CS352: Cybersecurity Principles

Semester 1, 2025

Assignment - Report 2

Title: Penetration Testing Using Shodan: A Technical Analysis

Abstract

This technical document explains a penetration testing exercise where Shodan, the internet-connected device search engine, was used. After making an account on Shodan and running a virtual lab alone, I used searches focused on Fiji against SSH, HTTP and RTSP services. Reviewing service banners revealed that many Nginx services needed updates for CVE-2019-11043, SSH hosts with vulnerable ciphers were open to attack and IP cameras were entirely public with streams open to anyone. Every finding was examined using risk management, considering how it affected confidentiality, integrity and availability. You should automate applying patches, set firm configuration standards for systems, control access to the network and use Shodan to monitor regularly, all based on clear cybersecurity policies and a set response plan.

Declaration

We hereby acknowledge that this report titled “Penetration Testing Using Shodan: A Technical Analysis” is our original work. All sources used have been referenced using IEEE referencing style.

Name	Student ID	Contribution	Signature	Date
Kavish Chandra	S11219143	100%	KChandra	23/05/2025
Sudhansu Kisun	S11219520	100%	SKisun	23/05/2025
Shoneel Kumar	S11219651	100%	SKumar	23/05/2025
Fardeen Ali	S11219171	100%	FAli	23/05/2025
Vishant Chand	S11219214	100%	VChand	23/05/2025

Contents

Introduction 5

Detailed Background on Cybersecurity Vulnerabilities 5

Zero-day vulnerabilities 5

Common Vulnerabilities and Exposures (CVE) 6

Penetration Testing: An Effective Security Measure 6

Why Perform Penetration Tests? 6

Types of Penetration Testing 6

Black-box Penetration Testing 6

White-box Penetration Testing 7

Gray-box Penetration Testing 7

Shodan: A Specialized Search Engine 7

Overview and Purpose 7

Historical Background 7

How Shodan Operates 7

Information Revealed by Shodan 8

Example of Banners 8

Devices Discoverable via Shodan 9

Security Implications of Shodan 9

Applications of Shodan Data 9

Methodology and Test Environment Setup 10

Results and Discussion 11

Key Finding 1: Exposed Remote Desktop (RDP) with BlueKeep (CVE-2019-0708) 11

Overview of BlueKeep Vulnerability 11

Observed Data 11

Risk Analysis and Threat Scenario 12

Risk Management Perspective 12

Policies and Mitigation 13

Key Finding 2: Exposed IP cameras via WebcamXP 14

Overview of WebcamXp and Hikvision Vulnerabilities 14

Shodan Scan 14

Observed Data 14

Risk Analysis and Threat Scenario 15

Risk Management Perspective 15

Policies and Mitigation 16

Conclusion 17

Bibliography 18

Appendices 20

Appendix A: Shodan Account Setup 20

Appendix B: Vulnerability Scan- Target 1 23

Appendix C: Vulnerability Scan- Target 2 26

Introduction

A vulnerability can be defined as a living system or software that can be attacked or interrupted by an unauthorized malicious attacker, malicious software or network [1]. All transactions performed by a vulnerable system are at risk. Data security and transaction security are at the forefront of these risks. These risks cause serious financial losses and legal liabilities. Zero day is a phrase that means that a cyber attacker may easily attack the system. If a system is subject to a zero-day attack, then it has no time to be defended. Vulnerabilities in operating systems, web browsers, office applications, software, and IOT devices are called zero-day target vulnerabilities [2]. There are some standard steps that can be taken to avoid these attacks. You can do this by regularly updating the software and operating system, permanently turning on the firewall and using new anti-virus software.

Shodan is a search engine designed to find Internet-connected devices and plays a key part in network security by discovering problems in servers, applications and devices. Every day, it scans to identify IP addresses, services, open ports and possible weaknesses. Shodan shows systems and devices used in IoT that are not searchable on common engines, giving a full view of the world's internet. The use of Shodan's features enables cybersecurity experts to spot open devices, detect problems in the network and find cyber threats, therefore improving internet security [3]. Even though Shodan is a powerful tool in cybersecurity, it can be used improperly by individuals with malicious intentions on insecure devices, so all systems online should have strong security.

Detailed Background on Cybersecurity Vulnerabilities

Cybersecurity vulnerability is any weakness within an organization's information systems, internal controls, or system processes that cybercriminals or bad actors can exploit. Through points of vulnerability, cyber adversaries are able to gain access to your system and collect data. With regard to your organization's overall **security posture** [4], cybersecurity vulnerabilities are extremely important to monitor as gaps in a network can lead to a full-scale breach of a system.

Zero-day vulnerabilities

Zero-day threats are specific software vulnerabilities that are known to the attacker but have not yet been identified by an organization. This means that there is no available fix since the vulnerability has not yet been reported to the system vendor [5]. These are extremely dangerous as there is no way to defend against them until after the attack has been carried out. It is important to remain diligent and continuously monitor your systems for vulnerabilities to limit the likelihood of a zero-day attack [6].

Common Vulnerabilities and Exposures (CVE)

CVE is a system used to name and identify publicly disclosed information security vulnerabilities consistently. For IT security, a vulnerability is a flaw in software or hardware that, when used by attackers, negatively influences confidentiality, integrity or availability [7]. Every CVE assigned number has a prefix, the year it was reported and a sequence of digits. Its mission is to collect and track cybersecurity weaknesses known to the public [8]

Penetration Testing: An Effective Security Measure

Discovering weaknesses in IT systems is best done using penetration testing. Even so, it is necessary to monitor IT staff regularly to allow for continued assessment. Since databases, emails and financial data are managed by servers and web services, organizing daily checks for vulnerabilities is very important.

Why Perform Penetration Tests?

Organizations perform penetration tests to:

- Assess the real-world exploitability of vulnerabilities
- Validate the effectiveness of existing security controls
- Fulfill regulatory and compliance requirements (e.g., PCI DSS, HIPAA, SOC 2)
- Build trust with stakeholders by demonstrating proactive risk management
- Improve overall incident response and security maturity

Types of Penetration Testing

Penetration testing can be sorted at a high level by looking at the amount of knowledge and access the tester holds at the start. The method used will change according to what the client needs.

Black-box Penetration Testing

Black-box or outside-in testing does not give the tester access to the target system's inside. In this way, you experience how an external attacker might collect data and where the security is most vulnerable [9].

White-box Penetration Testing

With white-box testing, the tester has access to everything in the project's internal documentation, source code and architecture. It helps by looking carefully at possible weaknesses to find ones that can be easily attacked and others that might become an attacker's next target [10].

Gray-box Penetration Testing

Testers in gray-box testing benefit from having some details about the architecture and certain credentials. This testing examines the actions and outcomes of a privileged user (or an account taken over by an insider) [11].

Shodan: A Specialized Search Engine

Overview and Purpose

Shodan helps find servers, applications and connected devices on the Internet, making network security possible by identifying their weaknesses. Many times, it inspects IP addresses, finds available services, looks at open ports and searches for vulnerabilities. A retrieval from Shodan is used in the report to determine whether the server contains any ongoing or past vulnerabilities, paying close attention to the state of the server, services being used and the ports. Its purpose is to find existing risks in the servers and help organizations act before these risks become a problem for network security [3].

Historical Background

Shodan began in 2003 when it was built by the computer programmer John Matherly. By regularly mining the internet for IP addresses, Matherly was able to identify every device on the network and, later, built a search engine to sift through his collection of internet devices. He made Shodan available to the internet in 2009 [3].

How Shodan Operates

Shodan contacts each possible IP address on the internet, gets data from those connections and stores the information discovered in a searchable index. Shodan scans the web by using a network of computers and servers that run all the time worldwide [3].

Your device's IP address is similar to a digital nameplate that directs searches to your area and enables various devices to speak to one another online. Some types of data are sent through specific “ports” found in internet-connected devices. Gaining the IP address of your device lets you access and work on each of its ports [3].

Information Revealed by Shodan

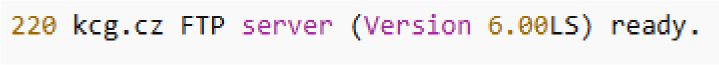
Banners can provide all sorts of identifying information, but here are some of the more common fields you will see in a banner:

- Device name
- IP address
- Port number
- Organization
- Location

Some devices even include their default login and password, make and model, and software version, which can all be exploited by hackers.

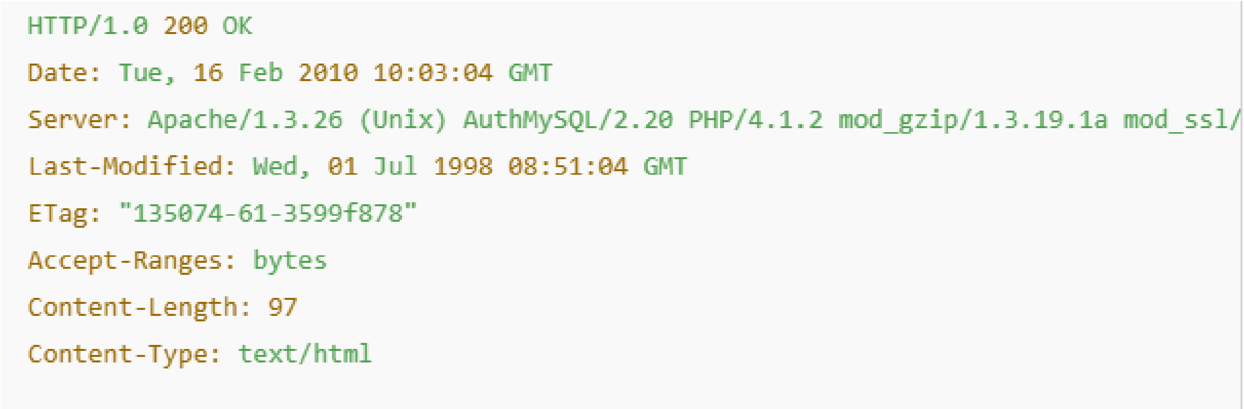
Example of Banners

FTP banner example:



```
220 kcg.cz FTP server (Version 6.00LS) ready.
```

HTTP banner example:



```
HTTP/1.0 200 OK
Date: Tue, 16 Feb 2010 10:03:04 GMT
Server: Apache/1.3.26 (Unix) AuthMySQL/2.20 PHP/4.1.2 mod_gzip/1.3.19.1a mod_ssl/
Last-Modified: Wed, 01 Jul 1998 08:51:04 GMT
ETag: "135074-61-3599f878"
Accept-Ranges: bytes
Content-Length: 97
Content-Type: text/html
```

Devices Discoverable via Shodan

Any device connected to the internet can potentially show up in a Shodan search, including:

- Baby monitors
- Internet routers
- Security cameras
- Maritime satellites
- Water treatment facilities
- Traffic light systems
- Prison pay phones
- Nuclear power plants

Security Implications of Shodan

Shodan only collects data that is made public. But using Shodan shows how much of our data is viewable to the public. If you have an internet-facing webcam and didn't change its original settings, hackers can walk right in through your device.

Applications of Shodan Data

The information gained from these services is applied to many areas:

- Network Security: Keep an eye on all devices at your company that are facing the Internet
- Market Research: Find out which products people are using in the real-world
- Cyber Risk: Include the online exposure of your vendors as a risk metric
- Internet of Things (IoT): Track the growing usage of smart devices
- Tracking Ransomware: Measure how many devices have been impacted by ransomware

Methodology and Test Environment Setup

Additionally, a Shodan account was created to carry out vulnerability scans and conduct basic penetration testing for this report. Shodan.io is “the world’s first search engine for internet-connected devices” and is used to scan devices connected to the internet using search filters to find **Common Vulnerabilities and Exposures** (CVE) on different platforms, open ports, versions of different web services running on machines, IP addresses and geographical locations [12]. Shodan offers a free account for basic reconnaissance and learning and practicing OSINT (Open-Source Intelligence), which will be sufficient for our use case. You will need a username, password and a valid email to create the free account or sign in using an existing google account on Microsoft account.

While using Shodan, all cybersecurity ethics were considered and only passive scans (analyzing network traffic without directly interacting with devices) were conducted. This allowed us to only strictly observe vulnerable systems without directly targeting them as this can be illegal and requires permissions from the system owner before conducting any active scans or attack.

Shodan’s GUI (Graphical User Interface) was used which offers a dashboard providing a search bar (allows different filters to narrow down search results), a filters cheat sheet, beginners guide page and many other features. The overall user interface is well structured and easy to navigate for beginners. A windows 11 host machine was used, and the choice of browser was Google Chrome.

The following search filters were used Shodan to conduct passive scans:

Port numbers

- port:3389 to find machines running RDP services
- port:81 for streaming services used by default

Geographical filters

- country:“FJ” show’s hosts located in Fiji
- country:“SE” show’s hosts located in Sweden

Screenshots from active interfaces

- has_screenshot:true, this can be used for visual confirmations

Service banners

- product:webcamXP, is an IP camera streaming software

Results and Discussion

Key Finding 1: Exposed Remote Desktop (RDP) with BlueKeep (CVE-2019-0708)

Overview of BlueKeep Vulnerability

RDP (Remote Desktop Protocol) is a network communication protocol that allows users to connect to another computer from a remote location. This is usually used by employees in organizations to establish a “Remote Desktop Connection” [13]. However, RDP is vulnerable to “BlueKeep” (CVE-2019-0708) which affects older windows systems such as (Windows 7, Vista, XP, 2000 and Windows Server editions 2003 and 2008). This vulnerability allows an attacker to exploit the system remotely by sending crafted packets over port 3389(TCP) causing a buffer overflow which leads to a memory error. This error allows the attacker to run malicious code on the system allowing them to steal data or exploit other vulnerable systems as BlueKeep is considered “wormable”, meaning it can spread across vulnerable systems. [14]

Shodan Scan

Using the filter- port:3389 has_screenshot:true country:"FJ", Shodan confirmed the system is running an RDP service on open port 3389 which is vulnerable to BlueKeep with a Common Vulnerability Scoring System (CVSS) score of 9.8 (Critical). Shodan also revealed screenshots of the user account during the initial scan on 2025-05-12 which indicates the system is still active and vulnerable to exploits.

Observed Data

IP Address

- 192.235.98.34 (a public IP address can be used for reconnaissance via tools such as Nmap)

Location

- Suva, Fiji

User Accounts

- ‘Vandana’ was identified as the active remote user along with other users visible on the login screen.

Vulnerability

- BlueKeep (CVE-2019-0708)

Security Weakness

- SHA-1 hashing algorithm is considered insecure and outdated. It is one of several cryptographic hash functions used to verify the authenticity and integrity of (digital messages, files or documents) [15].

Open Ports

- Port 3389 used for default RDP port

Risk Analysis and Threat Scenario

The systems that are vulnerable with the (CVE-2019-0708) allow attackers to remotely execute malicious codes on the vulnerable machine itself. This does not require any authentication, and the remote user does not have to open any links or executable files to be affected. Everything happens remotely which is why the "BlueKeep" exploit is considered critical (CVSS score of 9.8) and needs to be mitigated immediately. Failure to recognize such vulnerability and not taking immediate actions can result in the following:

Remote exploitation- The attacker can install ransomware (like WannaCry variant) and encrypt all files on the system and the network, demanding a ransom in exchange for a key to decrypt all affected data.

Lateral movement- Once the attacker has gained unauthorized access to one vulnerable machine, they can also pivot their way inside the network and gain access to other vulnerable systems connected on it. This can lead to a high scale attack.

Credential exposure- Screenshots retrieved from the scan reveals all user accounts on the machine which can be used for credential harvesting or carrying out brute-force attack using password cracking tools like "Hydra" or "John the Ripper"[12].

Risk Management Perspective

Additionally, from a risk management viewpoint this unsolved vulnerability implies:

Poor patch management- The legacy systems have not been updated to patch the critical vulnerabilities present despite Microsoft making an official announcement emphasizing customers to "download and install the updates as soon as possible" while providing security updates for all vulnerable platforms on their Microsoft Update Catalog [16]

Absence of monitoring- A vulnerable and open RDP port (3389) indicates the lack of regular monitoring as the CVE-2019-0708 was officially reported by Microsoft on May 14th, 2019. It has been almost 6 years, and the threat has still not been mitigated, this shows a failure in continuous monitoring.

Policies and Mitigation

Disable unused services- Change default ports (TCP 3389) to a non-standard port to avoid detection during automated scans by attackers [17].

Update firmware/software- Patch all legacy systems against CVE-2019-0708 immediately

Audit and incident response processes- It is recommended to do regular and continuous vulnerability scans on systems and perform port audits. Develop and maintain an incident response plan for possible attacks such as brute-force or ransomware.

Key Finding 2: Exposed IP cameras via WebcamXP

Overview of WebcamXp and Hikvision Vulnerabilities

Internet protocol (IP) cameras are used for digital surveillance. These devices are connected to a LAN and can be accessed remotely on any devices via authorized logins. However, they may also pose security risks due to outdated software's or using default credentials. The system in this scan is running both WebcamXP and Hikvision IP cameras and Shodan revealed critical vulnerabilities such as CVE-2019-11072(allows code execution remotely via web) and CVE-2018-19052(exposes sensitive credentials and diagnostic details).

The cameras can be accessed publicly without needing any authentication, this is a serious risk to privacy as it exposes the interior and exterior of the premises. Also, the unpatched vulnerabilities on the systems can result in exploitation allowing the attacker to control cameras and access files on the network via directory traversal, which allows an attacker to traverse directories on an IP cameras file system, potentially allowing unauthorized access to sensitive files [18].

Shodan Scan

Using the filter- "webcamXP" port:81, Shodan confirmed the system is hosting live camera feeds using WebcamXP (streaming software) on port 81 and can be accessed publicly. WebcamXP uses port 81 on default and needs to be configured during the initial setup.

Observed Data

IP Address

- 31.208.147.163 (a public IP address can be used for reconnaissance via tools such as Nmap)

Location

- Trelleborg, Sweden

Open Ports

- Port 21(FTP)

- Port 53
- Port 81(webcamXP server),
- Port 137
- Port 443(Hikvision IP camera),
- Port 445
- Port 10000(lighttpd)

Technologies active

- WebcamXP
- Hikvision IP camera
- lighttpd server

Risk Analysis and Threat Scenario

Additionally, if an attacker exploits the vulnerability indicated by Shodan, the system (including the IP cameras and lighttpd server) can be exposed to the following potential security risks:

Unauthorized camera access- the attacker can have access to real-time camera feeds which is a serious privacy violation

Camera control- attackers can gain control over the IP cameras and carry out operations such as recording footage, disabling feed, zooming in and rotating to view other possible angles.

Criminal reconnaissance- attackers can use the real-time feed to monitor people's daily routine, scout the layout of the house and plan burglaries with perfect execution.

Risk Management Perspective

Additionally, from a risk management viewpoint this unsolved vulnerability implies:

Poor configuration- The IP camera is exposed directly to the public, allowing anyone to access the live feed without authentication.

Unpatched systems- There exists known vulnerabilities such as (CVE-2018-9995 and CVE-2019-3929) that were identified via Shodan on a recent scan from 11-05-25.

Policies and Mitigation

Strengthening access controls- Setting up stronger passwords instead of using default passwords is the first step in securing your devices. This makes it difficult for attackers to easily guess your passwords and gain unauthorized access to the system.

Update firmware/software- Vulnerabilities flagged by Shodan needs to be addressed immediately and all firmware updates needs to be installed from the vendors website. This ensures that your devices are protected from any security threats

Conclusion

This report aimed to identify real world vulnerabilities on internet connected devices through passive scanning using Shodan. During the scans using search filters mentioned in the report, Shodan revealed critical security risks such exposed RDP (Remote Desktop Protocol) services which is vulnerable to “BlueKeep” (CVE-2019-0708) and poorly configured IP cameras allowing access without needing any authentication, exposing real-time feed to the internet. These vulnerabilities can be exploited through remote code executions and allow attackers to gain unauthorized access such as access to camera feeds. Therefore, existing vulnerabilities need to be identified and mitigated immediately as leaving systems unpatched could become a potential threat to other connected systems on the network as well.

Bibliography

[1] W. N. Adger, "Vulnerability," *Global Environmental Change,* vol. 16, no. 3, p. 268–281, 2006.

[2] İ. Kara, " Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi," *Sakarya University Journal of Computer and Information Sciences,* vol. 2, no. 2, p. 61–69, 2019.

[3] Shodan, "What is Shodan?," Shodan, 2023. [Online]. Available: https://help.shodan.io/the-basics/what-is-shodan. [Accessed 22 May 2025].

[4] "What Is a Cybersecurity Posture?," SecurityScorecard, 2023. [Online]. Available: https://securityscorecard.com/blog/what-is-a-cybersecurity-posture/. [Accessed 22 May 2025].

[5] "What Is a Cybersecurity Vulnerability and How Do They Lead to Breaches?," SecurityScorecard, 2023. [Online]. Available: https://securityscorecard.com/blog/what-is-a-cybersecurity-vulnerability. [Accessed 22 May 2025].

[6] "What Is Continuous Cybersecurity Monitoring?," SecurityScorecard, 2023. [Online]. Available: https://securityscorecard.com/blog/what-is-continuous-cybersecurity-monitoring/. [Accessed 22 May 2023].

[7] MITRE, "CVE - Common Vulnerabilities and Exposures: Background," MITRE Corporation, 2000. [Online]. Available: https://web.archive.org/web/20250418034843/https:/cve.mitre.org/docs/docs-2000/cerias.html. [Accessed 22 May 2025].

[8] Wikipedia Foundation, "Common Vulnerabilities and Exposures," Wikipedia , [Online]. Available: https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures#cite_note-1. [Accessed 2 22 2025].

[9] VaultMatrix, "Black Box Penetration Testing," VaultMatrix, 2023. [Online]. Available: https://www.vaultmatrix.com/black-box-penetration-testing/. [Accessed 22 5 2025].

[10] GeeksforGeeks, "Software Testing – White Box Penetration Testing," GeeksforGeeks, 2023. [Online]. Available: https://www.geeksforgeeks.org/software-testing-white-box-penetration-testing/. [Accessed 22 5 2025].

[11] Check Point Software Technologies Ltd., "What is Gray Box Testing?," Check Point Software Technologies Ltd., 2022. [Online]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-gray-box-testing/. [Accessed 22 5 2025].

[12] S. H. Center, "What is Shodan?," 23 May 2025. [Online]. Available: https://help.shodan.io/the-basics/what-is-shodan. [Accessed 23 May 2025].

[13] E. Software, "What is RDP?," [Online]. Available: https://www.ericom.com/glossary/what-is-rdp/. [Accessed 23 May 2025].

[14] C. a. I. S. Agency, "Microsoft Operating Systems BlueKeep Vulnerability," 17 June 2019. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-168a. [Accessed 23 May 2025].

[15] T. Nguyen, "SHA-1: What It Is & How It's Used for Data Verification," [Online]. Available: https://www.lifewire.com/what-is-sha-1-2626011. [Accessed 23 May 2025].

[16] M. Corporation, "Customer guidance for CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: May 14, 2019," 14 May 2019. [Online]. Available: https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e. [Accessed 23 May 2025].

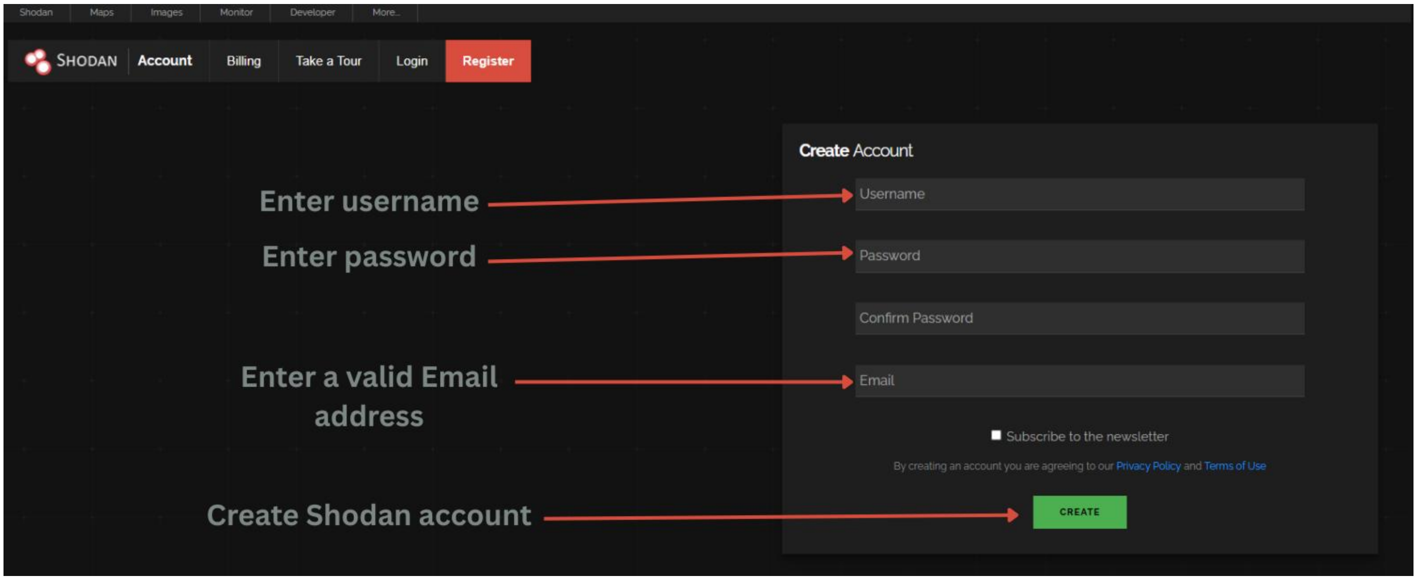
[17] C. f. C. Belgium, "CCB’s Cyber Tips: How to mitigate security risks for Remote Desktop Protocol (RDP)," 16 May 2024. [Online]. Available: https://atwork.safeonweb.be/news/ccbs-cyber-tips-how-mitigate-security-risks-remote-desktop-protocol-rdp. [Accessed 16 May 2025].

[18] SecuriThings, "Camera Vulnerability: Tutorial, Sample CVEs, and Best Practices," [Online]. Available: https://securithings.com/camera-vulnerability/. [Accessed 23 May 2025].

Appendices

Appendix A: Shodan Account Setup

This appendix contains three screenshots showing the login page, account page and the Shodan dashboard.



By creating an account you are agreeing to our Privacy Policy and Terms of Use

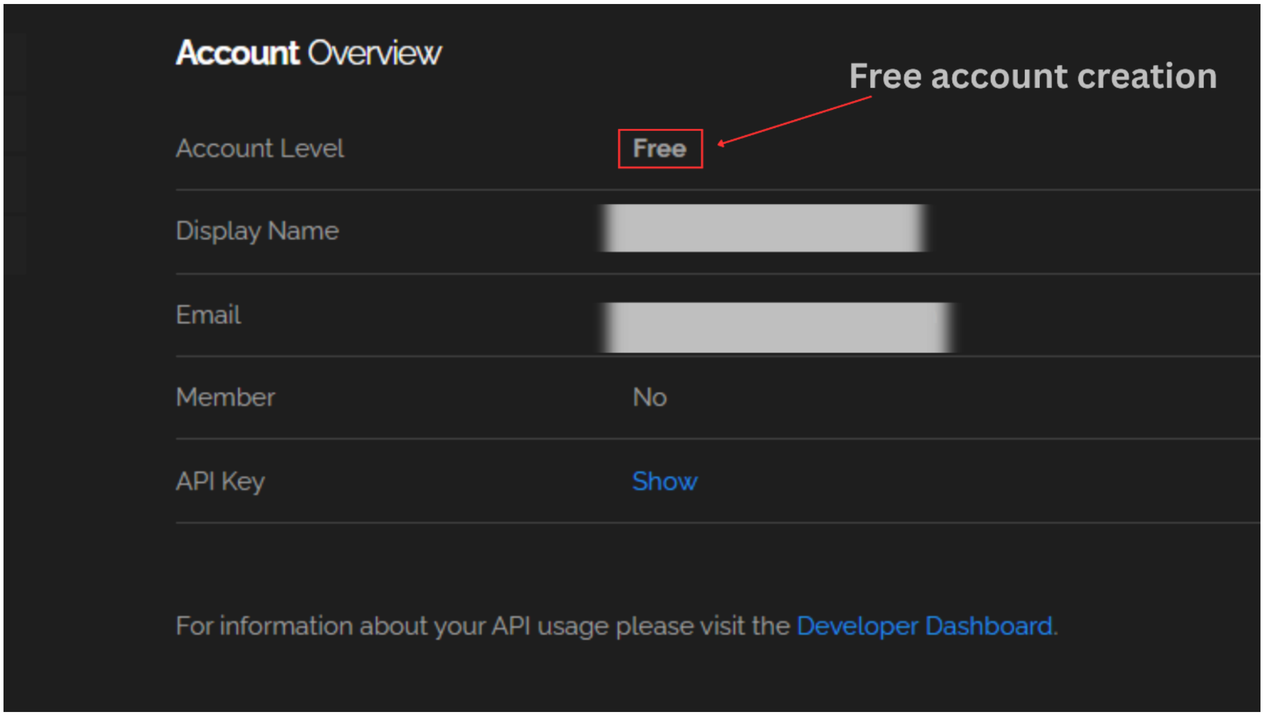
Enter username

Enter password

Enter a valid Email address

Create Shodan account

Figure 1: Shodan Sign-Up Page



Account Overview

Free account creation

Account Level: Free

Display Name: [redacted]

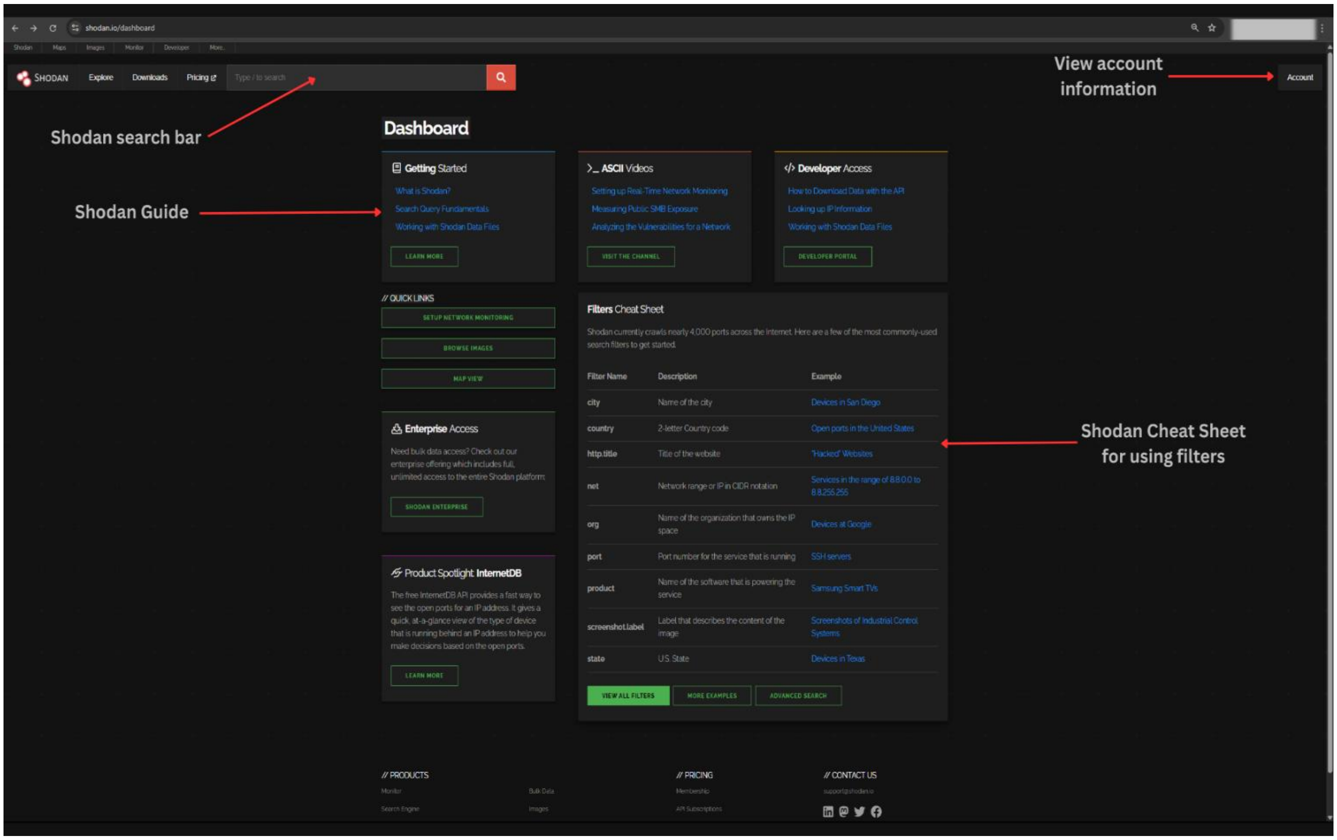
Email: [redacted]

Member: No

API Key: Show

For information about your API usage please visit the Developer Dashboard.

Figure 2: Successful Free Account Creation



Dashboard

Getting Started

- What is Shodan?
- Search Query Fundamentals
- Working with Shodan Data Files

>_ **ASCII** Videos

- Setting up Real-Time Network Monitoring
- Measuring Public SMB Exposure
- Analyzing the Vulnerabilities for a Network

</> **Developer** Access

- How to Download Data with the API
- Looking up IP Information
- Working with Shodan Data Files

// QUICK LINKS

Filters Cheat Sheet

Shodan currently crawls nearly 4,000 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	2-letter Country code	Open ports in the United States
http.title	Title of the website	"Hacked" Websites
net	Network range or IP in CIDR notation	Services in the range of 8.8.0.0 to 8.8.255.255
org	Name of the organization that owns the IP space	Devices at Google
port	Port number for the service that is running	SSH servers
product	Name of the software that is powering the service	Samsung Smart TVs
screenshot.label	Label that describes the content of the image	Screenshots of Industrial Control Systems
state	U.S. State	Devices in Texas

Enterprise Access

Need bulk data access? Check out our enterprise offering which includes full, unlimited access to the entire Shodan platform.

Product Spotlight: **InternetDB**

The free InternetDB API provides a fast way to see the open ports for an IP address. It gives a quick, at-a-glance view of the type of device that is running behind an IP address to help you make decisions based on the open ports.

// PRODUCTS

Monitor
Bulk Data
Search Engine
Images

// PRICING

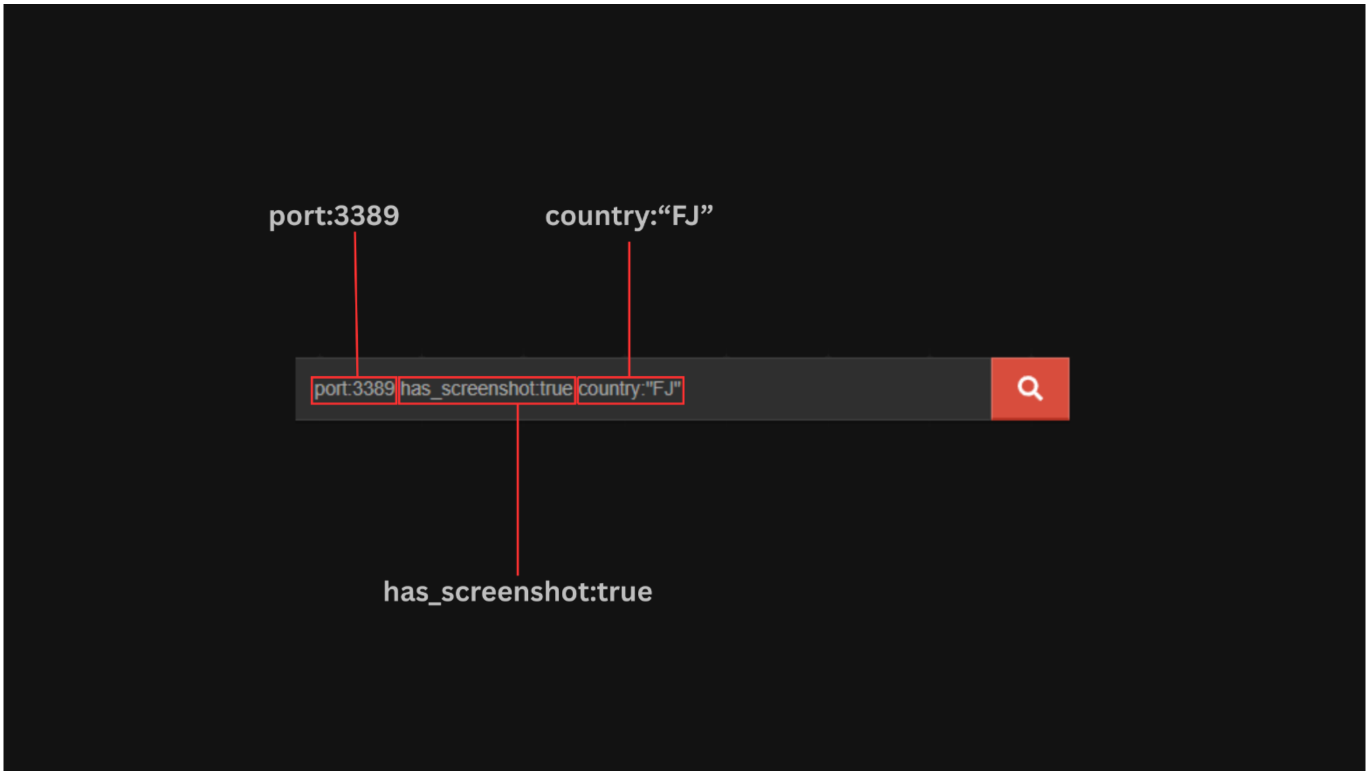
Membership
API Subscriptions

// CONTACT US

support@shodan.io

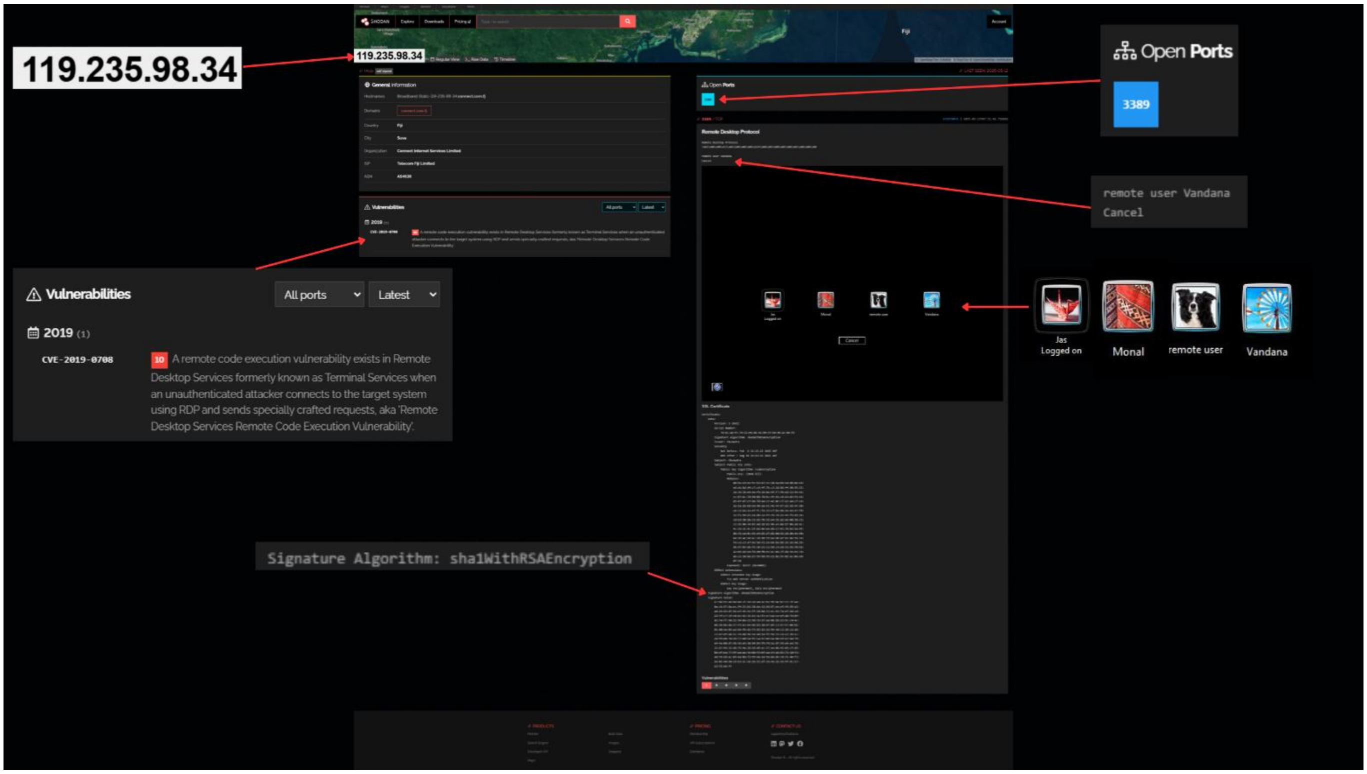
Figure 3: Shodan dashboard

Appendix B: Vulnerability Scan- Target 1



port:3389 has_screenshot:true country:"FJ"

Figure 4: Search filer used in Shodan



```
remote user Vandana
Cancel
```

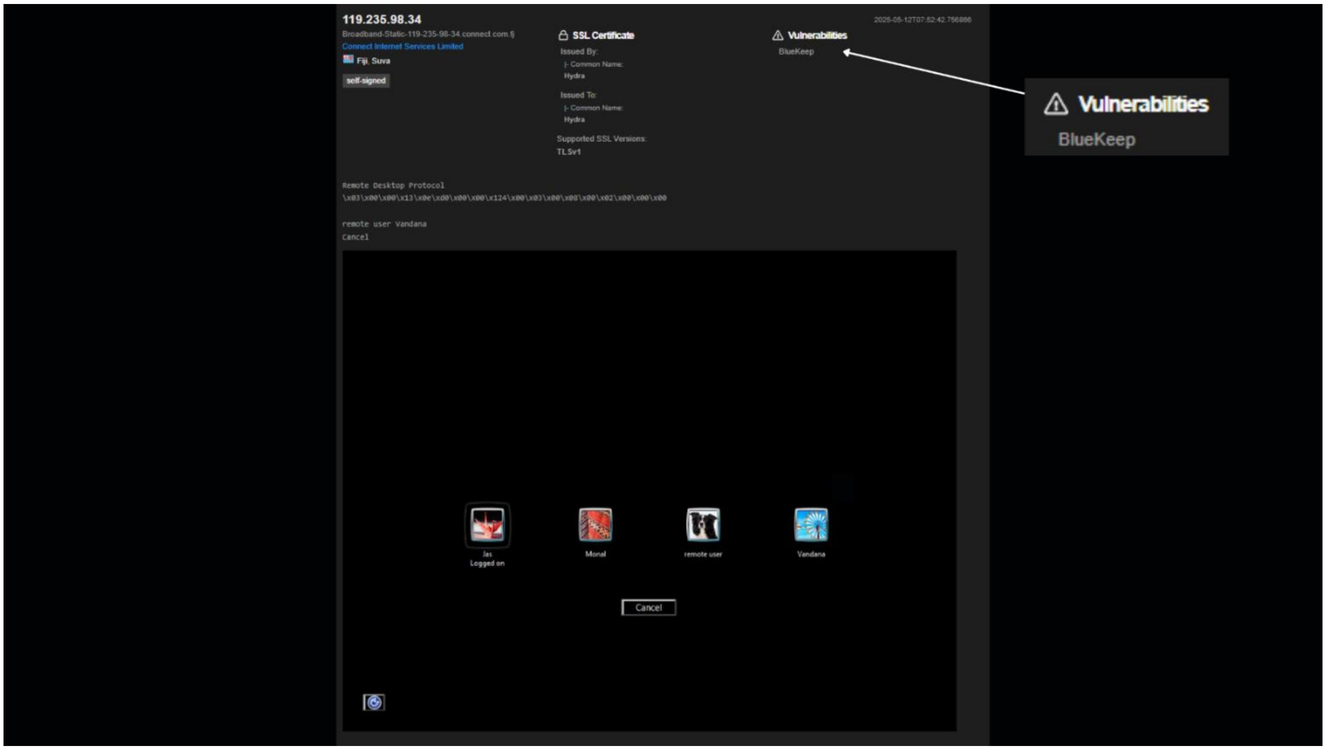
Vulnerabilities All ports Latest

2019 (1)

CVE-2019-0708 — 10 A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

```
Signature Algorithm: sha1WithRSAEncryption
```

Figure 5: Results from search filter show the public IP address, CVE, signature algorithm used, open ports and user accounts on the system



119.235.98.34

2025-05-12T07:52:42.756886

Broadband-Static-119-235-98-34.connect.com.fj

Connect Internet Services Limited

Fiji, Suva

self-signed

SSL Certificate

Issued By:
|- Common Name:
Hydra

Issued To:
|- Common Name:
Hydra

Supported SSL Versions:
TLSv1

Vulnerabilities

BlueKeep

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x03\x00\x08\x00\x02\x00\x00\x00

remote user Vandana
Cancel
```

Figure 6:Presense of BlueKeep vulnerabilities

Appendix C: Vulnerability Scan- Target 2

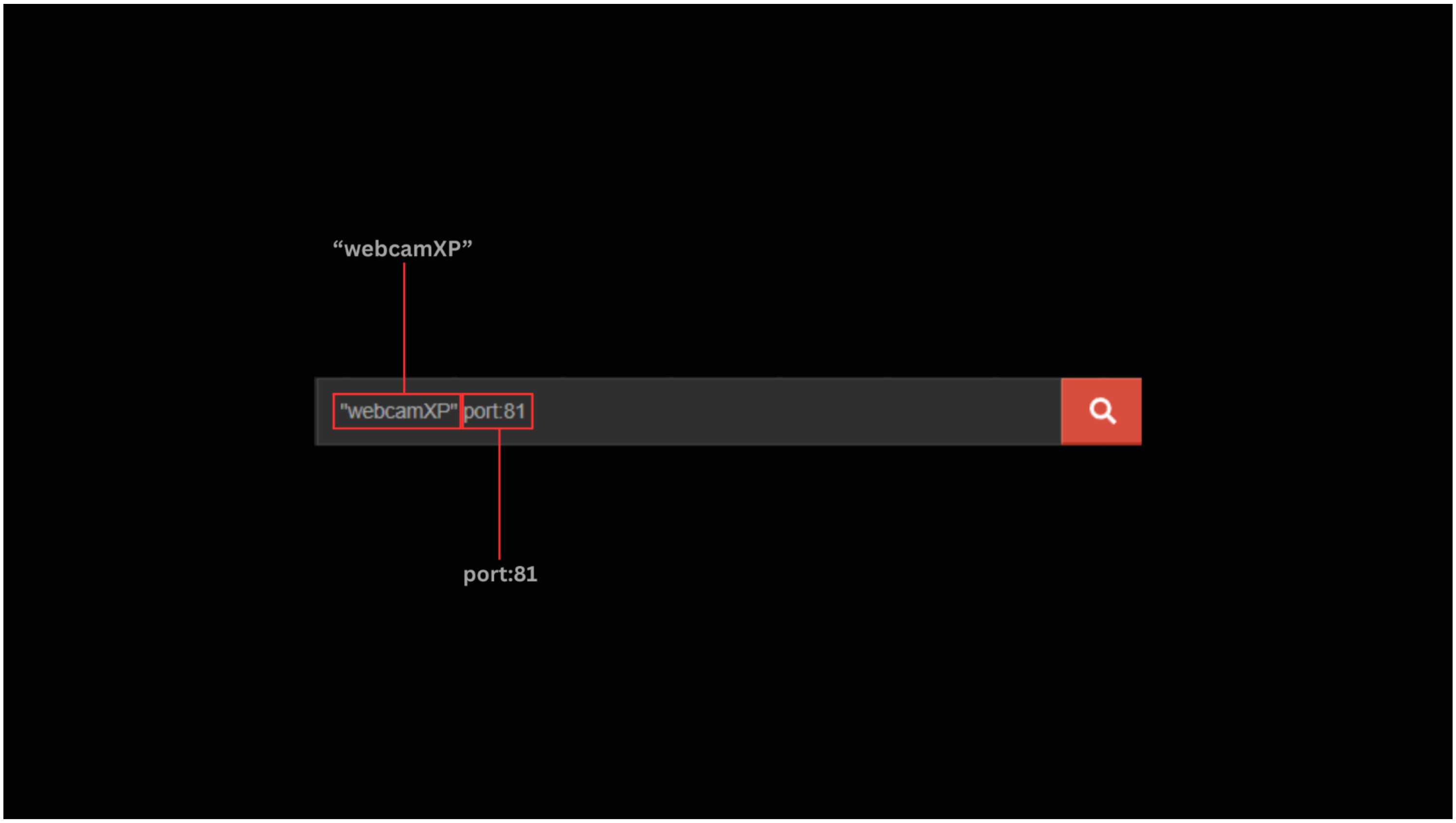
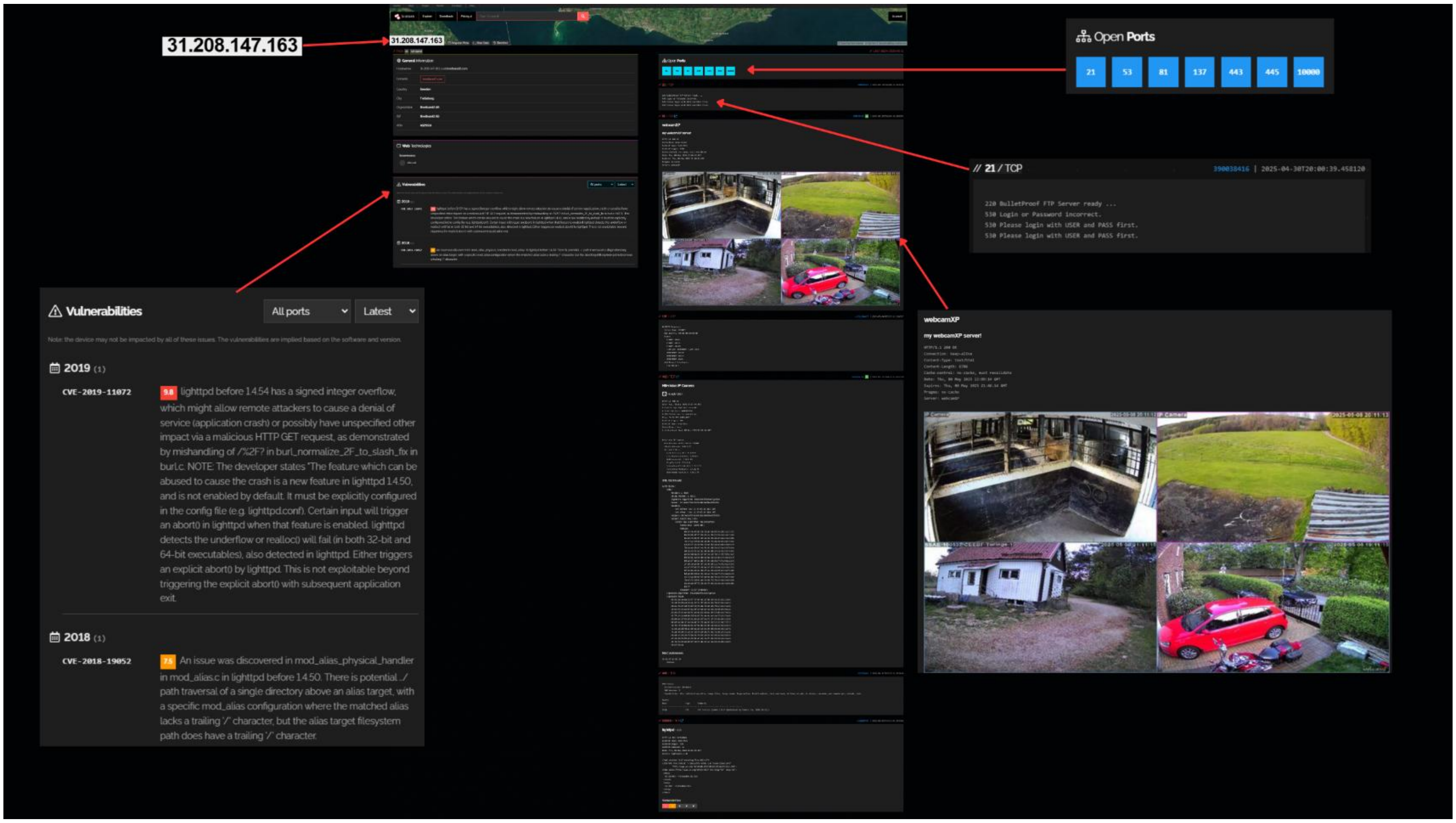


Figure 7: Search filter used to find second vulnerability



Open Ports

// 21 / TCP 390038416 | 2025-04-30T20:00:39.458120

```
220 BulletProof FTP Server ready ...
530 Login or Password incorrect.
530 Please login with USER and PASS first.
530 Please login with USER and PASS first.
```

webcamXP

my webcamXP server!

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Type: text/html
Content-Length: [illegible]
Cache-control: no-cache, must revalidate
Date: Thu, 08 May 2025 [illegible] GMT
Expires: Thu, 08 May 2025 [illegible] GMT
Pragma: no-cache
Server: webcamXP
```

⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2019 (1)

CVE-2019-11072 9.8 lighttpd before 1.4.54 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a malicious HTTP GET request, as demonstrated by mishandling of /%2F? in burl_normalize_2F_to_slash_fix in burl.c. NOTE: The developer states "The feature which can be abused to cause the crash is a new feature in lighttpd 1.4.50, and is not enabled by default. It must be explicitly configured in the config file (e.g. lighttpd.conf). Certain input will trigger an abort() in lighttpd when that feature is enabled. lighttpd detects the underflow or realloc() will fail (in both 32-bit and 64-bit executables), also detected in lighttpd. Either triggers an explicit abort() by lighttpd. This is not exploitable beyond triggering the explicit abort() with subsequent application exit.

2018 (1)

CVE-2018-19052 7.5 An issue was discovered in mod_alias_physical_handler in mod_alias.c in lighttpd before 1.4.50. There is potential ../ path traversal of a single directory above an alias target, with a specific mod_alias configuration where the matched alias lacks a trailing '/' character, but the alias target filesystem path does have a trailing '/' character.

Figure 8: The search result indicates the public IP address, vulnerabilities on the system, open ports, weak credentials on the FTP Server, exposed IP cameras to the internet

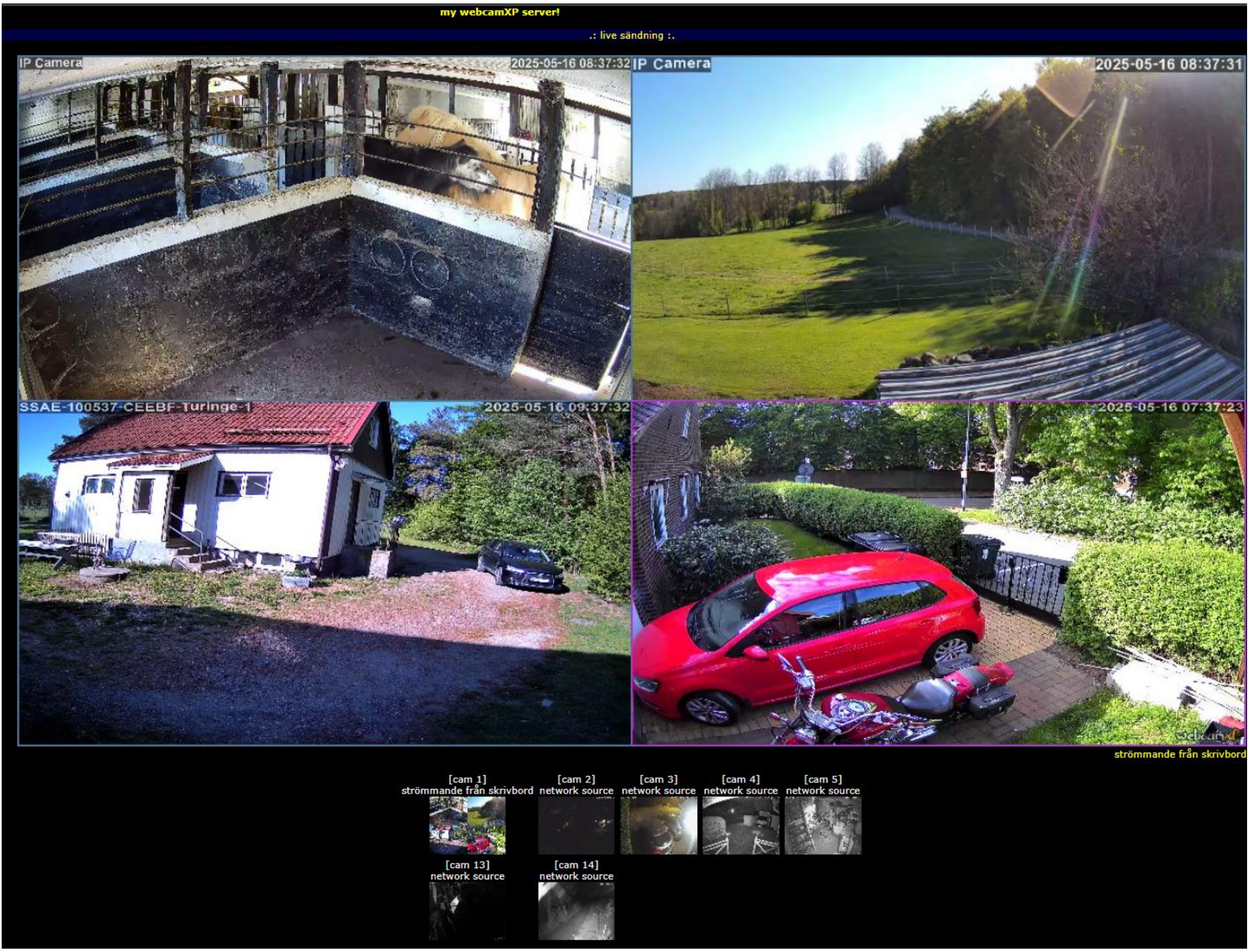


Figure 9: Real-time camera feed from the exposed IP camera