

Cant_Even_Unplug_It (Intro/Recon/Web)(102 pts)

By: Not_C0ps

The challenge says they created a website at the *military-grade-secrets.dev* subdomain, then they changed their website name before their boss finally took the website offline.

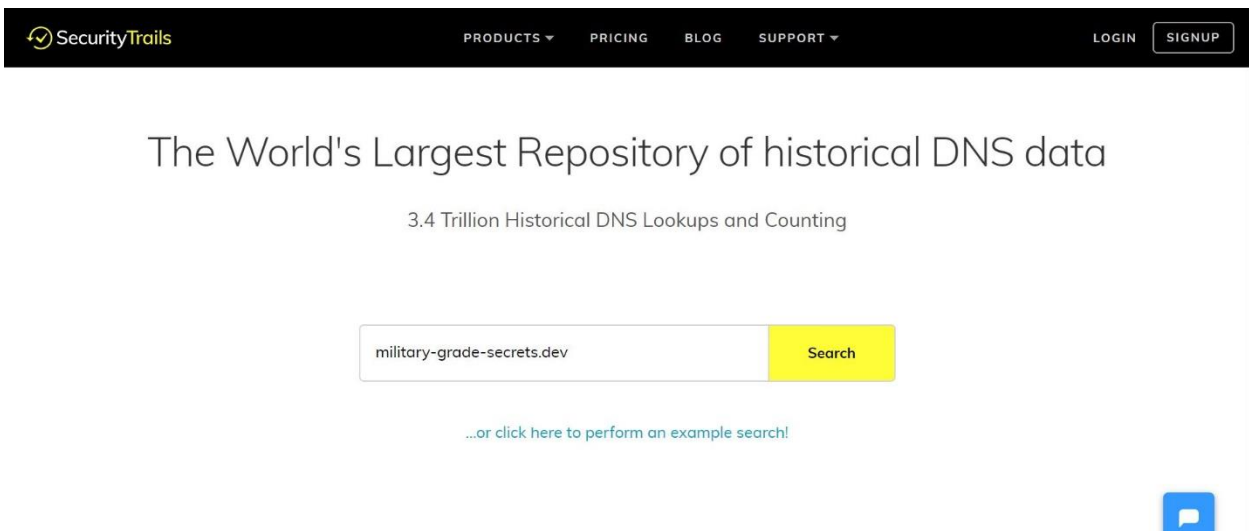
Hints:

These are HTTPS sites. Who is publicly and transparently logging the info you need?

Just in case: all info is freely accessible; no subscriptions are necessary. The names cannot really be guessed.

Where to begin... Well we start off by knowing that all domain names and name changes are routed through and tracked by DNS (Domain Name System). Using nslookup (on powershell or cmd) *military-grade-secrets.dev* doesn't return us any useful information. So, I found a website which gives historical DNS data for a given domain.

<https://securitytrails.com/dns-trails>



The screenshot shows the SecurityTrails website interface. At the top is a black navigation bar with the SecurityTrails logo on the left and links for PRODUCTS, PRICING, BLOG, and SUPPORT in the center. On the right of the bar are LOGIN and SIGNUP buttons. Below the navigation bar, the main heading reads "The World's Largest Repository of historical DNS data" in a large, dark font. Underneath this heading is a subtitle: "3.4 Trillion Historical DNS Lookups and Counting". In the center of the page is a search form consisting of a white input field and a yellow "Search" button. The input field contains the text "military-grade-secrets.dev". Below the search form, there is a link that says "...or click here to perform an example search!". In the bottom right corner of the page, there is a blue square button with a white speech bubble icon.

So, let's see what we can find about the domain we are given.

DNS Records

Historical Data

Subdomains 4

APEX_DOMAIN RECORDS military-grade-secrets.dev

Filter by keyword ... Filter Clear Filter

View by Hosting

1 - 4 of 4 results

#	Domain	Alexa Rank	Hosting Provider	Mail Provider
1	military-grade-secrets.dev	-	-	-
2	www.military-grade-secrets.dev	-	-	-
3	secret-storage.military-grade-secrets.dev	-	Google LLC	-
4	now.under.even-more-militarygrade.pw.military-grade-secrets.dev	-	Google LLC	-

Nothing to note in the DNS Records or Historical Data section, but we have found 4 subdomains. The most important ones are the bottom two. Let's check if either of these domains lead us to a website. Unfortunately, in both cases we get the same result.



This site can't be reached

forget-me-not.even-more-militarygrade.pw took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

Details

So, we don't find a website, but we do find out that both those domains are aliases for another domain, *forget-me-not.even-more-militarygrade.pw*.

Running this domain through the historical data tool we find:

The screenshot shows a web interface for DNS Records. On the left is a sidebar with 'DNS Records', 'Historical Data', and 'Subdomains' (with a green badge showing '3'). The main area is titled 'APEX_DOMAIN RECORDS' and shows the domain 'forget-me-not.even-more-militarygrade.pw'. Below this is a search bar with 'Filter by keyword ...' and buttons for 'Filter' and 'Clear Filter'. A 'View by' dropdown is set to 'Hosting'. The results show '1 - 3 of 3 results' in a table:

#	Domain	Alexa Rank	Hosting Provider	Mail Provider
1	www.even-more-militarygrade.pw	-	-	-
2	forget-me-not.even-more-militarygrade.pw	-	DigitalOcean, LLC	-
3	even-more-militarygrade.pw	-	-	-

At the bottom left is a 'Give Us Feedback' link, and at the bottom right is a blue chat bubble icon.

This is even better! This means this domain *forget-me-not.even-more-militarygrade.pw* was once run on Digital Ocean (A service that hosts VMs for people). We can logically conclude then, that this domain once held the website we want to look at. The best place to find information on archived websites is the Way Back Machine (<https://archive.org/web/>).

The screenshot shows the Internet Archive WayBack Machine interface. At the top, it says 'INTERNET ARCHIVE' and 'Explore more than 357 billion web pages saved over time'. There is a 'DONATE' button and the 'WayBackMachine' logo. A search bar contains the domain 'forget-me-not.even-more-militarygrade.pw'. Below the search bar are links for 'Calendar', 'Collections' (with a 'beta' badge), 'Summary', and 'Site Map'. It states 'Saved 6 times between March 9, 2019 and April 27, 2019.' At the bottom is a timeline grid with 16 empty slots.

Checking the most recent snapshot on April 27, 2019:

Congrats!

**THE FLAG IS:
OOO{DAMNATIO_MEMORIAE}**

Thank you for playing, and enjoy the rest of the CTF!

OOO{DAMNATIO_MEMORIAE}

And there we have it, the flag is ooo{DAMNATIO_MEMORIAE}

It is important to note that using the two domains (*secret-storage.military-grade-secrets.dev* or *now.under.even-more-militarygrade.pw.military-grade-secrets.dev*) that aliased *forget-me-not.even-more-militarygrade.pw* in the Way Back Machine would redirect us to the same page seen in the previous Way Back search result picture. A straightforward challenge, but time consuming and interesting none the less. Until next time, thanks for reading!