

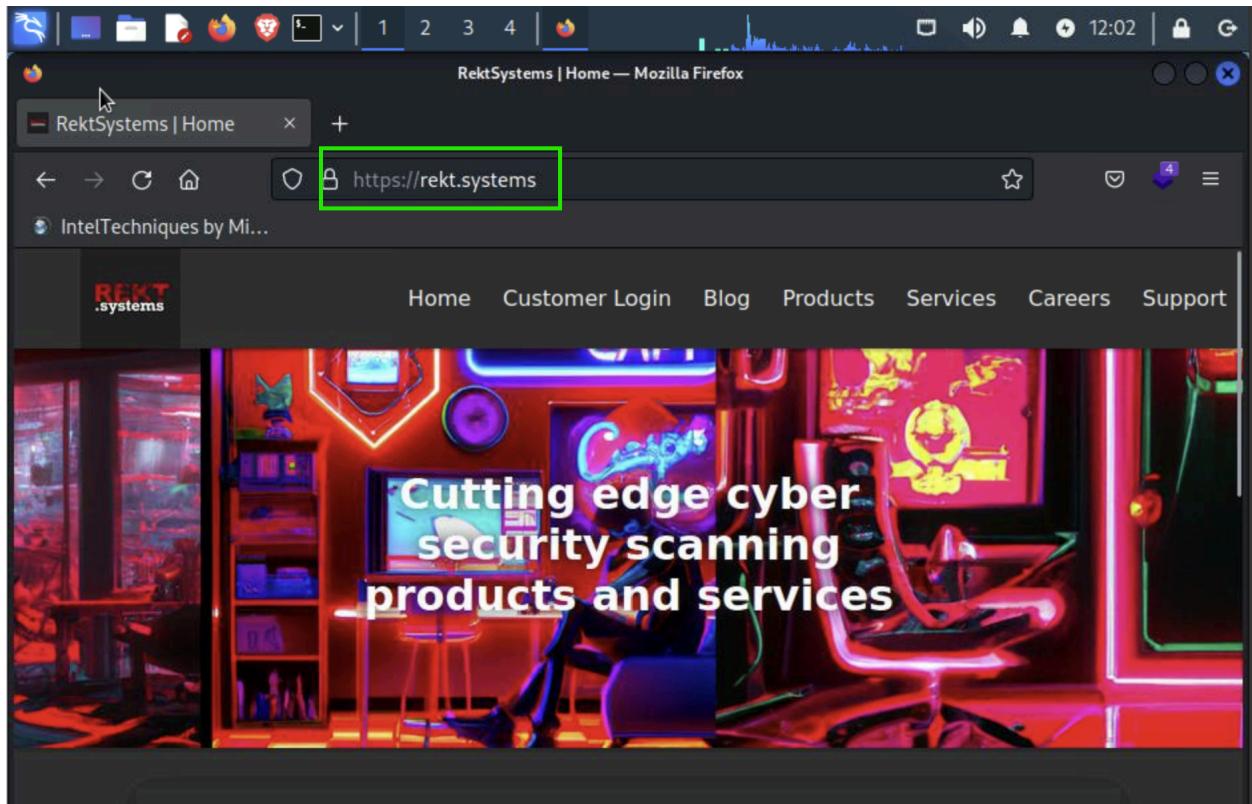
Listing the website urls | xml site map | exploring website's images,pdf etc for metadata (about device used,user,infrastructure of the website company)|Found a printer vulnerability(infrastructure)|| Search vulnerability in the NVD

## Exploring Company vulnerability using websites | OSINT

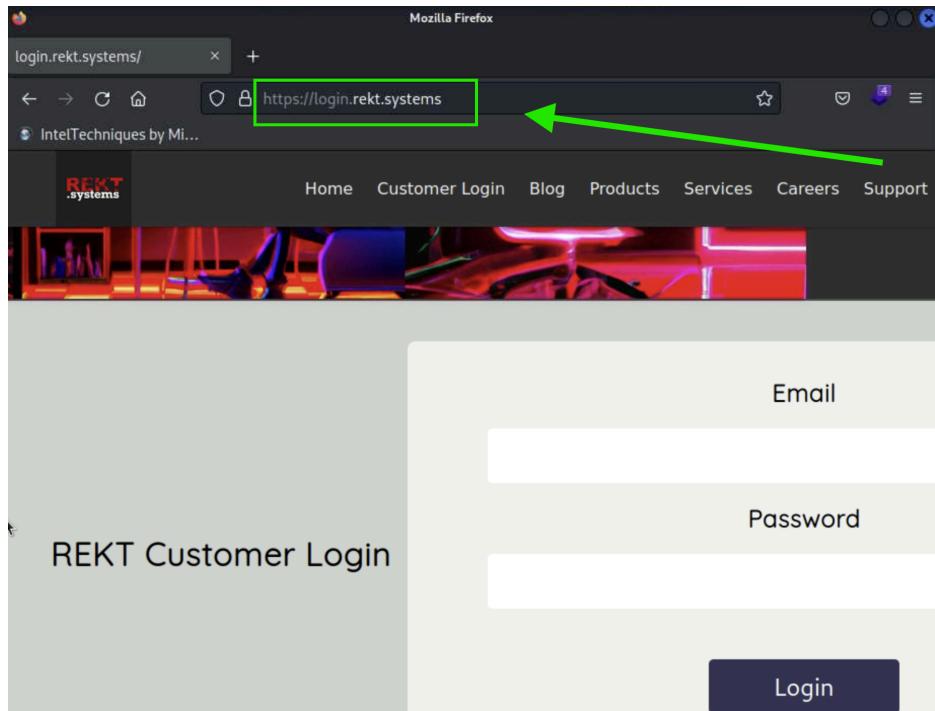
Our target is Rekt Systems, a cybersecurity company with a web presence at [rekt.systems](https://rekt.systems).

---

### 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

A screenshot of a Mozilla Firefox browser window showing a job listing for a "Software Engineer" on the website "Rekt Systems". The URL in the address bar is "https://rekt.systems/software-engineer.html".

The job description includes:

- Experience migrating legacy systems into modern cloud infrastructures.
- Proficiency with PHP, Windows XP, Jenkins, Amazon Web Services, phpMyAdmin (version 4.8.1 experience preferred)

Responsibilities:

- sets product requirements
- coding standards and best
- peers on projects
- experienced engineers
- existing databases

Requirements:

- Minimum of 5 years experience as a Software Engineer or equivalent experience in programming or a related field such as computer science or electrical engineering.
- Excellent understanding of object oriented programming principles such as encapsulation, inheritance, polymorphism, data abstraction, and interfaces

A green box highlights the first two bullet points under "Responsibilities". A green arrow points from the text "Experience migrating legacy systems into modern cloud infrastructures." in the job description to this highlighted box.

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

The screenshot shows a terminal window on a Kali Linux system. The user has run the command `onehistory backup`, which has generated a file named `onehistory-2025-04-15.csv`. This file is then listed in the current directory. A green arrow points from the terminal output to the file in the file manager, indicating they are the same.

```
(cybrary㉿kali)-[~]
$ onehistory backup
(cybrary㉿kali)-[~]
$ onehistory export
(cybrary㉿kali)-[~]
$ ls
Desktop  Music   Templates  gf  onehistory.db  thinclient_drives
Documents Pictures Videos   go  rekt-systems  waymore
Downloads Public   ctfr      onehistory-2025-04-15.csv
(cybrary㉿kali)-[~]
$
```

#### 4. Captured browser history

The screenshot shows a terminal window displaying the contents of the `onehistory-2025-04-15.csv` file. The output is a list of browser visits, each row containing time, title, URL, and visit type. A large green box highlights the entire output of the `cat` command.

```
(cybrary㉿kali)-[~]
$ cat onehistory-2025-04-15.csv
time,title,url,visit_type
2023-11-30 20:53:34,YOU ROCK!,http://rekt.systems/thescanner-tng/?invite_token=sdf9g87,0
2023-11-30 20:53:34,YOU ROCK!,https://rekt.systems/thescanner-tng/?invite_token=sdf9g87,0
2023-11-30 20:53:35,YOU ROCK!,https://rekt.systems/thescanner-tng/sdf9g87_welcome.html,0
2025-04-15 12:01:51,Kali Linux,file:///usr/share/kali-defaults/web/homepage.html,0
2025-04-15 12:02:20,,http://rekt.systems/,0
2025-04-15 12:02:20,RektSystems | Home,https://rekt.systems/,0
2025-04-15 12:04:07,,http://login.rekt.systems/,0
2025-04-15 12:04:07,,https://login.rekt.systems/,0
2025-04-15 12:08:34,,http://rekt.systems/careers.html,0
2025-04-15 12:08:34,RektSystems | Careers,https://rekt.systems/careers.html,0
2025-04-15 12:08:49,RektSystems | Careers,https://rekt.systems/software-engineer.html,0
2025-04-15 12:19:11,RektSystems | Home,https://rekt.systems/index.html,0
2025-04-15 12:19:13,,http://login.rekt.systems/,0
2025-04-15 12:19:13,,https://login.rekt.systems/,0
2025-04-15 12:19:16,,http://rekt.systems/blog.html,0
2025-04-15 12:19:16,,https://rekt.systems/blog.html,0
```

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.

The screenshot shows a terminal window where the user has used the `gf` command to search for URLs in the `onehistory-2025-04-15.csv` file and then passed the results to `anew > url.lst` to create a new file named `url.lst`. The file contains the URLs found in the CSV file.

```
(cybrary㉿kali)-[~]
$ gf urls onehistory-2025-04-15.csv | anew > url.lst
(cybrary㉿kali)-[~]
$ cat url.lst
http://rekt.systems
https://rekt.systems
http://login.rekt.systems
https://login.rekt.systems
```

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

```
(cybary@kali)-[~]
$ getJS --input url.lst --complete | xargs wget
--2025-04-15 12:40:31-- http://login.rekt.systems/main.js
Resolving login.rekt.systems (login.rekt.systems) ... 108.138.64.10, 108.138.64.72, 108.138.64.4, ...
Connecting to login.rekt.systems (login.rekt.systems)|108.138.64.10|:80 ... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://login.rekt.systems/main.js [following]
--2025-04-15 12:40:31-- https://login.rekt.systems/main.js
Connecting to login.rekt.systems (login.rekt.systems)|108.138.64.10|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 567 [application/javascript]
Saving to: 'main.js'

main.js          100%[=====]      567  --.-KB/s   in 0s

2025-04-15 12:40:31 (20.7 MB/s) - 'main.js' saved [567/567]
[1]
--2025-04-15 12:40:31-- https://login.rekt.systems/main.js
Reusing existing connection to login.rekt.systems:443.
HTTP request sent, awaiting response... 200 OK
Length: 567 [application/javascript]
Saving to: 'main.js.1'

main.js.1        100%[=====]      567  --.-KB/s   in 0s

2025-04-15 12:40:31 (13.1 MB/s) - 'main.js.1' saved [567/567]

FINISHED --2025-04-15 12:40:31--
Total wall clock time: 0.1s
Downloaded: 2 files, 1.1K in 0s (16.0 MB/s)
```

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

```

Mozilla Firefox
IntelTechniques Search T rekt.systems/sitemap.xml +
https://rekt.systems/sitemap.xml
IntelTechniques by Mi...
<url>
  <loc>https://rekt.systems/blog2.html</loc>
  <lastmod>2023-01-11T18:35:46+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>https://rekt.systems/blog3.html</loc>
  <lastmod>2023-01-11T18:35:46+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>https://rekt.systems/blog4.html</loc>
  <lastmod>2023-11-14T16:20:15+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>https://rekt.systems/merry_rektsmas.html</loc>
  <lastmod>2023-11-18T16:24:15+00:00</lastmod>
  <priority>0.70</priority>
</url>
<url>
  <loc>https://rekt.systems/xmas-flyer.pdf</loc>
  <lastmod>2023-11-18T16:24:15+00:00</lastmod>
  <priority>0.70</priority>
</url>
</urlset>

```

## 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**

```

cybrary@kali: ~
File Actions Edit View Help
testsystems/sitemap.xml + 14:37
File Name : xmas-flyer.pdf
Directory : .
File Size : 853 kB
File Modification Date/Time : 2023:11:13 23:34:31+00:00
File Access Date/Time : 2025:04:15 14:27:22+00:00
File Inode Change Date/Time : 2025:04:15 14:27:22+00:00
File Permissions : -rw-r--r--
File Type : PDF
File Type Extension : 0.9/sitemap
MIME Type : application/pdf
PDF Version : 1.3
Linearized : No
XMP Toolkit : https://rekt.systems
Producer : Xerox AltaLink C8055
Creator : Xerox AltaLink C8055
Format : application/pdf
Author : DKinney
Page Count : 1
Profile CMM Type : Linotronic
Profile Version : 2.1.0
Profile Class : Display Device Profile
Color Space Data : RGB
Profile Connection Space : XYZ
Profile Date Time : 1998:02:09 06:49:00
Profile File Signature : acsp
Primary Platform : Microsoft Corporation
CMM Flags : Not Embedded, Independent
Device Manufacturer : Hewlett-Packard
Device Model : sRGB

```

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**

The screenshot shows the Xerox website's product support page. At the top, there is a navigation bar with links for Printers & Supplies, Solutions & Services, Customer Support, and Partners. Below the navigation is a search bar. The main content area is titled "PRODUCT SUPPORT" and features a large image of a white Xerox AltaLink multifunction printer. To the left of the printer, the text "AltaLink C8030 / C8035 / C8045 / C8055 / C8070 Color Multifunction Printer" is displayed, with the model numbers highlighted by a green rectangular box.

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

The screenshot shows the NIST National Vulnerability Database (NVD) page for CVE-2019-10881. The page has a dark blue header with the NIST logo and "NATIONAL VULNERABILITY DATABASE". Below the header, there is a green button labeled "VULNERABILITIES". The main content area is titled "CVE-2019-10881 Detail". It includes sections for "MODIFIED" (with a note about enrichment), "Description" (which is highlighted with a red box and contains a red arrow pointing to it), "Metrics" (with options for CVSS Version 4.0, 3.x, and 2.0), and "QUICK INFO" (listing the CVE dictionary entry, published date, last modified date, and source). A red arrow points from the "Description" section to the "Description" text in the screenshot below.

## 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

```
cybrary@kali:~$ whois rekt.systems
Domain Name: rekt.systems
Registry Domain ID: 11224dc9a963844858c96be288f5f9ea0-DONUTS
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://www.namecheap.com/
Updated Date: 2023-10-23T16:28:21Z
Creation Date: 2022-12-01T21:37:11Z
Registry Expiry Date: 2027-12-01T21:37:11Z
Registrar: Namecheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: Capital Region
Registrant Postal Code: REDACTED
Registrant Country: IS
Registrant Phone: REDACTED
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED
Registrant Email: REDACTED
Registry Admin ID: REDACTED
Tech Email: REDACTED
Name Server: ns-429.awsdns-53.com
Name Server: ns-1428.awsdns-50.org
Name Server: ns-1994.awsdns-57.co.uk
Name Server: ns-690.awsdns-22.net
DNSSEC: unsigned
>>> Last update of WHOIS database: 2025-04-20T21:48:04Z <<
```

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

Domain Registrar - NameCheap  
Registrar Country - IS(Iceland)

### 2. From Certificate Transparency Log

Find certificates registered for subdomains of \*rekt.systems.

```
cybrary@kali:~$ ctfr -d rekt.systems
[!] —— TARGET: rekt.systems [!]
[-] *.rekt.systems
rekt.systems
[-] jira.rekt.systems
[-] login.rekt.systems
[-] vpn.rekt.systems
[!] Done. Have a nice day! ;).
```

We found some more additional subdomains for active recon.

