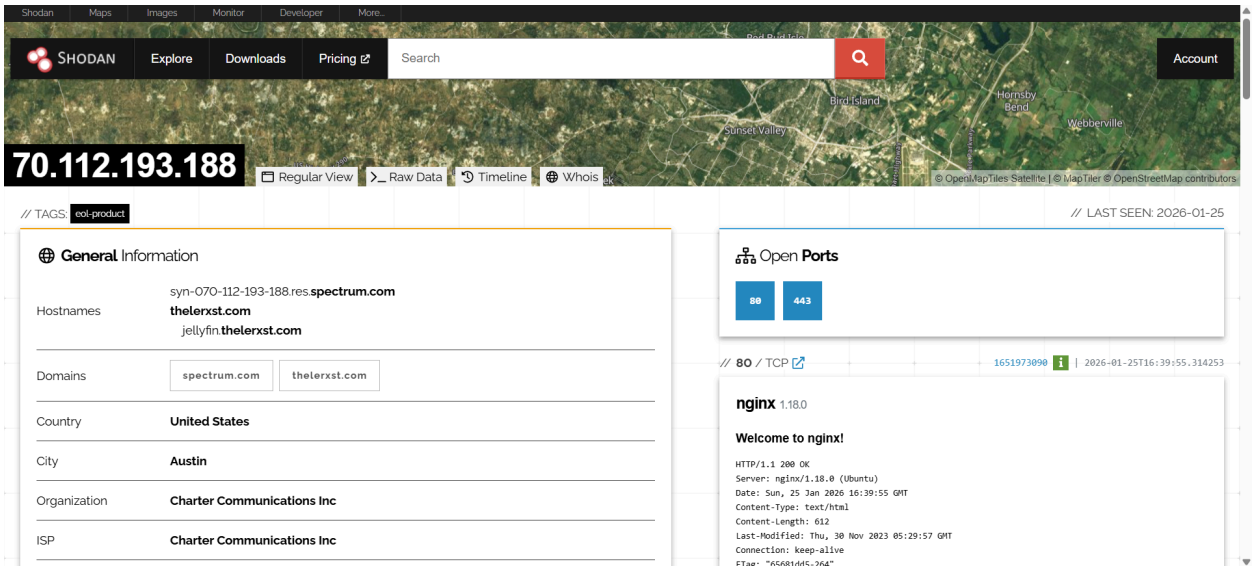
Diane Gilzow
February 16, 2026
CYSE 450: Ethical Hacking and Penetration Testing
Dr. Md Morshed Alam

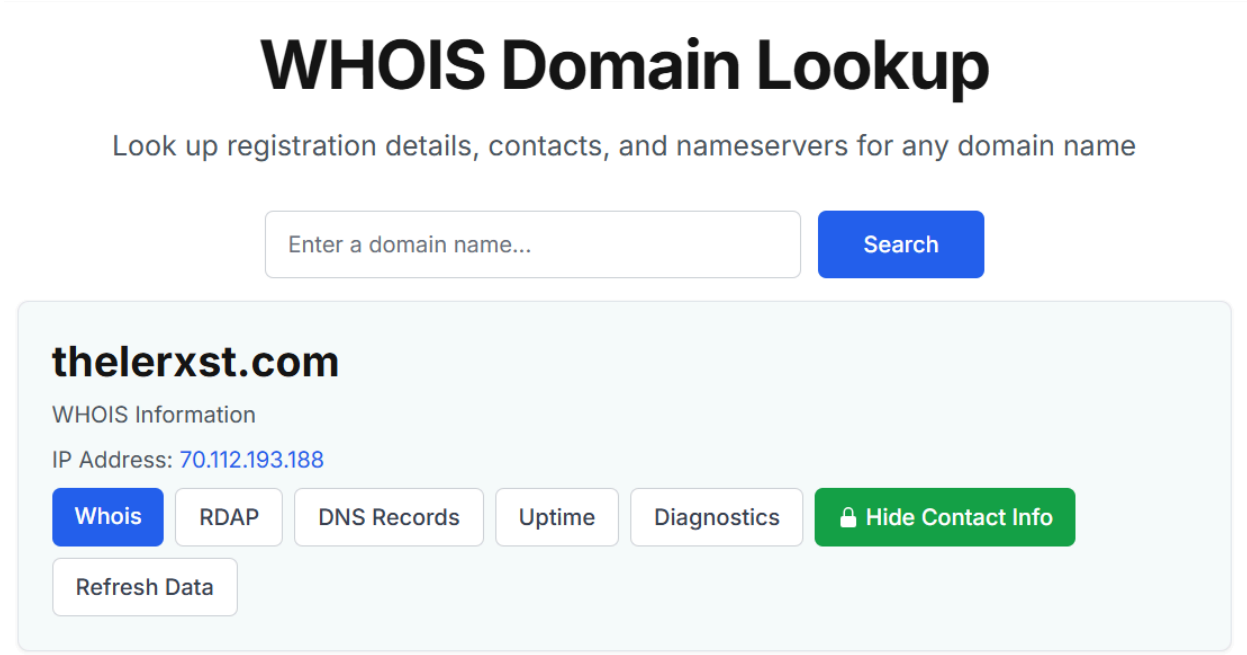
Lab 3: Passive Reconnaissance

Question 1: Login to Shodan (https://www.shodan.io/) using your Gmail account or any other account you have created with the portal. Search Web Camera or Web Cam in the search bar, and you will be shown a report where a number of accessible web cameras are listed.

- **Task 1:** Find a device where there is at least one open port and the domain name (URL) is displayed. If you find multiple such devices, just choose one arbitrarily. Take a screenshot highlighting the domain name and the open ports. Attach the screenshot in your submission.



- **Task 2:** Using WHOIS (https://who.is/) or Netcraft (https://sitereport.netcraft.com/), find the IP address of the domain name you found in Task 1. Take a screenshot highlighting the IP address and attach it in your submission. Go through the complete report you retrieved from WHOIS or Netcraft. Do some research online about the vulnerabilities or weakness the device has. Briefly describe all the security weakness or vulnerabilities you found.



There were multiple vulnerabilities found in the website, most of which were related to Jellyfin. One vulnerability I found involved argument injection in FFmpeg, which could allow attackers to write files and potentially execute remote code. Other vulnerabilities I found included cross-site scripting and directory traversal, and if combined together, they could result in file write and remote code execution. Additional vulnerabilities included TLS session resumption authentication bypass, memory corruption, HTTP/2 denial-of-service, uncontrolled resource consumption, and cross-protocol TLS attacks.

Question 2: Login to Shodan again, but this time search for port:502. Select a device that meets the following criteria:

1. There is at least some information in the device identification field.
2. There is at least one CVE listed in the Vulnerabilities section.

- **Task 1:** Capture some screenshots showing the device id, open ports, and the CVE lists. Attach the screenshots in your submission.

// TAGS: videogame

General Information

Hostnames	abts-north-static-177.77.176.122.**airtelbroadband.in**
Domains	airtelbroadband.in
Country	**India**
City	**Noida**
Organization	**BHARTI TELENET LTD. NEW DELHI**
ISP	**Bharti Airtel Ltd., Telemedia Services**
ASN	**AS24560**
Operating System	**Windows**

Web Technologies

Operating Systems

Windows Server

Web Frameworks

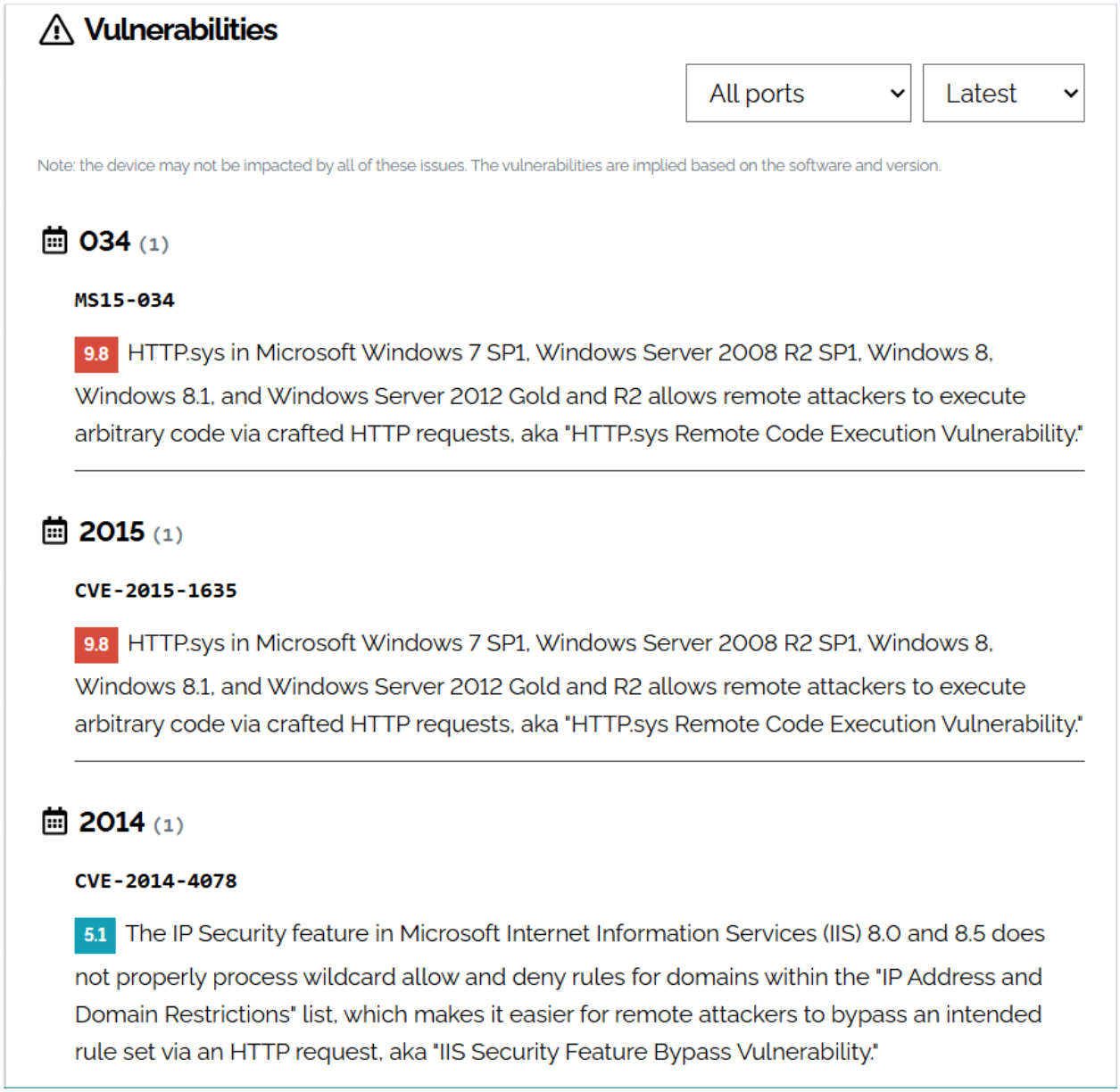
Microsoft ASP.NET

Web Servers

IIS 8.5

Open **Ports**

11	13	15	17	19	21	22	23	25	26	37
49	51	70	79	80	82	83	86	88	102	104
110	111	113	119	122	143	175	179	180	195	211
221	264	311	314	385	389	427	441	443	444	445
446	447	451	453	461	491	502	503	513	515	522
541	548	554	555	587	593	632	636	666	685	771
806	831	873	885	902	993	1024	1080	1099	1111	1153
1177	1200	1224	1234	1244	1249	1283	1291	1311	1337	1355
1366	1414	1433	1443	1456	1471	1515	1521	1599	1604	1723
1741	1800	1801	1883	1911	1925	1926	1951	1962	1983	1988
2002	2003	2008	2030	2065	2067	2081	2082	2083	2086	2087



- **Task 2:** Do some research about the device you chose and describe the device type and found vulnerabilities in a paragraph. Try to keep the paragraph limited into 5-10 sentences.
    - The device that I found is a Windows server running Microsoft IIS, which is widely used to host websites and web applications. This server uses the HTTP.sys component to manage HTTP requests. One vulnerability that I found in this system is MS15-034, or CVE-2015-1635 flaw, that enables remote attackers to execute arbitrary code by sending specially crafted HTTP requests. Another vulnerability that I found was CVE-2014-4078, which affected the IP Security

feature in IIS 8.0 and 8.5. In this flaw, wildcard rules for domain restrictions were improperly processed that allowed attackers to bypass access controls.

- **Task 3:** Select a CVE from the CVE list shown in the Vulnerabilities section and search for that CVE in https://cve.mitre.org/. Identify the attack/vulnerability described in the CVE. Go to https://attack.mitre.org/matrices/enterprise/network/ and find the attack from the matrix. If the attack is not listed there, try to search in other attack matrices given in the MITRE ATT&CK website. Once you find the attack listed as a technique, try to find out one relevant detection and one mitigation methods. Take screenshots showing the detection id and the mitigation id. Attach your screenshots in your submission and briefly summarize the selected detection and mitigation methods.

  The CVE I have selected is CVE-2014-4078. The description of the CVE states that the IP Security feature in Microsoft ISS improperly handles wildcard allow and deny rules for domains in the “IP Address and Domain Restrictions” list, which allows remote attackers to bypass intended access controls through crafted HTTP requests. The technique that I found that aligns with this CVE is T1190: Exploit Public-Facing Application. This technique describes adversaries exploiting weaknesses in an Internet-accessible service to gain access to a system. A relevant detection method for this attack is DET0080 that identifies abnormal request patterns to public endpoints, unusual error responses, server processes spawning shells or loading non-standard modules, and optional outbound connections from the host. A relevant mitigation method for this attack is Application Isolation and Sandboxing (M1048), which limits the access that an exploited process has to other system resources and reduces the impact of the attack.

ID	Name	Analytic ID	Analytic Description
DET0080	Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)	AN0219	Adversary sends crafted HTTP/S (or other service) input to an Internet-facing app (IIS/ASP.NET, API, device portal). Chain: (1) abnormal request patterns to public endpoint → (2) elevated 4xx/5xx or unusual methods/paths → (3) server process (w3wp.exe/other service) spawns shell/LOLbins or loads non-standard modules → (4) optional outbound callback from the host/container.

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Application isolation will limit what other processes and system features the exploited target can access.