Jak zostać **pentesterem**?

PODCAST

Jak zostać pentesterem/jak zacząć naukę bezpieczeństwa?

Jak zostać pentesterem/specjalistą bezpieczeństwa? Od czego zacząć naukę? Gdzie szukać materiałów edukacyjnych? Jakie ścieżki kariery istnieją? Czy znajomość programowania jest potrzebna? Czy kursy coś dają?

29-03-2020 20 MINUT

PODCAST

Bezpieczeństwo pracy zdalnej

Na co zwrócić uwagę podczas pracy z domu? Co ustawić i czego się obawiać? Proste porady w przystępnej formie z obszernymi wytłumaczeniami.

20-03-2020 7 MINUT

PODCAST

BadWPAD

Atak BadWPAD, dzięki któremu można podsłuchiwać i modyfikować niezaszyfrowany ruch internetowy na twoim komputerze.

16-03-2020 8 MINUT

UWAGA!

To tylko *slajdy*
Ich omówienie na
blogu lub *YouTube*

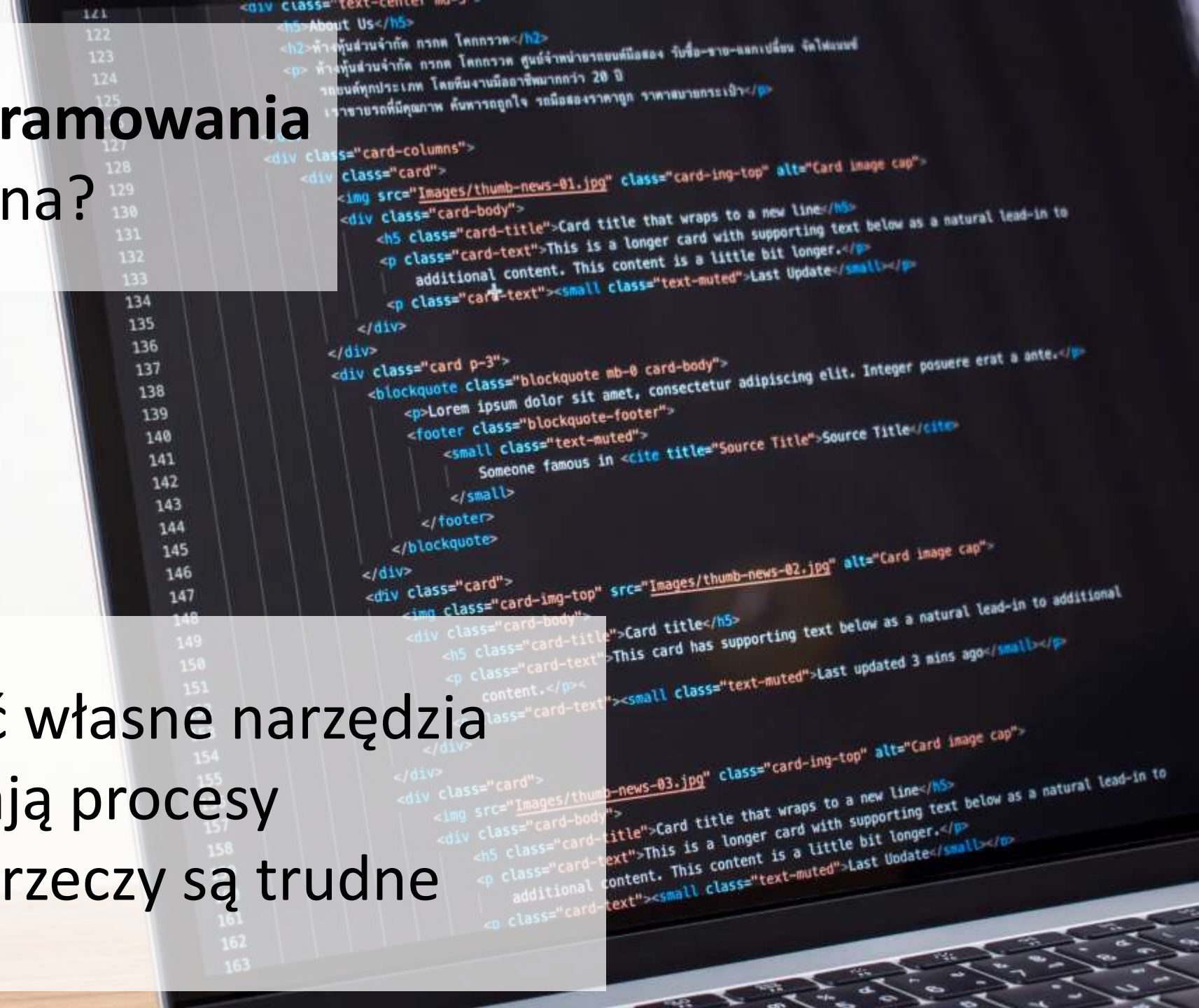
Naucz się **szukać**

manual/instrukcja/google

Czy studia są **konieczne**?

- Czasami w korpo – tak
- To jeden z dłuższych życiowych projektów
- Uczą cierpliwości
- Kontakty/znajomości
- Dobre podstawy

Czy znajomość **programowania** jest potrzebna?



1. Możesz tworzyć własne narzędzia
2. Wiesz jak działają procesy
3. Kojarzysz które rzeczy są trudne

Ścieżki kariery

1. Pentester
2. Red Teaming
3. Analiza malware
4. SOC
5. Threat hunting/intelligence
6. Informatyka śledcza
7. Exploity


PENTEST
kontrolowany
atak
na *system*

PODSTAWY

1. Obsługi Windows/Linux
2. Jak działa sieć
3. Jakiś język programowania
4. Docker/Maszyny wirtualne
5. OWASP TOP 10
6. IDE
7. BURP

TOC Table of Contents

Table of Contents

About OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

At OWASP, you'll find free and open:

- Application security tools and standards.
- Complete books on application security testing, secure code development, and secure code review.
- Presentations and videos.
- Cheat sheets on many common topics.
- Standard security controls and libraries.
- Local chapters worldwide.
- Cutting edge research.
- Extensive conferences worldwide.
- Mailing lists.

Learn more at: https://www.owasp.org.

All OWASP tools, documents, videos, presentations, and chapters are free and open to anyone interested in improving application security.

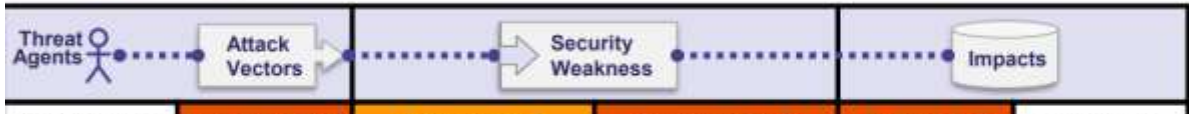
We advocate approaching application security as a people, process, and technology problem, because the most effective approaches to application security require improvements in these areas.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, and cost-effective information about application security.

OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. OWASP produces many types of materials in a collaborative, transparent, and open way.

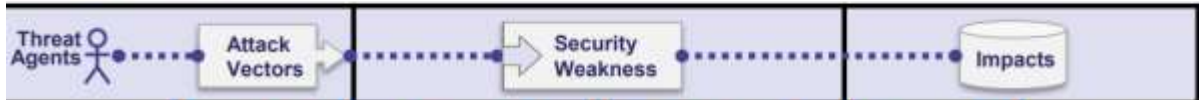
The OWASP Foundation is the non-profit entity that ensures the project's long-term success. Almost everyone associated with OWASP is a volunteer, including the OWASP board, chapter leaders, project leaders, and project members. We support innovative security research with grants and infrastructure.

A1 :2017 Injection



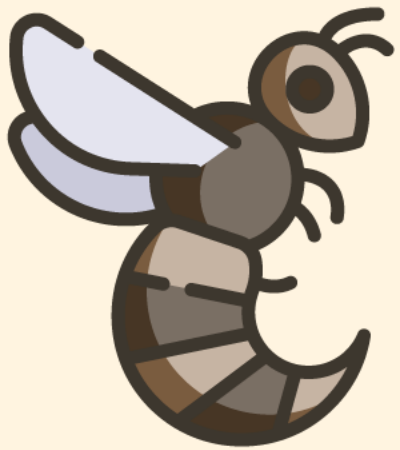
App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 3	Technical: 3	Business ?
Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.		Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.	

A7 :2017 Cross-Site Scripting (XSS)



App. Specific	Exploitability: 3	Prevalence: 3	Detectability: 3	Technical: 2	Business ?
Automated tools can detect and exploit all three forms of XSS, and there are freely available exploitation frameworks.		XSS is the second most prevalent issue in the OWASP Top 10, and is found in around two-thirds of all applications. Automated tools can find some XSS problems automatically, particularly in mature technologies such as PHP, J2EE / JSP, and ASP.NET.		The impact of XSS is moderate for reflected and DOM XSS, and severe for stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.	

https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf



OWASP TOP10

#1 INJECTION

https://www.youtube.com/watch?v=3HdGkshOoOg

Flagship Projects

- OWASP Amass
- OWASP Application Security Verification Standa
- OWASP Cheat Sheet Series
- OWASP CSFRGuard
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Security Testing Guide
- OWASP Mobile Top 10
- OWASP ModSecurity Core Rule Set
- OWASP Risk Assessment Framework
- OWASP SAMM
- OWASP security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP

Lab Projects

- OWASP AntiSamy
- OWASP Automated Threats to Web Applications
- OWASP Benchmark
- OWASP Code Pulse
- OWASP Cornucopia
- OWASP Enterprise Security API (ESAPI)
- OWASP Internet of Things
- OWASP mobile security
- OWASP Proactive Controls
- OWASP Snakes And Ladders
- OWASP WebGoat

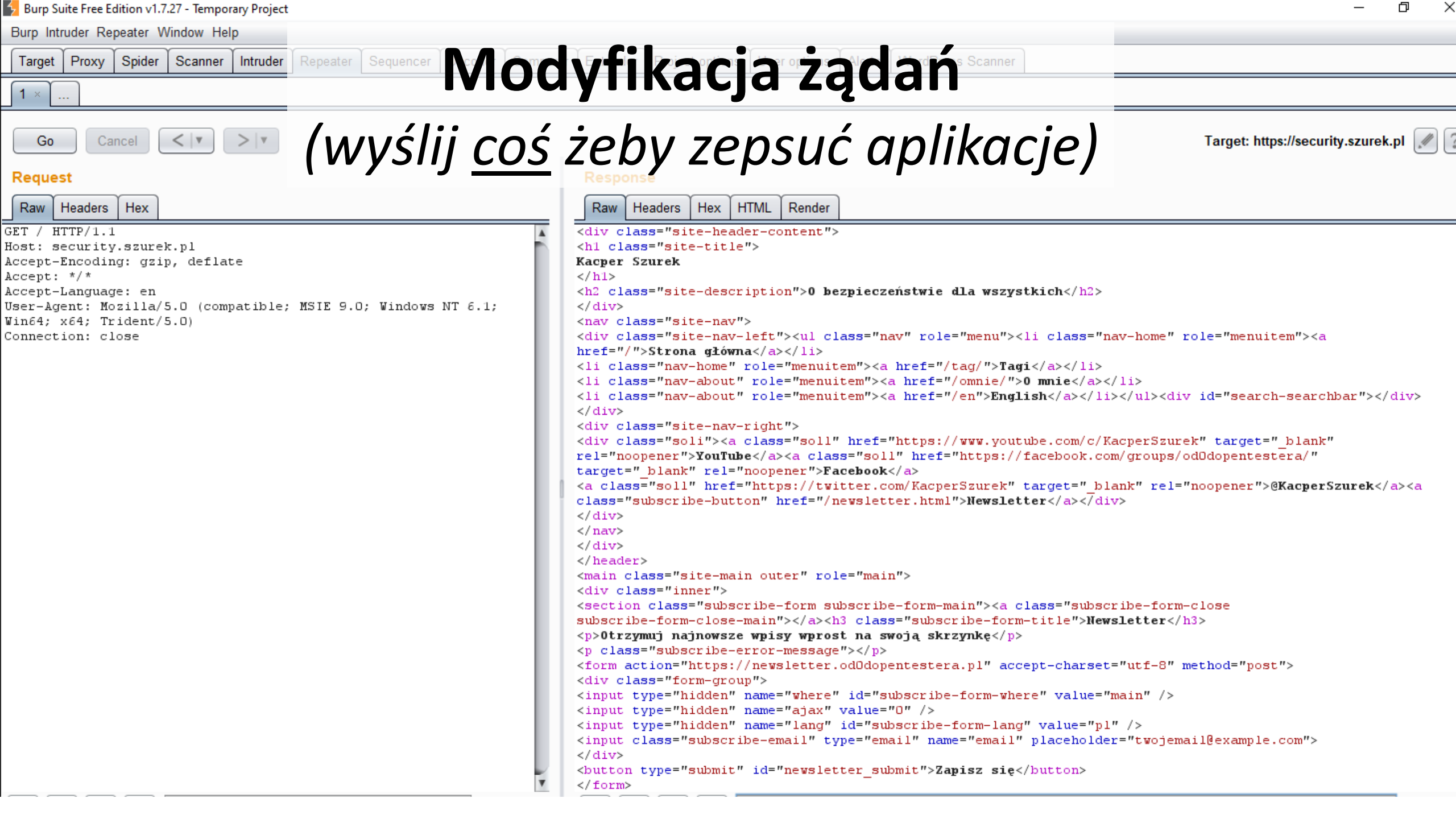
Incubator Projects

- OWASP API Security Project
- OWASP Appsec Pipeline
- OWASP Attack Surface Detector
- OWASP CSRFProtector Project
- OWASP Cyber Defense Matrix
- OWASP D4N155
- OWASP Docker Top 10
- OWASP Go Secure Coding Practices Guide
- OWASP Honeypot
- OWASP Node.js Goat
- OWASP SamuraiWTF
- OWASP Secure Coding Dojo
- OWASP Secure Headers Project
- OWASP secureCodeBox

https://owasp.org/projects/

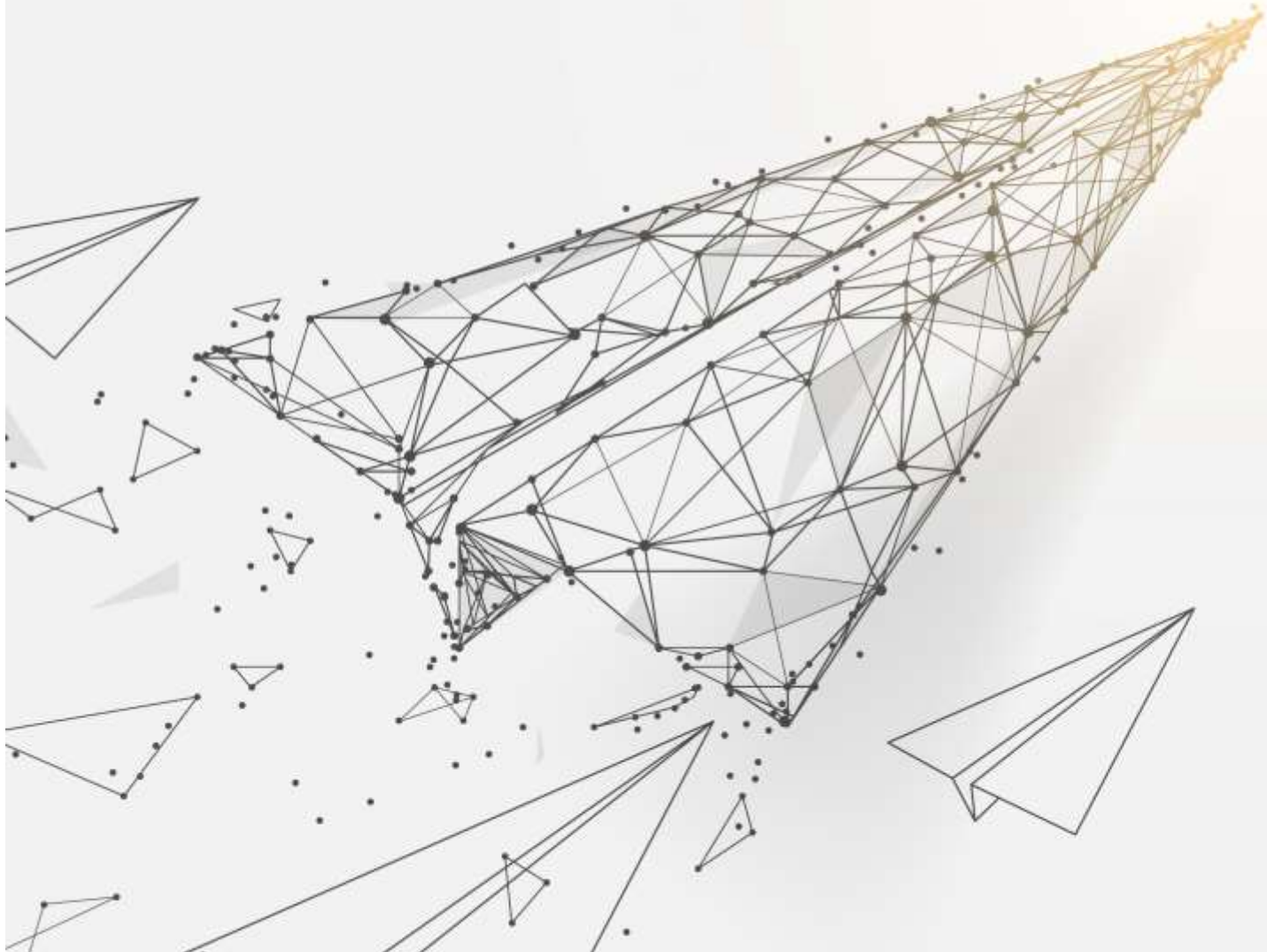
Modyfikacja żądań

(wyślij coś żeby zepsuć aplikacje)



Vulnerable-by-Design

(aplikacje specjalnie źle napisane)



WebGoat
bWAPP
Juice Shop
Damn Vulnerable Web App
Damn Vulnerable NodeJS

Skąd się **uczyć**?

1. https://pentester.land/
2. https://www.reddit.com/r/netsec/
3. https://portswigger.net/
4. https://github.com/Simpsonpt/AppSecEzine
5. https://twitter.com/hashtag/BugBountytips
6. https://ctftime.org/writeups
7. https://hackerone.com/hacktivity
8. PDF-y z konferencji

PENTESTER LAND
OFFENSIVE INFOSEC

The 5 Hacking NewsLetter 96

10 Mar 2020 • newsletter

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

This issue covers the week from 28 of February to 06 of March.

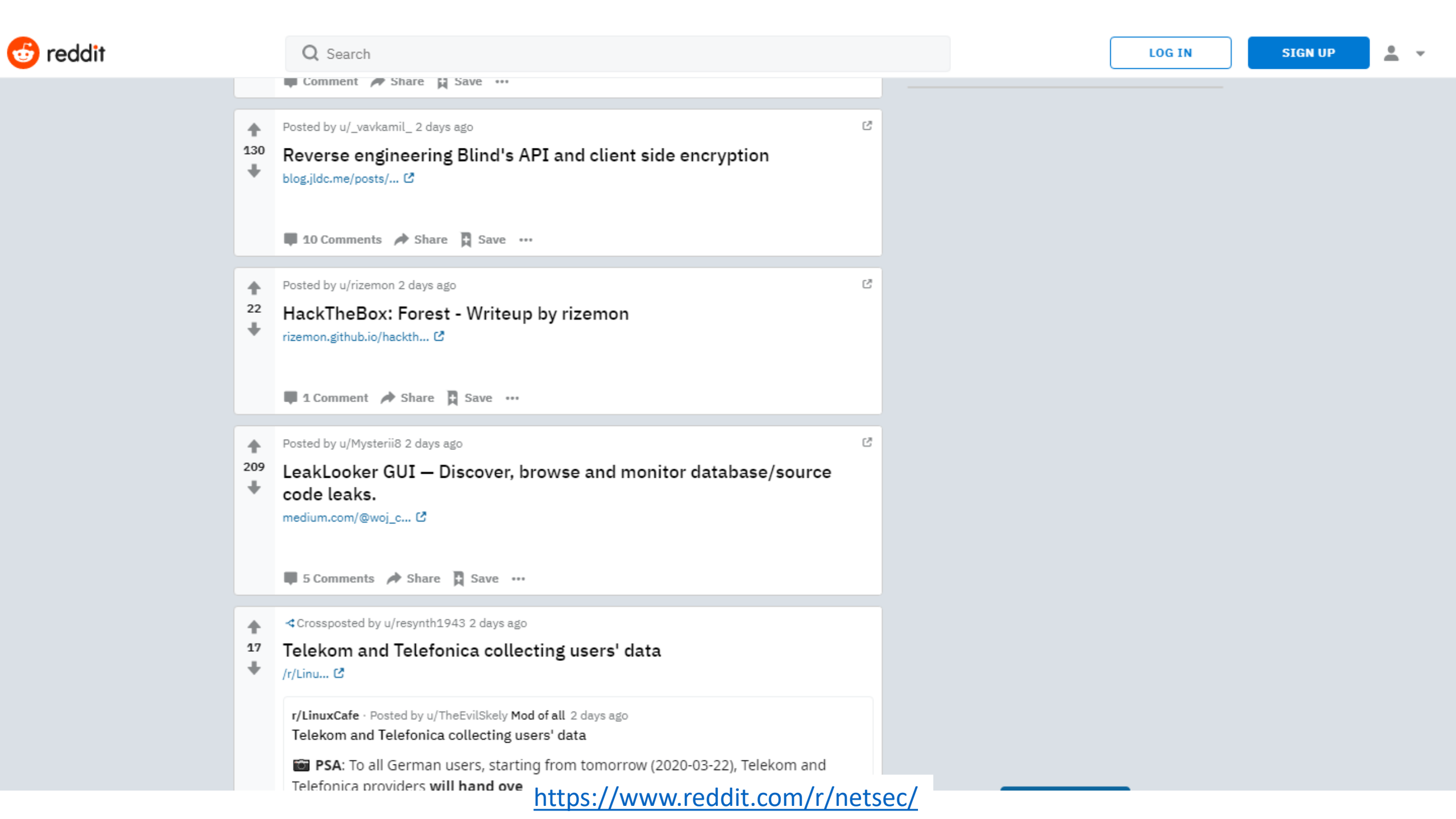
Our favorite 5 hacking items

1. Tools of the week

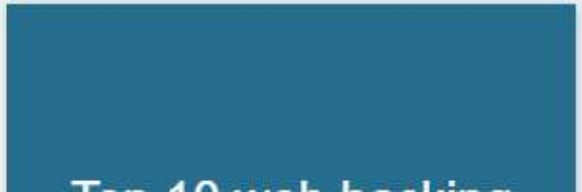
> - FUSE & FUSE: Finding File Upload Bugs via Penetration Testing
> - Pulsar

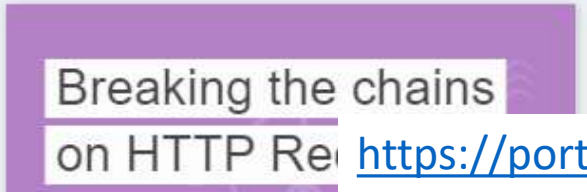
Pulsar is described as a Network footprint scanner platform. I didn't get to test it yet, but it d many recon tools, automates many recon , cloud resources discovery and basic

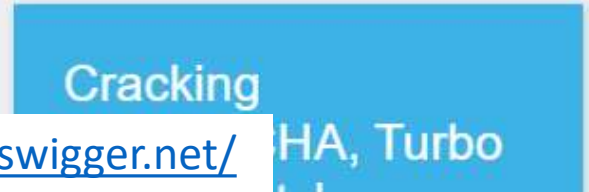
https://pentester.land/

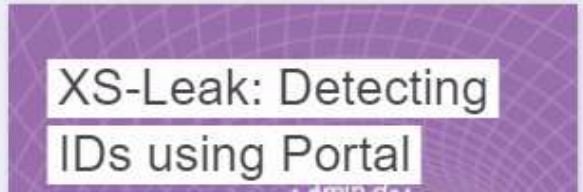


https://www.reddit.com/r/netsec/





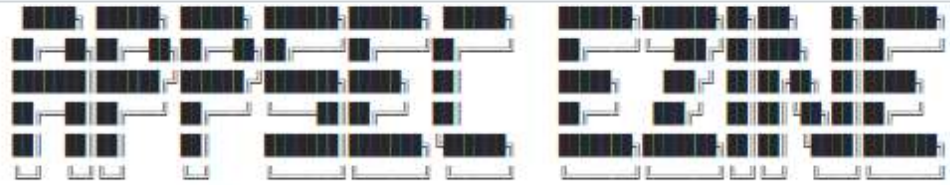




https://portswigger.net/

135 lines (90 sloc) | 6.01 KB

Raw | Blame | History



Week: 41 | Month: October | Year: 2018 | Release Date: 12/10/2018 | Edition: #243

' Something that's really worth your time!

URL: https://blog.sheddow.xyz/css-timing-attack/
Description: A timing attack with CSS selectors and Javascript.

URL: http://www.sec-down.com/wordpress/?p=809
Description: An interesting Google vulnerability that got me 3133.7 reward.

URL: http://bit.ly/2OQkWuJ (+)
Description: Get as image() pulls Insights/NRQL data from New Relic accounts (IDOR).

' Some Kung Fu Techniques.

URL: https://github.com/hdm/mac-ages
Description: MAC address age tracking.

URL: https://github.com/nulpwn/wiPray
Description: Wifi Password Spray in EAP-MSCHAPv2 networks.

URL: https://github.com/hausec/ADAPE-Script
Description: Active Directory Assessment and Privilege Escalation Script.

URL: https://github.com
Description: Rules for

https://github.com/Simpsonpt/AppSecEzine

https://twitter.com/hashtag/BugBountytips

DEF CON Media Server

/

File Name	File Size	Date
DEF CON 1/	-	2019-Apr-08 13:14
DEF CON 10/	-	2019-Apr-11 13:26
DEF CON 11/	-	2019-Apr-11 13:26
DEF CON 12/	-	2019-Apr-11 13:26
DEF CON 13/	-	2019-Apr-11 13:26
DEF CON 14/	-	2019-Aug-05 22:19
DEF CON 15/	-	2019-Apr-12 05:25
DEF CON 16/	-	2019-Apr-12 10:08
DEF CON 17/	-	2019-Apr-12 10:08
DEF CON 18/	-	2019-Aug-05 22:27
DEF CON 19/	-	2019-Apr-12 10:08
DEF CON 2/	-	2019-Apr-08 13:14
DEF CON 20/	-	2019-Apr-12 12:46
DEF CON 21/	-	2019-Apr-14 03:14
DEF CON 22/	-	2019-May-09 14:28

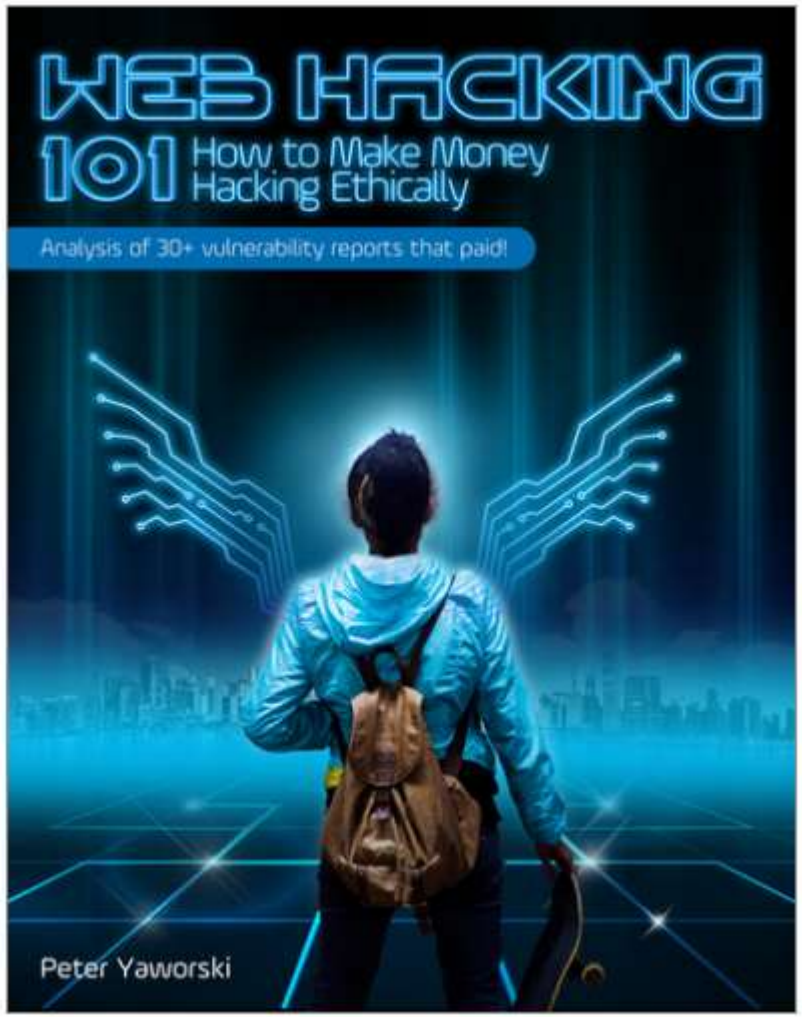
https://media.defcon.org/

Certyfikaty:

- segregują wiedzę
- zazwyczaj są drogie
- egzamin o niczym nie świadczy
- praktyka vs teoria
- nie są gwarantem pracy
- czasem wymagają doświadczenia

kursy/szkolenia/książki

1. Tak, ale pamiętaj – jakość nie ilość
2. Samo czytanie to nie wszystko
3. Praktyka, praktyka, praktyka
4. Nie czytaj całości od razu
5. Książki segregują wiedze z Internetu



https://leanpub.com/web-hacking-101

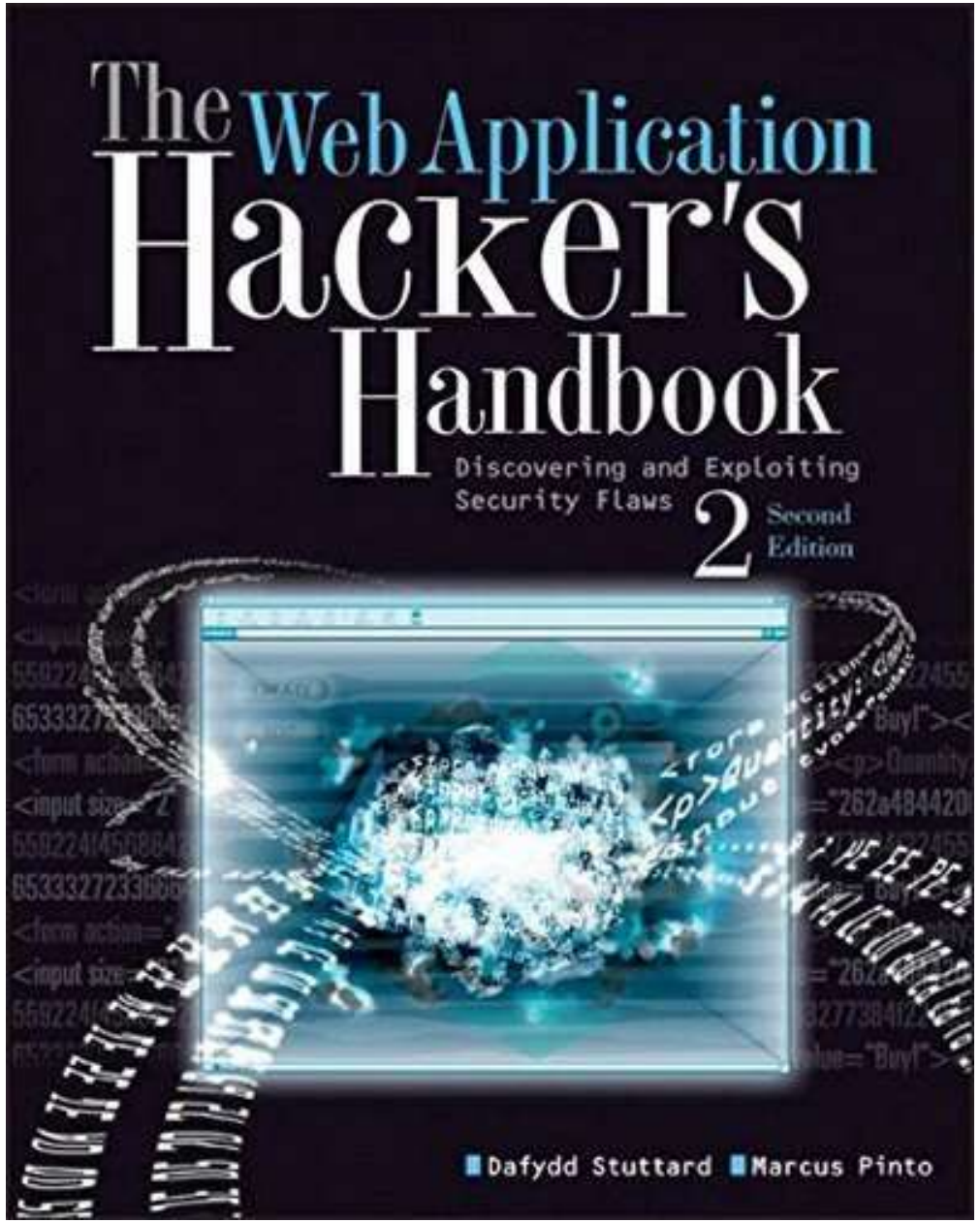
Podatności

- Podatność Cross-Site Scripting (XSS) [Michał Bentkowski]
- Content Security Policy (CSP) [Michał Bentkowski]
- Same-Origin Policy i Cross-Origin Resource Sharing (CORS) [Mateusz Niezabitowski]
- Podatność Cross-Site Request Forgery (CSRF) [Michał Sajdak]
- Podatność Server-Side Template Injection (SSTI) [Mateusz Niezabitowski]
- Podatność Server-Side Request Forgery (SSRF) [Michał Sajdak]
- Podatność SQL injection [Michał Bentkowski]
- Podatność Path Traversal [Marcin Piosek]
- Podatności Command Injection / Code Injection [Marcin Piosek]

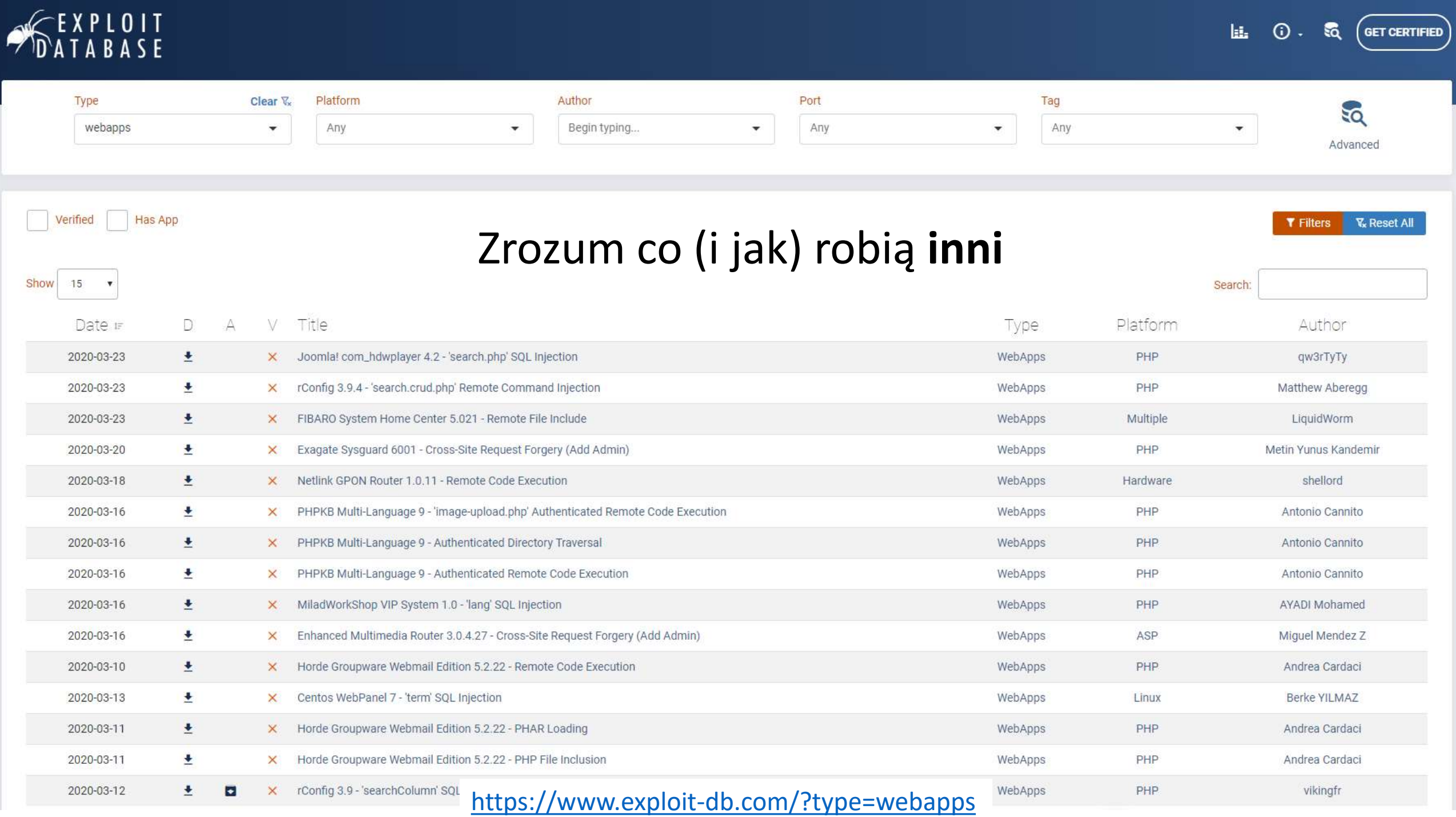
Inne obszary

- Uwierzytelnianie, zarządzanie sesją, autoryzacja [Marcin Piosek]
- Pułapki w przetwarzaniu plików XML [Michał Bentkowski]
- Bezpieczeństwo API REST [Michał Sajdak]
- Niebezpieczeństwa JSON Web Token (JWT) [Michał Sajdak]
- Zalety i wady OAuth 2.0 z perspektywy bezpieczeństwa [Marcin Piosek]
- Bezpieczeństwo protokołu WebSocket [Marcin Piosek]
- Wprowadzenie do programów Bug Bounty [Jarosław Kamiński]
- Flaga SameSite - jak działa i przed czym zapewnia ochronę? [Marcin Piosek]

https://sklep.sekurak.pl/



https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470



Zrozum co (i jak) robią **inni**

https://www.exploit-db.com/?type=webapps

Infrastruktura

(serwery i relacje między nimi)

1. Atakujesz aplikację **X**
2. Limitowany dostęp do serwera **Y**
3. Podniesienie uprawnień do **root**
4. Przejście na serwer **Z**

Podniesienie **uprawnień**

(jak zostać administratorem)

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

https://www.fuzzysecurity.com/tutorials/16.html

Enumeracja

(co znajduje się na serwerze)

- ✓Pliki na dysku
- ✓Programy/usługi
- ✓Konfiguracja
- ✓Uprawnienia

- Kali Linux
- Burp Suite
- Metasploit
- Nmap
- Wireshark

Linux/Windows?

COMMANDOVM

COMPLETE MANDIANT OFFENSIVE VM

https://www.fireeye.com/blog/threat-research/2019/08/commando-vm-customization-containers-kali.html


COMMANDOVM
COMPLETE MANDIANT OFFENSIVE VM

Networked

OS:	Linux
Difficulty:	Easy
Points:	20
Release:	24 Aug 2019
IP:	10.10.10.146

Heist

OS:	Windows
Difficulty:	Easy
Points:	20
Release:	10 Aug 2019
IP:	10.10.10.149

Hack The Box
PEN-TESTING LABS

[+] RastaLabs
Red Team Simulation Labs

https://www.hackthebox.eu/press/prolab-rastalabs

IPPSEC

Twitter • Patreon • Youtube

metaspl

Video	Description
Postman	Running searchsploit, then using Metasploit to exploit Webmin
Postman	Root shell returned, set Metasploit to go through burp and play with it until we get the exploit working.
Heist	Using Metasploit to do the same thing (smb_login), to show it keeps tracks of creds. Then doing a WinRM Login
Kryptos	Starting up metasploit to steal the login hash of a MYSQL Login
LaCasaDePapel	Triggering the backdoor without Metasploit
Redcross	Using Metasploit to exploit haraka, get shell as penelope
Jerry	Logging into tomcat and using msfvenom + metasploit to upload a malicious war file
Reel	Using Metasploit to do the box
Reel	Attempting to do the ALPC Exploit within Metasploit
DropZone	Examining PSExec Metasploit Module
DropZone	Using irb within metasploit to print a powershell payload
DropZone	Using irb within metasploit to print the MOF File
DropZone	Installing pry.byebug in order to allow us to drop to a debug console and step through metasploit modules
Bounty	Start of doing this box again, with Metasploit! Creating a payload with Unicorn
Bounty	Metasploit Session Returned! Checking local_exploit_suggester

https://ippsec.rocks

OFFENSIVE security

COURSES AND CERTIFICATIONS | LABS | PENTEST SERVICES | TRAINING FOR ORGS | WHY OFFSEC? | KALI AND INFOSEC TOOLS

GET MORE PWK

The official OSCP certification course.
All-new for 2020.

REGISTER

COURSE OVERVIEW

https://www.offensive-security.com/pwk-oscp/

Active Directory

https://adsecurity.org/

https://www.active-directory-security.com/

https://www.harmj0y.net/blog/

Blackbox

(bez kodu źródłowego)

Whitebox

(z kodem źródłowym)

Open Source

Repositories | Developers

Spoken Language: **Any** ▾ Language: **PHP** ▾ Date range: **Today** ▾

codeigniter4 / CodeIgniter4

Open Source PHP Framework (originally from EllisLab)

PHP ★ 2,467 ⑂ 918 Built by  ★ 6 stars today

pterodactyl / panel

Pterodactyl is the open-source game server management panel built with PHP7, Nodejs, and Go. Designed with security in mind, Pterodactyl runs all game servers in isolated Docker containers while exposing a beautiful and intuitive UI to administrators and users.

PHP ★ 1,662 ⑂ 381 Built by  ★ 2 stars today

bagisto / bagisto

A Free and Opensource laravel eCommerce framework built for all to build and scale your business.

PHP ★ 2,174 ⑂ 635 Built by  ★ 4 stars today

cretueusebiu / laravel-nuxt

A Laravel-Nuxt starter project template.

PHP ★ 693 ⑂ 149 Built by  ★ 4 stars today

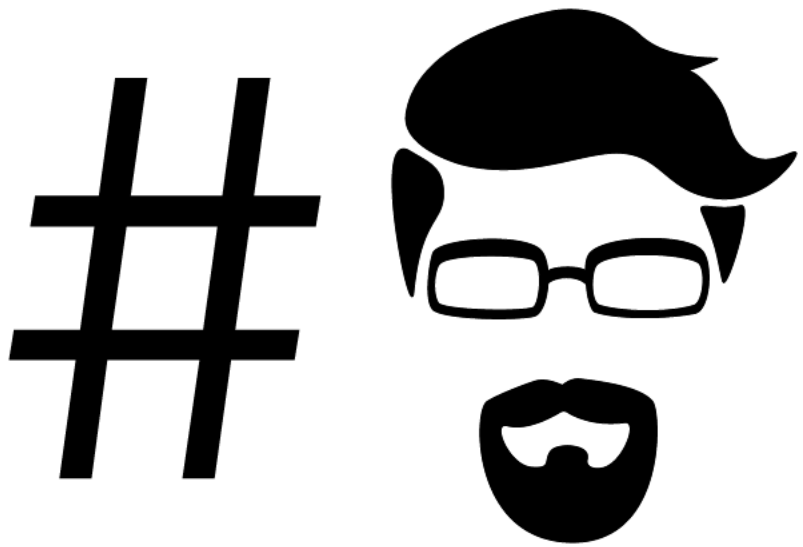
- system()
- exec()
- popen()
- eval()
- unlink()

Szukaj **potencjalnie niebezpiecznych** funkcji

- Nie hakuj **bez pozwolenia**
- Nie żądaj pieniędzy
- Nie hejtuj

Bug Bounty

1. Każdy może spróbować
2. Duża konkurencja
3. Duplikaty
4. Często długi czas oczekiwania
5. Brak gwarancji rezultatu



Szukanie błędów.

Jak zacząć?

bug bounty

pentester

https://www.youtube.com/watch?v=QJsaDX2URrA

Program	Launch date ↓	Reports resolved	Bounties minimum	Bounties average
Qulture.Rocks	03 / 2020	2	-	-
Every.org	03 / 2020	12	-	-
PegaSys Managed	03 / 2020	1	$50	$250
Myndr	03 / 2020	10	-	-
DigitalOcean Managed	03 / 2020	108	-	-
Glassdoor Managed	03 / 2020	464	$50	$300-$400
Orion Labs Managed	03 / 2020	-	-	-

Platformy

- HackerOne
- Bugcrowd
- Synack

114	[api.pandao.ru] IDOR for order delivery address	By n4sty to Mail.ru	Resolved	Medium	$3,000.00	disclosed 18 days ago
296	Connection informaton is sent to a third-party service	By martinbydefault to NordVPN	Resolved	Critical		disclosed 30 days ago
19	scripts loader (denial of service) vulnerability	By badis to MariaDB	Resolved	Low		disclosed 5 days ago
111	A non-administrator user can change his email even when it is restricted by an administrator	By agnidevan to Visma Bug Bounty Program	Resolved	Medium	$250.00	disclosed 18 days ago
651	H1514 Remote Code Execution on kitcrm using bulk customer update of Priority Products	By fransrosen to Shopify	Resolved	Medium	$15,000.00	disclosed 2 months ago
28	athome.starbucks.com - URL parameter tampering of review forms permitted possible content injection	By jackb898 to Starbucks	Resolved	Medium		disclosed 7 days ago
139	Access to all files of remote user through shared file	By xuesheng to Nextcloud	Resolved	Medium	$750.00	disclosed 23 days ago
180	sdrc.starbucks.com - Information Disclosure via unsecured attachment directory	By l00ph0le to Starbucks				disclosed 27 days ago

https://hackerone.com/

Allegro

Allegro is a real European-born tech leader, #1 online shopping destination in Poland and #6 eTail business in Europe.

https://allegro.pl.allegrosandbox.pl/ · @allegrotech

Submit report

Bug Bounty Program
Launched on Oct 2019

Managed by HackerOne

Reports resolved	Assets in scope	Average bounty
8	1	$250-$300

Rewards

Critical	High	Medium	Low
$3,000	$1,000	$500	$200

We will reward reports according to their severity on a case-by-case basis as determined by our security team. We may pay more for unique, hard-to-find bugs; we may also pay less for bugs with complex prerequisites that lower risk of exploitation. Our minimum reward is $200 USD.

Last updated on October 8, 2019. View changes

Response Efficiency

3 hrs
Average time to first response

5 days
Average time to bounty

2 months
Average time to resolution

98% of reports
Meet response standards
Based on last 90 days

Policy

https://hackerone.com/allegro

OLX

OLX is an online classifieds platform that enables its users to create ads and display them on social networks.

http://olx.com · @OLX

Reports resolved
358

Assets in scope
-

Submit report

Vulnerability Disclosure Program
Launched on Jun 2016

Policy | Hacktivity | Thanks | Updates (2)

OLX is taking a break and is not accepting new submissions.

Policy

At OLX, we take security issues seriously. If you believe you've detected a vulnerability within our products we'd like to hear about it. We'll investigate all reports and do our best to fix these issues as soon as possible.

Scope

The scope of our program includes the following sites:

- Poland: olx.pl, otodom.pl, otomoto.pl
- Portugal: olx.pt
- United Arab Emirates: dubizzle.com
- South Africa: olx.co.za
- Pakistan: olx.com.pk

https://hackerone.com/olx

Response Efficiency

-
Average time to first response

3 months
Average time to resolution

-
Meet response standards
Based on last 90 days

Zakres

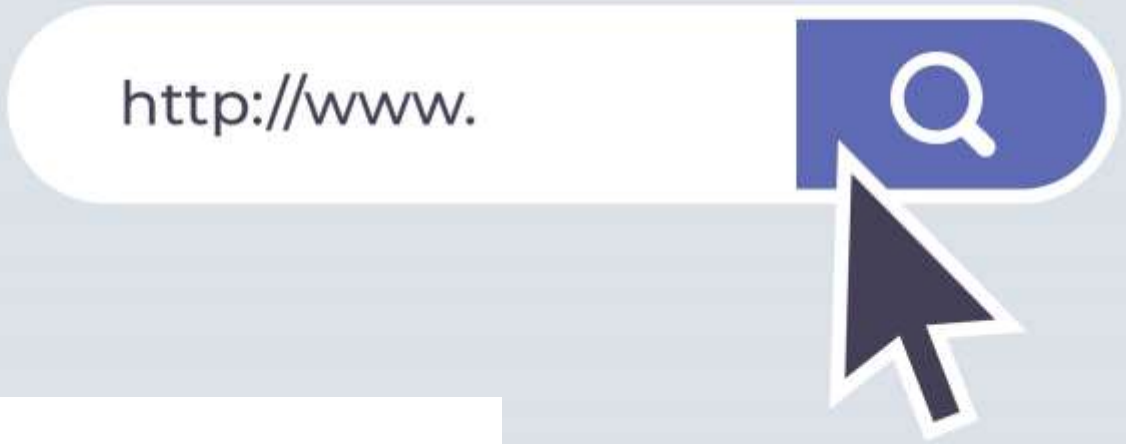
(co <u>wolno</u> a czego <u>nie</u>)

a. Jakie domeny można atakować
b. Za co się płaci
c. Czego nie wolno robić
d. Czy jest infrastruktura testowa

Prywatne **programy:**

- **na zaproszenie**
- **większy zakres**
- **mniejsza konkurencja**

"security hall of fame"



Security Hall of Fame

The following researchers have taken the time to identify and report security concerns with Sellfy. Their work is truly appreciated.

Muhammad Mujtaba
Muhammad Waqar
Jay Turla
Ehraz Ahmed
Kamil Sevi
Ali Hasan Ghauri
Ali Zahir
Vaibhav Deshmukh
Parichay Rai
Sebastian Neef
Adeel Imtiaz
Riaz Ebrahim

Jan Aumar Badinas
Sumit Sahoo (54H00)
Jay Patel
Ashish Pathak
Pradeep Kumar
Arpit Gupta
Nehal Ghoratkar
Asif Balasinor
Sukhjiwan Singh Matharu
Mahender Singh & Deepali Malekar
Russel Van Laurio
Akshay Shinde

Shubham Sharma
Shubham Sahu
Waqeeh Ul Hasan
Jatinder Singh Saini, Vikas Khanna,
Gurjant Singh Sadhra
Kaushik Roy
Ali Tabish
Mohammed Abd Elmageed
Muhammad Amr Nasef
Abhishek Baru
Nitesh Sharma
Omkar Avasthi

Rekonesans:

- zakres z wildcard
- nowe domeny
- nowe funkcje
- nowe możliwości
- zapomniane podstrony

SPECJALIZACJA!

Weź jeden produkt/funkcje/typ błędu
i stań się ekspertem


Szukanie to **połowa** pracy:
raport

- Opis
- Jak znalazłeś
- POC
- Dodatkowe warunki do exploitacji
- **Impakt** na organizacje
- Rekomendacje naprawy
- Referencje
- Obrazek/Video

CTF

- Praca w grupie
- Ciekawe zadania
- Presja czasu
- Cierpliwość /pokora
- Często nowe podatności

CTFTIME | CTFs | Upcoming | Archive | Calendar | Teams | FAQ | Contact us | About | Sign in

Event	Task	Tags	Author team	Action
FireShell CTF 2020	Dungeon Escape	ppc	BambooFox	Read
UTCTF 2020	Random ECB	ecb crypto	misc	Read
Securinets CTF Quals 2020	UNCRACKABLE		misc	Read
Securinets CTF Quals 2020	Destruction	crytpography	Fword	Read
Securinets CTF Quals 2020	The Secured channel		Fword	Read
Securinets CTF Quals 2020	C is G ? Ez Camel	elgamal	Fword	Read
FireShell CTF 2020	Miscrypto Alphabet		BambooFox	Read
FireShell CTF 2020	Is this Rev?		BambooFox	Read
Securinets CTF Quals 2020	TRIPLE	reverse-engineering 3des	OpenToAll	Read
Securinets CTF Quals 2020	UNCRACKABLE	rev pwn	K@i	Read
FireShell CTF 2020	Welcome	web	UnderDawgs	Read
FireShell CTF 2020	wfPM	web	UnderDawgs	Read
FireShell CTF 2020	URL to PDF	web	UnderDawgs	Read
FireShell CTF 2020	Screenshoter	web	UnderDawgs	Read
FireShell CTF 2020	CaaS	web	UnderDawgs	Read
FireShell CTF 2020	Temporary File System Storage	uaf pwn	House of Suicide	Read
CONFidence CTF 2020 Teaser	Angry Defender		Balsn	Read
CONFidence CTF 2020 Teaser	Temple JS		Balsn	Read
CONFidence CTF 2020 Teaser	Cat web		Balsn	Read

https://ctftime.org/

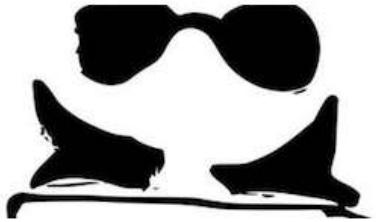
Android/Iphone

1. OWASP Mobile Security Testing Guide
2. Bezpieczeństwo API
3. Dekompilacja aplikacji
4. Jailbreak/root
5. SSL Pinning


AWS/Azure/Google

CloudGoat

(podatna infrastruktura)



Playing with CloudGoat part 2: fooling AWS CloudTrail and getting persistent access

69 1 response

Pawel Rzepa
Sep 16, 2018 · 8 min read

Playing with CloudGoat part 1: hacking AWS EC2 service for privilege escalation

https://github.com/RhinoSecurityLabs/cloudgoat
https://medium.com/@rzepsky

Before diving into this blog post, you should consider reviewing our recent post on phishing users with MFA on AWS. The research discussed in this post was discovered during an AWS phishing engagement that Rhino was performing on a client,...

Read more ›

https://rhinosecuritylabs.com/blog/

Patrz jak robią to **inni**

https://rhinosecuritylabs.com/landing/penetration-test-report/
https://cdn.sekurak.pl/eventory-sample-pentest-report.pdf
https://github.com/juliocesarfort/public-pentesting-reports
https://cure53.de/#publications

Identified Vulnerabilities

The following sections list both vulnerabilities and implementation issues spotted during the testing period. Note that findings are listed in chronological order rather than by their degree of severity and impact. The aforementioned severity rank is simply given in brackets following the title heading for each vulnerability. Each vulnerability is additionally given a unique identifier (e.g. *SAF-01-001*) for the purpose of facilitating any future follow-up correspondence.

SAF-01-001 Crypto: Secure key deletion ineffective *(Medium)*

***Note:** This issue has been discussed with the Safing team and a fix has been confirmed by the Cure53 team.*

In many instances, Jess calls *helper* functions that appear to be designed as a way to "burn" cryptographic keys and similarly sensitive material from the device's memory in order to prevent recovery. These "*burn*" functions are called frequently throughout the cryptographic stack of Jess, including locations in the *Signet, RSA, X25519* and *NIST* components.

However, the tactic used in order to achieve key erasure is likely ineffective, due to the limitations of the Go's garbage collection-based memory management model[1]. Furthermore, it does not attempt to target residual values, such as intermediate computations, which thus may remain in memory.

Affected Files:
helper.go
tools/ecdh/nist.go

Affected Code:

```
// Burn gets rid of the given []byte slice(s).
func Burn(data ...[]byte) {
    for _, slice := range data {
        for i := 0; i < len(slice); i++ {
            slice[i] = 0xFF
        }
    }
}

[...]

func (ec *NistCurve) BurnKey(signet tools.SignetInt) error {
    pubKey := signet.PublicKey()
```

SAF-01-003 Crypto: Secure channel protocol weaknesses *(High)*

***Note:** This issue has been discussed with the Safing team and a fix has been confirmed by the Cure53 team.*

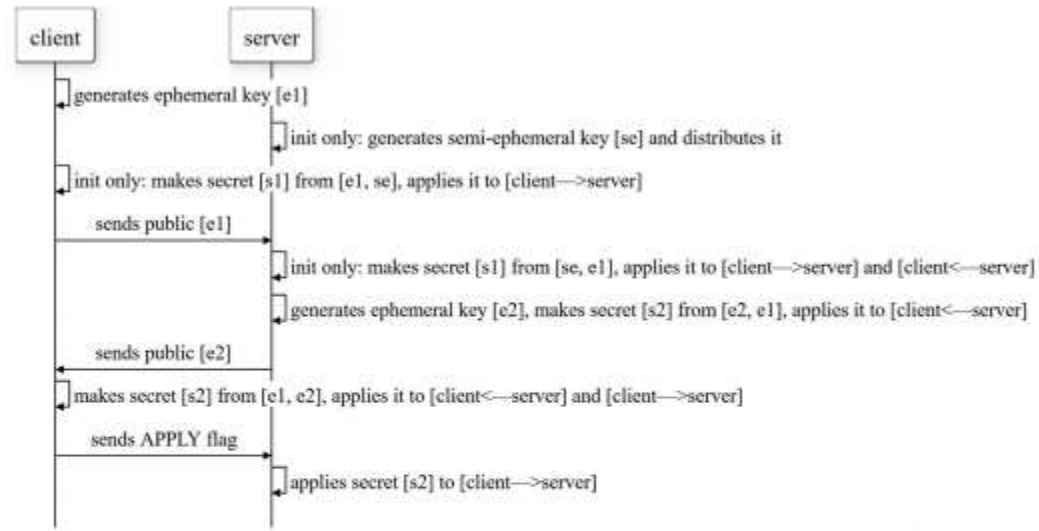


Fig.: Jess' Diffie-Hellman secure channel protocol, based on the NK[6] Noise Protocol Framework Handshake Pattern.

The secure channel protocol deployed by Jess - in both Diffie-Hellman and Key Encapsulation variants, was modeled and evaluated using the Verifpal automated protocol analysis software[7]. The results were the following:

```
Result • authentication? Client -> Server: enc1: When the following values are
mutated by the attacker:
            ge1 → G^nil (originally G^e1)
            enc1, sent by Client and resolving to AEAD_ENC(G^se^e1, msg1,
nil), is successfully used in primitive AEAD_DEC(G^nil^se, AEAD_ENC(G^se^e1,
```

https://cure53.de/pentest-report_safing-jess.pdf

Red Teaming

(symulacja realnych ataków)

Zazwyczaj mają szeroki zakres
Można stosować socjotechnikę
Nie ilość błędów a włamanie do firmy
Weryfikacja zabezpieczeń korporacji

Marcin Ludwiszewski

Director
of Cyber Security

Deloitte

https://www.youtube.com/watch?v=SmNThn-uhcc

https://twitter.com/pawelmaziarz/

- Wifi Pineapple
- Proxmark
- Rubberducky
- Wytrychy

Narzędzia

Atak trwa **krótko** a przygotowania …

- ❑ Powershell
- ❑ Infrastruktura C&C
- ❑ Omijanie antywirusów
- ❑ Socjotechnika
- ❑ Rekonesans
- ❑ Własne narzędzia

You're Probably Not Red Teaming (And Usually I'm Not, Either)

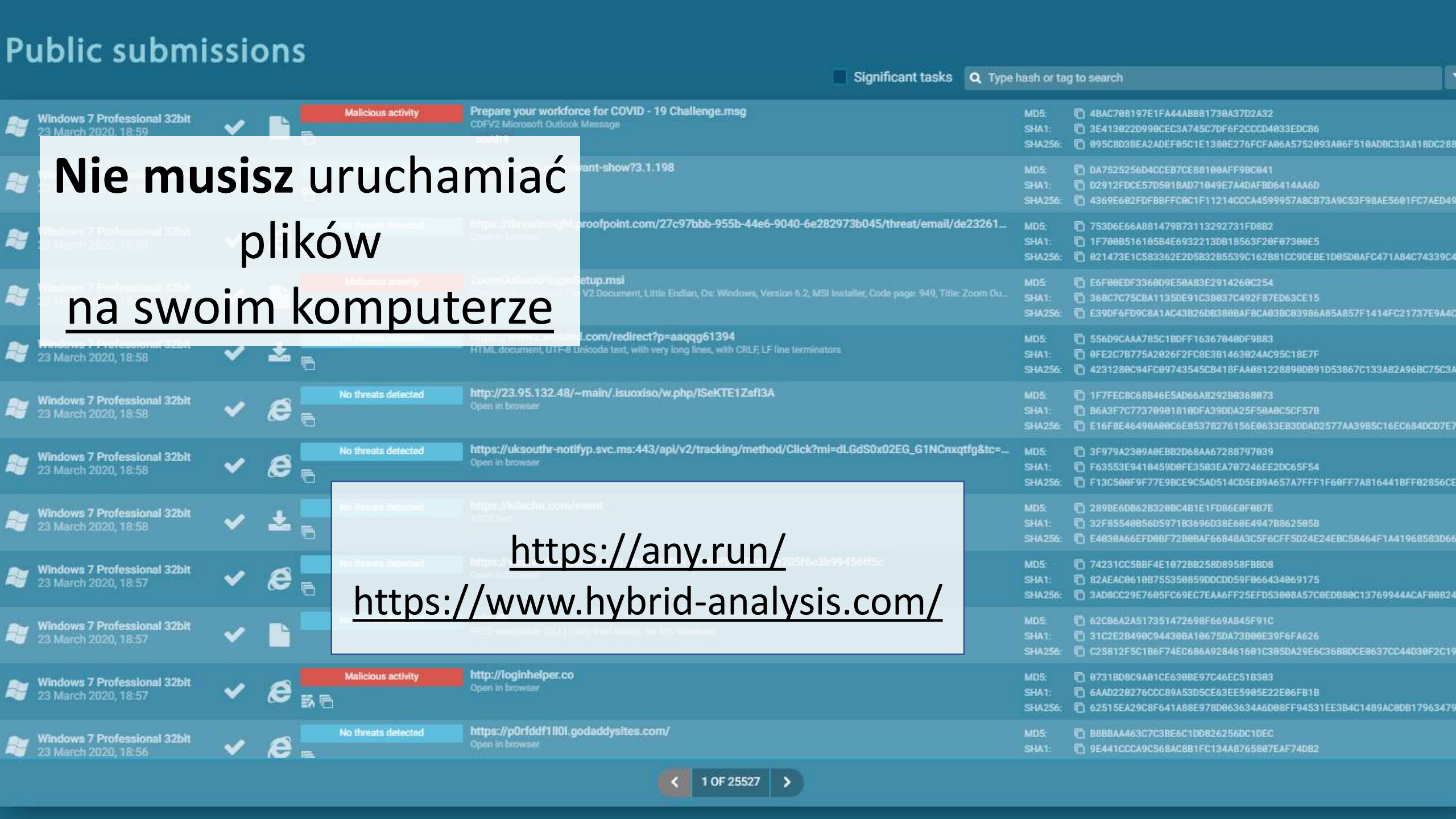
https://www.youtube.com/watch?v=mj2iSdBw4-0

Deviant Ollam
Security Auditor & Pen Test Consultant
The CORE Group

SANS ICS SECURITY ORLANDO SUMMIT & TRAINING

MALWARE
UWAGA!!!

Możesz *stracić* dane


Public submissions
Significant tasks
Type hash or tag to search
Nie musisz uruchamiać plików na swoim komputerze
https://any.run/
https://www.hybrid-analysis.com/
1 OF 25527

Podszywanie się pod witryny

Jak próbują Cię **oszukać**

PhishTank® Out of the Net, into the Tank.

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http:// Is it a phish?

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL
6464878	https://acctmgr.evoice.com/acctmgr/Common/ClickToC...
6464877	http://track.smtpsendemail.com/9016770/c?p=JsS2CAL...
6464876	http://bbfunding-my.sharepoint.com/personal/accoun...
6464875	http://bbfunding-my.sharepoint.com/personal/accoun...
6464873	http://bbfunding-my.sharepoint.com/personal/accoun...
6464872	http://bbfunding-my.sharepoint.com/personal/accoun...
6464871	http://bbfunding-my.sharepoint.com/personal/accoun...
6464870	http://bbfunding-my.sharepoint.com/personal/accoun...
6464869	http://appleid.apple.com.olikjokjn.com/R1zqgM7K3kG...
6464867	http://adamengdesigns.com/wella/wells/wells_fargo/
6464866	https://paypal-unlockservices.blogspot.com/?m=1
6464864	http://36.160.224.35.bc.googleusercontent.com/bank...
6464863	http://35.224.160.36/bank_of_america/22-03-2020/AS...
6464862	https://produtosstore.com/789630756/?smartphone-sa...
6464861	http://35.224.160.36/bank_of_america/22-03-2020/AS...

https://www.phishtank.com/

OpenPhish / Phishing Feeds / Global Phishing Activity

Timely. Accurate. Relevant Threat Intelligence.

5,000+	1,000+	400+
active phishing URLs discovered daily	online accounts at risk monthly	brands targeted by phishing campaigns

Phishing URL	Targeted Brand
https://account-verification.haroldebell.com/verify/amazon/signin.php?country=NL-Netherlan...	Amazon.com Inc.
http://split.to/VUUBdAY	Amazon.com Inc.
http://pls210515strom-com.preview-domain.com/1081110121.htm	Facebook, Inc.
http://paypal.com-re-secure-your-account-verification-support.nerimsport.com.br/account/si...	PayPal Inc.
http://freephubpremium.000webhostapp.com/	PayPal Inc.
https://pemsum.org/secure/	Office365
https://4ktvmagazineluiza.tftpd.net/lg-tv/smart-tv-4k-led-60-lg-60uk6200-wi-fi-hdr-inteligencia...	Magalu
http://ssfsdf.hostingem.ru/oauth/?i=1	VKontakte
https://tikilove.ru/vk.login.php	VKontakte
http://oauth.vk.com.authorize-client-id-4083558scope-107374redirecturi.mcn-realty.ru/	VKontakte
https://4ktvmagazineluiza.ownip.net/lg-tv/smart-tv-4k-led-60-lg-60uk6200-wi-fi-hdr-inteligenci...	Magalu

https://openphish.com/

[2017-10-30T01:03:08.732756] sabre.ct.comodo.com - calebfong.com
[2017-10-30T01:03:08.736403] sabre.ct.comodo.com - omakotiblogi.fi
[2017-10-30T01:03:08.739438] sabre.ct.comodo.com - cyd.rinocerontesoftware.com.br
[2017-10-30T01:03:08.743357] sabre.ct.comodo.com - sni242366.cloudflaressl.com
[2017-10-30T01:03:08.746985] sabre.ct.comodo.com - nomorefatigue.jackchallem.jp
[2017-10-30T01:03:08.750505] sabre.ct.comodo.com - buh.stasmoda.com
[2017-10-30T01:03:08.753803] sabre.ct.comodo.com - vanstadsif.se
[2017-10-30T01:03:08.757251] sabre.ct.comodo.com - www.nightofthelivingdeadfilms.com
[2017-10-30T01:03:08.760780] sabre.ct.comodo.com - www.love-market.com.ua
[2017-10-30T01:03:08.764062] sabre.ct.comodo.com - www.nespressocapsuleart.com
[2017-10-30T01:03:08.767400] sabre.ct.comodo.com - rociopelaez.com
[2017-10-30T01:03:08.771454] sabre.ct.comodo.com - www.novecoconstruction.com
[2017-10-30T01:03:08.774979] sabre.ct.comodo.com - www.thecandidentrepreneur.com
[2017-10-30T01:03:08.778695] sabre.ct.comodo.com - apaci.org
[2017-10-30T01:03:08.782650] sabre.ct.comodo.com - acitaquarituba.com.br
[2017-10-30T01:03:08.787273] sabre.ct.comodo.com - www.notofwealth.com
[2017-10-30T01:03:08.792718] sabre.ct.comodo.com - sni94890.cloudflaressl.com
[2017-10-30T01:03:08.796569] sabre.ct.comodo.com - m.empleo.demo.bizneo.com
[2017-10-30T01:03:08.800223] sabre.ct.comodo.com - micro-recycle.com
[2017-10-30T01:03:08.803834] sabre.ct.comodo.com - evron.fi
[2017-10-30T01:03:08.807935] sabre.ct.comodo.com - nascent49.com
[2017-10-30T01:03:08.813716] sabre.ct.comodo.com - sni46701.cloudflaressl.com
[2017-10-30T01:03:08.818207] sabre.ct.comodo.com - dewittcountyill.com
[2017-10-30T01:03:08.823387] sabre.ct.comodo.com - sni147765.cloudflaressl.com
[2017-10-30T01:03:08.829475] sabre.ct.comodo.com - sni111763.cloudflaressl.com
[2017-10-30T01:03:08.834468] sabre.ct.comodo.com - sni211485.cloudflaressl.com
[2017-10-30T01:03:08.838345] sabre.ct.comodo.com - www.opticagalens.com
[2017-10-30T01:03:08.846112] sabre.ct.comodo.com - aqurban.xyz
[2017-10-30T01:03:08.854347] sabre.ct.comodo.com - mywaydanceagency.com
[2017-10-30T01:03:08.857939] sabre.ct.comodo.com - eosydney.com.au
[2017-10-30T01:03:08.861686] sabre.ct.comodo.com - www.nsbcoalition.com

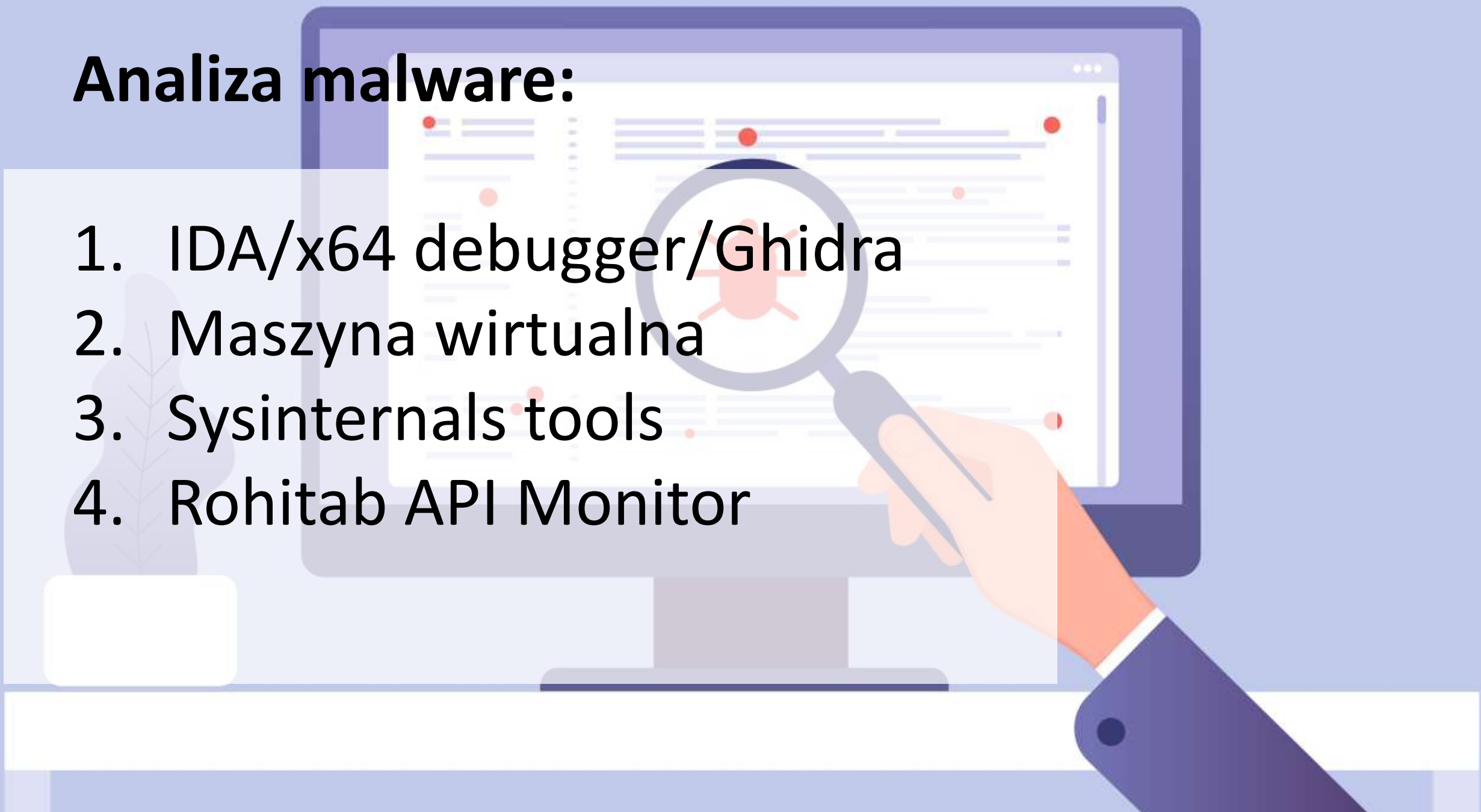
lista wystawionych certyfikatów SSL

https://certstream.calidog.io/

Macro/JS/VBS

Analiza malware:

1. IDA/x64 debugger/Ghidra
2. Maszyna wirtualna
3. Sysinternals tools
4. Rohitab API Monitor



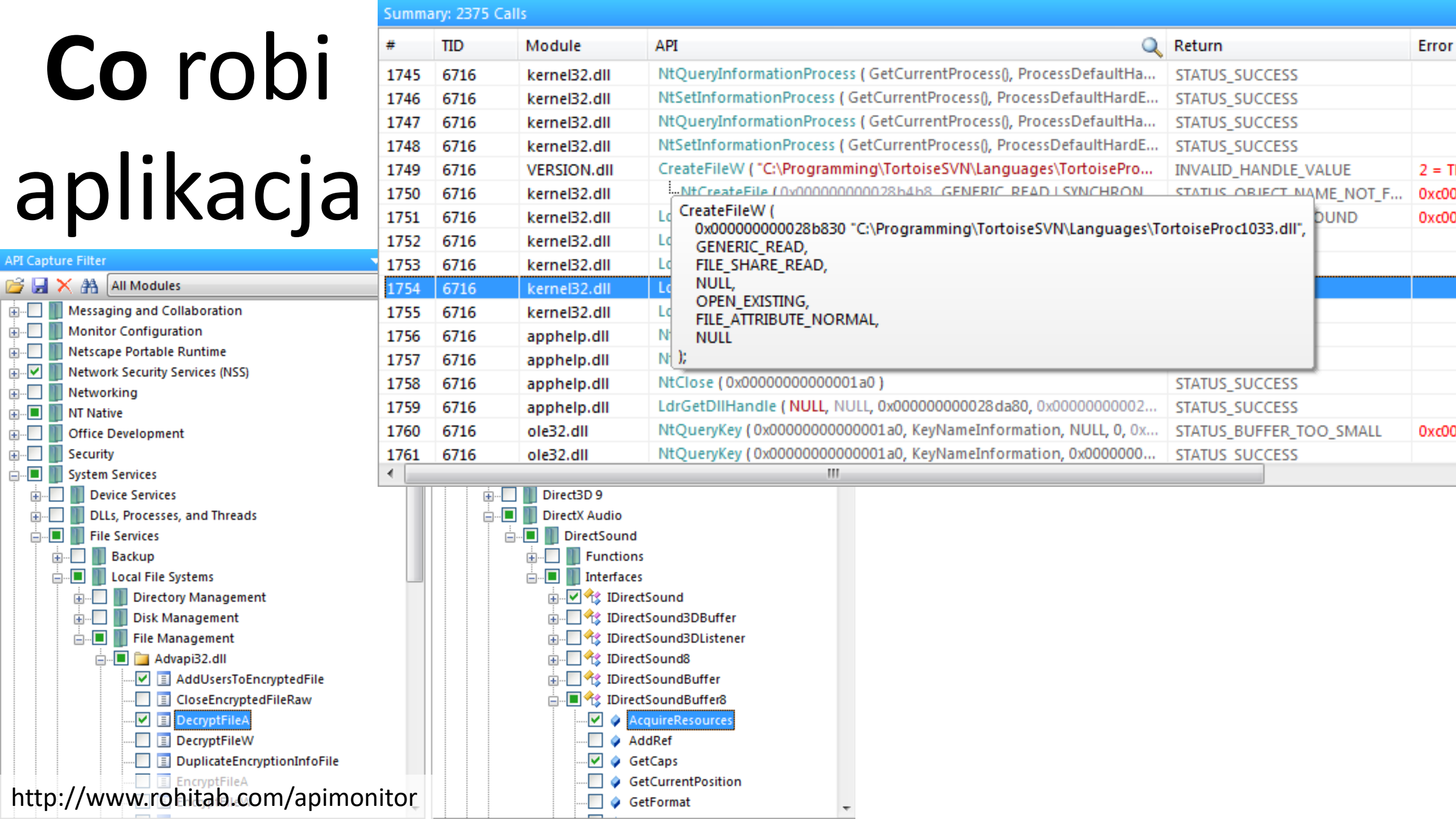
Asembler **vs** dekompilacja

```
; ============== S U B R O U T I N E =======================================

wndproc         proc near               ; DATA XREF: sub_4010E0+21o

Paint           = tagPAINTSTRUCT ptr -0A4h
Buffer          = byte ptr -64h
hWnd            = dword ptr  4
Msg             = dword ptr  8
wParam          = dword ptr  0Ch
lParam          = dword ptr  10h

                mov     ecx, hInstance
                sub     esp, 0A4h
                lea     eax, [esp+0A4h+Buffer]
                push    64h             ; nBufferMax
push    eax             ; lpBuffer
push    6Ah             ; uID
push    ecx             ; hInstance
call    ds:LoadStringA
mov     ecx, [esp+0A4h+Msg]
mov     eax, ecx
sub     eax, 2
jz      loc_4013E8
sub     eax, 0Dh
jz      loc_4013B2
sub     eax, 102h
jz      short loc_401336
mov     edx, [esp+0A4h+lParam]
mov     eax, [esp+0A4h+wParam]
push    edx             ; lParam
                        push    eax             ; wParam
                        push    ecx             ; Msg
                        mov     ecx, [esp+0B0h+hWnd]
push    ecx             ; hWnd
                        call    ds:DefWindowProcA
add     esp, 0A4h
retn    10h
; ---------------------------------------------------------------------------

loc_401336:                             ; CODE XREF: wndproc+3C↓j
mov     ecx, [esp+0A4h+wParam]
mov     eax, ecx
and     eax, 0FFFFh
sub     eax, 68h
jz      short loc_40138A
dec     eax
jz      short loc_401371
```

```
LRESULT __stdcall WndProc(HWND hWnd, UINT Msg, WPARAM wParam, LPARAM lParam)
{
  LRESULT result; // eax@4
  HWND h; // esi@10
  HDC dc; // eax@10
  CHAR Buffer; // [sp+40h] [bp-64h]@1
  struct tagPAINTSTRUCT Paint; // [sp+0h] [bp-A4h]@10

  LoadStringA(hInstance, 0x6Au, &Buffer, 100);
  switch ( Msg )
  {
    case 2u:
      PostQuitMessage(0);
      result = 0;
      break;
    case 15u:
      h = hWnd;
      dc = BeginPaint(hWnd, &Paint);
      my_paint(h, dc);
      EndPaint(h, &Paint);
      result = 0;
      break;
    case 273u:
      if ( (_WORD)wParam == 104 )
      {
        DialogBoxParamA(hInstance, (LPCSTR)0x67, hWnd, DialogFunc, 0);
        result = 0;
      }
      else
      {
        if ( (_WORD)wParam == 105 )
        {
          DestroyWindow(hWnd);
          result = 0;
        }
        else
        {
          result = DefWindowProcA(hWnd, 0x111u, wParam, lParam);
        }
      }
      break;
    default:
      result = DefWindowProcA(hWnd, Msg, wParam, lParam);
      break;
  }
  return result;
}
```

https://www.hex-rays.com/products/decompiler/compare_vs_disassembly/

Co robi aplikacja



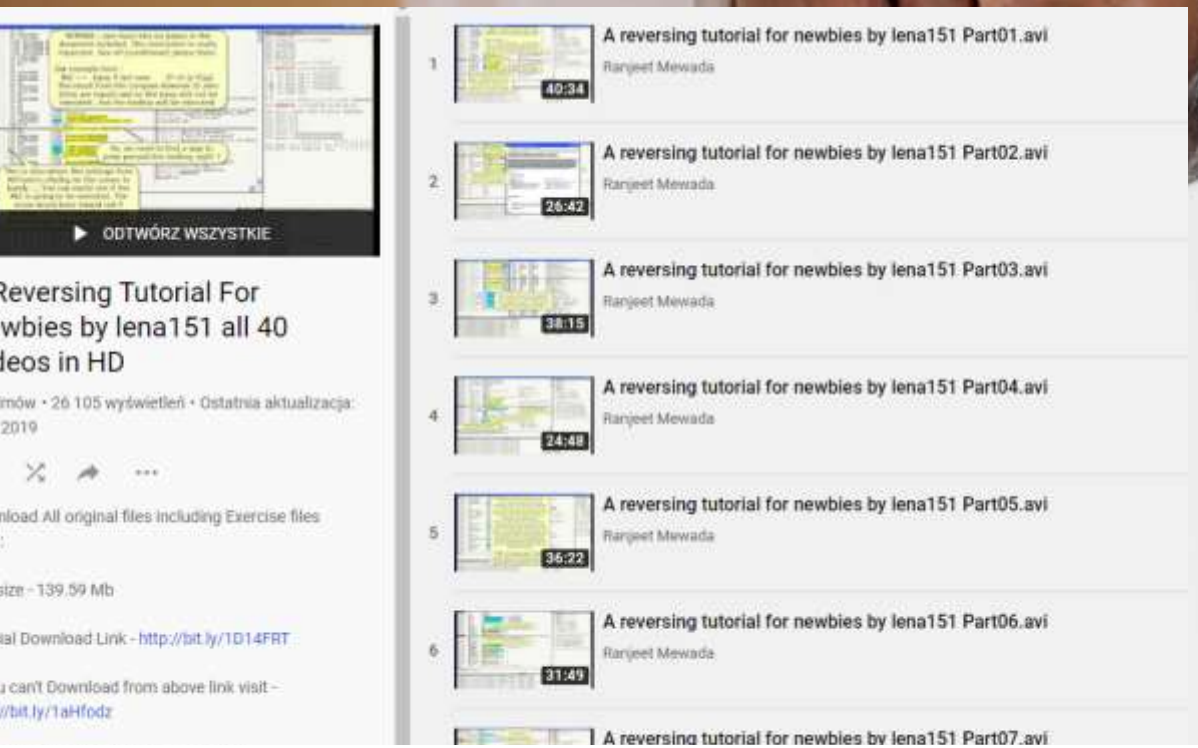
http://www.rohitab.com/apimonitor

Reverse Engineering for Beginners

https://beginners.re/

CONTENTS

„**Wypakowywanie**” aplikacji
(mniejszy rozmiar – dłuższe wykonywanie)



ttps://www.youtube.com/playlist?list=PLcFUp5WYCxVYeR7AgsmjzGW6PjamaY6JO

Latest Crackmes

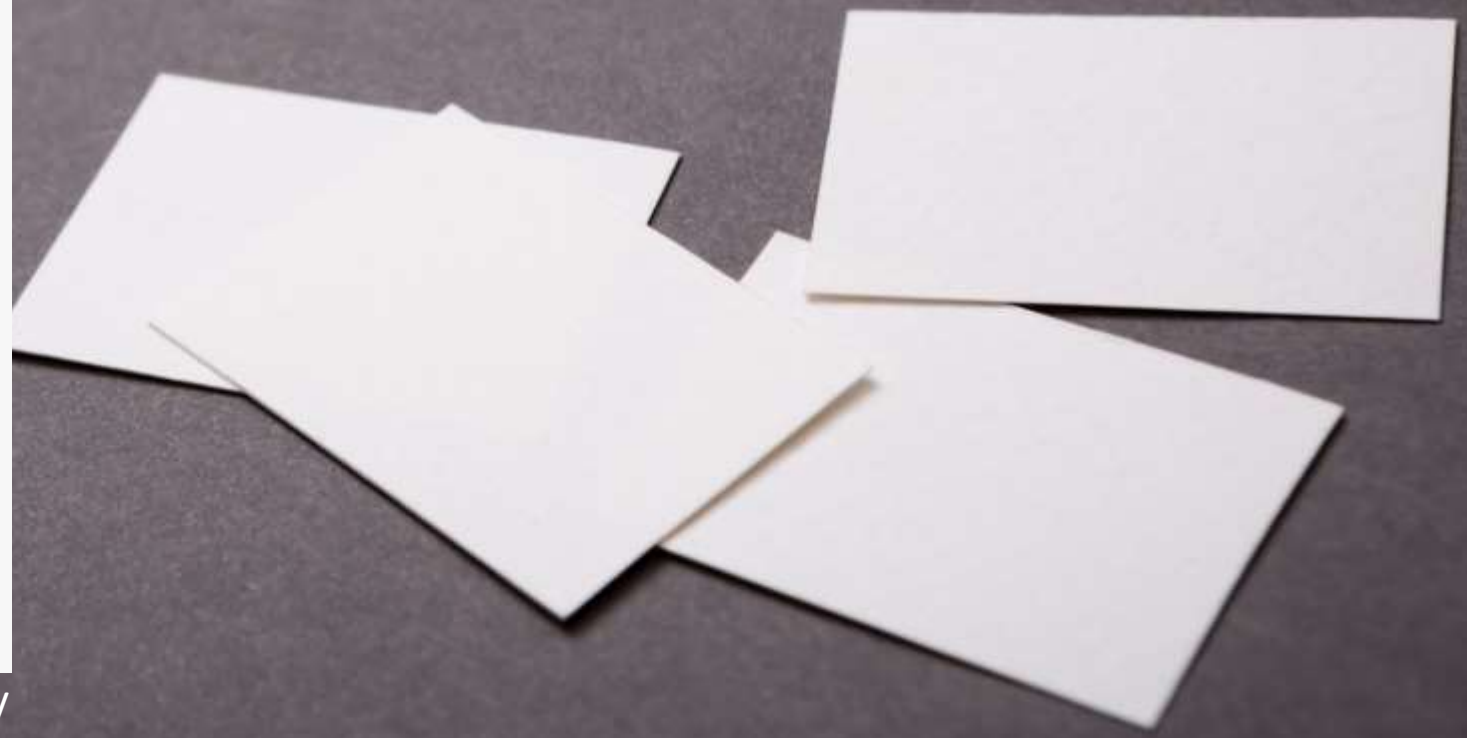
Name	Author	Language	Difficulty	Platform	Date	Solution	Comments
racecars	chillywilly	C/C++	2	Unix/linux etc.	1:46 AM 03/22/2020	0	1
admin_panel	BitFriends	C/C++	2	Unix/linux etc.	11:10 AM 03/20/2020	0	0
Tr1cky Cr4ckm3	BinaryNewbie	C/C++	4	Unix/linux etc.	7:59 PM 03/18/2020	0	0
WhatDOyouLove	Terminal_junkie	C/C++	2	Windows	7:49 PM 03/18/2020	0	1
Very Special Number v1	owo_whats_this	C/C++	2	Unix/linux etc.	11:42 PM 03/12/2020	0	0
Password Keeper	n30np14gu3	C/C++	3	Windows	2:36 PM 03/11/2020	2	5
CrackMe (FujiFuscator 1.2)	Charliezkie	.NET	4	Windows	9:55 AM 03/11/2020	0	0
Keyg3n_M1#1	Shad3	C/C++	1	Multiplatform	9:01 PM 03/09/2020	0	1

https://crackmes.one/lasts

Skąd **pliki?**

- ANY.RUN: Registration required
- Contagio Malware Dump: Password required
- CAPE Sandbox
- Das Malwerk
- FreeTrojanBotnet: Registration required
- Hybrid Analysis: Registration required
- KernelMode.info: Registration required
- MalShare: Registration required
- Malware.lu's AVCaesar: Registration required
- Malware DB
- Objective-See Collection: Mac malware
- PacketTotal: Malware inside downloadable PCAP files
- SNDBOX: Registration required
- theZoo aka Malware DB
- URLhaus: Links to live sites hosting malware
- VirusBay: Registration required
- Virusign
- VirusSign: Registration required

https://zeltser.com/malware-sample-sources/

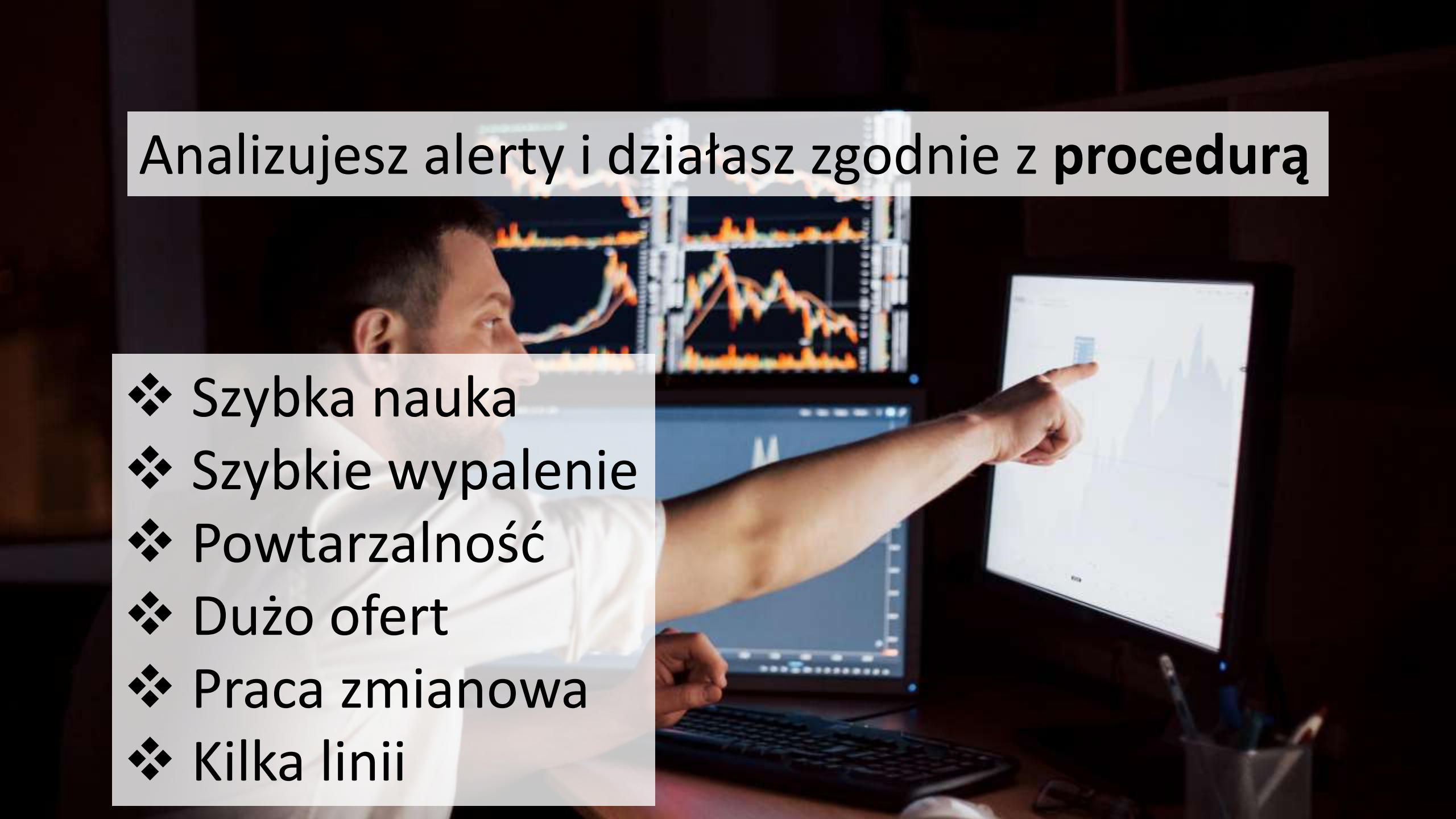


Nie zawsze masz **dostęp** do kodu źródłowego

1. IOT
2. Windows
3. Iphone


SOC

Analizujesz alerty i działasz zgodnie z **procedurą**



- Szybka nauka
- Szybkie wypalenie
- Powtarzalność
- Dużo ofert
- Praca zmianowa
- Kilka linii


SOC działa na podstawie **alertów**
Threat Hunting próbuje działać proaktywnie

Dużo rzeczy **nie znasz**:

- Bo są oparte na sprzęcie
- Bo są dostępne dla firm
- Bo są drogie
- Bo są wewnętrznymi narzędziami

Adam Lange

VP, Head of Cyber Threat Hunting

Standard Chartered Bank

https://www.youtube.com/watch?v=Msh4i-vIfB4

- ❑Czy nie loguje się ktoś z zagranicy
- ❑Czy nie zarejestrowano domeny podobnej do naszej
- ❑Czy administrator nie wykonuje podejrzanych operacji

Welcome to YARA's documentation!

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

The above rule is telling YARA that any file containing one of the three strings must be reported as silent_banker. This is just a simple example, more complex and powerful rules can be created by using wild-cards, case-insensitive strings, regular expressions, special operators and many other features that you'll find explained in this documentation.

Contents:

https://yara.readthedocs.io/en/stable/

MITRE | ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute

Search

Jak **działają** przestępcy

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Accou Manipula						Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash His	Discovery	Software	Collection	Removable Media	Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
		cit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery

https://attack.mitre.org/

Brute Force

Adversaries may use brute force techniques to attempt access to accou
unknown or when password hashes are obtained.

Credential Dumping is used to obtain password hashes, this may only g
when Pass the Hash is not an option. Techniques to systematically gue
compute hashes are available, or the adversary may use a pre-compute
hashes. Cracking hashes is usually done on adversary-controlled syster
network. [1]

Adversaries may attempt to brute force logins without knowledge of pa
an operation either with zero knowledge or by attempting a list of know
This is a riskier option because it could cause numerous authentication
lockouts, depending on the organization's login failure policies. [2]

A related technique called password spraying uses one password (e.g.
list of passwords, that matches the complexity policy of the domain an
used password. Logins are attempted with that password and many dif
network to avoid account lockouts that would normally occur when brut
account with many passwords. [3]

Procedure Examples

Name	Description
APT3	APT3 has been known to brute force password hashes to be able to leve
APT33	APT33 has used password spraying to gain access to target systems.[28]
APT41	APT41 performed password brute-force attacks on the local admin accou
Chaos	Chaos conducts brute force attacks against SSH services to gain initial a
China Chopper	China Chopper's server component can perform brute force password gu
Dragonfly 2.0	Dragonfly 2.0 dropped and executed tools used for password cracking, in
Emotet	Emotet has been observed using a hard coded list of passwords to brute

https://attack.mitre.org/techniques/T1110/

Informatyka śledcza

- Sprzęt/licencje
- Dobra znajomość systemu
- Poszukiwanie metadanych, logów, plików tymczasowych
- Jak/kiedy/gdzie się włamano
- Urządzenia mobilne
- Rekonstrukcja macierzy
- Współpraca z policją
- Znajomość prawa

Fuzzing

(losowe dane do programu)

Szukanie błędów w:

- ✓Chrome
- ✓Windows
- ✓Office

Zgodność ze standardami

ISO/IEC 27001

RODO

PCI SDD

CISSP

Wykaz certyfikatów uprawniających do przeprowadzenia audytu.

Dz.U.2018.1999

ROZPORZĄDZENIE

MINISTRA CYFRYZACJI 1

z dnia 12 października 2018 r.

w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

Na podstawie art. 15 ust. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) zarządza się, co następuje:

§ 1. Rozporządzenie określa wykaz certyfikatów uprawniających do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stanowiący załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

ZAŁĄCZNIK

WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZANIA AUDYTU

1. Certified Internal Auditor (CIA);

2. Certified Information System Auditor (CISA);

Architektura aplikacji Threat Modeling

(bezpieczeństwo na etapie projektowania)

Czytaj, **ćwicz**, powtarzaj

https://security.szurek.pl

postMessage

Zabezpiecz **wymienianie danych** pomiędzy różnymi domenami przy użyciu **JavaScript**.

PODCAST

BadWPAD

Atak BadWPAD, dzięki któremu można podsłuchiwać i modyfikować niezaszyfrowany ruch internetowy na twoim komputerze.

16-03-2020 8 MINUT

PODCAST

Skutki XSS

Jak wytłumaczyć błąd typu XSS prezesowi firmy? Może pokazując jego skutki dla organizacji? Opowiedz o XSS worm – czyli kawałku kodu, który zaraża innych użytkowników, podobnie jak grypa w świecie rzeczywistym.

09-03-2020 9 MINUT

ODODOPENTESTERA

Problematyczne znaki UTF - Unicode Case Mapping Collisions

Zamiana liter z dużych na małe to prosta operacja, no chyba, że korzystasz z UTF 8. Czy może być niebezpieczna? Czy słyszałeś o Unicode Case Mapping Collisions?

24-02-2020 4 MINUT

PODCAST

XS-leaks - Cross Site Leaks

Błędy tego rodzaju w specyficznych okolicznościach pozwalają na odpowiedź tak/nie na zadane wcześniej pytanie. Na pozór wydaje się zatem, że to nic nie znacząca klasa podatności. Ale czy aby na pewno?

17-02-2020 9 MINUT