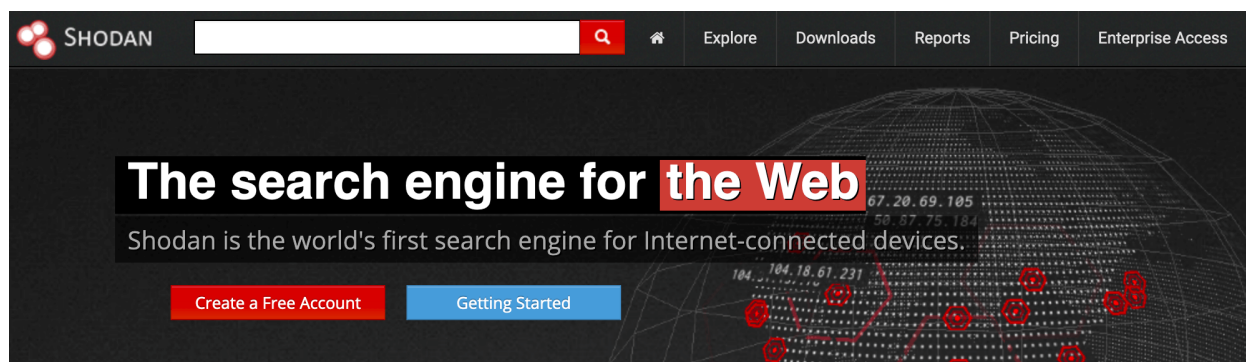


Awesome Shodan Search Queries

Over time, I've collected an assortment of interesting, funny, and depressing search queries to plug into [Shodan](#), the ([literal](#)) internet search engine. Some return facepalm-inducing results, while others return serious and/or ancient vulnerabilities in the wild.



[Most search filters require a Shodan account.](#)

You can assume these queries only return unsecured/open instances when possible. For your own legal benefit, do not attempt to login (even with default passwords) if they aren't! Narrow down results by adding filters like `country:US` or `org:"Harvard University"` or `hostname:"nasa.gov"` to the end.

The world and its devices are quickly becoming more connected through the shiny new [Internet of Things Sh*t](#) — and exponentially [more dangerous](#) as a result. To that end, I hope this list spreads awareness (and, quite frankly, pant-wetting fear) rather than harm.

And as always, [discover and disclose responsibly!](#) 🙈

Table of Contents

- [Industrial Control Systems](#)
- [Remote Desktop](#)
- [Network Infrastructure](#)
- [Network Attached Storage \(NAS\)](#)
- [Webcams](#)
- [Printers & Copiers](#)
- [Home Devices](#)

- [Random Stuff](#)
-

Industrial Control Systems

Samsung Electronic Billboards [→](#)

"Server: Prismview Player"

Schedule playing: New Generic (Cycle: 11 of 28)

Content playing: .wmv

Date: 09/19/2019

Time: 6:47 AM

Outside temperature: 11.00

Inside temperature: -273.15

Operating level: 100.00%

Current output:



Gas Station Pump Controllers [→](#)

"in-tank inventory" port:10001

7-ELEVEN

IN-TANK INVENTORY

TANK	PRODUCT	VOLUME TC	VOLUME	ULLAGE	HEIGHT	WATER	TEMP
1	REGULAR	5716	5675	6191	44.06	0.91	70.02
2	MID-GRADE	2382	2369	3345	39.74	0.00	67.54
3	PREMIUM	3142	3124	2618	51.51	0.00	67.81

Automatic License Plate Readers →

P372 "ANPR enabled"



Main Menu

- System
- Update
- Preferences
- Monitor
- Configuration
- Diagnostics
- Contact us
- Legal

Plate Database

Database File: mem:\plates.db Separator: ,

Update FTP Server: 10.1.1.1 Update FTP Account: [redacted]

Update FTP Password: [redacted] Update FTP Filename: update.csv

Enable: 0x00 Plate DB Debug: 0

Hash Size: 50021 Confidence Threshold: 75

Update time: 0

Apply

Traffic Light Controllers / Red Light Cameras →

mikrotik streetlight

Voting Machines in the United States →

"voter system serial" country:US

Telcos Running [Cisco Lawful Intercept](#) Wiretaps →

"Cisco IOS" "ADVIPSERVICESK9_LI-M"

Wiretapping mechanism outlined by Cisco in [RFC 3924](#):

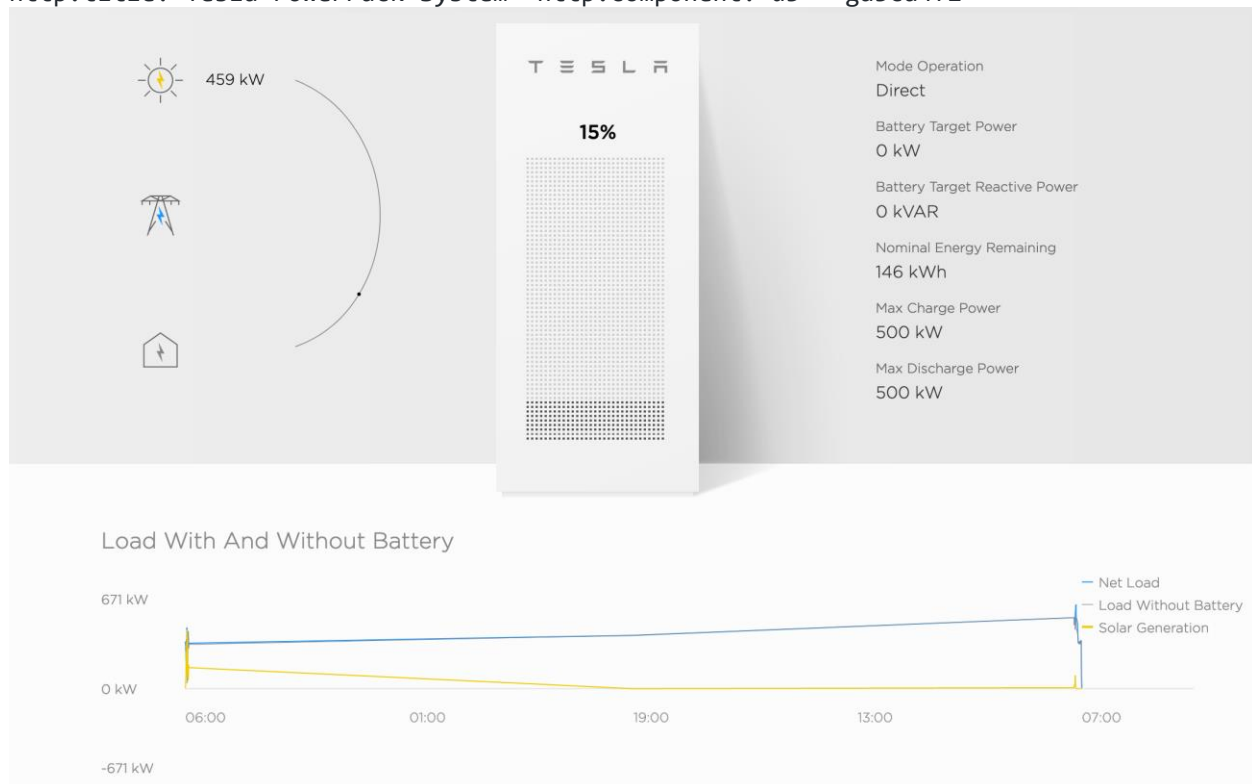
Lawful intercept is the lawfully authorized interception and monitoring of communications of an intercept subject. The term "intercept subject" [...] refers to the subscriber of a telecommunications service whose communications and/or intercept related information (IRI) has been lawfully authorized to be intercepted and delivered to some agency.

Prison Pay Phones →

"[2J[H Encartele Confidential"

Tesla PowerPack Charging Status →

http.title:"Tesla PowerPack System" http.component:"d3" -ga3ca4f2



Electric Vehicle Chargers →

"Server: gSOAP/2.8" "Content-Length: 583"

Maritime Satellites →

Shodan made a pretty sweet [Ship Tracker](#) that maps ship locations in real time, too!

[Nordex Wind Turbine Farms](#) 🔍 →

http.title:"Nordex Control" "Windows 2000 5.0 x86" "Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0_14)"

[C4 Max Commercial Vehicle GPS Trackers](#) 🔍 →

"[1m[35mWelcome on console"

gpspos

```
Internal antenna
GPRMC Frame value is
$GPRMC,
GPGLL Frame value is
$GPGLL,
```


[DICOM Medical X-Ray Machines](#) 🔍 →

Secured by default, thankfully, but these 1,700+ machines still [have no business](#) being on the internet.

"DICOM Server Response" port:104

[GaugeTech Electricity Meters](#) 🔍 →

"Server: EIG Embedded Web Server" "200 Document follows"

**Electro Industries/GaugeTech**
The Leader in Web Accessed Power Monitoring

://Web Explorer

Volts/Amps
Power/Energy
Power Quality
Pulse Accumulation
Inputs
Meter Information
Emails
Diagnostic

Meter Name [REDACTED]

Date/Time 2019-05-12 11:56:53.660

Voltage/Frequency

	Instantaneous	Maximum	Minimum
Volts AN	125.45	128.61	120.67
Volts BN	125.77	129.30	120.97
Volts CN	124.84	128.37	120.20
Volts A-B	218.09	223.77	209.66
Volts B-C	216.69	222.72	208.49
Volts C-A	216.56	222.40	208.56

[Siemens Industrial Automation](#) 🔍 →

"Siemens, SIMATIC" port:161

Siemens HVAC Controllers →

"Server: Microsoft-WinCE" "Content-Length: 12581"

Door / Lock Access Controllers →

"HID VertX" port:4070

Railroad Management →

"log off" "select the appropriate"

Remote Desktop

Unprotected VNC →

"authentication disabled" "RFB 003.008"

[Shodan Images](#) is a great supplementary tool to browse screenshots, by the way!  →



The first result right now. ☹️

Windows RDP 🔗 →

99.99% are secured by a secondary Windows login screen.

"\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00"

Network Infrastructure

Weave Scope Dashboards 🔗 →

Command-line access inside Kubernetes pods and Docker containers, and real-time visualization/monitoring of the entire infrastructure.

title:"Weave Scope" http.favicon.hash:567176827

The WeaveScope interface displays a cluster of pods. The main view shows a grid of pod icons with labels such as 'weave-scope...', 'filebeat', 'metricbeat', 'The Internet Outbound conne...', 'kube-state-met...', 'auditd', 'alert', 'apigw', 'download', 'log-client', 'nats', 'nginx', 'nodecloud', 'notification', 'orchapp', 'otp', 'report', 'sync', 'troubleshoot', 'ui', 'dashboard-me...', 'kube-dns', 'kube-flannel', 'kubedns-autos...', and 'kubernetes-da...'. A sidebar on the right shows 'redis' details.

redis

Info

- Type: Deployment
- Namespace: **default**
- Created: a year ago
- Observed gen.: 1
- Desired replic...: 1
- # Pods: 1
- Strategy: RollingUpdate

Pods	State	#	IP
redis-7d6c9bc6dd...	Running	1	10.0.0.1

Kubernetes labels

redis

28 nodes (11 filtered)

Show unmanaged Hide unmanaged

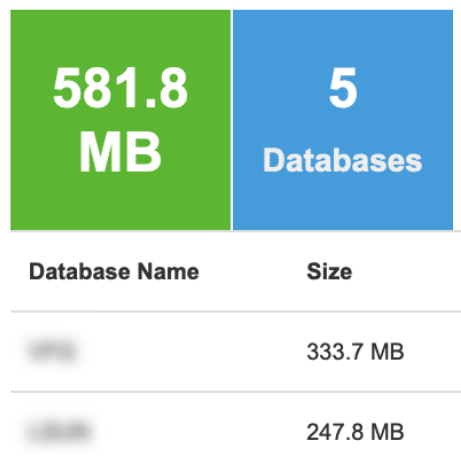
All Namespaces default

Update available: 1.13.0 Version 1.12.0 on

MongoDB →

Older versions were insecure by default. [Very scary.](#)

"MongoDB Server Information" port:27017 -authentication



MongoDB Server Information

```
{
  "metrics": {
    "commands": {
      "updateUser": {
        "failed": 0,
        "total": 0
      },
      "killAllSessions": {
        "failed": 0,
        "total": 0
      }
    }
  }
}
```

Mongo Express Web GUI →

Like the [infamous phpMyAdmin](#) but for MongoDB.

"Set-Cookie: mongo-express=" "200 OK"

Viewing Collection: trips

New Document

New Index

Simple

Advanced

Key

Value

String

Find

Delete all 1990273 documents retrieved

First

Prev


Next

Last

_id	trip	duration	status	location	date	time	user	notes

Jenkins CI






"X-Jenkins" "Set-Cookie: JSESSIONID" http.title:"Dashboard"


Jenkins







[log in](#)

Jenkins

ENABLE AUTO REFRESH

 People
  Build History
  Project Relationship
  Check File Fingerprint
  Credentials

All

S	W	Name ↓	Last Success	Last Failure	Last Duration
			N/A	2 yr 4 mo - #120	3 min 3 sec
			1 mo 6 days - #876	N/A	41 sec
			15 days - #443	1 mo 5 days - #441	1 min 29 sec

Docker APIs

"Docker Containers:" port:2375

Docker Private Registries

"Docker-Distribution-Api-Version: registry" "200 OK" -gitlab

Pi-hole Open DNS Servers

"dnsmasq-pi-hole" "Recursion: enabled"

Already Logged-In as root via Telnet 🔑 →

"root@" port:23 -login -password -name -Session

Android Root Bridges 🔑 →

A tangential result of Google's sloppy fractured update approach. 😬 [More information here.](#)

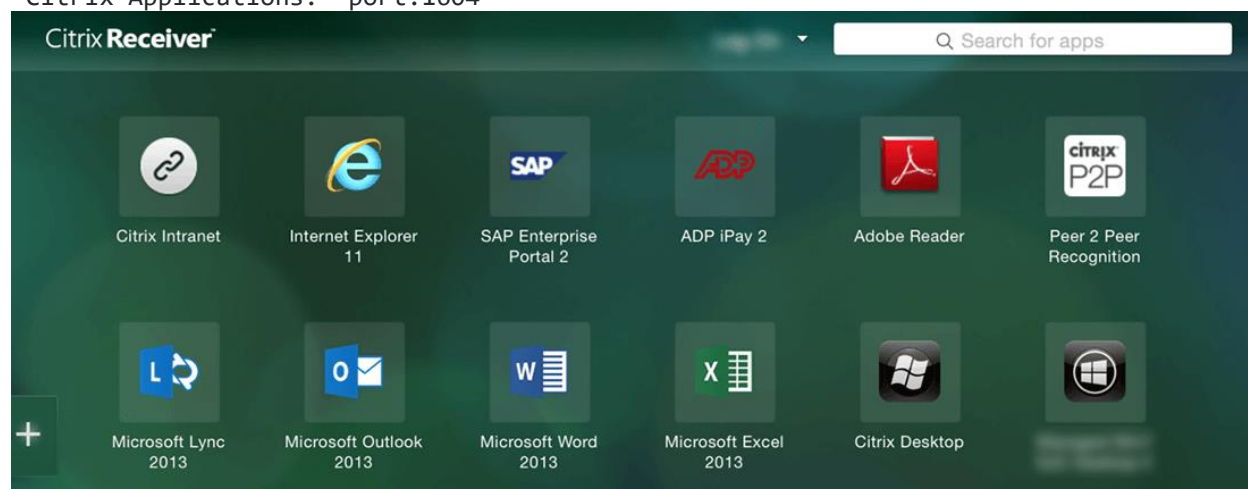
"Android Debug Bridge" "Device" port:5555

Lantronix Serial-to-Ethernet Adapter [Leaking Telnet Passwords](#) 🔑 →

Lantronix password port:30718 -secured

Citrix Virtual Apps 🔑 →

"Citrix Applications:" port:1604



Cisco Smart Install 🔑 →

[Vulnerable](#) (kind of "by design," but especially when exposed).

"smart install client active"

PBX IP Phone Gateways 🔑 →

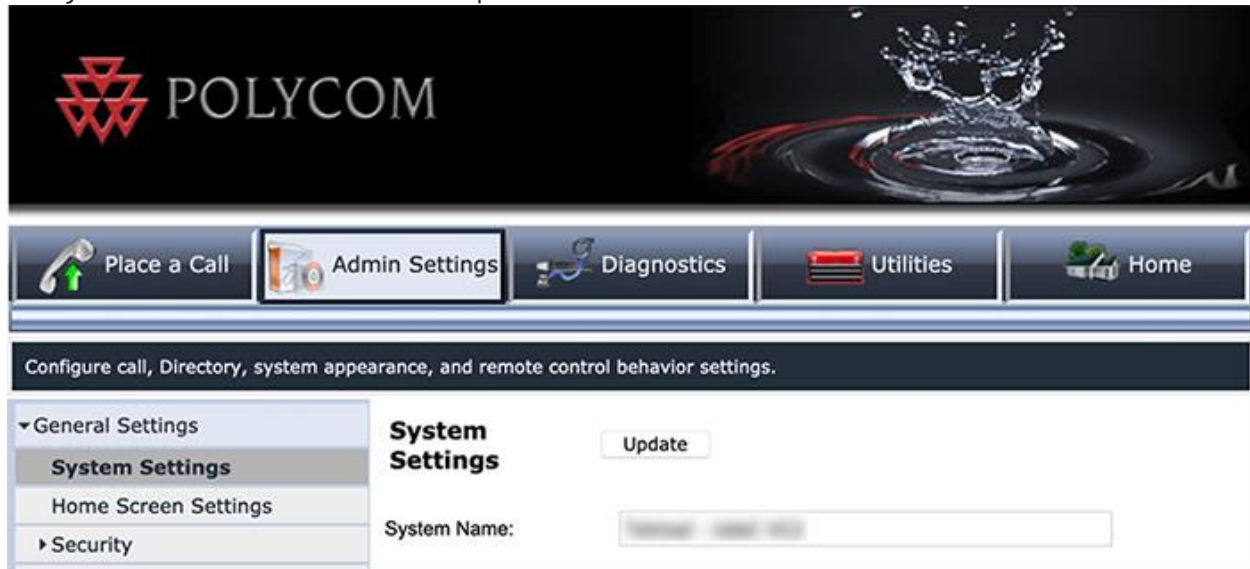
PBX "gateway console" -password port:23

[Polycom Video Conferencing](#) 🔍 →

http.title:"- Polycom" "Server: lighttpd"

Telnet Configuration: 🔍 →

"Polycom Command Shell" -failed port:23



[Bomgar Help Desk Portal](#) 🔍 →

"Server: Bomgar" "200 OK"

[Intel Active Management CVE-2017-5689](#) 🔍 →

"Intel(R) Active Management Technology" port:623,664,16992,16993,16994,16995

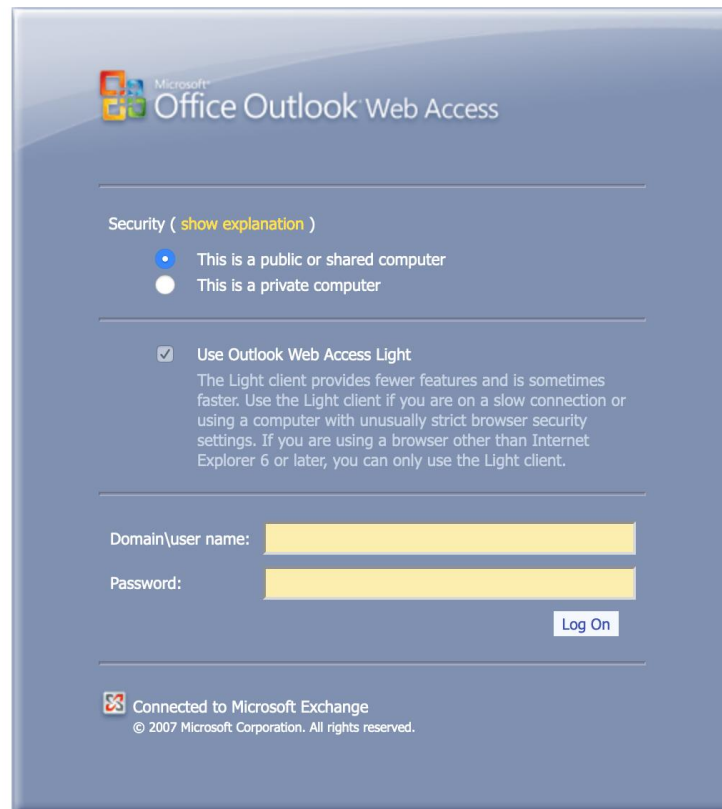
[HP iLO 4 CVE-2017-12542](#) 🔍 →

HP-ILO-4 !"HP-ILO-4/2.53" !"HP-ILO-4/2.54" !"HP-ILO-4/2.55" !"HP-ILO-4/2.60" !"HP-ILO-4/2.61" !"HP-ILO-4/2.62" !"HP-iLO-4/2.70" port:1900

Outlook Web Access:

[Exchange 2007](#) 🔍 →

"x-owa-version" "IE=EmulateIE7" "Server: Microsoft-IIS/7.0"



The screenshot shows the Microsoft Office Outlook Web Access login interface. At the top, the Microsoft logo and 'Office Outlook Web Access' title are displayed. Below this, a 'Security' section contains two radio buttons: 'This is a public or shared computer' (selected) and 'This is a private computer'. A 'Use Outlook Web Access Light' checkbox is checked, with a descriptive paragraph below it. The login fields include 'Domain\user name:' and 'Password:', both with yellow input boxes. A 'Log On' button is positioned to the right of the password field. At the bottom, a status bar indicates 'Connected to Microsoft Exchange' and includes a copyright notice for 2007 Microsoft Corporation.

Microsoft Office Outlook Web Access

Security ([show explanation](#))


☒ This is a public or shared computer
☐ This is a private computer

☒ Use Outlook Web Access Light
The Light client provides fewer features and is sometimes faster. Use the Light client if you are on a slow connection or using a computer with unusually strict browser security settings. If you are using a browser other than Internet Explorer 6 or later, you can only use the Light client.

Domain\user name:

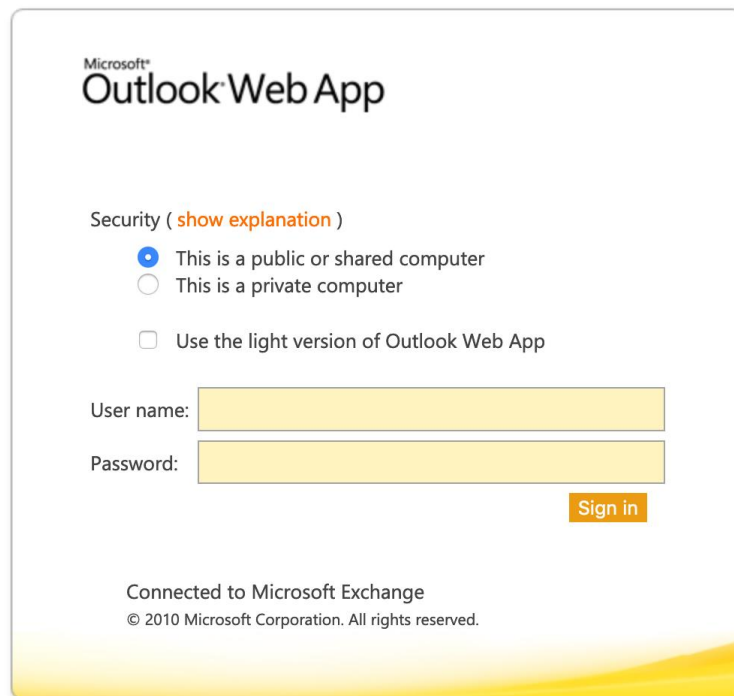
Password:

[Log On](#)

 Connected to Microsoft Exchange
© 2007 Microsoft Corporation. All rights reserved.

Exchange 2010 →

"x-owa-version" "IE=EmulateIE7" http.favicon.hash:442749392



Microsoft®
Outlook® Web App

Security ([show explanation](#))

☒ This is a public or shared computer
☐ This is a private computer

☐ Use the light version of Outlook Web App

User name:

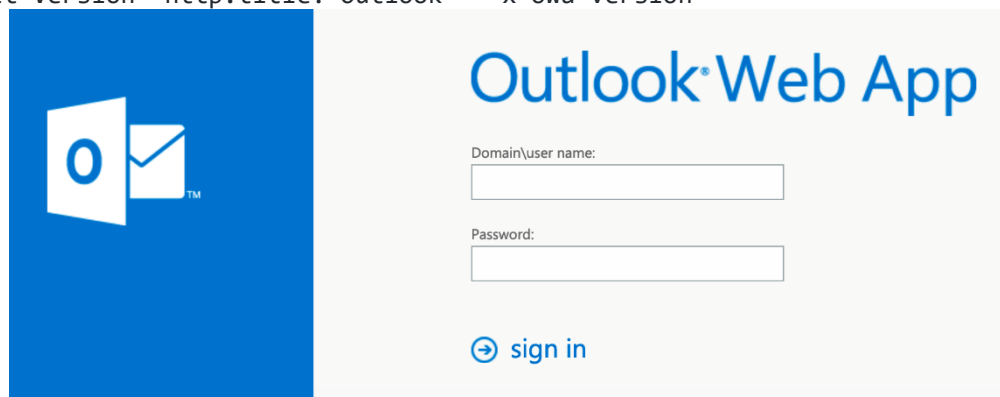
Password:

[Sign in](#)

Connected to Microsoft Exchange
 © 2010 Microsoft Corporation. All rights reserved.

Exchange 2013 / 2016 [→](#)

"X-AspNet-Version" http.title:"Outlook" -"x-owa-version"



Outlook® Web App

Domain\user name:

Password:

[sign in](#)

Lync / Skype for Business [→](#)

"X-MS-Server-Fqdn"

Network Attached Storage (NAS)

SMB (Samba) File Shares 🔍 →

Produces ~500,000 results...narrow down by adding "Documents" or "Videos", etc.

"Authentication: disabled" port:445

Specifically domain controllers: 🔍 →

"Authentication: disabled" NETLOGON SYSVOL -unix port:445

Concerning [default network shares of QuickBooks](#) files: 🔍 →

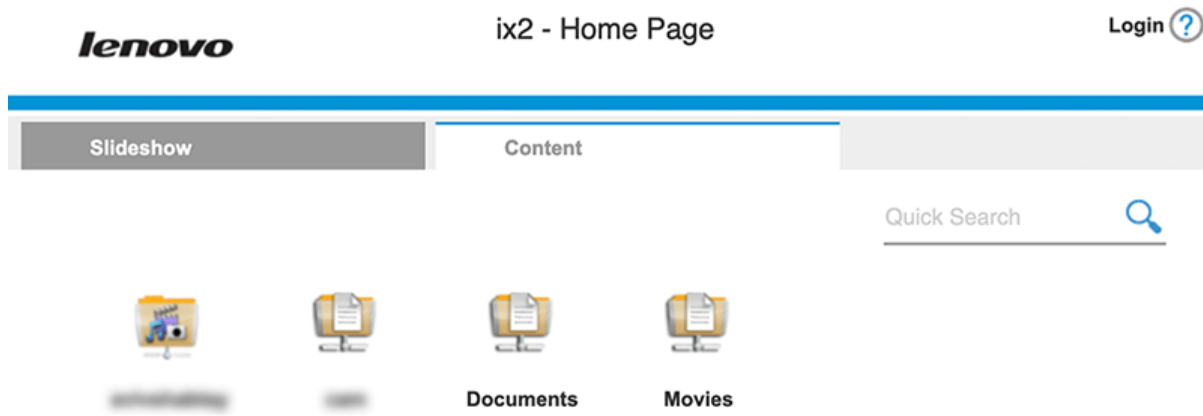
"Authentication: disabled" "Shared this folder to access QuickBooks files OverNetwork" -unix port:445

FTP Servers with Anonymous Login 🔍 →

"220" "230 Login successful." port:21

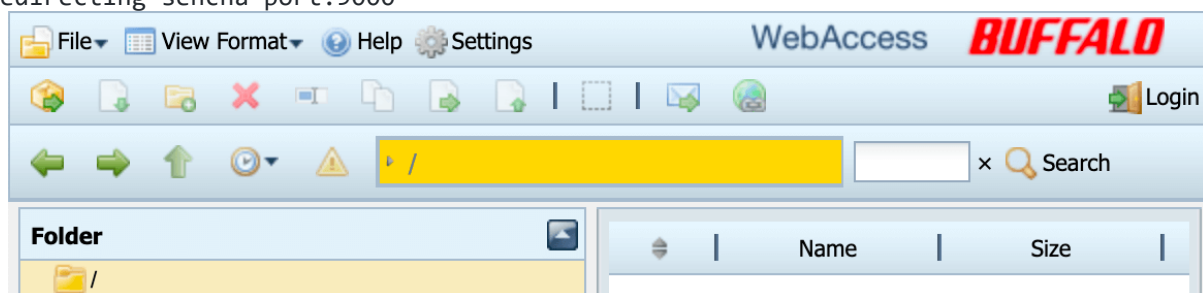
Iomega / LenovoEMC NAS Drives 🔍 →

"Set-Cookie: iomega=" -"manage/login.html" -http.title:"Log In"



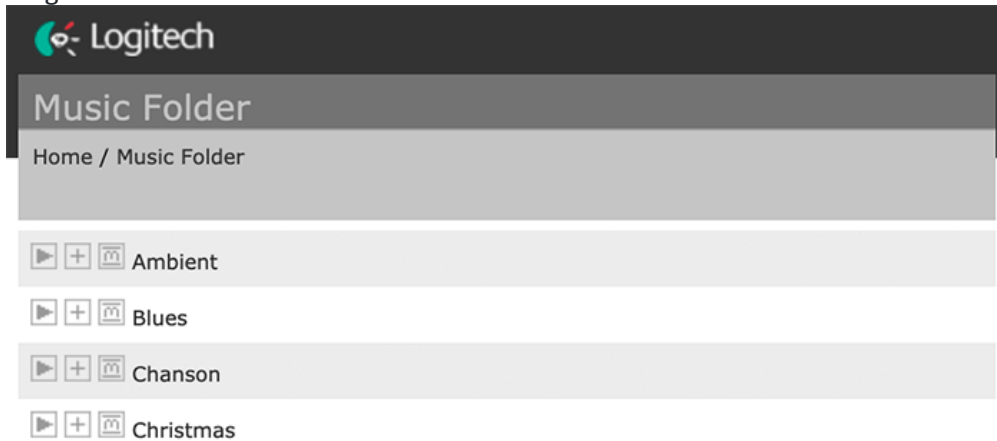
Buffalo TeraStation NAS Drives 🔍 →

Redirecting sencha port:9000



Logitech Media Servers

"Server: Logitech Media Server" "200 OK"

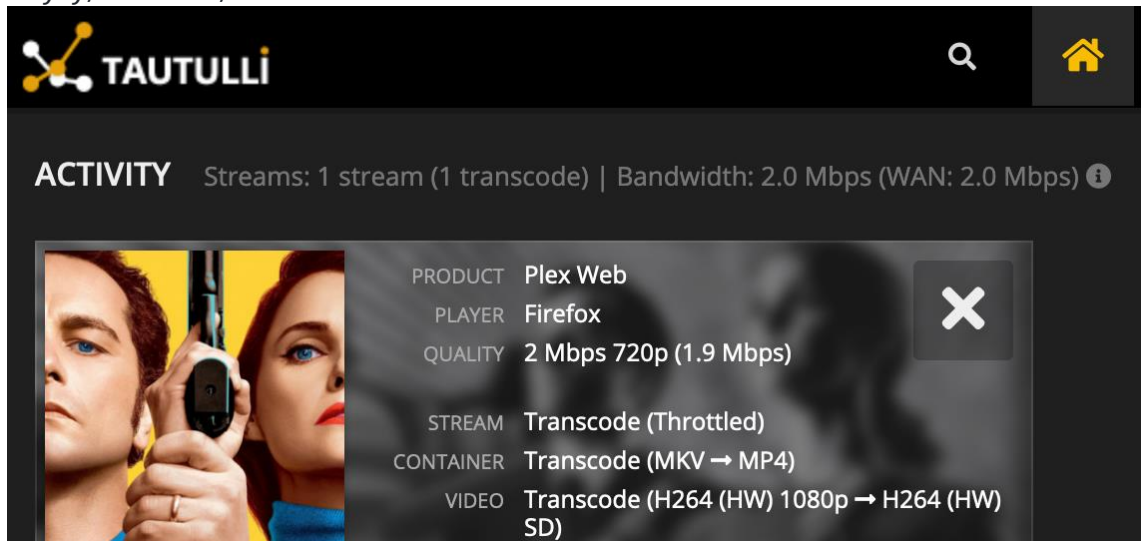


Plex Media Servers


"X-Plex-Protocol" "200 OK" port:32400

Tautulli / PlexPy Dashboards

"CherryPy/5.1.0" "/home"



Webcams

Example images not necessary. 

Yawcams →

"Server: yawcam" "Mime-Type: text/html"

webcamXP/webcam7 →

("webcam 7" OR "webcamXP") http.component:"mootools" -401

Android IP Webcam Server →

"Server: IP Webcam Server" "200 OK"


Security DVRs →


html:"DVR_H264 ActiveX"

Printers & Copiers:

HP Printers →



"Serial Number:" "Built:" "Server: HP HTTP"

 **HP OfficeJet Pro 7740 Wide Format All-in-One**
Embedded Web Server

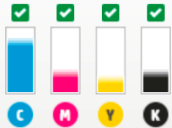
Search 

Home Scan Fax Web Services Network Tools Settings

Energy Save Mode
Energy Save after:
5 min

Web Services
 ... 
HP ePrint: On
print apps: On

Printer Update
Check for new printer updates.

Estimated Cartridge Le...

*Actual levels may vary.

Xerox Copiers/Printers →

ssl:"Xerox Generic Root"

Centware®
Internet Services
XEROX® WorkCentre® 5875

Status
Jobs
Print
Scan
Address Book
Properties
Support

Status
Welcome
Description & Alerts
Billing Information
Usage Counters
Configuration Report
Supplies
Trays
Information Pages
SMart eSolutions

124

Usage Counters

Refresh
 Download File to Your Computer

Counter	Count
Total Impressions	431511
Black Copied Impressions	332888
Black Printed Impressions	98582
Single Impressions	431511

Epson Printers →

"SERVER: EPSON_Linux UPnP" "200 OK"

"Server: EPSON-HTTP" "200 OK"

EPSON XP-440 Series

Product Status

Basic
Network
Wi-Fi Direct

English

Printer Status
Available.

BK

Y

M

C

Canon Printers →

"Server: KS_HTTP" "200 OK"

"Server: CANON HTTP Server"



Home Devices

Yamaha Stereos [🔗 →](#)

"Server: AV_Receiver" "HTTP/1.1 406"



Apple AirPlay Receivers [🔗 →](#)

Apple TVs, HomePods, etc.

"\x08_airplay" port:5353

Chromecasts / Smart TVs [🔗 →](#)

"Chromecast:" port:8008

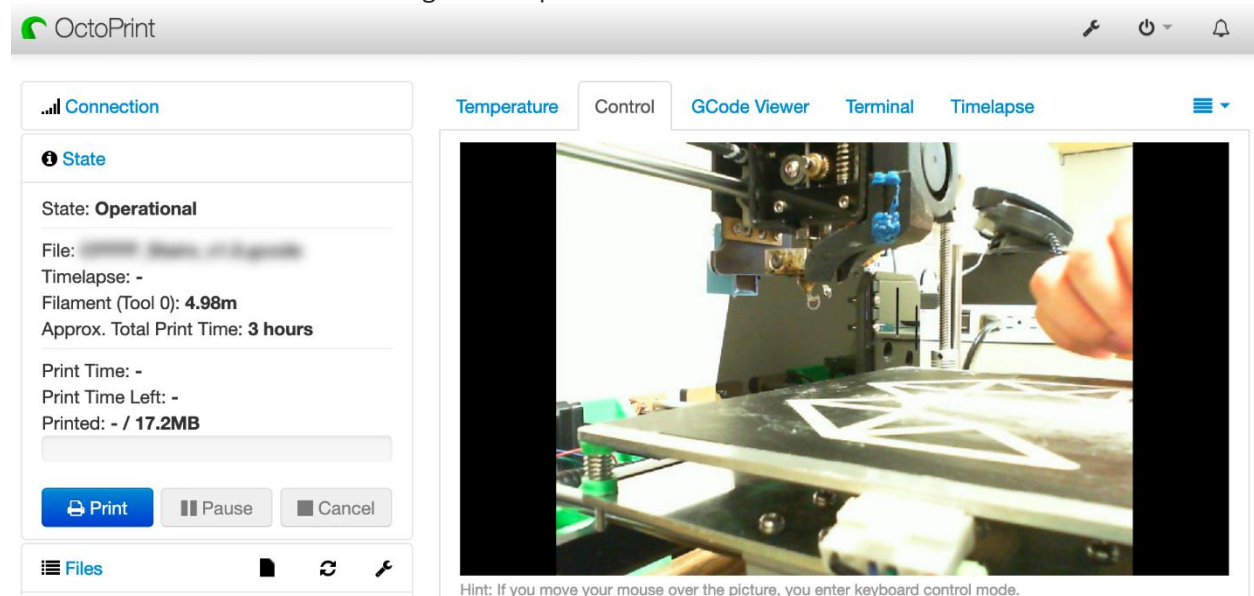
[Crestron Smart Home Controllers](#) →

"Model: PYNG-HUB"

Random Stuff

[OctoPrint 3D Printer Controllers](#) →

title:"OctoPrint" -title:"Login" http.favicon.hash:1307375944



[Ethereum Miners](#) →

"ETH - Total speed"

```
ETH: 04/23/19-21:03:09 - New job from
ETH - Total Speed: 251.918 Mh/s, Total Shares: 5457, Rejected: 0, Time: 99:16
ETH: GPU0 31.282 Mh/s, GPU1 31.569 Mh/s, GPU2 31.190 Mh/s, GPU3 31.566 Mh/s, GPU4 31.574 Mh/s, GPU5 31.583
Mh/s, GPU6 31.593 Mh/s, GPU7 31.561 Mh/s
ETH: 04/23/19-21:03:13 - SHARE FOUND - (GPU 1)
ETH: Share accepted (141 ms)!!
ETH: 04/23/19-21:03:13 - New job from
ETH - Total Speed: 251.957 Mh/s, Total Shares: 5458, Rejected: 0, Time: 99:16
ETH: GPU0 31.295 Mh/s, GPU1 31.574 Mh/s, GPU2 31.211 Mh/s, GPU3 31.586 Mh/s, GPU4 31.584 Mh/s, GPU5 31.583
Mh/s, GPU6 31.583 Mh/s, GPU7 31.540 Mh/s
ETH: 04/23/19-21:03:17 - New job from
```

[Apache Directory Listings](#) →

Substitute .pem with any extension or a filename like phpinfo.php.

http.title:"Index of /" http.html:".pem"

Misconfigured WordPress 🔍 →

Exposed [wp-config.php](#) files containing database credentials.
http.html:"* The wp-config.php creation script uses this file"

Too Many Minecraft Servers 🔍 →

"Minecraft Server" "protocol 340" port:25565

Literally [Everything](#) in North Korea 🇰🇵 🔍 →

net:175.45.176.0/22,210.52.109.0/24,77.94.35.0/24

TCP Quote of the Day 🔍 →

Port 17 ([RFC 865](#)) has a [bizarre history](#)...

port:17 product:"Windows qotd"

Find a Job Doing This! 👤 🔍 →

"X-Recruiting:"

Credit: <https://github.com/jakejarvis/awesome-shodan-queries>