# 铱迅漏洞扫描系统
# 安全评估报告

| | |
|---|---|
| 报表名称 | 单IP报表<br>39.105.86.118 |
| 报表编号 | NVS-20191012-001H |
| 生成时间 | 2019-10-12 13:51:33 |
| 任务名称 | http://39.105.86.118/ |

# 目录

# 1 综述

主机 39.105.86.118 共存在风险 77 个（另有信息级风险15个），信息安全风险总评级为 中风险 。

高风险及以上风险总数 0 个，其中主机漏洞 0 个，Web漏洞 0 个，弱密码 0 个。

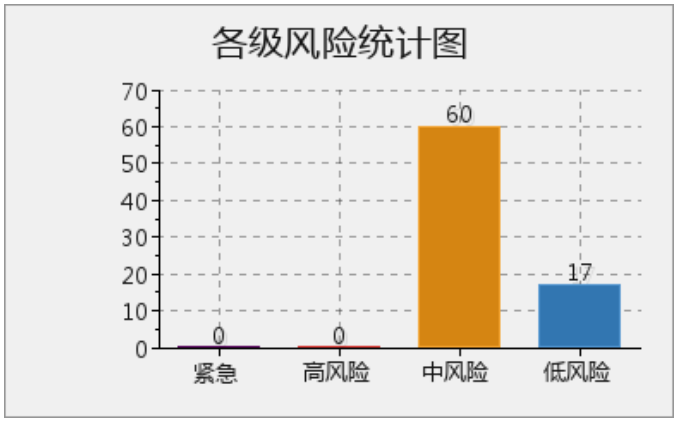
该主机下所有域名中不存在含有高风险漏洞的域名。

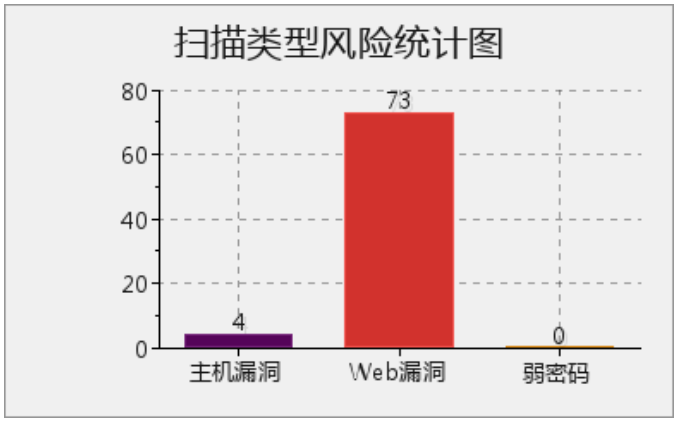
主机漏洞中高风险及以上漏洞为 0 个。

Web漏洞中高风险及以上漏洞为 0 个。

弱密码 0 个。

# 2 总体风险分析




# 3 主机信息统计

## 3.1 基本信息

| | |
|---|---|
| 主机IP | 39.105.86.118 |
| MAC地址 | -- |
| 操作系统 | Linux Kernel 4.4 on Ubuntu 16.04 (xenial) |

## 3.2 端口信息

| 端口 | 协议 | 服务 | 版本 |
|---|---|---|---|
| 22 | TCP | ssh | OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0) |
| 80 | TCP | http | Apache httpd 2.4.18 ((Ubuntu)) |

# 4 主机漏洞分析

## 4.1 主机漏洞统计

| 类别 | 紧急 | 高风险 | 中风险 | 低风险 | 信息 | 总计（不含信息） |
|---|---|---|---|---|---|---|
| Web服务器漏洞检测 | 0 | 0 | 2 | 0 | 5 | 2 |
| Windows漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| MacOS漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| UNIX漏洞检测 | 0 | 0 | 1 | 0 | 2 | 1 |
| 数据库漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| CGI漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| DNS漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| FTP/TFTP漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| 虚拟化漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| 网络设备漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| 邮件服务器漏洞检测 | 0 | 0 | 0 | 0 | 0 | 0 |
| 杂项漏洞检测 | 0 | 0 | 0 | 1 | 8 | 1 |

## 4.2 主机漏洞列表

### 4.2.1 Web服务器漏洞检测

本次扫描共发现该风险 2 种，共 2 个。另有信息级风险 5 种，共 5 个。

[ 中风险 ] 多个厂商TLS协议和SSL协议会话协商明文注入漏洞

主机列表（共1项）

| 主机及端口 | 输出信息 |
|---|---|
| 39.105.86.118 [ tcp / 22 ] | -- |

风险描述

[CVE-2009-3555]

传输层安全协议（TLS）是确保互联网上通信应用和其用户隐私的协议。

Apache HTTP Server 2.2.14及之前版本，OpenSSL 0.9.8l之前版本，GnuTLS 2.8.5及之前版本，Mozilla Network Security Services (NSS) 3.12.4及之前版本，多个Cisco产品，以及其他产品的TLS协议和SSL协议中存在会话协商明文注入漏洞。

由于TLS协议和SSL协议实现模块没有适当将会话协商与现存连接关联，中间人攻击者可以通过发送一个未认证的请求，将数据注入到受TLS和SSL协议保护的HTTP会话和其它类型会话中。

解决方案

联系供应商或产品文档删除weakciphers商量。

相关编号

CVE :CVE-2009-3555

CNNVD :CNNVD-200911-069

参考信息

http//www.securityfocus.com/archive/1/archive/1/508075/100/0/threaded
http//www.securityfocus.com/archive/1/archive/1/507952/100/0/threaded
http//www.securityfocus.com/archive/1/archive/1/508130/100/0/threaded
http//www.securityfocus.com/archive/1/archive/1/515055/100/0/threaded
http//www.securityfocus.com/archive/1/archive/1/516397/100/0/threaded
http//archives.neohapsis.com/archives/bugtraq/2013-11/0120.html
http//seclists.org/fulldisclosure/2009/Nov/139
http//marc.info/?l=apache-httpd-announce&m=125755783724966&w=2
http//marc.info/?l=cryptography&m=125752275331877&w=2
http//lists.gnu.org/archive/html/gnutls-devel/2009-11/msg00029.html
http//www.openwall.com/lists/oss-security/2009/11/05/3
http//www.openwall.com/lists/oss-security/2009/11/05/5
http//www.openwall.com/lists/oss-security/2009/11/06/3
http//www.openwall.com/lists/oss-security/2009/11/07/3
http//www.ietf.org/mail-archive/web/tls/current/msg03928.html
http//www.ietf.org/mail-archive/web/tls/current/msg03948.html
http//www.openwall.com/lists/oss-security/2009/11/20/1
http//www.openwall.com/lists/oss-security/2009/11/23/10
http//www-1.ibm.com/support/search.wss?rs=0&q=PM00675&apar=only
http//www-01.ibm.com/support/docview.wss?uid=swg1IC67848
http//www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http//www-01.ibm.com/support/docview.wss?uid=swg1IC68054
http//www-01.ibm.com/support/docview.wss?uid=swg1IC68055
http//lists.apple.com/archives/security-announce/2010/Jan/msg00000.html
http//lists.apple.com/archives/security-announce/2010//May/msg00001.html
http//lists.apple.com/archives/security-announce/2010//May/msg00002.html
http//www.cisco.com/en/US/products/products_security_advisory09186a0080b01d1d.shtml
http//www.debian.org/security/2009/dsa-1934
http//www.debian.org/security/2011/dsa-2141
http//www.debian.org/security/2015/dsa-3253
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg00428.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg00442.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg00449.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg00634.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg00645.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg01029.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg01020.html
https//www.redhat.com/archives/fedora-package-announce/2009-December/msg00944.html
http//lists.fedoraproject.org/pipermail/package-announce/2010-April/039561.html
http//lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html
http//lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html

http//lists.fedoraproject.org/pipermail/package-announce/2010-October/049702.html
http//lists.fedoraproject.org/pipermail/package-announce/2010-October/049528.html
http//lists.fedoraproject.org/pipermail/package-announce/2010-October/049455.html
http//security.gentoo.org/glsa/glsa-200912-01.xml
http//security.gentoo.org/glsa/glsa-201203-22.xml
http//security.gentoo.org/glsa/glsa-201406-32.xml
http//h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01945686
http//h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01945686
http//marc.info/?l=bugtraq&m=127419602507642&w=2
http//marc.info/?l=bugtraq&m=127419602507642&w=2
http//itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02273751
http//itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02273751
http//h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02436041
http//www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02512995
http//www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02512995
http//marc.info/?l=bugtraq&m=130497311408250&w=2
http//marc.info/?l=bugtraq&m=130497311408250&w=2
http//marc.info/?l=bugtraq&m=132077688910227&w=2
http//marc.info/?l=bugtraq&m=132077688910227&w=2
http//www.securityfocus.com/archive/1/522176
http//www.securityfocus.com/archive/1/522176

[ 中风险 ] Apache HTTP Server 安全漏洞

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

[CVE-2016-0736]
Apache HTTP Server是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。
Apache HTTP Server 2.4.0版本至2.4.23版本中存在安全漏洞。攻击者可利用该漏洞解密和更改会话数据。

[CVE-2016-2161]
Apache HTTP Server是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。
Apache HTTP Server
2.4.0版本至2.4.23版本中存在安全漏洞。攻击者可通过向mod_auth_digest发送恶意的利用该漏洞造成服务器和进程崩溃。

[CVE-2016-5387]
Apache HTTP Server是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。

Apache HTTP Server 2.4.23及之前的版本中存在安全漏洞，该漏洞源于程序没有解决RFC 3875模式下的命名空间冲突。程序没有正确处理来自HTTP_PROXY环境变量中不可信客户端数据应用程序。远程攻击者借助HTTP请求中特制的Proxy header消息利用该漏洞实施中间人攻击，指引服务器发送连接到任意主机。

[CVE-2016-8740]
Apache HTTP Server是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。
Apache HTTP Server 2.4.17至2.4.23版本的‘mod_http2’模块中存在安全漏洞，该漏洞源于当Protocols配置文件包含h2或h2c时，程序没有限制request-header长度。远程攻击者可通过发送特制的HTTP/2请求利用该漏洞造成拒绝服务（内存消耗）。

[CVE-2016-8743]
Apache HTTP Server是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。
Apache HTTP Server中存在安全漏洞。远程攻击者可利用该漏洞执行任意的HTTP代码，使服务器返回一个拆分响应。以下版本受到影响：Apache HTTP Server 2.4.23版本，2.4.20版本，2.4.18版本，2.4.17版本，2.4.16版本，2.4.12版本，2.4.10版本，2.4.9版本，2.4.7版本，2.4.6版本，2.4.4版本，2.4.3版本，2.4.2版本，2.4.1版本。

### 解决方案

升级到Apache版本2.4.25或更高版本。
请注意，可以通过应用程序来减轻“httpoxy”漏洞
在供应商咨询中引用的工作区或补丁
asf-httpoxy-response.txt。此外，为了减轻其他的影响
漏洞，确保受影响的模块(mod_session_crypto，mod_auth_digest和mod_http2)没有使用。

### 相关编号

CVE :CVE-2016-0736,CVE-2016-2161,CVE-2016-5387,CVE-2016-8740,CVE-2016-8743
CNNVD :CNNVD-201612-646

### 参考信息

https://httpd.apache.org/dev/dist/Announcement2.4.html
http://httpd.apache.org/security/vulnerabilities_24.html
https://github.com/apache/httpd/blob/2.4.x/CHANGES
https://www.apache.org/security/asf-httpoxy-response.txt
https://httpoxy.org

[ 信息 ] Web服务器目录列举

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

这个插件试图确定各种常见远程Web服务器存在的目录。通过发送一个请求到目录，Web服务器的响应代码表示，判断它是否是一个有效的目录。

解决方案

n/a

相关编号

参考信息

http://projects.webappsec.org/Predictable-Resource-Location

[ 信息 ] Web镜像漏洞

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

这个脚本可以远程Web镜像和提取所使用远程主机的CGI程序的列表。
建议修改镜像在客户端的“选项”部分的页面数量。

解决方案

n/a

相关编号

参考信息

[ 信息 ] HTTP服务器的Cookie设置

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

HTTP cookies是通过网络提交的信息服务器和发送回浏览器。由于HTTP是无状态的协议，COOKIES机制跟踪会话。当它被抓取时这个插件显示由HTTP cookie的列表Web服务器。

解决方案

n/a

相关编号

参考信息

[ 信息 ] 远程WEB服务器允许OPTIONS请求

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

通过调用选择方法,可以确定哪些HTTP方法是允许在每个目录。

解决方案

n/a

相关编号

参考信息

[ 信息 ] 外部URL

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

系统爬虫获取到链接到外部网站Web服务器的HREF链接。

解决方案

n/a

相关编号

参考信息

### 4.2.2 Windows漏洞检测

本次扫描没有发现该风险。

### 4.2.3 MacOS漏洞检测

本次扫描没有发现该风险。

### 4.2.4 UNIX漏洞检测

本次扫描共发现该风险 1 种，共 1 个。另有信息级风险 2 种，共 2 个。

[ 中风险 ] OpenSSL DTLS 双重释放漏洞

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 22 ] | -- |

风险描述

[CVE-2014-3505]
OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL的DTLS实现过程中d1_both.c文件存在双重释放漏洞。远程攻击者可通过发送特制DTLS数据包利用该漏洞造成拒绝服务（应用程序崩溃）。以下版本受到影响：OpenSSL 0.9.8zb之前0.9.8版本，1.0.0n之前1.0.0版本，1.0.1i之前1.0.1版本。
[CVE-2014-3506]
OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL的DTLS实现过程中的d1_both.c文件存在安全漏洞。远程攻击者可通过发送特制的DTLS握手消息利用该漏洞造成拒绝服务（内存消耗）。以下版本受到影响：OpenSSL 0.9.8zb之前0.9.8版本，1.0.0n之前1.0.0版本，1.0.1i之前1.0.1版本。
[CVE-2014-3507]
OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL的DTLS实现中的d1_both.c文件存在内存泄露漏洞，该漏洞源于程序接收到零长度DTLS分片时，没有正确处理插入函数的返回值。远程攻击者可利用该漏洞造成拒绝服务（内存消耗）。以下版本受到影响：OpenSSL 0.9.8zb之前0.9.8版本，1.0.0n之前1.0.0版本，1.0.1i之前1
[CVE-2014-3509]
OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.0.0n之前1.0.0版本和1.0.1i之前1.0.1版本的t1_lib.c文件中的‘ssl_parse_serverhello_tlsext’函数中存在竞争条件漏洞。当程序使用多线程和会话恢复功能时，远程攻击者可通过发送‘Elliptic Curve (EC) Supported Poi
[CVE-2014-3510]
OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL的s3_clnt.c文件中‘ssl3_send_client_key_exchange’函数存在安全漏洞。远程攻击者可通过带有匿名的DH或ECDH加密套件的握手消息利用该漏洞造成拒绝服务（空指针逆向引用和客户端应用程序崩溃）。以下版本受到影响：OpenSSL 0.9.8zb之前0.9.8版本，1
[CVE-2014-3512]
OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.0.1i之前1.0.1版本的SRP实现的crypto/srp/srp_lib.c文件中存在缓冲区溢出漏洞。远程攻击者可借助无效的SRP‘g’、‘A’、‘B’参数利用该漏洞造成拒绝服务（应用程序崩溃）。
[CVE-2014-5139]

OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.0.1i之前1.0.1版本的t1_lib.c文件的‘ssl_set_client_disabled’函数中存在安全漏洞。远程攻击者可通过发送ServerHello消息利用该漏洞造成拒绝服务（空指针逆向引用和客户端应用程序崩溃）。

## 解决方案

n/a

## 相关编号

CVE :CVE-2014-3505,CVE-2014-3506,CVE-2014-3507,CVE-2014-3509,CVE-2014-3510,CVE-2014-3512,CVE-2014-5139

CNNVD :CNNVD-201408-126,CNNVD-201408-128,CNNVD-201408-131,CNNVD-201408-124,CNNVD-201408-130,CNNVD-201408-129,CNNVD-201408-127

## 参考信息

https//lists.balabit.hu/pipermail/syslog-ng-announce/2014-September/000196.html
http//www.debian.org/security/2014/dsa-2998
http//lists.fedoraproject.org/pipermail/package-announce/2014-August/136470.html
http//lists.fedoraproject.org/pipermail/package-announce/2014-August/136473.html
http//security.gentoo.org/glsa/glsa-201412-39.xml
http//marc.info/?l=bugtraq&m=141077370928502&w=2
http//marc.info/?l=bugtraq&m=140853041709441&w=2
http//marc.info/?l=bugtraq&m=140853041709441&w=2
http//marc.info/?l=bugtraq&m=142660345230545&w=2
http//marc.info/?l=bugtraq&m=142660345230545&w=2
http//www.mandriva.com/security/advisories?name=MDVSA-2014
ftp//ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2014-008.txt.asc
http//rhn.redhat.com/errata/RHSA-2014-1256.html
http//rhn.redhat.com/errata/RHSA-2014-1297.html
http//lists.opensuse.org/opensuse-updates/2014-08/msg00036.html
http//lists.opensuse.org/opensuse-security-announce/2016-03/msg00011.html
http//www.securityfocus.com/bid/69081
http//www.securitytracker.com/id/1030693
http//secunia.com/advisories/59221
http//secunia.com/advisories/60687
http//secunia.com/advisories/60824
http//secunia.com/advisories/60917
http//secunia.com/advisories/60921
http//secunia.com/advisories/60938
http//secunia.com/advisories/61775
http//secunia.com/advisories/61959

http//secunia.com/advisories/59756
http//secunia.com/advisories/60803
http//secunia.com/advisories/61040
http//secunia.com/advisories/61100
http//secunia.com/advisories/61250
http//secunia.com/advisories/61184
http//secunia.com/advisories/59743
http//secunia.com/advisories/60778
http//secunia.com/advisories/58962
http//secunia.com/advisories/59700
http//secunia.com/advisories/59710
http//secunia.com/advisories/60022
http//secunia.com/advisories/60684
http//secunia.com/advisories/60221
http//secunia.com/advisories/60493

[ 信息 ] 检测到SSH服务器类型和版本信息

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 22 ] | -- |

风险描述

可能通过发送一个空的认证请求来获取到远程SSH服务器的信息。

解决方案

n/a

相关编号

参考信息

[ 信息 ] 检测到SSH协议支持的版本

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 22 ] | -- |

风险描述

这个插件可以确定的远程SSH进程所支持的SSH协议版本。

解决方案

n/a

相关编号

参考信息

### 4.2.5 数据库漏洞检测

本次扫描没有发现该风险。

### 4.2.6 CGI漏洞检测

本次扫描没有发现该风险。

### 4.2.7 DNS漏洞检测

本次扫描没有发现该风险。

### 4.2.8 FTP/TFTP漏洞检测

本次扫描没有发现该风险。

### 4.2.9 虚拟化漏洞检测

本次扫描没有发现该风险。

### 4.2.10 网络设备漏洞检测

本次扫描没有发现该风险。

### 4.2.11 邮件服务器漏洞检测

本次扫描没有发现该风险。

### 4.2.12 杂项漏洞检测

本次扫描共发现该风险 1 种，共 1 个。另有信息级风险 6 种，共 8 个。

[ 低风险 ] Web服务器使用明文身份认证表单

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

远程Web服务器包含多个HTML表单字段，在明文的远程Web服务器输入类型'密码'发送信息。攻击者窃听的网络浏览器和之间的交通服务器可获取合法用户的登录名和密码。

解决方案

通过HTTPS传输的内容，确保每一个敏感的形式。

相关编号

参考信息

[ 信息 ] 系统的TCP扫描器（辅助插件）

主机列表（共2项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 22 ] | -- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

解决方案

相关编号

参考信息

[ 信息 ] 系统SYN扫描器（辅助插件）

主机列表（共2项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 22 ] | -- |
| 39.105.86.118 [ tcp / 80 ] | -- |

风险描述

解决方案

相关编号

参考信息

[ 信息 ] TCP/IP时间戳支持

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 0 ] | -- |

风险描述

远程主机上实现的TCP时间戳是由RFC1323定义的。该功能的作用是，该远程主机的正常运行时间是可以计算的。

解决方案

n/a

相关编号

参考信息

链接：http://www.ietf.org/rfc/rfc1323.txt

[ 信息 ] 远程主机操作系统识别

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 0 ] | -- |

风险描述

使用各种远程协议（TCP / IP，SMB, HTTP，NTP，SNMP等）来探测远程主机运行的系统及版本信息。

解决方案

n/a

相关编号

参考信息

[ 信息 ] 远程主机设备类型检测

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 0 ] | -- |

风险描述

基于远程主机操作系统来确定远程主机的系统类型(如:打印机,路由器,通用电脑等等)。

解决方案

n/a

相关编号

参考信息

[ 信息 ] 通用平台枚举(CPE)

主机列表（共1项）

| 主机及端口 | 输出信息 |
| --- | --- |
| 39.105.86.118 [ tcp / 0 ] | -- |

风险描述

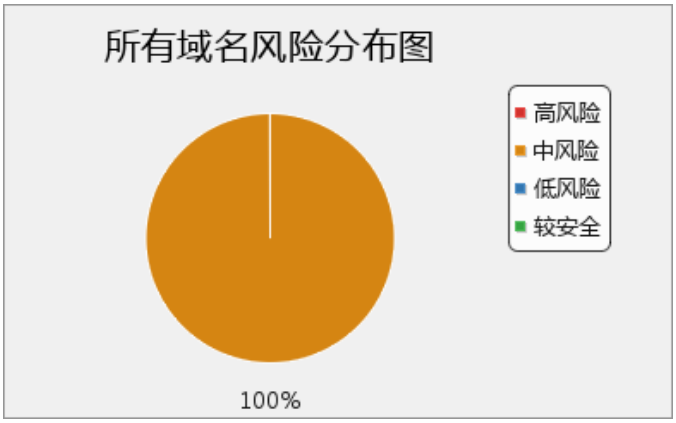
解决方案

相关编号

参考信息

# 5 Web漏洞分析

## 5.1 概述




本次共扫描域名 1 个，其中：
高风险域名 0 个；
中风险域名 1 个，占 100% ；
低风险域名 0 个；
较安全域名 0 个。

## 5.2 Web漏洞统计

| 域名 | 标题 | 紧急 | 高风险 | 中风险 | 低风险 | 信息 | 域名风险评级 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| http://39.105.86.118/ | 河南城建学院... | 0 | 0 | 57 | 16 | 0 | 中风险 |

## 5.3 Web漏洞列表

### 5.3.1 SQL注入

本次扫描没有发现该风险。

### 5.3.2 弱密码

本次扫描没有发现该风险。

### 5.3.3 目录遍历

本次扫描共发现该风险 1 种，共 54 个。

[ 中风险 ] 检测到遍历目录漏洞

URL列表（共54项）

| URL | http://39.105.86.118/include/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/css/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/css/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/js/lib/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/js/ |
| --- | --- |

| | |
|---|---|
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| | |
|---|---|
| URL | http://39.105.86.118/images/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| | |
|---|---|
| URL | http://39.105.86.118/lib/menu/css/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| | |
|---|---|
| URL | http://39.105.86.118/lib/menu/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| | |
|---|---|
| URL | http://39.105.86.118/lib/layui230/css/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| | |
|---|---|
| URL | http://39.105.86.118/lib/layui230/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| | |
|---|---|
| URL | http://39.105.86.118/person/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/voteinformation/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/css/modules/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/font/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/images/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/lay/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/bootstrap/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/ckeditor/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/excel/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layer/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/phpass/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/upload/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/menu/fonts/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/menu/images/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/menu/js/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/css/modules/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/font/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/images/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/lay/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/css/modules/laydate/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/css/modules/layer/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/images/face/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/lay/modules/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/ckeditor/adapters/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/ckeditor/lang/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/ckeditor/plugins/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/ckeditor/skins/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/excel/PHPExcel/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layer/mobile/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layer/theme/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/phpass/c/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/upload/css/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/upload/images/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/upload/swfupload/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/menu/js/extends/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/css/modules/laydate/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/css/modules/layer/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/images/face/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui230/lay/modules/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layer/theme/default/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/css/modules/laydate/default/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

| URL | http://39.105.86.118/lib/layui245/css/modules/layer/default/ |
| --- | --- |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。 |

### 风险描述

可以查看和下载特定Web应用程序虚拟目录下的内容，其中可能包含访问被限制的文件。

原因：开启了目录浏览功能。

Web 服务器通常配置成不允许目录浏览。不过，如果Web服务器配置不当，便有可能发送对于特定目录（而不是文件）的请求来获取目录列表。名称为“some_dir”的目录，其目录的列出请求示例如下：http://www.xxxx.com/some_dir/

利用Web服务器和Web应用程序中会强迫Web服务器返回目录列表的特定问题，例如“URL 诡计”攻击，或形态异常的HTTP请求，是另一个获取目录列表的可能方式。可以从应用程序或服务器供应商下载补丁，以解决这些安全漏洞。
在某些运行于Win32操作系统的Web服务器中，使用短文件名（8.3 DOS 格式）可以略过访问控制。
例如，Web服务器会拒绝浏览/longdirname/目录，但它的DOS 8.3对等名称/LONGDI~1/却开放浏览。
注意：攻击者使用目录列表来查找Web目录中，通常不通过Web站点上的链接显现出来的文件。配置文件及可能含有敏感信息的Web应用程序其他组件，都可以利用这个方式来查看。

解决方案

1. 将 Web 服务器配置成拒绝列出目录。
2. 根据 Web 服务器或 Web
应用程序上现有的问题来下载特定安全补丁。部分已知的目录列表问题列在这个咨询的“引用”字段中。
3. 利用“CERT”咨询中的变通方法（在这项咨询的“引用”字段中）来修订短文件名（8.3 DOS 格式）问题：
----a. 想要完全由Web服务器来保护的文件仅用 8.3 标准短文件名。在FAT文件系统（16
位）上，您可以启用“Win31FileSystem”注册表键（设为
1，注册表路径：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\）来强制这一点。
----b. 在 NTFS（32 位）上，您可以启用“NtfsDisable8dot3NameCreation”注册表键（设为
1，注册表路径：HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control\FileSystem\）来禁用创建长文件名文件的8.3 标准短文件名。不过，这个步骤可能会引起与16 位应用程序的兼容性问题。
----c. 使用基于NTFS的ACL（目录或文件级别的访问控制表）来扩增或替换基于Web服务器的安全。

## 5.3.4 系统命令执行

本次扫描没有发现该风险。

## 5.3.5 越权访问

本次扫描没有发现该风险。

## 5.3.6 信息泄露

本次扫描共发现该风险 1 种，共 10 个。

[ 低风险 ] 发现电子邮件地址模式

URL列表（共10项）

| URL | http://39.105.86.118/ |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/?usertype=1&usertype=2 |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/lib/JSEncrypt.js |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/icons/blank.gif |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/icons/back.gif |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/icons/unknown.gif |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/index.php |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/icons/text.gif |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/icons/folder.gif |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

| URL | http://39.105.86.118/js/lib/base64.js |
| --- | --- |
| 风险评级 | 低风险 |

| | |
|---|---|
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 检测到邮件信息，可能导致信息泄露。 |

#### 风险描述

发现页面上存在电子邮箱地址，可能存在敏感信息泄露。

#### 解决方案

删除页面上不必要存在的电子邮箱地址。

### 5.3.7 跨站脚本攻击

本次扫描共发现该风险 3 种，共 6 个。

[ 中风险 ] 表单CSRF攻击

URL列表（共3项）

| | |
|---|---|
| URL | http://39.105.86.118/ |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 该页面表单容易受到CSRF攻击，请检查该页面所有表单。 |

| | |
|---|---|
| URL | http://39.105.86.118/index.php |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 该页面表单容易受到CSRF攻击，请检查该页面所有表单。 |

| | |
|---|---|
| URL | http://39.105.86.118/person/update_dept_user.php |
| 风险评级 | 中风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 该页面表单容易受到CSRF攻击，请检查该页面所有表单。 |

#### 风险描述

所谓的CSRF(跨站请求伪造)攻击，就是攻击者盗用了被攻击者的身份，以被攻击者的名义发送恶意请求。CSRF漏洞可能会危及最终用户的数据和操作，如果被攻击对象是管理员，可能会危及整个Web应用程序。

#### 解决方案

详细检查该页面表单是否需要CSRF防护。

如果需要，解决方法如下：

1.使用token，增加一隐藏表单项，服务器校验该token合法性。

[ 低风险 ] 客户端（ JavaScript ） Cookie引用

URL列表（共2项）

| | |
|---|---|
| URL | http://39.105.86.118/lib/jquery.cookie.js |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | Cookie 是在客户端创建的。代码用于操纵站点的 cookie。可以将实施 cookie 逻辑的功能移至客户端（浏览器）。这样一来，攻击者就能发送其本无权发送的 cookie。 |

| | |
|---|---|
| URL | http://39.105.86.118/lib/ckeditor/ckeditor.js |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | Cookie 是在客户端创建的。代码用于操纵站点的 cookie。可以将实施 cookie 逻辑的功能移至客户端（浏览器）。这样一来，攻击者就能发送其本无权发送的 cookie。 |

风险描述

Cookie 是在客户端创建的。代码用于操纵站点的 cookie。可以将实施 cookie
逻辑的功能移至客户端（浏览器）。这样一来，攻击者就能发送其本无权发送的 cookie。

解决方案

Cookie 是在客户端创建的，可能会被恶意用户篡改，所以建议利用Session进行控制。

[ 低风险 ] 点击劫持

URL列表（共1项）

| | |
|---|---|
| URL | http://39.105.86.118/ |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | 服务器未设置X-Frame-Options响应头，易受到点击劫持攻击 |

风险描述

点击劫持是一种视觉上的欺骗手段。攻击者使用一个透明的、不可见的iframe，覆盖在一个网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击在iframe页面的一些功能性按钮上。

解决方案

设置X-Frame-Options响应头
它有三个可选的值：
DENY
SAMEORIGIN
ALLOW-FROM origin

当值为DENY时，浏览器会拒绝当前页面加载任何frame页面；若值为SAMEORIGIN，则frame页面的地址只能为同源域名下的页面；若值为ALLOW-FROM，则可以定义允许frame加载的页面地址。

### 5.3.8 拒绝服务

本次扫描没有发现该风险。

### 5.3.9 资源位置可预测

本次扫描没有发现该风险。

### 5.3.10 逻辑错误

本次扫描没有发现该风险。

### 5.3.11 配置不当

本次扫描没有发现该风险。

### 5.3.12 内容电子欺骗

本次扫描没有发现该风险。

### 5.3.13 外链信息

本次扫描共发现该风险 1 种，共 3 个。

[ 低风险 ] 检测出网站存在死链接

URL列表（共3项）

| URL | http://39.105.86.118/lib/Login.html?r= |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | -- |

| URL | http://39.105.86.118/lib/PhoneBinding.html?r= |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |
| 漏洞简述 | -- |

| URL | http://39.105.86.118/lib/Role.html?r= |
| --- | --- |
| 风险评级 | 低风险 |
| 相关域名 | http://39.105.86.118/ 访问域名 访问URL |

| 漏洞简述 | -- |
| --- | --- |

### 风险描述

死链就是服务器的地址已经改变了，无法找到当前地址位置。这样会影响到网站的用户体验和搜索引擎优化。

### 解决方案

去除死链接。

## 6 弱密码

本次扫描没有发现弱密码。