Web VPN

Web VPN 3389 RDP 3389

image.png
Image not found or type unknown

SmartBear RDP

3.142.53.101
ec2-3-142-53-101.us-east-2.compute.amazonaws.com
Amazon Technologies Inc.
United States, Hilliard
cloud self-signed

SSL Certificate
Issued By:
|- Common Name:
QA-SmartBear
Issued To:
|- Common Name:
QA-SmartBear
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10/Windows Server 2019
  OS Build: 10.0.17763
  Target Name: QA-SMARTBEAR
  NetBIOS Domain Name: QA-SMARTBEAR
  NetBIOS Computer Name: QA-SMARTBEAR
  ...
```

RDP SMB WinRM VNC App

Lab

raven-medicine.org

Port 21: vsftpd 3.0.3

FTP

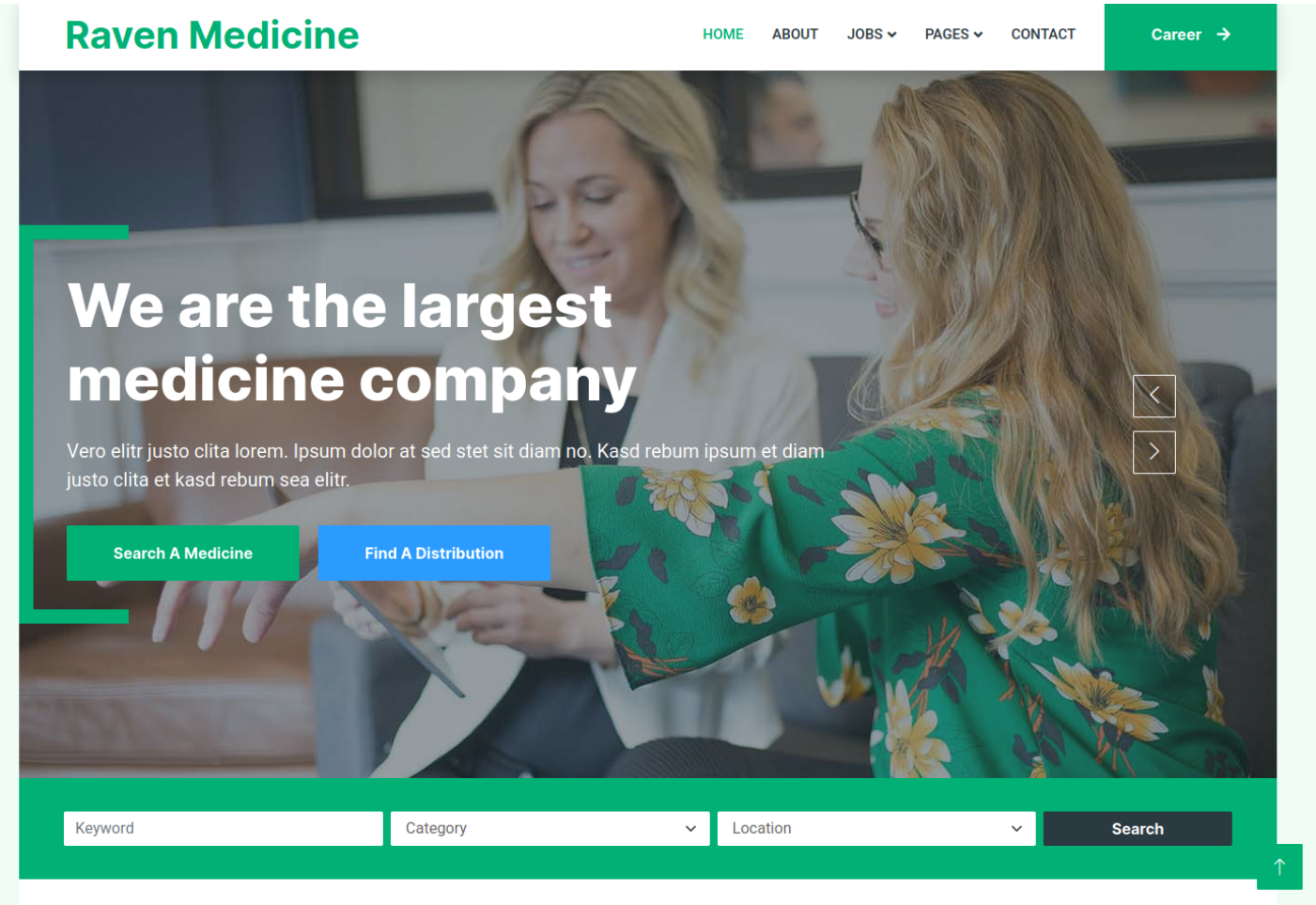
```
┌──(root㉿kali)-[~/Desktop]
└─# ftp raven-medicine.org
Connected to raven-medicine.org.
220 (vsFTPd 3.0.3)
Name (raven-medicine.org:root): 
```

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 110 vsftpd 3.0.3
Service Info: OS: Unix
```

Port 80: Apache 2.4.41

Apache 2.4.41 Web

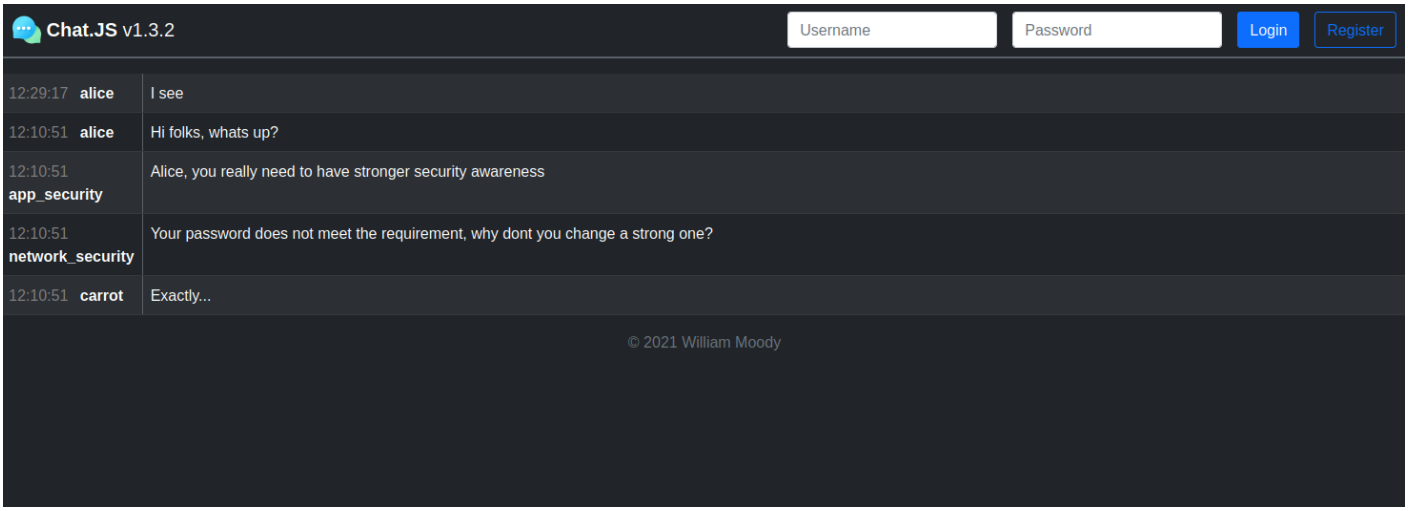
```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 110 Apache httpd 2.4.41 ((Ubuntu))
```



Port 3000: Node.js

Node.js Express

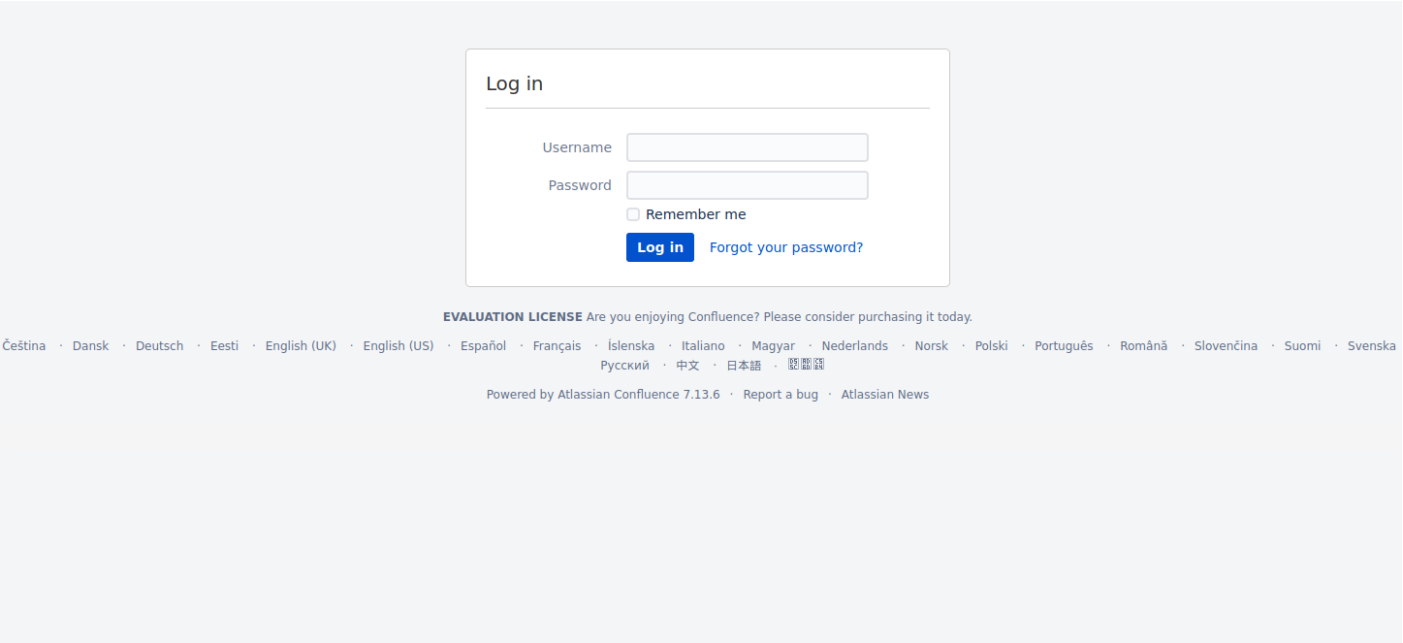
```
PORT     STATE SERVICE REASON          VERSION
3000/tcp open  http    syn-ack ttl 110 Node.js (Express middleware)
```



Port 8090

Confluence wiki

```
PORT     STATE SERVICE       REASON          VERSION
8090/tcp open  opsmessaging? syn-ack ttl 110
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bi
n/submit.cgi?new-service :
SF-Port8090-TCP:V=7.92%I=7%D=2/11%Time=63E84A03%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,22F,"HTTP/1\.1\x20302\x20\r\nCache-Control:\x20no-store\r\nExp
SF:ires:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nX-Confluence-R
SF:equest-Time:\x201676167682542\r\nSet-Cookie:\x20JSESSIONID=D8AA770A4723
SF:B751B7C7A285511D2650;\x20Path=/;\x20HttpOnly\r\nX-XSS-Protection:\x201;
SF:\x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nContent-Security-Policy:\x20frame-ancestors\x20'self
SF:'\r\nLocation:\x20http://localhost:8090/login\.action\?os_destination=%
SF:2Findex\.action&permissionViolation=true\r\nContent-Type:\x20text/html;
SF:charset=UTF-8\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2012\x20Feb\x20
SF:2023\x2002:08:02\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions
SF:,97,"HTTP/1\.1\x20200\x20\r\nMS-Author-Via:\x20DAV\r\nContent-Type:\x20
SF:text/html;charset=UTF-8\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2012\
SF:x20Feb\x202023\x2002:08:02\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(R
SF:TSPRequest,821,"HTTP/1\.1\x20400\x20\r\nContent-Type:\x20text/html;char
SF:set=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x201925\r\nDate
SF::\x20Sun,\x2012\x20Feb\x202023\x2002:08:02\x20GMT\r\nConnection:\x20clo
SF:se\r\n\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20S
SF:tatus\x20400\x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20type=\"
SF:text/css\">body\x20{font-family:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,
SF:\x20h3,\x20b\x20{color:white;background-color:#525D76;}\x20h1\x20{font-
SF:size:22px;}\x20h2\x20{font-size:16px;}\x20h3\x20{font-size:14px;}\x20p\
SF:x20{font-size:12px;}\x20a\x20{color:black;}\x20\.line\x20{height:1px;ba
SF:ckground-color:#525D76;border:none;}</style></head><body><h1>HTTP\x20St
SF:atus\x20400\x20\xe2\x80\x93\x20Bad\x20Request</h1><hr\x20class=\"line\"
SF:\x20/><p><b>Type</b>\x20Exception\x20Report</p><p><b>Message</b>\x20Inv
SF:alid\x20character\x20found\x20in\x20the\x20HTTP\x20protocol\x20\[RTSP&#
SF:47;1\.00×0d0×0a0×0d0×0a\.\.\.\]</p><p><b>Description</b>\x20The\x20serv
SF:er\x20cannot\x20or\x20will\x20not\x20process\x20the\x20request\x20due\x
SF:20to\x20something\x20that\x20is\x20perceived\x20to\x20be\x20a\x20client
SF:\x20error\x20\(e\.g\.,\x20malformed\x20request\x20syntax,\x20invalid\x2
SF:0");
```



white-bird.org

Port 8090 IIS 10.0

.Net Web .Net

```
PORT     STATE SERVICE REASON          VERSION
8080/tcp open  http    syn-ack ttl 110 Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Home About Contact

Raven Medicine Storage Database

Medicine **Brand** **Price**

Search Reset

Query List

Upload Medicine Document!

Medicine

Brand

Price

Document Browse... No file selected.

upload

Revision #9
Created 5 September 2022 03:00:26 by
Updated 19 June 2023 11:54:40 by