting/	meeting.arj
低	http://192.168.133.196/adm/seal/	seal.ace
低	http://192.168.133.196/adm/meeting/	meeting.arc
低	http://192.168.133.196/oa/approve/	approve.gz
低	http://192.168.133.196/adm/meeting/	meeting.rar
低	http://192.168.133.196/adm/seal/	seal.lha
低	http://192.168.133.196/oa/approve/	approve.rar
低	http://192.168.133.196/adm/meeting/	meeting.tar.gz
低	http://192.168.133.196/oa/approve/	approve.ace
低	http://192.168.133.196/adm/seal/	seal.lzh
低	http://192.168.133.196/oa/work/	work.rar
低	http://192.168.133.196/adm/seal/	seal.tar
低	http://192.168.133.196/oa/approve/	approve.lha
低	http://192.168.133.196/adm/seal/	seal.arj
低	http://192.168.133.196/oa/approve/	approve.lzh
低	http://192.168.133.196/oa/schedule/	schedule.ace
低	http://192.168.133.196/adm/seal/	seal.arc
低	http://192.168.133.196/oa/plan/	plan.lha
低	http://192.168.133.196/adm/meeting/	meeting.ace
低	http://192.168.133.196/adm/meeting/	meeting.lzh
低	http://192.168.133.196/user/position/	position.ace
低	http://192.168.133.196/oa/plan/	plan.zip
低	http://192.168.133.196/oa/work/	work.ace
低	http://192.168.133.196/oa/schedule/	schedule.lha
低	http://192.168.133.196/oa/plan/	plan.lzh

低	http://192.168.133.196/oa/plan/	plan.tar
低	http://192.168.133.196/oa/schedule/	schedule.tar
低	http://192.168.133.196/oa/work/	work.lzh
低	http://192.168.133.196/oa/plan/	plan.arj
低	http://192.168.133.196/oa/work/	work.tar
低	http://192.168.133.196/oa/schedule/	schedule.arj
低	http://192.168.133.196/oa/plan/	plan.arc
低	http://192.168.133.196/finance/expense/	expense.zip
低	http://192.168.133.196/finance/income/	income.zip
低	http://192.168.133.196/oa/schedule/	schedule.arc
低	http://192.168.133.196/oa/work/	work.arj
低	http://192.168.133.196/oa/plan/	plan.tar.gz
低	http://192.168.133.196/finance/expense/	expense.gz
低	http://192.168.133.196/finance/income/	income.gz
低	http://192.168.133.196/oa/work/	work.arc
低	http://192.168.133.196/oa/schedule/	schedule.tar.gz
低	http://192.168.133.196/finance/expense/	expense.rar
低	http://192.168.133.196/oa/work/	work.tar.gz
低	http://192.168.133.196/finance/income/	income.rar
低	http://192.168.133.196/finance/expense/	expense.ace
低	http://192.168.133.196/finance/income/	income.ace
低	http://192.168.133.196/finance/expense/	expense.lha
低	http://192.168.133.196/finance/expense/	expense.lzh
低	http://192.168.133.196/finance/income/	income.lzh
低	http://192.168.133.196/finance/expense/	expense.tar
低	http://192.168.133.196/finance/income/	income.tar
低	http://192.168.133.196/finance/expense/	expense.arj
低	http://192.168.133.196/finance/income/	income.arj
低	http://192.168.133.196/finance/expense/	expense.arc
低	http://192.168.133.196/finance/income/	income.arc
低	http://192.168.133.196/finance/income/	income.tar.gz
低	http://192.168.133.196/finance/expense/	expense.tar.gz

低	http://192.168.133.196/oa/work/	work.lha
低	http://192.168.133.196/oa/schedule/	schedule.lzh

归档文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/user/personal/leave	leave
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate

低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

检测到隐藏目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/customer/	customer/
低	http://192.168.133.196/install/	install/
低	http://192.168.133.196/home/	home/

跨帧脚本编制防御缺失或不安全

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: 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/index/index	index
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/	

临时文件下载		
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	
CVSS 分数:	5.0	
严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/user/personal/leave	leave

低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

发现电子邮件地址模式

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

CVSS 分数: 0.0

严重性	URL	实体
-----	-----	----

参考	http://192.168.133.196/user/user/index	index
----	---	-------

发现可能的服务器路径泄露模式

风险: 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修补程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	index.html
参考	http://192.168.133.196/home/login/lock.html	lock.html
参考	http://192.168.133.196/home/cate/flow_type	flow_type
参考	http://192.168.133.196/	
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/index/main.html	main.html
参考	http://192.168.133.196/home/flow/add	add
参考	http://192.168.133.196/oa/plan/calendar	calendar
参考	http://192.168.133.196/static/assets/layui/layui.js	layui.js

发现内部 IP 泄露模式

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 站点中的内部 IP 地址

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/user/user/index	index

客户端（JavaScript）Cookie 引用

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

CVSS 分数: 0.0

严重性

URL

实体

参考

<http://192.168.133.196/home/login/index.html>

layui.use(['form'], function() {var form = layui.
i.form,\$ = layui.\$,layer = layui.layer;// {U
i...

参考

<http://192.168.133.196/static/assets/gougu/module/admin.js>

layui.define(['element'], function (exports) {

应用程序错误		
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	
CVSS 分数:	0.0	
严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/oa/approve/index	limit
参考	http://192.168.133.196/user/personal/leave	limit
参考	http://192.168.133.196/oa/approve/list	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/user/personal/change	limit
参考	http://192.168.133.196/oa/plan/calendar	uid
参考	http://192.168.133.196/oa/approve/copy	limit
参考	http://192.168.133.196/home/cate/flow_type_check	id
参考	http://192.168.133.196/oa/plan/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/api/index/get_department_select	keyword
参考	http://192.168.133.196/home/cate/expense_cate_add	title
参考	http://192.168.133.196/home/cate/expense_cate_add	id
参考	http://192.168.133.196/home/cate/expense_cate_check	id
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/finance/invoice/index	limit
参考	http://192.168.133.196/oa/work/index	limit
参考	http://192.168.133.196/oa/schedule/calendar	uid
参考	http://192.168.133.196/oa/schedule/calendar	end
参考	http://192.168.133.196/oa/plan/calendar	end

参考	http://192.168.133.196/oa/schedule/index	limit
参考	http://192.168.133.196/oa/plan/calendar	start
参考	http://192.168.133.196/oa/schedule/calendar	start
参考	http://192.168.133.196/oa/work/index	send
参考	http://192.168.133.196/finance/income/index	limit
参考	http://192.168.133.196/finance/expense/index	limit
参考	http://192.168.133.196/home/api/log_list	limit
参考	http://192.168.133.196/home/login/login_submit	password

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

高

12.5.4 - Opportunities for information leakage should be prevented.

313

查询中的密码参数

风险: 可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

原因: 查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

固定值: 发送敏感信息时，始终使用 **SSL** 和 **POST**（主体）参数。

CVSS 分数: 8.5

严重性

URL

实体

高

<http://192.168.133.196/home/login/lock.htm> lock_password

“Content-Security-Policy”头缺失或不安全

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: 将服务器配置为使用安全策略的“Content-Security-Policy”头

CVSS 分数: 5.0

严重性

URL

实体

低

<http://192.168.133.196/home/login/lock.htm> lock.html

低

<http://192.168.133.196/home/login/index.html> index.html

低

<http://192.168.133.196/>

低

http://192.168.133.196/home/api/get_article_list get_article_list

低

http://192.168.133.196/home/api/get_view_log get_view_log

“X-Content-Type-Options”头缺失或不安全

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: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-XSS-Protection”头缺失或不安全

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: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

Oracle 日志文件信息泄露

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 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: 关闭跟踪，限制对日志文件的访问，或者将其除去

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/finance/expense/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.log
低	http://192.168.133.196/adm/seal/	sqlnet.log
低	http://192.168.133.196/adm/meeting/	sqlnet.log
低	http://192.168.133.196/oa/approve/	sqlnet.trc
低	http://192.168.133.196/oa/work/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.log
低	http://192.168.133.196/home/flow/	sqlnet.log
低	http://192.168.133.196/user/position/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.trc
低	http://192.168.133.196/home/flow/	sqlnet.trc
低	http://192.168.133.196/user/personal/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.trc
低	http://192.168.133.196/finance/expense/	sqlnet.trc
低	http://192.168.133.196/user/position/	sqlnet.log
低	http://192.168.133.196/user/personal/	sqlnet.trc
低	http://192.168.133.196/oa/approve/	sqlnet.log
低	http://192.168.133.196/oa/schedule/	sqlnet.trc
低	http://192.168.133.196/adm/meeting/	sqlnet.trc
低	http://192.168.133.196/adm/seal/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.trc

低	http://192.168.133.196/oa/schedule/	sqlnet.log
低	http://192.168.133.196/oa/work/	sqlnet.trc
低	http://192.168.133.196/finance/income/	sqlnet.log
低	http://192.168.133.196/finance/income/	sqlnet.trc

查询中接受的主体参数

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/oa/schedule/calendar	calendar
低	http://192.168.133.196/home/login/login_submit	login_submit

发现压缩目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/user/department/	department.arc
低	http://192.168.133.196/adm/seal/	seal.rar
低	http://192.168.133.196/oa/schedule/	schedule.zip
低	http://192.168.133.196/home/cate/	cate.tar.gz
低	http://192.168.133.196/oa/approve/	approve.tar
低	http://192.168.133.196/home/keywords/	keywords.lzh
低	http://192.168.133.196/user/department/	department.lha
低	http://192.168.133.196/home/flow/	flow.tar.gz
低	http://192.168.133.196/user/department/	department.lzh
低	http://192.168.133.196/home/keywords/	keywords.tar
低	http://192.168.133.196/home/	home.ar
低	http://192.168.133.196/user/department/	department.tar
低	http://192.168.133.196/home/	home.ear
低	http://192.168.133.196/home/keywords/	keywords.arj
低	http://192.168.133.196/user/department/	department.arj
低	http://192.168.133.196/home/keywords/	keywords.arc
低	http://192.168.133.196/home/keywords/	keywords.tar.gz
低	http://192.168.133.196/user/department/	department.tar.gz
低	http://192.168.133.196/user/position/	position.zip
低	http://192.168.133.196/home/	home.tar.lzma
低	http://192.168.133.196/home/	home.war
低	http://192.168.133.196/home/	home.wim
低	http://192.168.133.196/home/cate/	cate.zip
低	http://192.168.133.196/user/position/	position.gz
低	http://192.168.133.196/home/flow/	flow.zip

低	http://192.168.133.196/user/position/	position.rar
低	http://192.168.133.196/home/keywords/	keywords.zip
低	http://192.168.133.196/home/cate/	cate.gz
低	http://192.168.133.196/home/flow/	flow.gz
低	http://192.168.133.196/home/cate/	cate.rar
低	http://192.168.133.196/home/flow/	flow.rar
低	http://192.168.133.196/home/cate/	cate.ace
低	http://192.168.133.196/home/flow/	flow.ace
低	http://192.168.133.196/home/cate/	cate.lha
低	http://192.168.133.196/home/flow/	flow.lha
低	http://192.168.133.196/home/cate/	cate.lzh
低	http://192.168.133.196/oa/plan/	plan.gz
低	http://192.168.133.196/home/keywords/	keywords.gz
低	http://192.168.133.196/user/position/	position.lzh
低	http://192.168.133.196/home/flow/	flow.lzh
低	http://192.168.133.196/user/department/	department.zip
低	http://192.168.133.196/home/keywords/	keywords.rar
低	http://192.168.133.196/home/cate/	cate.tar
低	http://192.168.133.196/user/department/	department.gz
低	http://192.168.133.196/user/user/	user.zip
低	http://192.168.133.196/home/flow/	flow.tar
低	http://192.168.133.196/home/keywords/	keywords.ace
低	http://192.168.133.196/home/cate/	cate.arj
低	http://192.168.133.196/user/position/	position.tar
低	http://192.168.133.196/user/department/	department.rar
低	http://192.168.133.196/user/user/	user.gz
低	http://192.168.133.196/home/flow/	flow.arj
低	http://192.168.133.196/home/keywords/	keywords.lha
低	http://192.168.133.196/home/cate/	cate.arc
低	http://192.168.133.196/user/department/	department.ace
低	http://192.168.133.196/home/flow/	flow.arc
低	http://192.168.133.196/oa/schedule/	schedule.gz

低	http://192.168.133.196/user/user/	user.rar
低	http://192.168.133.196/user/position/	position.lha
低	http://192.168.133.196/user/position/	position.arj
低	http://192.168.133.196/user/personal/	personal.zip
低	http://192.168.133.196/oa/work/	work.zip
低	http://192.168.133.196/user/user/	user.ace
低	http://192.168.133.196/oa/plan/	plan.rar
低	http://192.168.133.196/user/personal/	personal.gz
低	http://192.168.133.196/user/user/	user.lha
低	http://192.168.133.196/user/personal/	personal.rar
低	http://192.168.133.196/user/position/	position.arc
低	http://192.168.133.196/oa/schedule/	schedule.rar
低	http://192.168.133.196/user/user/	user.lzh
低	http://192.168.133.196/adm/seal/	seal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.lha
低	http://192.168.133.196/oa/approve/	approve.arj
低	http://192.168.133.196/oa/work/	work.gz
低	http://192.168.133.196/user/personal/	personal.ace
低	http://192.168.133.196/oa/plan/	plan.ace
低	http://192.168.133.196/user/position/	position.tar.gz
低	http://192.168.133.196/user/user/	user.tar
低	http://192.168.133.196/user/personal/	personal.lha
低	http://192.168.133.196/user/user/	user.arj
低	http://192.168.133.196/user/personal/	personal.lzh
低	http://192.168.133.196/finance/income/	income.lha
低	http://192.168.133.196/user/personal/	personal.tar
低	http://192.168.133.196/oa/approve/	approve.arc
低	http://192.168.133.196/user/user/	user.arc
低	http://192.168.133.196/user/user/	user.tar.gz
低	http://192.168.133.196/user/personal/	personal.arj
低	http://192.168.133.196/adm/seal/	seal.zip
低	http://192.168.133.196/adm/meeting/	meeting.tar

低	http://192.168.133.196/user/personal/	personal.arc
低	http://192.168.133.196/oa/approve/	approve.tar.gz
低	http://192.168.133.196/adm/seal/	seal.gz
低	http://192.168.133.196/user/personal/	personal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.zip
低	http://192.168.133.196/oa/approve/	approve.zip
低	http://192.168.133.196/adm/meeting/	meeting.gz
低	http://192.168.133.196/adm/meeting/	meeting.arj
低	http://192.168.133.196/adm/seal/	seal.ace
低	http://192.168.133.196/adm/meeting/	meeting.arc
低	http://192.168.133.196/oa/approve/	approve.gz
低	http://192.168.133.196/adm/meeting/	meeting.rar
低	http://192.168.133.196/adm/seal/	seal.lha
低	http://192.168.133.196/oa/approve/	approve.rar
低	http://192.168.133.196/adm/meeting/	meeting.tar.gz
低	http://192.168.133.196/oa/approve/	approve.ace
低	http://192.168.133.196/adm/seal/	seal.lzh
低	http://192.168.133.196/oa/work/	work.rar
低	http://192.168.133.196/adm/seal/	seal.tar
低	http://192.168.133.196/oa/approve/	approve.lha
低	http://192.168.133.196/adm/seal/	seal.arj
低	http://192.168.133.196/oa/approve/	approve.lzh
低	http://192.168.133.196/oa/schedule/	schedule.ace
低	http://192.168.133.196/adm/seal/	seal.arc
低	http://192.168.133.196/oa/plan/	plan.lha
低	http://192.168.133.196/adm/meeting/	meeting.ace
低	http://192.168.133.196/adm/meeting/	meeting.lzh
低	http://192.168.133.196/user/position/	position.ace
低	http://192.168.133.196/oa/plan/	plan.zip
低	http://192.168.133.196/oa/work/	work.ace
低	http://192.168.133.196/oa/schedule/	schedule.lha
低	http://192.168.133.196/oa/plan/	plan.lzh

低	http://192.168.133.196/oa/plan/	plan.tar
低	http://192.168.133.196/oa/schedule/	schedule.tar
低	http://192.168.133.196/oa/work/	work.lzh
低	http://192.168.133.196/oa/plan/	plan.arj
低	http://192.168.133.196/oa/work/	work.tar
低	http://192.168.133.196/oa/schedule/	schedule.arj
低	http://192.168.133.196/oa/plan/	plan.arc
低	http://192.168.133.196/finance/expense/	expense.zip
低	http://192.168.133.196/finance/income/	income.zip
低	http://192.168.133.196/oa/schedule/	schedule.arc
低	http://192.168.133.196/oa/work/	work.arj
低	http://192.168.133.196/oa/plan/	plan.tar.gz
低	http://192.168.133.196/finance/expense/	expense.gz
低	http://192.168.133.196/finance/income/	income.gz
低	http://192.168.133.196/oa/work/	work.arc
低	http://192.168.133.196/oa/schedule/	schedule.tar.gz
低	http://192.168.133.196/finance/expense/	expense.rar
低	http://192.168.133.196/oa/work/	work.tar.gz
低	http://192.168.133.196/finance/income/	income.rar
低	http://192.168.133.196/finance/expense/	expense.ace
低	http://192.168.133.196/finance/income/	income.ace
低	http://192.168.133.196/finance/expense/	expense.lha
低	http://192.168.133.196/finance/expense/	expense.lzh
低	http://192.168.133.196/finance/income/	income.lzh
低	http://192.168.133.196/finance/expense/	expense.tar
低	http://192.168.133.196/finance/income/	income.tar
低	http://192.168.133.196/finance/expense/	expense.arj
低	http://192.168.133.196/finance/income/	income.arj
低	http://192.168.133.196/finance/expense/	expense.arc
低	http://192.168.133.196/finance/income/	income.arc
低	http://192.168.133.196/finance/income/	income.tar.gz
低	http://192.168.133.196/finance/expense/	expense.tar.gz

低	http://192.168.133.196/oa/work/	work.lha
低	http://192.168.133.196/oa/schedule/	schedule.lzh

归档文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/user/personal/leave	leave
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate

低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

检测到隐藏目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/customer/	customer/
低	http://192.168.133.196/install/	install/
低	http://192.168.133.196/home/	home/

跨帧脚本编制防御缺失或不安全

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: 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/index/index	index
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/	

临时文件下载

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/cate/flow_type	flow_type
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/home/cate/expense_cate	expense_cate
低	http://192.168.133.196/home/cate/flow_type_check	flow_type_check
低	http://192.168.133.196/home/flow/index	index
低	http://192.168.133.196/home/cate/expense_cate_add	expense_cate_add
低	http://192.168.133.196/home/cate/cost_cate	cost_cate
低	http://192.168.133.196/home/cate/work_cate	work_cate
低	http://192.168.133.196/home/cate/industry_cate	industry_cate
低	http://192.168.133.196/home/cate/subject	subject
低	http://192.168.133.196/home/cate/services_cate	services_cate
低	http://192.168.133.196/home/keywords/index	index
低	http://192.168.133.196/user/department/index	index
低	http://192.168.133.196/user/position/index	index
低	http://192.168.133.196/oa/schedule/index	index
低	http://192.168.133.196/adm/meeting/meeting_cate	meeting_cate
低	http://192.168.133.196/oa/approve/copy	copy
低	http://192.168.133.196/user/user/index	index
低	http://192.168.133.196/oa/approve/index	index
低	http://192.168.133.196/user/personal/change	change
低	http://192.168.133.196/user/personal/leave	leave

低	http://192.168.133.196/adm/seal/seal_cate	seal_cate
低	http://192.168.133.196/oa/approve/list	list
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/oa/work/index	index
低	http://192.168.133.196/finance/expense/index	index
低	http://192.168.133.196/finance/income/index	index

发现电子邮件地址模式

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

CVSS 分数: 0.0

严重性	URL	实体
-----	-----	----

参考	http://192.168.133.196/user/user/index	index
----	---	-------

发现可能的服务器路径泄露模式

风险: 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修补程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/login/index.html	index.html
参考	http://192.168.133.196/home/login/lock.html	lock.html
参考	http://192.168.133.196/home/cate/flow_type	flow_type
参考	http://192.168.133.196/	
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/index/main.html	main.html
参考	http://192.168.133.196/home/flow/add	add
参考	http://192.168.133.196/oa/plan/calendar	calendar
参考	http://192.168.133.196/static/assets/layui/layui.js	layui.js

发现内部 IP 泄露模式

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 站点中的内部 IP 地址

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/user/user/index	index

客户端（JavaScript）Cookie 引用

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

CVSS 分数： 0.0

严重性

URL

实体

参考

<http://192.168.133.196/home/login/index.html>

layui.use(['form'], function() {var form = layui.
i.form,\$ = layui.\$,layer = layui.layer;// {U
i...

参考

<http://192.168.133.196/static/assets/gougu/module/admin.js>

layui.define(['element'], function (exports) {

应用程序错误		
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	
CVSS 分数:	0.0	
严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/oa/approve/index	limit
参考	http://192.168.133.196/user/personal/leave	limit
参考	http://192.168.133.196/oa/approve/list	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/user/personal/change	limit
参考	http://192.168.133.196/oa/plan/calendar	uid
参考	http://192.168.133.196/oa/approve/copy	limit
参考	http://192.168.133.196/home/cate/flow_type_check	id
参考	http://192.168.133.196/oa/plan/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/api/index/get_department_select	keyword
参考	http://192.168.133.196/home/cate/expense_cate_add	title
参考	http://192.168.133.196/home/cate/expense_cate_add	id
参考	http://192.168.133.196/home/cate/expense_cate_check	id
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/finance/invoice/index	limit
参考	http://192.168.133.196/oa/work/index	limit
参考	http://192.168.133.196/oa/schedule/calendar	uid
参考	http://192.168.133.196/oa/schedule/calendar	end
参考	http://192.168.133.196/oa/plan/calendar	end

参考	http://192.168.133.196/oa/schedule/index	limit
参考	http://192.168.133.196/oa/plan/calendar	start
参考	http://192.168.133.196/oa/schedule/calendar	start
参考	http://192.168.133.196/oa/work/index	send
参考	http://192.168.133.196/finance/income/index	limit
参考	http://192.168.133.196/finance/expense/index	limit
参考	http://192.168.133.196/home/api/log_list	limit
参考	http://192.168.133.196/home/login/login_submit	password

整数溢出

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

中

15.1.3 - Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. 229

不充分帐户封锁

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: Web 应用程序编程或配置不安全

固定值: 多次登录尝试失败后实施帐户封锁

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/login_sbmit	password

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_sbmit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html

“Content-Security-Policy”头缺失或不安全

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: 将服务器配置为使用安全策略的“Content-Security-Policy”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-Content-Type-Options”头缺失或不安全

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: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

“X-XSS-Protection”头缺失或不安全

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: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/	
低	http://192.168.133.196/home/login/index.html	index.html
低	http://192.168.133.196/home/api/get_article_list	get_article_list
低	http://192.168.133.196/home/api/get_view_log	get_view_log

Oracle 日志文件信息泄露

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 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: 关闭跟踪，限制对日志文件的访问，或者将其除去

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/finance/expense/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.log
低	http://192.168.133.196/adm/seal/	sqlnet.log
低	http://192.168.133.196/adm/meeting/	sqlnet.log
低	http://192.168.133.196/oa/approve/	sqlnet.trc
低	http://192.168.133.196/oa/work/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.log
低	http://192.168.133.196/user/user/	sqlnet.log
低	http://192.168.133.196/home/flow/	sqlnet.log
低	http://192.168.133.196/user/position/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.log
低	http://192.168.133.196/home/keywords/	sqlnet.trc
低	http://192.168.133.196/home/flow/	sqlnet.trc
低	http://192.168.133.196/user/personal/	sqlnet.log
低	http://192.168.133.196/user/department/	sqlnet.trc
低	http://192.168.133.196/home/cate/	sqlnet.trc
低	http://192.168.133.196/finance/expense/	sqlnet.trc
低	http://192.168.133.196/user/position/	sqlnet.log
低	http://192.168.133.196/user/personal/	sqlnet.trc
低	http://192.168.133.196/oa/approve/	sqlnet.log
低	http://192.168.133.196/oa/schedule/	sqlnet.trc
低	http://192.168.133.196/adm/meeting/	sqlnet.trc
低	http://192.168.133.196/adm/seal/	sqlnet.trc
低	http://192.168.133.196/oa/plan/	sqlnet.trc

低	http://192.168.133.196/oa/schedule/	sqlnet.log
低	http://192.168.133.196/oa/work/	sqlnet.trc
低	http://192.168.133.196/finance/income/	sqlnet.log
低	http://192.168.133.196/finance/income/	sqlnet.trc

查询中接受的主体参数

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/oa/plan/calendar	calendar
低	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
低	http://192.168.133.196/oa/schedule/calendar	calendar
低	http://192.168.133.196/home/login/login_submit	login_submit

发现压缩目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/user/department/	department.arc
低	http://192.168.133.196/adm/seal/	seal.rar
低	http://192.168.133.196/oa/schedule/	schedule.zip
低	http://192.168.133.196/home/cate/	cate.tar.gz
低	http://192.168.133.196/oa/approve/	approve.tar
低	http://192.168.133.196/home/keywords/	keywords.lzh
低	http://192.168.133.196/user/department/	department.lha
低	http://192.168.133.196/home/flow/	flow.tar.gz
低	http://192.168.133.196/user/department/	department.lzh
低	http://192.168.133.196/home/keywords/	keywords.tar
低	http://192.168.133.196/home/	home.ar
低	http://192.168.133.196/user/department/	department.tar
低	http://192.168.133.196/home/	home.ear
低	http://192.168.133.196/home/keywords/	keywords.arj
低	http://192.168.133.196/user/department/	department.arj
低	http://192.168.133.196/home/keywords/	keywords.arc
低	http://192.168.133.196/home/keywords/	keywords.tar.gz
低	http://192.168.133.196/user/department/	department.tar.gz
低	http://192.168.133.196/user/position/	position.zip
低	http://192.168.133.196/home/	home.tar.lzma
低	http://192.168.133.196/home/	home.war
低	http://192.168.133.196/home/	home.wim
低	http://192.168.133.196/home/cate/	cate.zip
低	http://192.168.133.196/user/position/	position.gz
低	http://192.168.133.196/home/flow/	flow.zip

低	http://192.168.133.196/user/position/	position.rar
低	http://192.168.133.196/home/keywords/	keywords.zip
低	http://192.168.133.196/home/cate/	cate.gz
低	http://192.168.133.196/home/flow/	flow.gz
低	http://192.168.133.196/home/cate/	cate.rar
低	http://192.168.133.196/home/flow/	flow.rar
低	http://192.168.133.196/home/cate/	cate.ace
低	http://192.168.133.196/home/flow/	flow.ace
低	http://192.168.133.196/home/cate/	cate.lha
低	http://192.168.133.196/home/flow/	flow.lha
低	http://192.168.133.196/home/cate/	cate.lzh
低	http://192.168.133.196/oa/plan/	plan.gz
低	http://192.168.133.196/home/keywords/	keywords.gz
低	http://192.168.133.196/user/position/	position.lzh
低	http://192.168.133.196/home/flow/	flow.lzh
低	http://192.168.133.196/user/department/	department.zip
低	http://192.168.133.196/home/keywords/	keywords.rar
低	http://192.168.133.196/home/cate/	cate.tar
低	http://192.168.133.196/user/department/	department.gz
低	http://192.168.133.196/user/user/	user.zip
低	http://192.168.133.196/home/flow/	flow.tar
低	http://192.168.133.196/home/keywords/	keywords.ace
低	http://192.168.133.196/home/cate/	cate.arj
低	http://192.168.133.196/user/position/	position.tar
低	http://192.168.133.196/user/department/	department.rar
低	http://192.168.133.196/user/user/	user.gz
低	http://192.168.133.196/home/flow/	flow.arj
低	http://192.168.133.196/home/keywords/	keywords.lha
低	http://192.168.133.196/home/cate/	cate.arc
低	http://192.168.133.196/user/department/	department.ace
低	http://192.168.133.196/home/flow/	flow.arc
低	http://192.168.133.196/oa/schedule/	schedule.gz

低	http://192.168.133.196/user/user/	user.rar
低	http://192.168.133.196/user/position/	position.lha
低	http://192.168.133.196/user/position/	position.arj
低	http://192.168.133.196/user/personal/	personal.zip
低	http://192.168.133.196/oa/work/	work.zip
低	http://192.168.133.196/user/user/	user.ace
低	http://192.168.133.196/oa/plan/	plan.rar
低	http://192.168.133.196/user/personal/	personal.gz
低	http://192.168.133.196/user/user/	user.lha
低	http://192.168.133.196/user/personal/	personal.rar
低	http://192.168.133.196/user/position/	position.arc
低	http://192.168.133.196/oa/schedule/	schedule.rar
低	http://192.168.133.196/user/user/	user.lzh
低	http://192.168.133.196/adm/seal/	seal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.lha
低	http://192.168.133.196/oa/approve/	approve.arj
低	http://192.168.133.196/oa/work/	work.gz
低	http://192.168.133.196/user/personal/	personal.ace
低	http://192.168.133.196/oa/plan/	plan.ace
低	http://192.168.133.196/user/position/	position.tar.gz
低	http://192.168.133.196/user/user/	user.tar
低	http://192.168.133.196/user/personal/	personal.lha
低	http://192.168.133.196/user/user/	user.arj
低	http://192.168.133.196/user/personal/	personal.lzh
低	http://192.168.133.196/finance/income/	income.lha
低	http://192.168.133.196/user/personal/	personal.tar
低	http://192.168.133.196/oa/approve/	approve.arc
低	http://192.168.133.196/user/user/	user.arc
低	http://192.168.133.196/user/user/	user.tar.gz
低	http://192.168.133.196/user/personal/	personal.arj
低	http://192.168.133.196/adm/seal/	seal.zip
低	http://192.168.133.196/adm/meeting/	meeting.tar

低	http://192.168.133.196/user/personal/	personal.arc
低	http://192.168.133.196/oa/approve/	approve.tar.gz
低	http://192.168.133.196/adm/seal/	seal.gz
低	http://192.168.133.196/user/personal/	personal.tar.gz
低	http://192.168.133.196/adm/meeting/	meeting.zip
低	http://192.168.133.196/oa/approve/	approve.zip
低	http://192.168.133.196/adm/meeting/	meeting.gz
低	http://192.168.133.196/adm/meeting/	meeting.arj
低	http://192.168.133.196/adm/seal/	seal.ace
低	http://192.168.133.196/adm/meeting/	meeting.arc
低	http://192.168.133.196/oa/approve/	approve.gz
低	http://192.168.133.196/adm/meeting/	meeting.rar
低	http://192.168.133.196/adm/seal/	seal.lha
低	http://192.168.133.196/oa/approve/	approve.rar
低	http://192.168.133.196/adm/meeting/	meeting.tar.gz
低	http://192.168.133.196/oa/approve/	approve.ace
低	http://192.168.133.196/adm/seal/	seal.lzh
低	http://192.168.133.196/oa/work/	work.rar
低	http://192.168.133.196/adm/seal/	seal.tar
低	http://192.168.133.196/oa/approve/	approve.lha
低	http://192.168.133.196/adm/seal/	seal.arj
低	http://192.168.133.196/oa/approve/	approve.lzh
低	http://192.168.133.196/oa/schedule/	schedule.ace
低	http://192.168.133.196/adm/seal/	seal.arc
低	http://192.168.133.196/oa/plan/	plan.lha
低	http://192.168.133.196/adm/meeting/	meeting.ace
低	http://192.168.133.196/adm/meeting/	meeting.lzh
低	http://192.168.133.196/user/position/	position.ace
低	http://192.168.133.196/oa/plan/	plan.zip
低	http://192.168.133.196/oa/work/	work.ace
低	http://192.168.133.196/oa/schedule/	schedule.lha
低	http://192.168.133.196/oa/plan/	plan.lzh

低	http://192.168.133.196/oa/plan/	plan.tar
低	http://192.168.133.196/oa/schedule/	schedule.tar
低	http://192.168.133.196/oa/work/	work.lzh
低	http://192.168.133.196/oa/plan/	plan.arj
低	http://192.168.133.196/oa/work/	work.tar
低	http://192.168.133.196/oa/schedule/	schedule.arj
低	http://192.168.133.196/oa/plan/	plan.arc
低	http://192.168.133.196/finance/expense/	expense.zip
低	http://192.168.133.196/finance/income/	income.zip
低	http://192.168.133.196/oa/schedule/	schedule.arc
低	http://192.168.133.196/oa/work/	work.arj
低	http://192.168.133.196/oa/plan/	plan.tar.gz
低	http://192.168.133.196/finance/expense/	expense.gz
低	http://192.168.133.196/finance/income/	income.gz
低	http://192.168.133.196/oa/work/	work.arc
低	http://192.168.133.196/oa/schedule/	schedule.tar.gz
低	http://192.168.133.196/finance/expense/	expense.rar
低	http://192.168.133.196/oa/work/	work.tar.gz
低	http://192.168.133.196/finance/income/	income.rar
低	http://192.168.133.196/finance/expense/	expense.ace
低	http://192.168.133.196/finance/income/	income.ace
低	http://192.168.133.196/finance/expense/	expense.lha
低	http://192.168.133.196/finance/expense/	expense.lzh
低	http://192.168.133.196/finance/income/	income.lzh
低	http://192.168.133.196/finance/expense/	expense.tar
低	http://192.168.133.196/finance/income/	income.tar
低	http://192.168.133.196/finance/expense/	expense.arj
低	http://192.168.133.196/finance/income/	income.arj
低	http://192.168.133.196/finance/expense/	expense.arc
低	http://192.168.133.196/finance/income/	income.arc
低	http://192.168.133.196/finance/income/	income.tar.gz
低	http://192.168.133.196/finance/expense/	expense.tar.gz

低	http://192.168.133.196/oa/work/	work.lha
低	http://192.168.133.196/oa/schedule/	schedule.lzh

检测到隐藏目录

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

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/customer/	customer/
低	http://192.168.133.196/install/	install/
低	http://192.168.133.196/home/	home/

跨帧脚本编制防御缺失或不安全

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: 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/home/index/index	index
低	http://192.168.133.196/home/login/lock.html	lock.html
低	http://192.168.133.196/home/	

启用了不安全的“OPTIONS”HTTP 方法

风险: 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: 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: 禁用 WebDAV，或者禁止不需要的 HTTP 方法。

CVSS 分数: 5.0

严重性	URL	实体
低	http://192.168.133.196/	/

JSON 中反映的未清理用户输入

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/home/api/log_list	limit

发现电子邮件地址模式

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

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/user/user/index	index

发现内部 IP 泄露模式

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** 站点中的内部 IP 地址

CVSS 分数: 0.0

严重性	URL	实体
参考	http://192.168.133.196/home/api/log_list	log_list
参考	http://192.168.133.196/user/user/index	index

整数溢出		
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	
CVSS 分数:	0.0	
严重性	URL	实体
参考	http://192.168.133.196/home/keywords/index	limit
参考	http://192.168.133.196/user/user/index	limit
参考	http://192.168.133.196/home/cate/flow_type_check	status
参考	http://192.168.133.196/home/cate/expense_cate_check	status
参考	http://192.168.133.196/home/api/log_list	limit

中

15.1.4 - Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

7

跨站点请求伪造

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/api/get_article_list	get_article_list
中	http://192.168.133.196/home/api/get_note_list	get_note_list
中	http://192.168.133.196/api/index/get_department_select	get_department_select
中	http://192.168.133.196/home/cate/expense_cate_check	expense_cate_check
中	http://192.168.133.196/home/login/lock.html	lock.html
中	http://192.168.133.196/home/login/login_submit	login_submit

使用 HTTP 动词篡改的认证旁路

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

CVSS 分数: 6.4

严重性	URL	实体
中	http://192.168.133.196/home/login/lock.html	lock.html