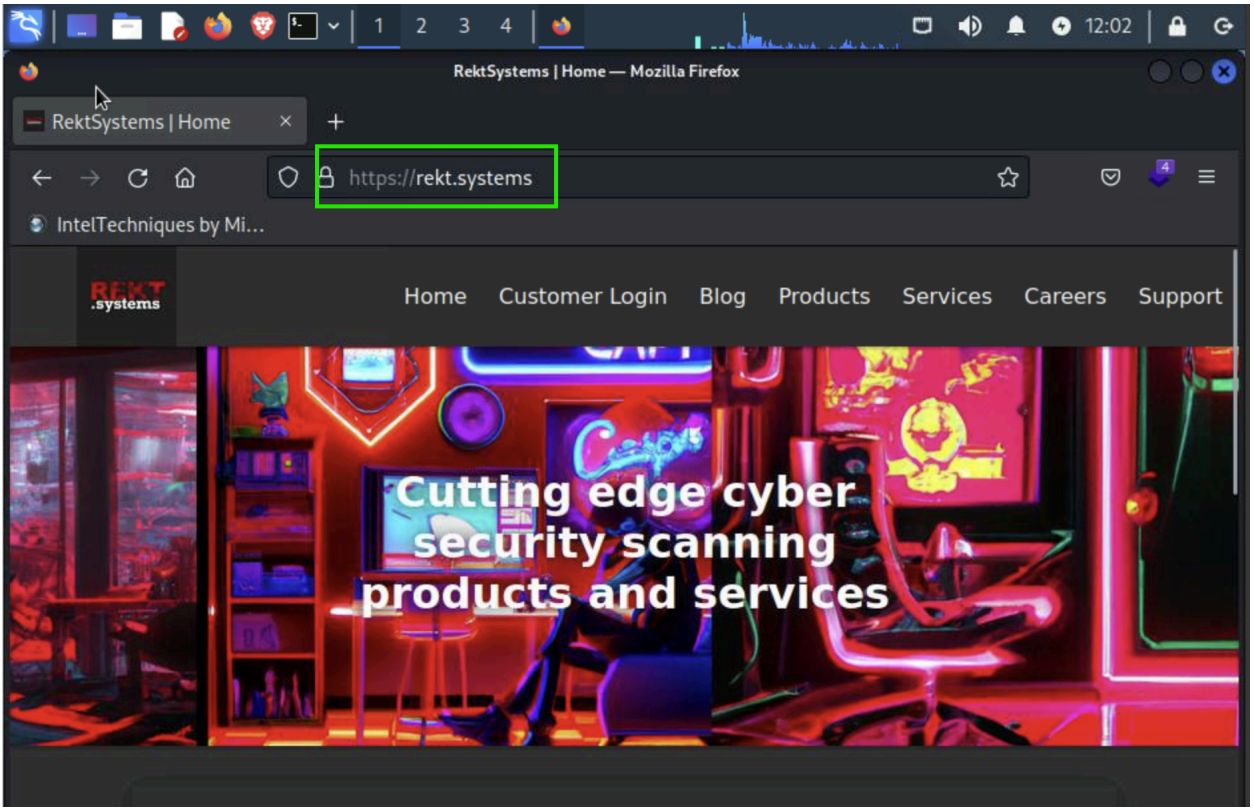
Listing the website urls | xml site map | exploring website's images,pdf etc for metadata (about device used,user,infrastructure of the website company)|Found a printer vulnerbiltiy(infursture)|| Search vulnerability in the NVD

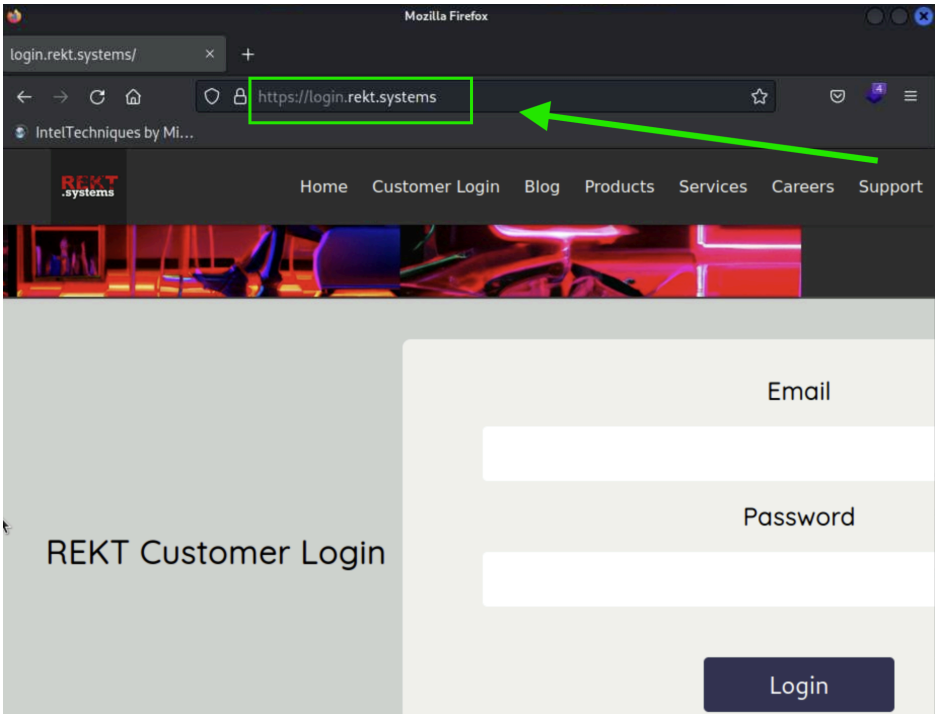
Exploring Company vulnerability using websites | OSINT

Our target is Rekt Systems, a cybersecurity company with a web presence at rekt.systems.

Part 1 - Collecting URL s

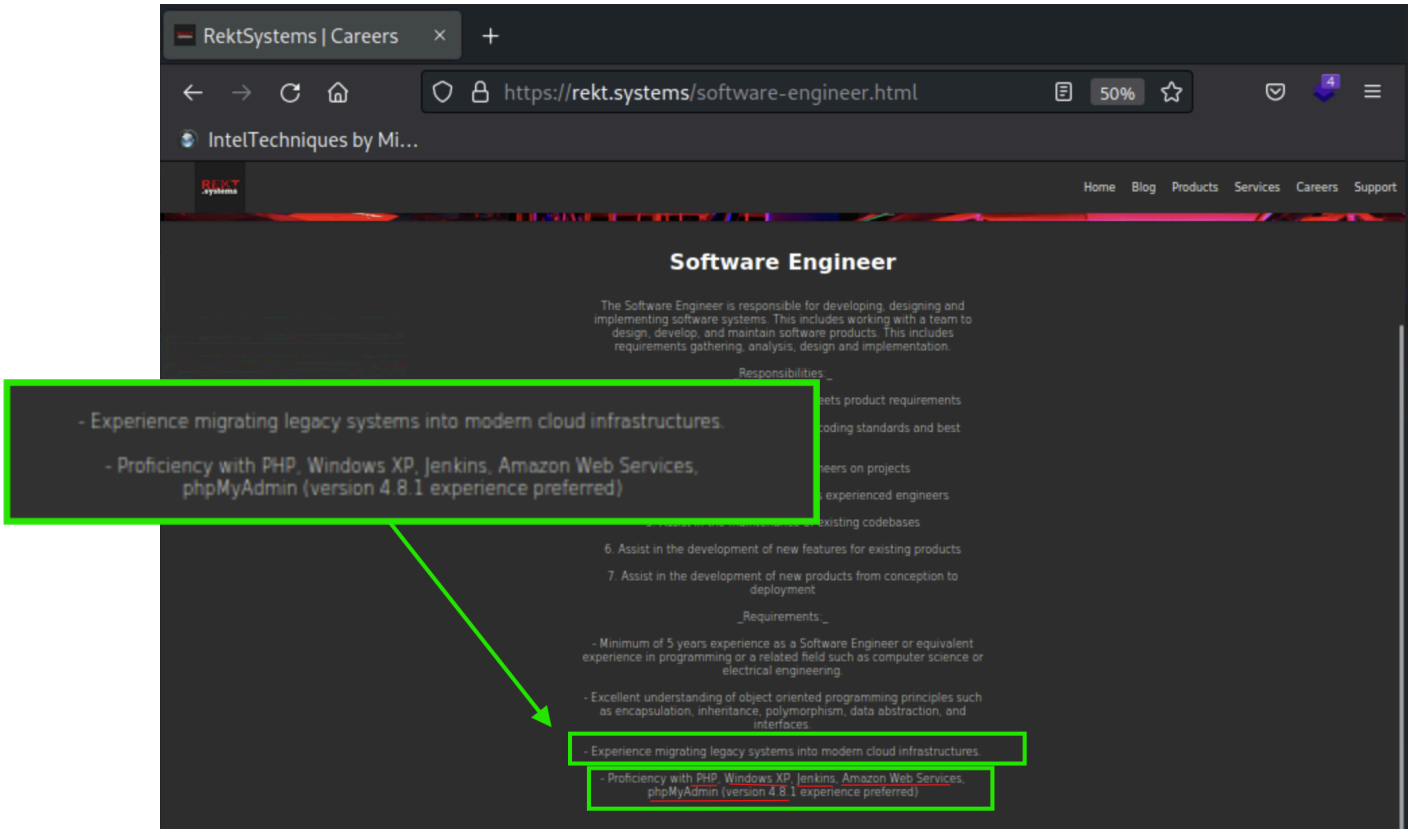


1. Looking for any subdomains

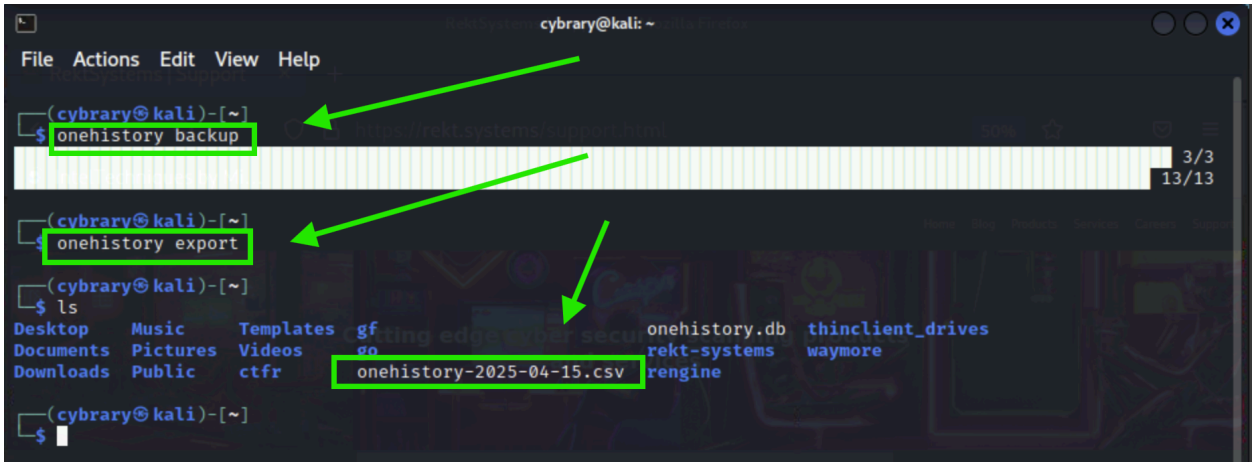


Noticed a new sub domain → https://login.rekt.systems

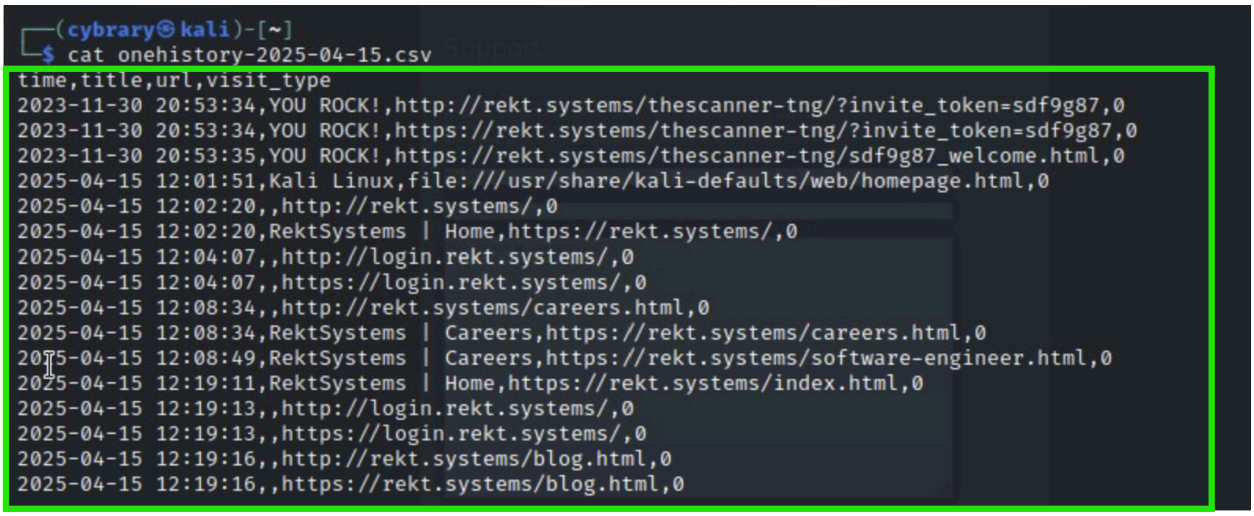
2. In the software engineering job description, an indication that this company is likely using a specific version of phpmyadmin .Indication that company is moving from legacy system to clous AWS



3. Execute **onehistory backup** to capture the browser history on this machine. Then execute **onehistory export** to export browser history to a CSV

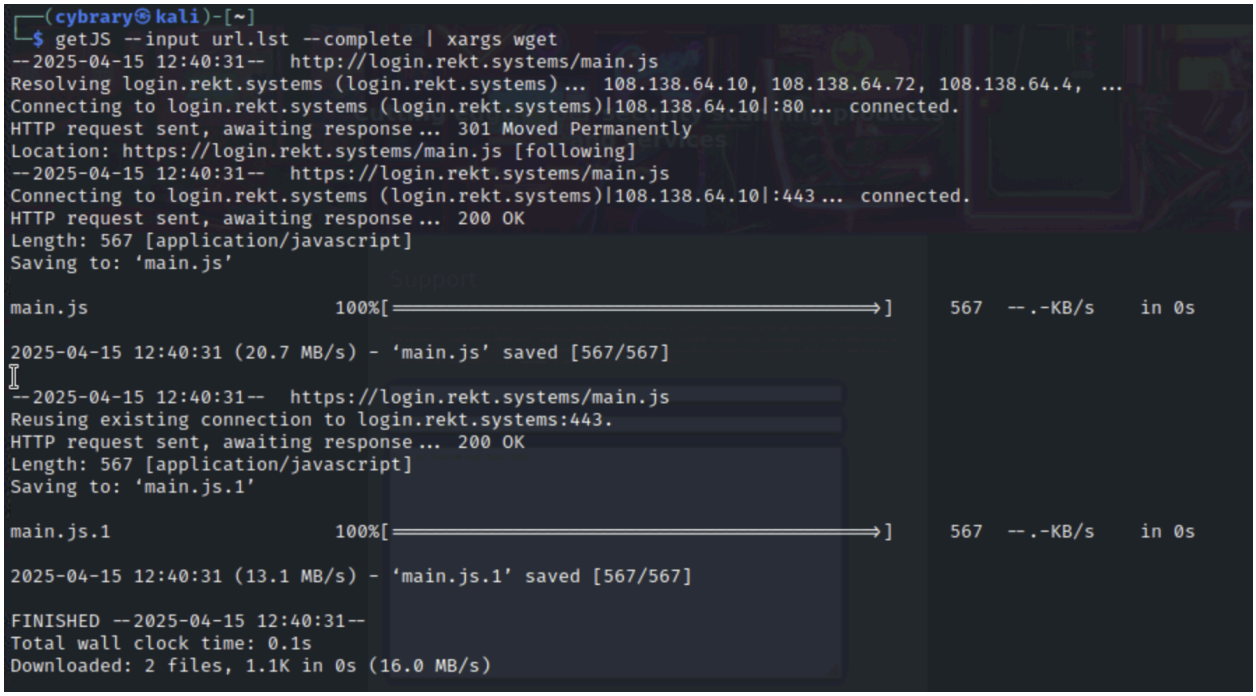


4. Captured browser history



5. We'll use ***gf*** to find specific patterns (URLs) in our output that we want to redirect to a list; and we'll pass our pattern matches through ***anew***, which ensures we only add entries not already in the file.

6. Find all javascript files referenced in the HTML of your discovered URLs



7. Now we already have a few interesting endpoints to target in our active recon phase.

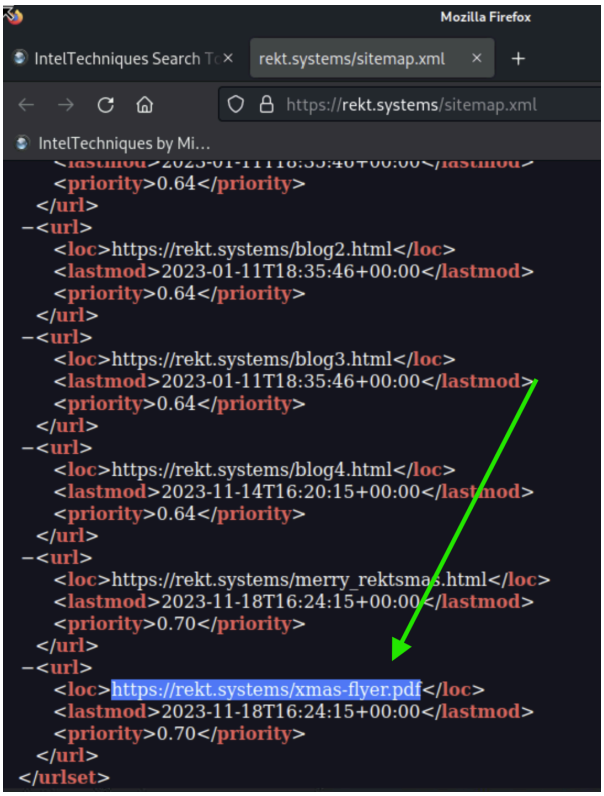
> **Why we collecting URLs ?**
>
> *We're collecting URLs because they tell us what parts of the website exist and what features or functions are available*
>
> .
>
> **JavaScript files often contain hidden URLs or API endpoints.**

---

8. Exploring the XML sitemap, which is used to expose a website's structure to search engines

> **HTML sitemap is for users; XML sitemap is for robots.**

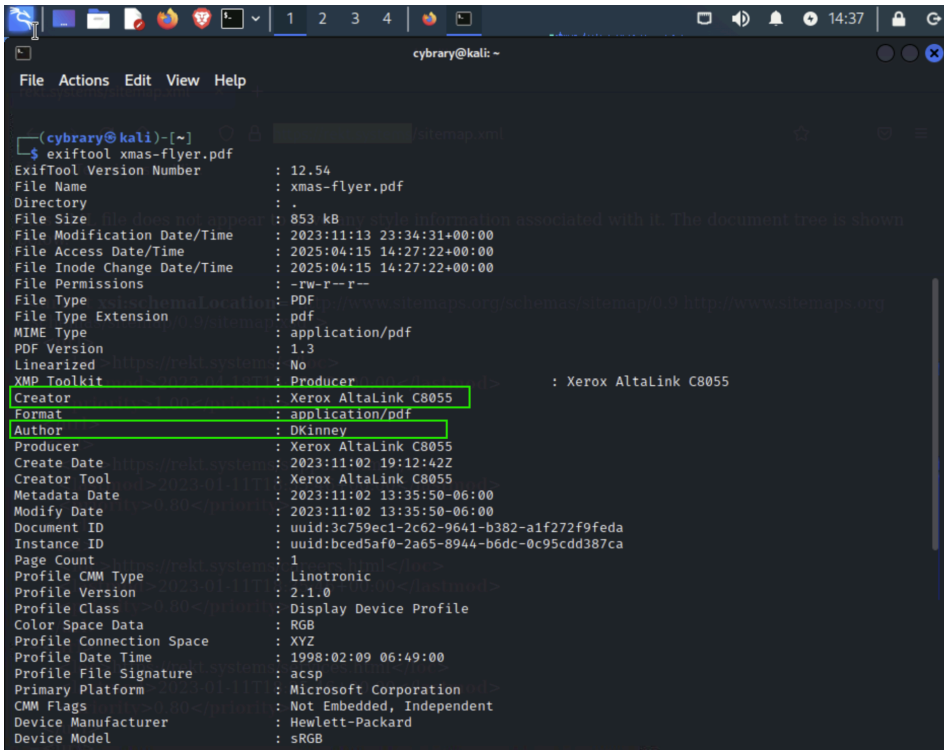
> **Search engines provide search operators that you can use to filter your results**
>
> Ex - site:example.com , filetype:pdf , inurl:login



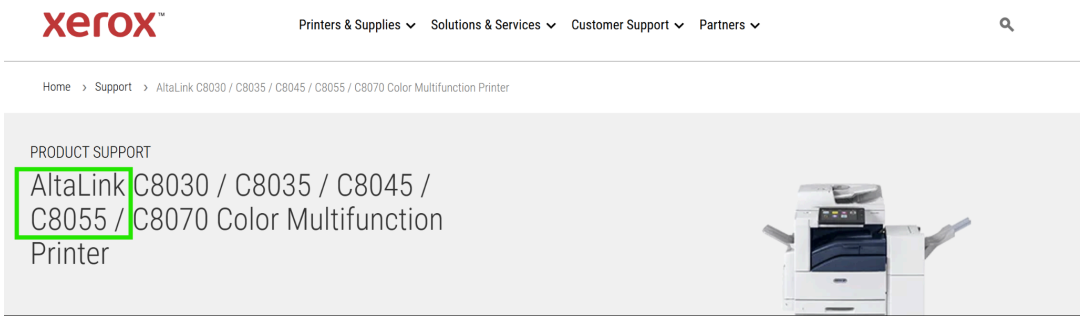
Part 2 - Explore metadata

1. **New Xmas-flyer PDF** found. Files can have metadata that reveals information about the company and its infrastructure, such as author names, GPS coordinates, software, and hardware information.

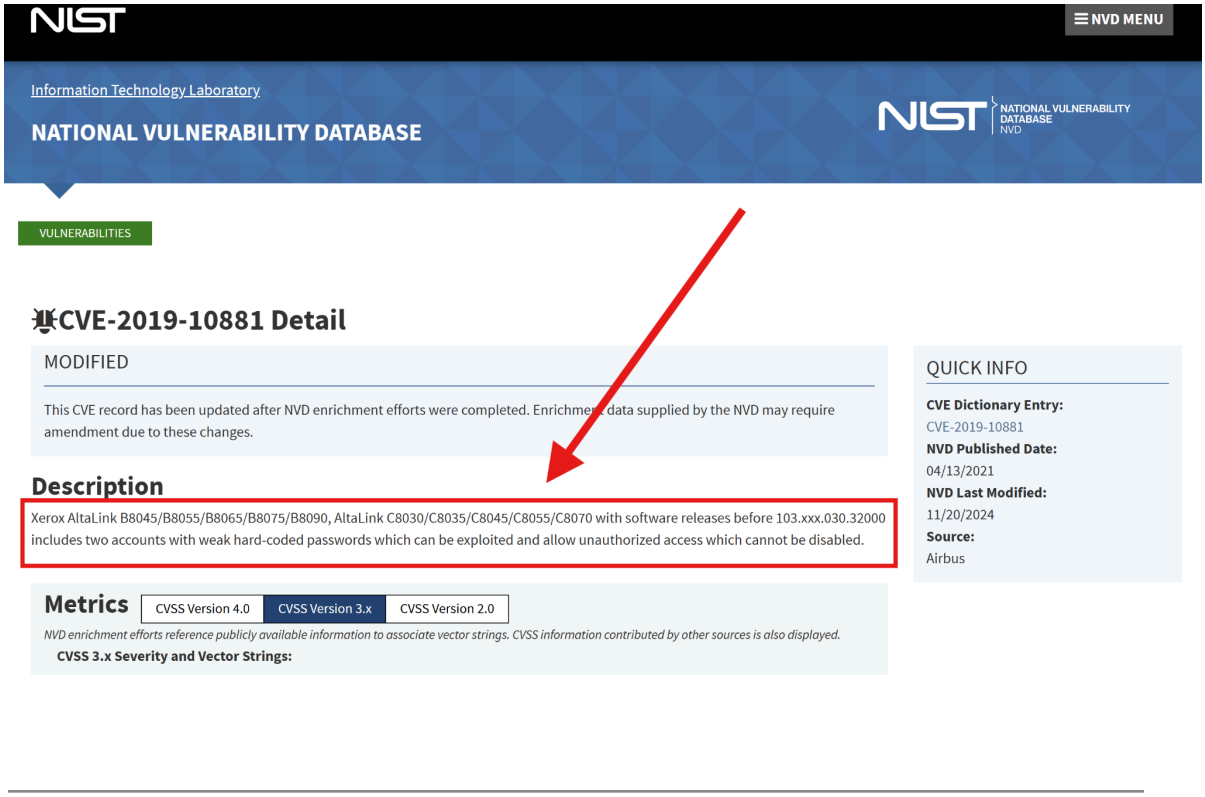
   Lets Explore PDF s metadata using **Exiftool**



Metadata discloses Creator as the printer-scanner device used to produce this PDF as **Xerox AltaLink C8055** and the Author of the PDF as **Dkinney**



2. Looking for vulnerabilities related to the **Xerox device**



Summary

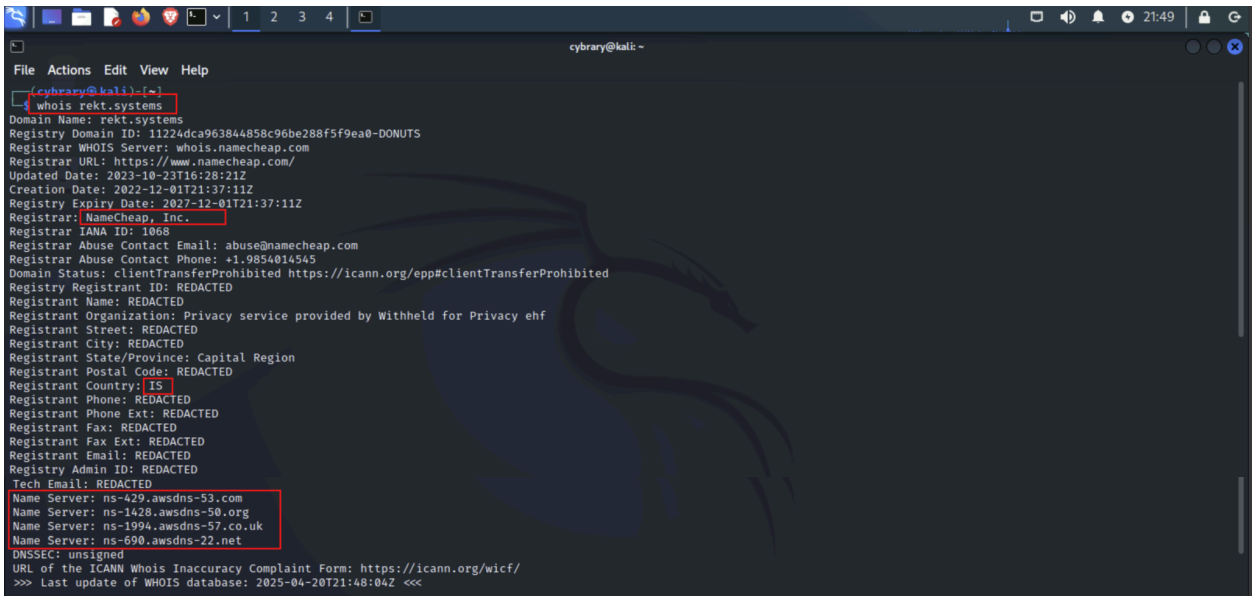
Security vulnerability in the Rekt system's Xerox AltaLink printers with outdated software have built-in accounts with weak, unchangeable passwords that allow unauthorized access.

Part 2 - Extracting data from domain Certificates and WHOIS services

1. **From WHOIS**

   This will show who owns the domain, which domain registrar they are using, and sometimes their name and contact information, depending on their privacy settings.

   The client's privacy settings prevent us from seeing any contact information, but we *can* see the target's domain registrar ,and the name servers they're using and some tools even provide historical WHOIS records



   *"**Redacted**" means some details are hidden from public view primarily due to regulatory compliances*

   Domain Registrar - NameCheap
   Registar Country - IS(Iceland)

2. **From Certificate Transparency Log**

   Find certificates registered for subdomains of *rekt.systems.

   We found some more additional subdomains for active recon.