. Use Nmap to Find Web Services

Run a full port scan first:

bash

CopyEdit

nmap -p- <IP>

Then scan for service versions:

bash

CopyEdit

nmap -sC -sV -p <open-ports> <IP>

Look for ports commonly used by web servers:

Port	**Description**
80	HTTP
443	HTTPS
8080	Alt HTTP
8000, 8888, 8443	Common web ports
5000, 7000+	Sometimes for custom apps

□ 2. If Web Service Found → Open in Browser

Example:

bash

CopyEdit

firefox http://<IP>:8080

If https is reported:

bash

CopyEdit

firefox https://<IP>

Or just type the IP into Firefox — but **check port numbers too**, especially if the web app is running on a non-standard port (e.g., 8080, 8888).

🛠 **3. Enumerate Web App for SQLi**

Tools & manual steps:

bash

CopyEdit

whatweb http://<IP>

Look for:

- Login forms
- Search fields
- URLs like ?id=1
- Forms that accept input

Then try basic manual SQLi:

text

CopyEdit

' OR 1=1 --

Or use:

bash

CopyEdit

sqlmap -u "http://<IP>/page.php?id=1" --batch

💡 **Notes:**

- SQLi can happen on **either Windows or Linux** — doesn't matter which OS is underneath.
- Always verify web services with nmap **before trying in browser**.
- Also, check **robots.txt**, /admin, /login, and hidden directories using:

bash

CopyEdit

gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt

---

□ Add This to Notes:

bash

CopyEdit

1. Find web ports

nmap -p- <IP>

nmap -sC -sV -p <open-ports> <IP>

2. Open browser (use correct port)

firefox http://<IP>

firefox http://<IP>:8080

3. Enumerate web app

whatweb http://<IP>

gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt

Look for forms, GET params, login pages

4. Check for SQLi

sqlmap -u "http://<IP>/page.php?id=1" --batch

Try payloads manually: ' OR 1=1 --

Let me know if you'd like a **web exploitation mini-checklist** too.