CERT.PL
NASK

How CERT PL finds vulnerabilities in our constituency at a scale: an update on the Artemis project

Krzysztof Zając

cert.pl

Purpose

After an incident, let's make sure it won't occur in other entities.

Example:

- exposed .git on an university website caused API key leak and unauthorized data access
- let's check whether other entities have exposed .git folders!

What do we check?

A couple dozen modules

- Subdomain enumeration (from various data sources)
- Domain expiration check
- Bad DNS configuration check:
  - Zone transfer
  - Subdomain takeover
- SPF/DMARC
- Bad/expired TLS certificates, https:// redirect

A couple dozen modules

- Port scanning
- WordPress, WordPress plugin, Drupal, and Joomla version check
- Closed WordPress plugins
- Nuclei support: thousands of vulnerabilities and misconfigurations
- SQLi and XSS

A couple dozen modules

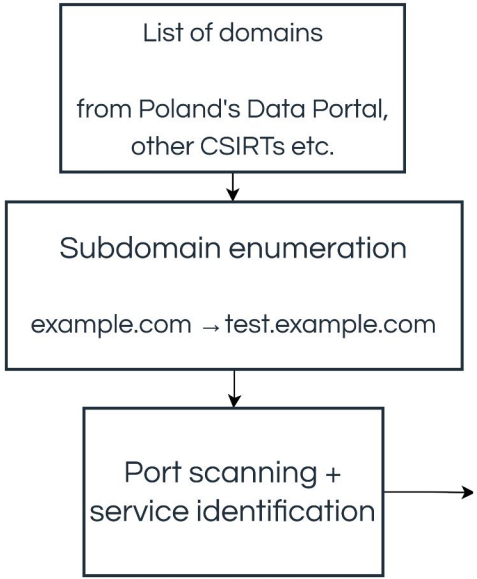
- Scripts loaded from nonexistent domains
- Directory index
- Weak passwords
- Exposed Git/SVN repositories
- Exposed login panels (RDP, phpMyAdmin, …)
- Accidentally published files (eg. SQL dumps, backups or wp-config.php.bak)
- …

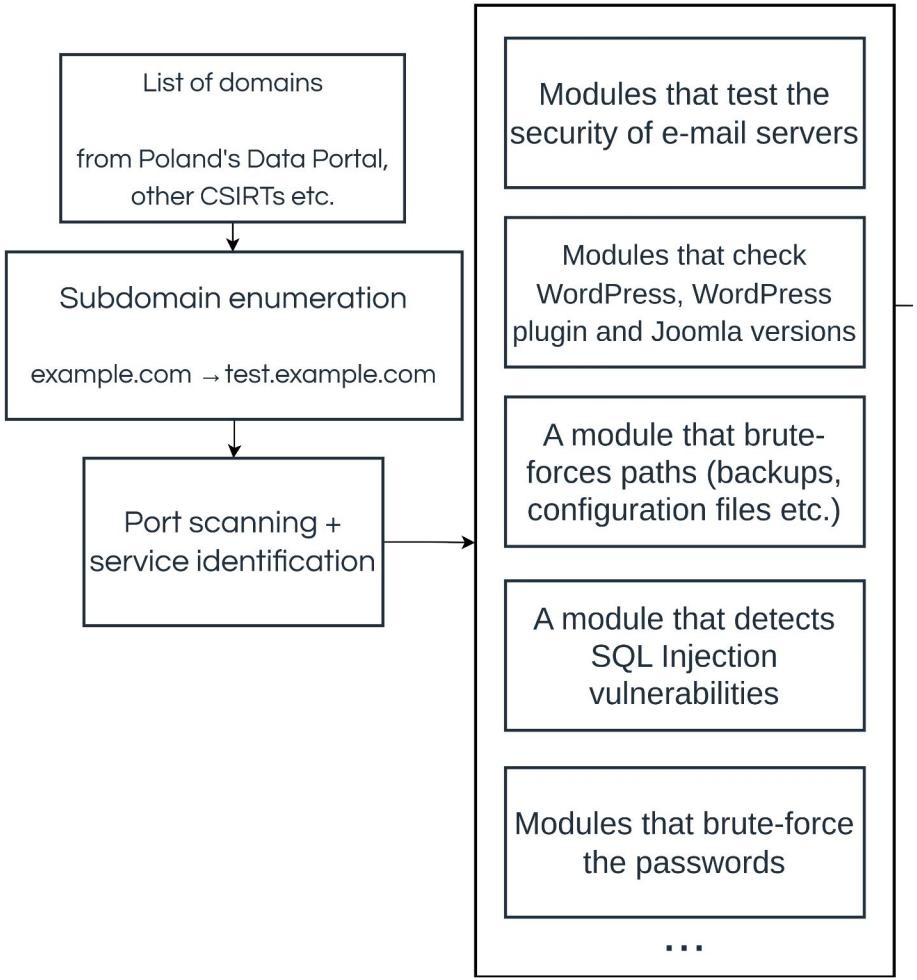
A couple dozen modules

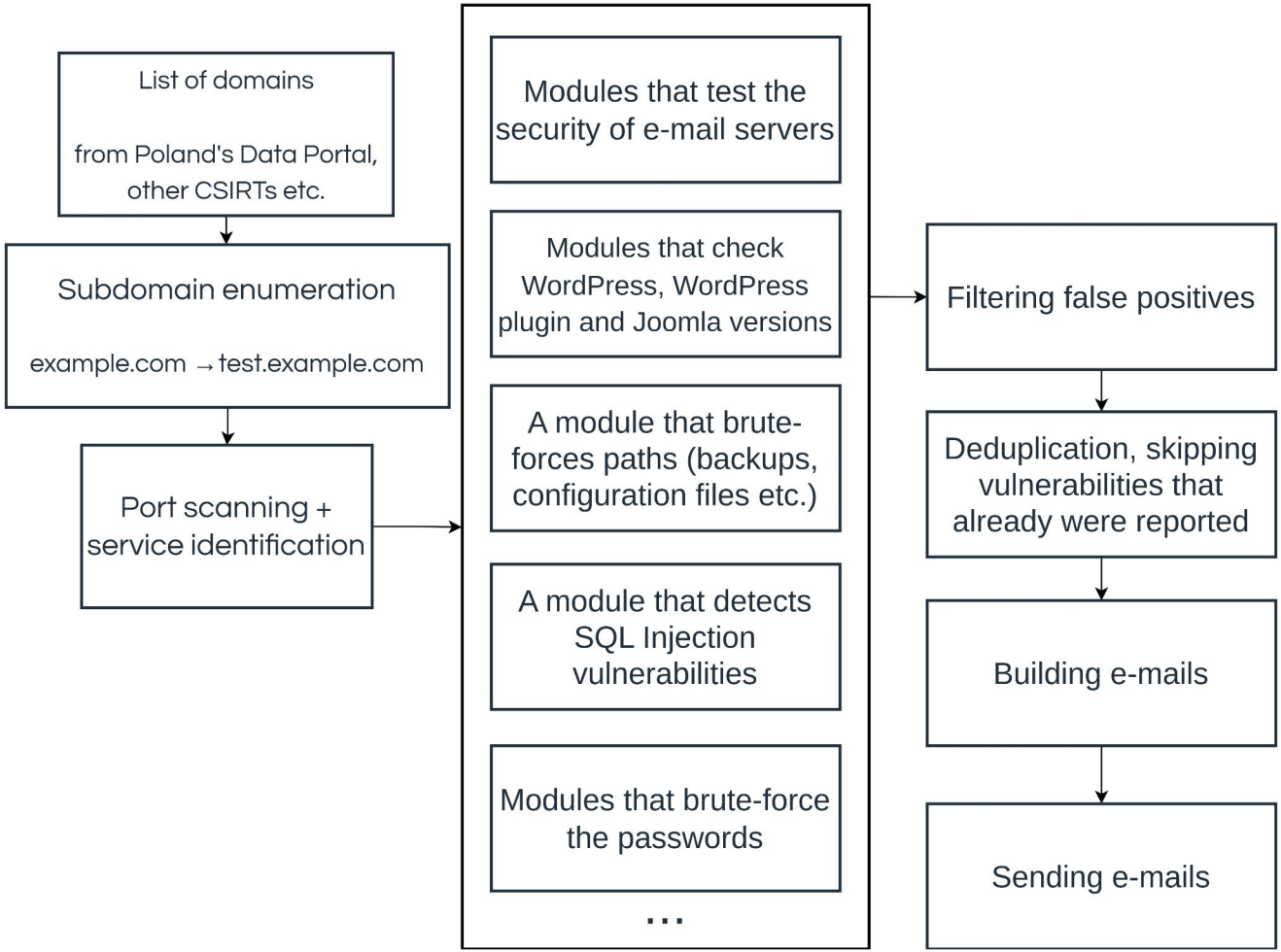
If you have an idea for a new module (e.g. because you detect a type of attacks in your constituency), you can:

- Submit it to: **artemis@cert.pl**

- Implement it yourself: **https://github.com/CERT-Polska/Artemis**


List of domains
from Poland's Data Portal, other CSIRTs etc.
Subdomain enumeration
example.com → test.example.com
Port scanning + service identification


List of domains
from Poland's Data Portal, other CSIRTs etc.
Subdomain enumeration
example.com → test.example.com
Port scanning + service identification
Modules that test the security of e-mail servers
Modules that check WordPress, WordPress plugin and Joomla versions
A module that brute-forces paths (backups, configuration files etc.)
A module that detects SQL Injection vulnerabilities
Modules that brute-force the passwords
...


List of domains
from Poland's Data Portal, other CSIRTs etc.
Subdomain enumeration
example.com → test.example.com
Port scanning + service identification
Modules that test the security of e-mail servers
Modules that check WordPress, WordPress plugin and Joomla versions
A module that brute-forces paths (backups, configuration files etc.)
A module that detects SQL Injection vulnerabilities
Modules that brute-force the passwords
...
Filtering false positives
Deduplication, skipping vulnerabilities that already were reported
Building e-mails
Sending e-mails

Example e-mail

The following addresses contain version control system data:

- https://[redacted]:443/.git/

Making a code repository public may allow an attacker to learn the inner workings of a system, and if it contains passwords or API keys - also gain unautorized access. Such data shouldn't be publicly available.

Example e-mail

The following addresses contain old Joomla versions:

- https://[redacted]:443 - Joomla 2.5.4

If a site is no longer used, we recommend shutting it down to eliminate the risk of exploitation of known vulnerabilities in older Joomla versions. Otherwise, we recommend regular Joomla core and plugin updates.

Example e-mail

The following domains don't have properly configured e-mail sender verification mechanisms:

- [redacted].pl: Valid DMARC record not found. We recommend using all three mechanisms: SPF, DKIM and DMARC to decrease the possibility of successful e-mail message spoofing.

These mechanisms greatly increase the chance that the recipient server will reject a spoofed message. (...)

Example e-mail

Such reports are sent by CERT PL to scanned entities.

What changed since 69th TF-CSIRT in 2023

- More modules
- **2x more** scanned groups of entities
- We find vulnerabilities in serious entities: **banks, gov.pl**
- We collaborate with **external contributors**
- We got accepted to **Google Summer of Code**
- We have external users, including other CSIRTs (Polish and foreign)

Who do we scan now?

Scanned entities

- All gov.pl domains
- Local government entities
- Municipal corporations: water management, waste collection, …
- Key Service Operators

Scanned entities

- Banks
- Universities, schools, preschools and other educational entities
- Professional self-governments (e.g. medical chambers)
- Hospitals

Scanned entities

- Local and country-level newspapers, TVs, information portals etc.
- Websites of politicians, political parties, candidates etc. (e.g. currently: European Parliament election candidates)
- Lists of domains provided by other CSIRTs, ministries etc.
- Domains provided voluntarily by companies

Results

Scanning

We've been scanning the websites since **January 2023**.

We are periodically scanning ~**66k domains and IP addresses** and ~**420k** subdomains (~2x times more than a year ago).

Every domain is scanned a couple times a year.

Communication

- We already sent **64k e-mails**.
- If an entity doesn't fix a serious issue, **we call them**. We already made >**4k** such calls.
- Reactions are mostly positive (but we sometimes receive bug reports).
- Important: sometimes our e-mail **gives "political" support to the admins** even if they know about a problem.

Scanning

Since January 2023 we reported ~**264k** vulnerabilities and misconfigurations (**2x more** than a year ago), including:

- ~**17.5k** high-severity
- ~**169k** medium-severity
- ~**77.5k** low-severity.

Reported issues since Jan 2023

~135.7k obsolete Joomla, Drupal, WordPress or WordPress plugin versions

~51.4k SSL/TLS misconfigurations

~33.8k SPF/DMARC misconfigurations

~19.3k exposed login panels, RDPs etc.

~13.8k information leaks: AXFR, directory listing, phpinfo(), etc.

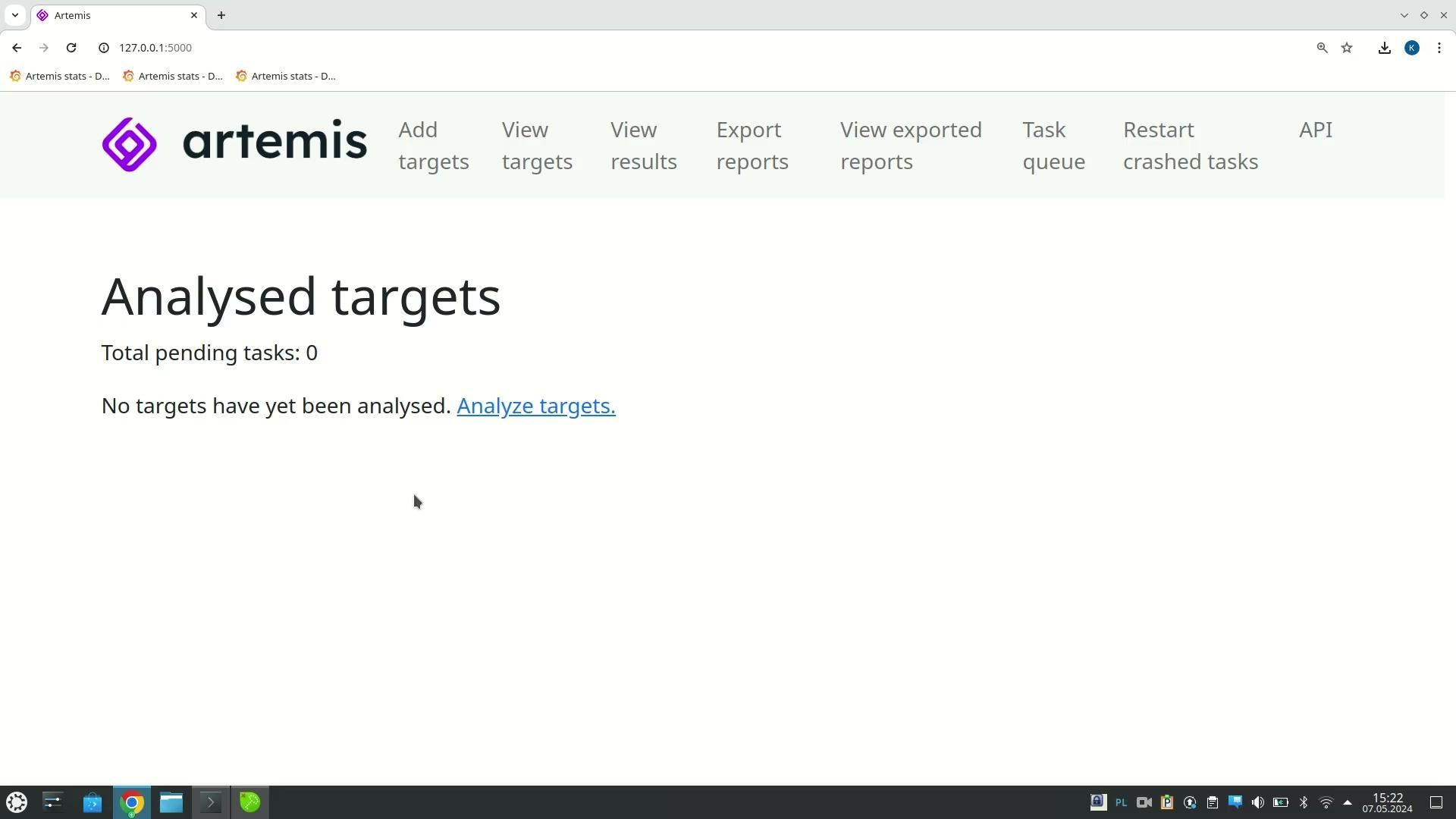
~5.6k high/critical vulnerabilities from Nuclei or sqlmap

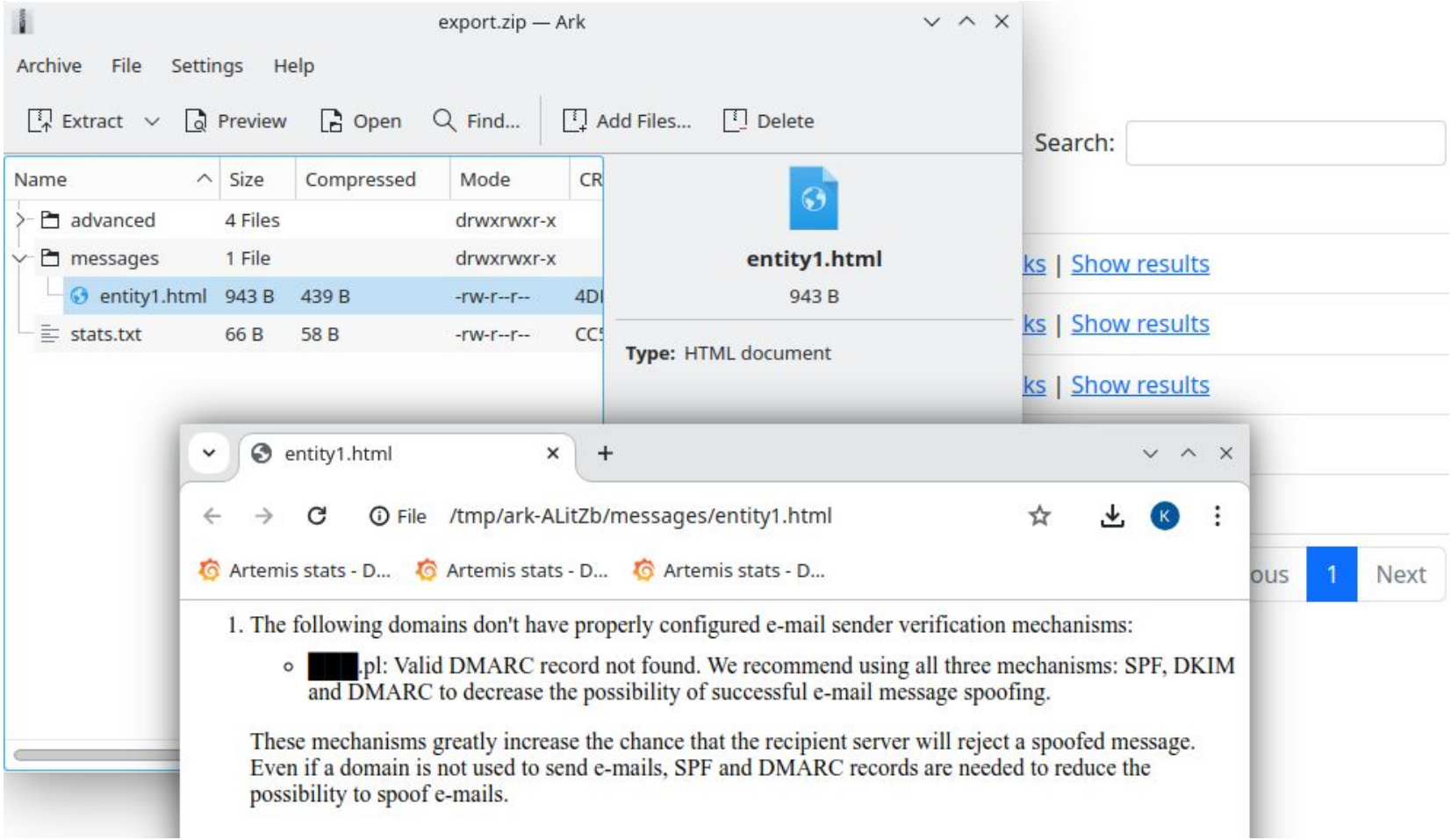
~4.3k exposed backups, source code, database dumps or logs

Demo

Demo

- I added domains+ports to scan so that we can skip port scanning
- To make the process faster:
  - I spawned some Artemis modules in 10 instances
  - I only run the WordPress version check


Artemis
127.0.0.1:5000
Artemis stats - D...
Artemis stats - D...
Artemis stats - D...
artemis
Add targets
View targets
View results
Export reports
View exported reports
Task queue
Restart crashed tasks
API
Analysed targets
Total pending tasks: 0
No targets have yet been analysed. Analyze targets.
PL
15:22
07.05.2024


export.zip — Ark
Archive File Settings Help
Extract Preview Open Find... Add Files... Delete
Name Size Compressed Mode CR
advanced 4 Files drwxrwxr-x
messages 1 File drwxrwxr-x
entity1.html 943 B 439 B -rw-r--r-- 4DI
stats.txt 66 B 58 B -rw-r--r-- CC
entity1.html
943 B
Type: HTML document
Search:
ks | Show results
ks | Show results
ks | Show results
ous 1 Next
entity1.html
File /tmp/ark-ALitZb/messages/entity1.html
Artemis stats - D...
Artemis stats - D...
Artemis stats - D...
1. The following domains don't have properly configured e-mail sender verification mechanisms:
[redacted].pl: Valid DMARC record not found. We recommend using all three mechanisms: SPF, DKIM and DMARC to decrease the possibility of successful e-mail message spoofing.
These mechanisms greatly increase the chance that the recipient server will reject a spoofed message. Even if a domain is not used to send e-mails, SPF and DMARC records are needed to reduce the possibility to spoof e-mails.

Demo

The exported zip package is then processed by a contact management and e-mail sending system.

Conclusions

Conclusions

- There are still low-hanging vulnerabilities.
- Iterative development contributed to the project success.
- The role of the ecosystem (example: WordPress plugins).
- The role of education: not fixing SQL Injection by banning `union`.

How to start

- Start small!
- Download Artemis (and https://github.com/CERT-Polska/Artemis-modules-extra)
- Set up Artemis using the quick-start documentation
- Take one list of domains (e.g. one you can get easy approval to scan), e.g. from a data portal

How to start

- (if needed) translate Artemis to your language - we have docs on how to do that and will show it during trainings!
- Scan, send the results.
- Show to the shareholders that the scanning makes sense.
- Iterate: increase scanning coverage.
- Contact artemis@cert.pl in case of any problems.

How to start

CERT PL will be glad to help with setting up your scanning pipeline.

It is easy to start a similar project and improve the security of your constituency!

Artemis trainings

- Both Artemis trainings at this TF-CSIRT meeting are full, but you can sign up for the waitlist for future online Artemis trainings at https://cert.pl/artemis-trainings!
- You will get an email as soon as we gather a group.

Links

https://github.com/CERT-Polska/Artemis

https://github.com/CERT-Polska/Artemis-modules-extra

https://cert.pl/artemis-trainings

artemis@cert.pl

https://discord.com/invite/GfUW4mZmy9

CERT.PL
NASK

Questions?

Appendix 1: scanning time