Internet of Things Vulnerabilities

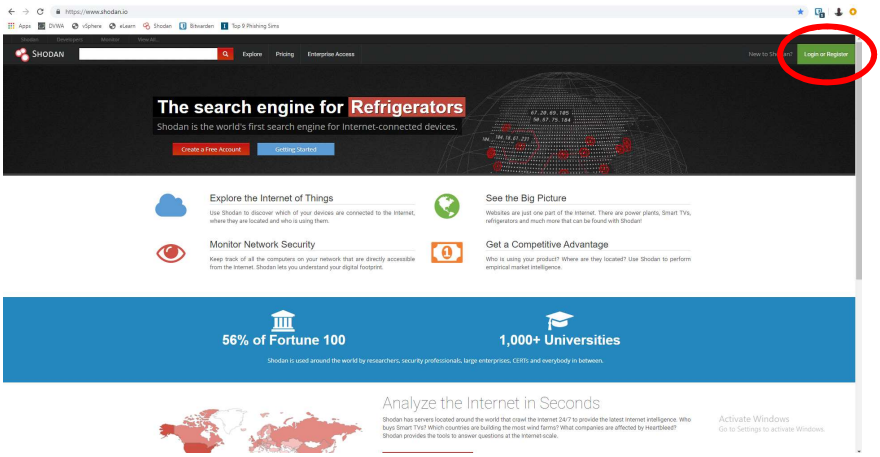
Mohawk College

HACKSTUDENT

2. Online IoT Reconnaissance

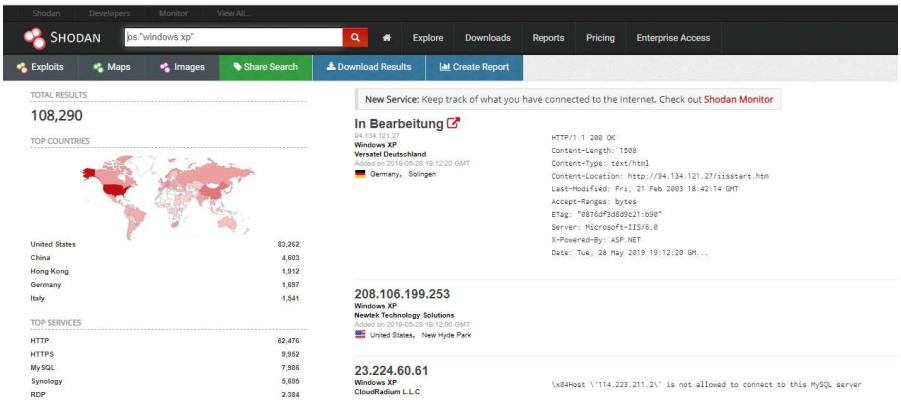
Shodan "the world's first search engine for Internet-connected devices". Shodan collects banner information, similar to the website header information we work with int he Web Application and Server lab. Unfortunately, many of these devices, along with hundreds of thousands of servers and other machines, are exposed and unsecured or poorly secured, and their owners don't realize their exposure and vulnerability online.

2.1. Browse to **https://shodan.io** and click on the **Login or Register** button.



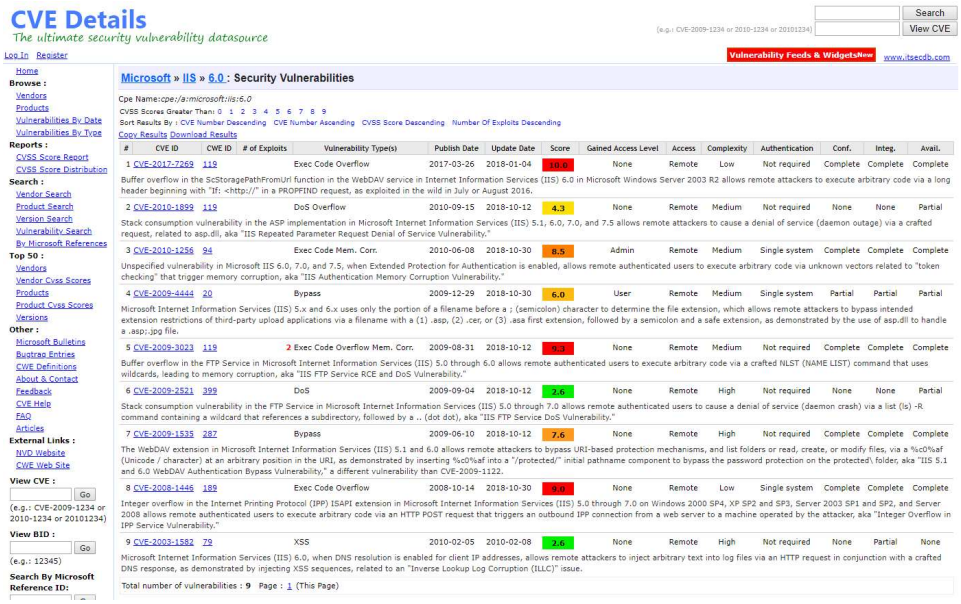
You must register your own account to use the website. There is a limitation to free accounts that you can only do a certain number of searches per day. When you register an account, it will send a verification email to the account you registered with. Once you verify your email by clicking the link inside the email, you can continue.

2.2. Now we can search the Internet for devices that are outdated, insecure, and poorly secured. For example, how many people would you expect to find still running Windows XP? Run a search using the command **os:"windows xp"** and you'll find more than 70,000 machines still running Windows XP despite the fact that Microsoft hasn't provided XP with security updates and software support since 2009.



2.3. See how many of those XP machines are running an IIS 6.0 web server, released in 2003, by searching using **"Microsoft-IIS/6.0" os:"Windows XP"**.

If we search for **IIS 6.0** in a database of security CVEs (Common Vulnerabilities and Exposures), like the one at **cvedetails.com**, we can find 6 serious or critical vulnerabilities just in the IIS 6.0 server software.



CVE Details
The ultimate security vulnerability datasource

Microsoft » IIS » 6.0 : Security Vulnerabilities

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-7269	119		Exec Code Overflow	2017-03-26	2018-01-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
	Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.													
2	CVE-2010-1899	119		DoS Overflow	2010-09-15	2018-10-12	4.3	None	Remote	Medium	Not required	None	None	Partial
	Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."													
3	CVE-2010-1256	94		Exec Code Mem. Corr.	2010-06-08	2018-10-30	8.5	Admin	Remote	Medium	Single system	Complete	Complete	Complete
	Unspecified vulnerability in Microsoft IIS 6.0, 7.0, and 7.5, when Extended Protection for Authentication is enabled, allows remote authenticated users to execute arbitrary code via unknown vectors related to "token checking" that trigger memory corruption, aka "IIS Authentication Memory Corruption Vulnerability."													
4	CVE-2009-4444	20		Bypass	2009-12-29	2018-10-30	6.0	User	Remote	Medium	Single system	Partial	Partial	Partial
	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.													
5	CVE-2009-3023	119	2	Exec Code Overflow Mem. Corr.	2009-08-31	2018-10-12	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
	Buffer overflow in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 6.0 allows remote authenticated users to execute arbitrary code via a crafted NLST (NAME LIST) command that uses wildcards, leading to memory corruption, aka "IIS FTP Service RCE and DoS Vulnerability."													
6	CVE-2009-2521	399		DoS	2009-09-04	2018-10-12	2.6	None	Remote	High	Not required	None	None	Partial
	Stack consumption vulnerability in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to cause a denial of service (daemon crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot), aka "IIS FTP Service DoS Vulnerability."													
7	CVE-2009-1535	287		Bypass	2009-06-10	2018-10-12	7.6	None	Remote	High	Not required	Complete	Complete	Complete
	The WebDAV extension in Microsoft Internet Information Services (IIS) 5.1 and 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files, via a %c0%af (Unicode / character) at an arbitrary position in the URI, as demonstrated by inserting %c0%af into a "/protected/" initial pathname component to bypass the password protection on the protected\ folder, aka "IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability," a different vulnerability than CVE-2009-1122.													
8	CVE-2008-1446	189		Exec Code Overflow	2008-10-14	2018-10-30	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
	Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka "Integer Overflow in IPP Service Vulnerability."													
9	CVE-2003-1582	79		XSS	2010-02-05	2010-02-08	2.6	None	Remote	High	Not required	None	Partial	None
	Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.													

Search for "**Windows XP**" vulnerabilities on cvedetails.com... There are literally hundreds of cataloged vulnerabilities for Windows XP. Compare that to the 70,000 windows XP machines that you discovered on Shodan. These are not just personal computers running Windows XP. A lot of these are businesses and it should make you realize how vulnerable these companies could be to a cyber attack.

Now we will do a search for "Windows 10". There are well over 1000 of them. If you select a vulnerability, It will bring you to a page that will display specific information about the vulnerability. This includes whether you require authentication, whether there are preconditions you must meet, and how it will affect your system. There is also a table that indicates which versions of which operating systems are affected by the vulnerability. This is why it's so important to update your operating system.

– Products Affected By CVE-2019-1359

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Microsoft	Windows 10	-				Version Details Vulnerabilities
2	OS	Microsoft	Windows 10	1607				Version Details Vulnerabilities
3	OS	Microsoft	Windows 10	1703				Version Details Vulnerabilities
4	OS	Microsoft	Windows 10	1709				Version Details Vulnerabilities
5	OS	Microsoft	Windows 10	1803				Version Details Vulnerabilities
6	OS	Microsoft	Windows 10	1809				Version Details Vulnerabilities
7	OS	Microsoft	Windows 10	1903				Version Details Vulnerabilities

2.4. Shodan also catalogues other devices, like security cameras, that are connected to the Internet for remote monitoring. One of the most popular searches on Shodan is of SQ-Webcam video servers. Search for **Server: SQ-WEBCAM** and you'll still find quite a few devices. Many will be offline at different times of the day, and some are no longer connected, but occasionally you will find a login screen like this:

This is the most common web portal to the SQ Webcam server, and many of them still have default credentials. And in many cases it is quite easy to locate a set of default credentials on websites like **http://open-sez.me**

This is why it is so important that manufacturers should not hard-code default credentials into a device and that you create strong, unique credentials when you set up a new Internet-connected device.

2.6. Another popular IP camera is the webcamxp, and they very frequently require no login credentials at all! Search **webcamxp** and see if you can locate an unsecured camera. As you only get 2 pages of results with a free Shodan account, you can find more results by providing a country search using **webcamxp country:EX** , replacing the EX with a country code like **CA**.

As it stands now, it is up to consumers to educate themselves about the privacy and security issues that come with the devices they purchase. There are, however, increasing calls for legislation that would require strong device security, remove hard-coded and default credentials, and provide clear, standardised labelling about the capabilities and exposure of connected devices (e.g., is there a microphone in my TV?, what online servers will it connect to?).

2.7. By no means is Shodan limited to old web servers and IP cameras. Google the manufacturers of some industrial building controllers and other IoT/IIoT devices, and see if you can find any of their products in Shodan. Try clicking on the device's IP address in Shodan and see what other information you can retrieve about the location and nature of the device.

Thankfully, many manufacturers and users are learning about the vulnerability of their Internet-connected devices using tools like Shodan, and are improving the security of their web interfaces or removing them from the open Internet altogether.