

Jak zostać pentesterem?



Kacper Szurek

o bezpieczeństwie dla wszystkich

STRONA GŁÓWNA TAGI O MNIE ENGLISH

YouTube Facebook @KacperSzurek Newsletter

Obsługa wielu serwerów



TrustedUserCAKeys /etc/ssh/cas.pub



pentestera

Obsługa wielu serwerów SSH

Poznaj opcję TrustedUserCAKeys, którą możesz skonfigurować w SSH.

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



Bezpieczeństwo pracy zdalnej

Kacper Szurek
<https://www.kasperszurek.pl>

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



BadWPAD

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

```
121 <div class="text-center">
122 <h5>About Us</h5>
123 <h2>หัวข้อข่าวจาก กรุงเทพ โลกวันนี้</h2>
124 <p>หัวข้อข่าวจาก กรุงเทพ โลกวันนี้ หัวข้อข่าวที่น่าสนใจ มีดังนี้</p>
125 <p>หัวข้อข่าวจาก กรุงเทพ โลกวันนี้ หัวข้อข่าวที่น่าสนใจ มีดังนี้</p>
126 <p>หัวข้อข่าวจาก กรุงเทพ โลกวันนี้ หัวข้อข่าวที่น่าสนใจ มีดังนี้</p>
127 </div>
128 <div class="card">
129 
130 <div class="card-body">
131 <h5 class="card-title">Card title that wraps to a new line</h5>
132 <p class="card-text">This is a longer card with supporting text below as a natural lead-in to
133 additional content. This content is a little bit longer.</p>
134 <p class="card-text"><small class="text-muted">Last Update</small></p>
135 </div>
136 </div>
137 <div class="card p-3">
138 <blockquote class="blockquote mb-0 card-body">
139 <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer posuere erat a ante.</p>
140 <div class="card-body">
141 <div class="card-body">
142 <div class="card-body">
143 <div class="card-body">
144 <div class="card-body">
145 <div class="card-body">
146 <div class="card-body">
147 <div class="card-body">
148 <div class="card-body">
149 <div class="card-body">
150 <div class="card-body">
151 <div class="card-body">
152 <div class="card-body">
153 <div class="card-body">
154 <div class="card-body">
155 <div class="card-body">
156 <div class="card-body">
157 <div class="card-body">
158 <div class="card-body">
159 <div class="card-body">
160 <div class="card-body">
161 <div class="card-body">
162 <div class="card-body">
163 <div class="card-body">
```

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

Table of Contents

TOC - About OWASP	1
FW - Foreword	2
I- Introduction	3
RN - Release Notes	4
Risk - Application Security Risks	5
T10 - OWASP Top 10 Application Security Risks – 2017	6
A1:2017 - Injection	7
A2:2017 - Broken Authentication	8
A3:2017 - Sensitive Data Exposure	9
A4:2017 - XML External Entities (XXE)	10
A5:2017 - Broken Access Control	11
A6:2017 - Security Misconfiguration	12
A7:2017 - Cross-Site Scripting (XSS)	13
A8:2017 - Insecure Deserialization	14
A9:2017 - Using Components with Known Vulnerabilities	15
A10:2017 - Insufficient Logging & Monitoring	16
+D - What's Next for Developers	17
+T - What's Next for Security Testers	18
+O - What's Next for Organizations	19
+A - What's Next for Application Managers	20
+R - Note About Risks	21
+RF - Details About Risk Factors	22
+DAT - Methodology and Data	23
+ACK - Acknowledgements	24

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

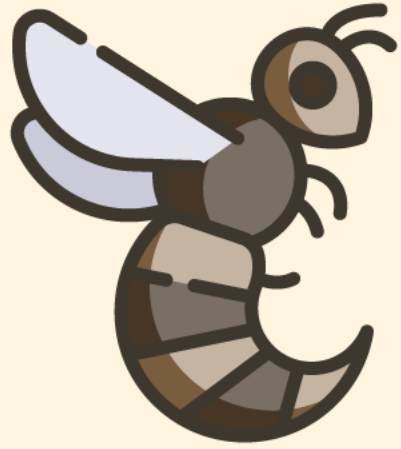
Injection

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.	



OWASP TOP10



#1 INJECTION

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



Flagship Projects

- OWASP Amass
- OWASP Application Security Verification Standard
- 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/>

Request

Raw Headers Hex

```
GET / HTTP/1.1
Host: security.szurek.pl
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1;
Win64; x64; Trident/5.0)
Connection: close
```

Modyfikacja żądań

(wyślij coś żeby zepsuć aplikację)

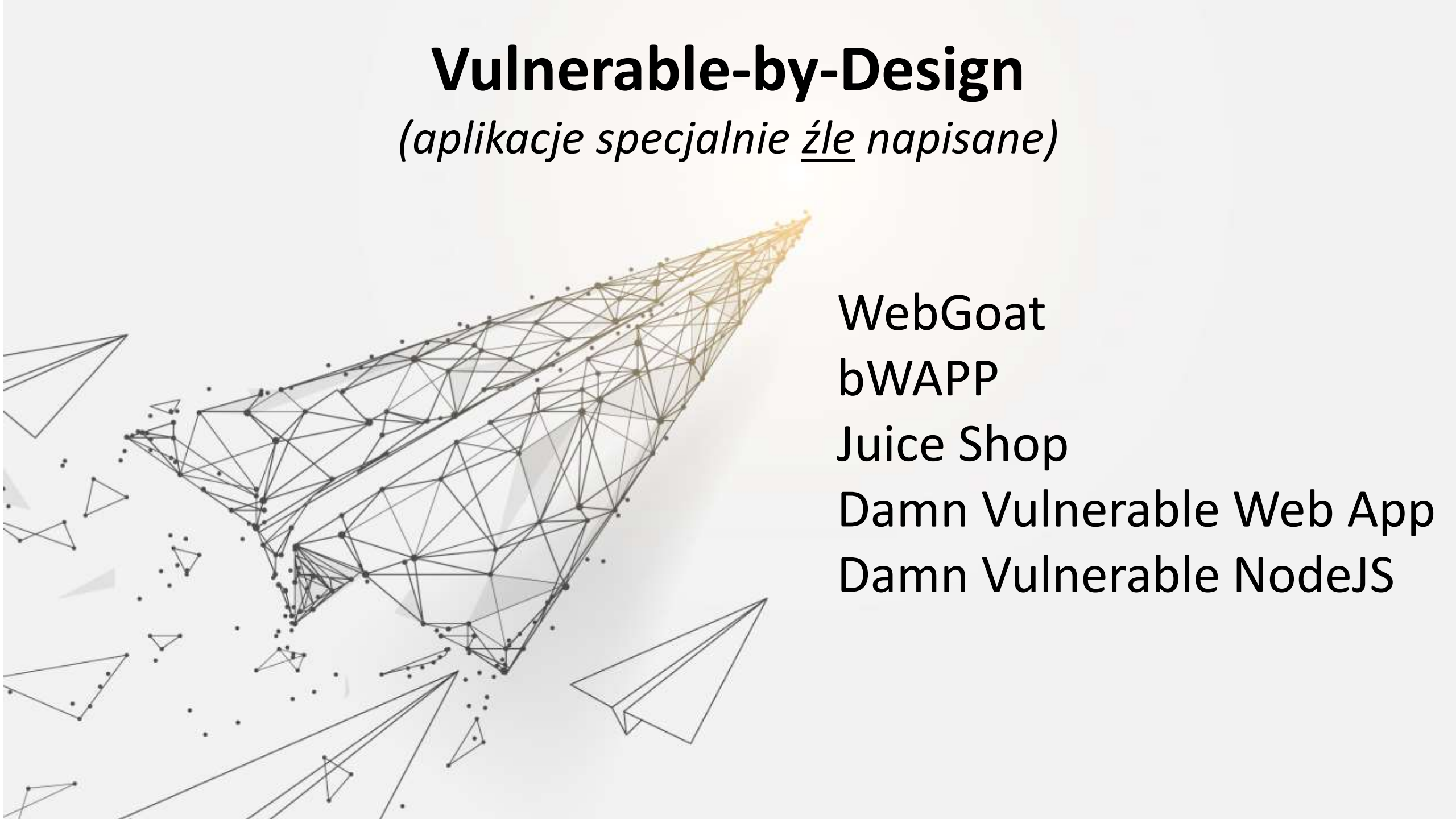
Response

Raw Headers Hex HTML Render

```
<div class="site-header-content">
<h1 class="site-title">
Kacper Szurek
</h1>
<h2 class="site-description">0 bezpieczeństwo dla wszystkich</h2>
</div>
<nav class="site-nav">
<div class="site-nav-left"><ul class="nav" role="menu"><li class="nav-home" role="menuitem"><a
href="/">Strona główna</a></li>
<li class="nav-home" role="menuitem"><a href="/tag/">Tagi</a></li>
<li class="nav-about" role="menuitem"><a href="/omnie/">0 mnie</a></li>
<li class="nav-about" role="menuitem"><a href="/en">English</a></li></ul><div id="search-searchbar"></div>
</div>
<div class="site-nav-right">
<div class="soli"><a class="soli" href="https://www.youtube.com/c/KacperSzurek" target="_blank"
rel="noopener">YouTube</a><a class="soli" href="https://facebook.com/groups/od0dopentestera/"
target="_blank" rel="noopener">Facebook</a>
<a class="soli" href="https://twitter.com/KacperSzurek" target="_blank" rel="noopener">@KacperSzurek</a><a
class="subscribe-button" href="/newsletter.html">Newsletter</a></div>
</div>
</nav>
</div>
</header>
<main class="site-main outer" role="main">
<div class="inner">
<section class="subscribe-form subscribe-form-main"><a class="subscribe-form-close
subscribe-form-close-main"></a><h3 class="subscribe-form-title">Newsletter</h3>
<p>Otrzymuj najnowsze wpisy wprost na swoją skrzynkę</p>
<p class="subscribe-error-message"></p>
<form action="https://newsletter.od0dopentestera.pl" accept-charset="utf-8" method="post">
<div class="form-group">
<input type="hidden" name="where" id="subscribe-form-where" value="main" />
<input type="hidden" name="ajax" value="0" />
<input type="hidden" name="lang" id="subscribe-form-lang" value="pl" />
<input class="subscribe-email" type="email" name="email" placeholder="twojemail@example.com">
</div>
<button type="submit" id="newsletter_submit">Zapisz się</button>
</form>
```


Vulnerable-by-Design

(aplikacje specjalnie źle napisane)

The background features a complex, abstract geometric design. A large, elongated wireframe structure, resembling a stylized arrow or a series of interconnected triangles, points towards the top right. It is composed of numerous small dots connected by thin lines. Several smaller, similar wireframe structures are scattered around the main one. In the bottom right corner, there is a simple line drawing of a paper airplane. The overall aesthetic is technical and modern, with a light gray and white color palette.

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



Home
AMA
Challenges
Cheatsheets
Conference notes
The 5 Hacking NewsLetter
The Bug Hunter Podcast
Tips & Tricks
Tutorials
About
Contact
List of bug bounty writeups
Subscribe

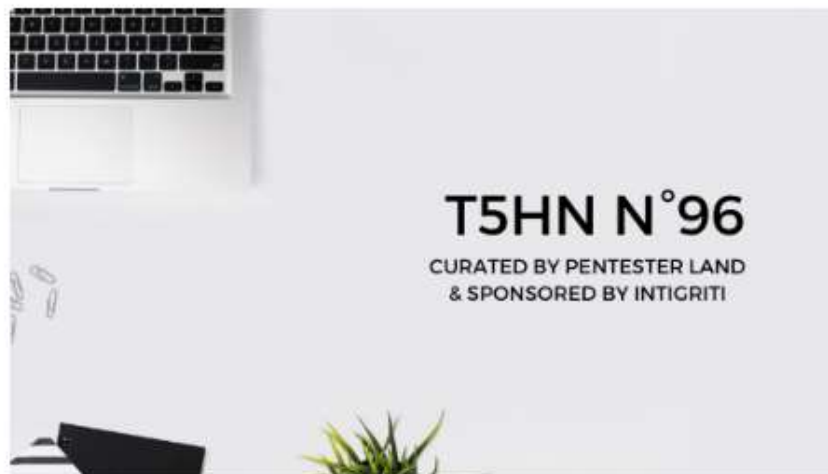


The 5 Hacking NewsLetter 96

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 <https://pentester.land/> d many recon tools, automates many recon <https://pentester.land/> cloud resources discovery and basic

 Comment  Share  Save ...

↑
130
↓

Posted by u/_vavkamil_ 2 days ago

Reverse engineering Blind's API and client side encryption

blog.jldc.me/posts/...

 10 Comments  Share  Save ...

↑
22
↓

Posted by u/rizemon 2 days ago

HackTheBox: Forest - Writeup by rizemon

rizemon.github.io/hackth...

 1 Comment  Share  Save ...

↑
209
↓

Posted by u/Mysterii8 2 days ago

LeakLooker GUI — Discover, browse and monitor database/source code leaks.

medium.com/@woj_c...

 5 Comments  Share  Save ...

↑
17
↓

↩ Crossposted by u/resynth1943 2 days ago

Telekom and Telefonica collecting users' data

[/r/Linu...](#)

[r/LinuxCafe](#) · Posted by u/TheEvilSkely Mod of all 2 days ago

Telekom and Telefonica collecting users' data

 **PSA:** To all German users, starting from tomorrow (2020-03-22), Telekom and Telefonica providers **will hand over**

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

JavaScript without parentheses using DOMMatrix

23 March 2020

```
matrix;  
x.a=1337;  
matrix=alert;  
location='javascript'+':'+x
```

GENERATE

Top 10 web hacking techniques of 2019

WEB HACKING TECHNIQUES

TOP
10

SVG animate XSS vector

28 January 2020

DOM Clobbering strikes back

06 February 2020



Breaking the chains

on HTTP Re <https://portswigger.net/>

Cracking

HA, Turbo

XS-Leak: Detecting IDs using Portal



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

* 

* Something that's really worth your time!

URL: <https://blog.sheddown.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>



Rafael Cintra @RafaelCintraSec · 19 mar

XSS Payload JSON:

```
"}}';alert('oBonito')</script>
```

#BugBounty #bugbountytips



1



57



118



Ali Tütüncü @alicanact60 · 20 mar

W odpowiedzi do @amayank77191

I use google dorks for finding reflected xss.

```
site:target[dot]com inurl:&
```

```
site:target[dot]com inurl:php
```

```
site:target[dot]com inurl:jsp
```

etc.. and I try find xss (I don't use any tool for find them)

#bugbountytips #bugbounty



1



18



46



Shahrukh Rafeeq @d3tonator · 13 g.

EasyBug but 80% dup | For New Hunter

Failure to Invalidate Session after Password Change

1. Login with the same account in `Chrome` and `Firefox` Simultaneously

2. Change the password in the `Chrome`

3. Go to `Firefox` and Update any info, If update, report then

#bugbountytips



6



15



60



<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/>



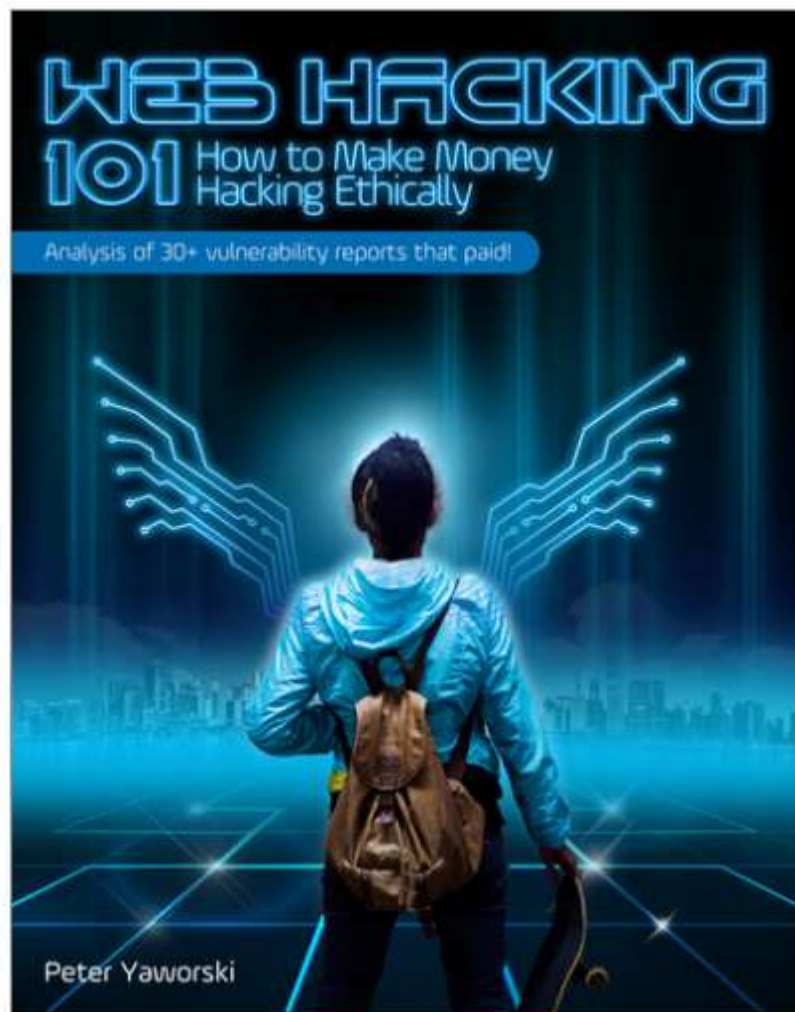
Certyfikaty:

- 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 wiedzę z Internetu



4. Open Redirect Vulnerabilities

Description

Examples

1. Shopify Theme Install Open Redirect
2. Shopify Login Open Redirect
3. HackerOne Interstitial Redirect

Summary

5. HTTP Parameter Pollution

Description

Examples

1. HackerOne Social Sharing Buttons
2. Twitter Unsubscribe Notifications
3. Twitter Web Intents

Summary

6. Cross-Site Request Forgery

Description

Examples

1. Shopify Twitter Disconnect
2. Change Users Instacart Zones
3. Badoo Full Account Takeover

Summary

7. HTML Injection

9. Cross-Site Scripting

Description

Examples

1. Shopify Wholesale
2. Shopify Giftcard Cart
3. Shopify Currency Formatting
4. Yahoo Mail Stored XSS
5. Google Image Search
6. Google Tagmanager Stored XSS
7. United Airlines XSS

Summary

10. Template Injection

Description

Server Side Template Injections

Client Side Template Injections

Examples

1. Uber Angular Template Injection
2. Uber Template Injection
3. Rails Dynamic Render

Summary

11. SQL Injection

Description

SQL Databases

Countermeasures Against SQLi

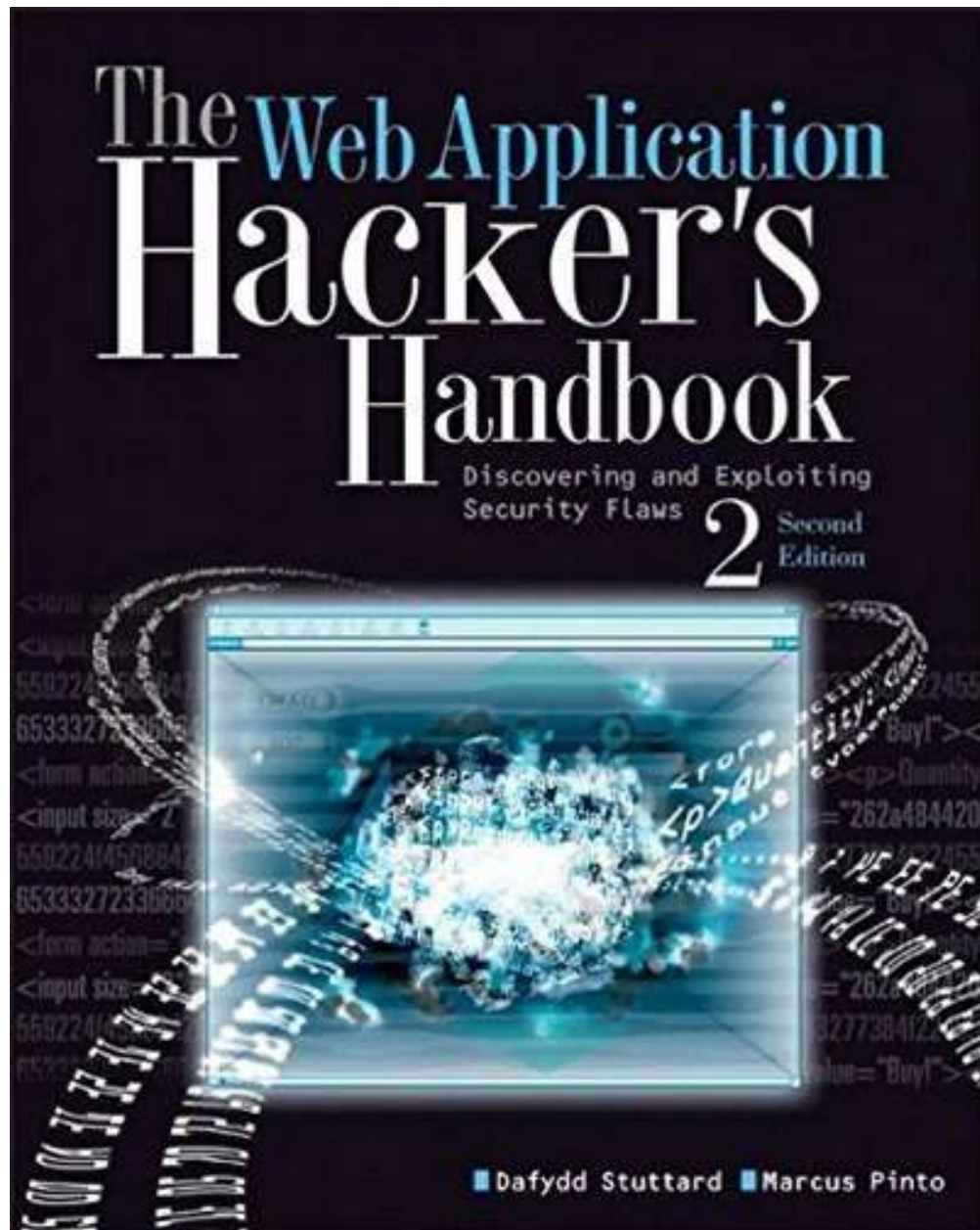


Podatności

- 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]



Introduction	xxiii
Chapter 1 Web Application (In)security	1
Chapter 2 Core Defense Mechanisms	17
Chapter 3 Web Application Technologies	39
Chapter 4 Mapping the Application	73
Chapter 5 Bypassing Client-Side Controls	117
Chapter 6 Attacking Authentication	159
Chapter 7 Attacking Session Management	205
Chapter 8 Attacking Access Controls	257
Chapter 9 Attacking Data Stores	287
Chapter 10 Attacking Back-End Components	357
Chapter 11 Attacking Application Logic	405
Chapter 12 Attacking Users: Cross-Site Scripting	431
Chapter 13 Attacking Users: Other Techniques	501
Chapter 14 Automating Customized Attacks	571
Chapter 15 Exploiting Information Disclosure	615
Chapter 16 Attacking Native Compiled Applications	633
Chapter 17 Attacking Application Architecture	647
Chapter 18 Attacking the Application Server	669
Chapter 19 Finding Vulnerabilities in Source Code	701
Chapter 20 A Web Application Hacker's Toolkit	747
Chapter 21 A Web Application Hacker's Methodology	791
Index	853

Type

Clear

Platform

Author

Port

Tag

webapps

Any

Begin typing...

Any

Any



Advanced

☐ Verified ☐ Has App

Show 15

Filters

Reset All

Zrozum co (i jak) robią inni

Search:

Date	D	A	V	Title	Type	Platform	Author
2020-03-23	↓		×	Joomla! com_hdwplayer 4.2 - 'search.php' SQL Injection	WebApps	PHP	qw3rTyTy
2020-03-23	↓		×	rConfig 3.9.4 - 'search.crud.php' Remote Command Injection	WebApps	PHP	Matthew Aberegg
2020-03-23	↓		×	FIBARO System Home Center 5.021 - Remote File Include	WebApps	Multiple	LiquidWorm
2020-03-20	↓		×	Exagate Sysguard 6001 - Cross-Site Request Forgery (Add Admin)	WebApps	PHP	Metin Yunus Kandemir
2020-03-18	↓		×	Netlink GPON Router 1.0.11 - Remote Code Execution	WebApps	Hardware	shellord
2020-03-16	↓		×	PHPKB Multi-Language 9 - 'image-upload.php' Authenticated Remote Code Execution	WebApps	PHP	Antonio Cannito
2020-03-16	↓		×	PHPKB Multi-Language 9 - Authenticated Directory Traversal	WebApps	PHP	Antonio Cannito
2020-03-16	↓		×	PHPKB Multi-Language 9 - Authenticated Remote Code Execution	WebApps	PHP	Antonio Cannito
2020-03-16	↓		×	MiladWorkShop VIP System 1.0 - 'lang' SQL Injection	WebApps	PHP	AYADI Mohamed
2020-03-16	↓		×	Enhanced Multimedia Router 3.0.4.27 - Cross-Site Request Forgery (Add Admin)	WebApps	ASP	Miguel Mendez Z
2020-03-10	↓		×	Horde Groupware Webmail Edition 5.2.22 - Remote Code Execution	WebApps	PHP	Andrea Cardaci
2020-03-13	↓		×	Centos WebPanel 7 - 'term' SQL Injection	WebApps	Linux	Berke YILMAZ
2020-03-11	↓		×	Horde Groupware Webmail Edition 5.2.22 - PHAR Loading	WebApps	PHP	Andrea Cardaci
2020-03-11	↓		×	Horde Groupware Webmail Edition 5.2.22 - PHP File Inclusion	WebApps	PHP	Andrea Cardaci
2020-03-12	↓	🔍	×	rConfig 3.9 - 'searchColumn' SQL	WebApps	PHP	vikingfr

<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>



COMMANDER V.I.V.I.

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**

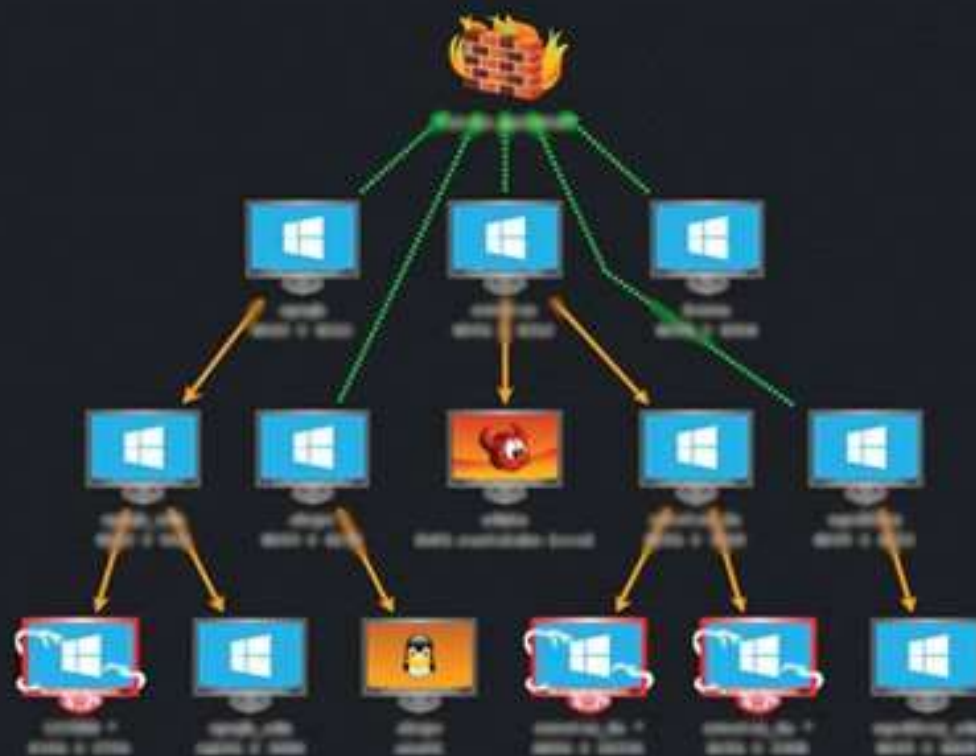
Points: **20**

Release: 10 Aug 2019

IP: 10.10.10.149



Hack The Box
PEN-TESTING LABS



[+] RastaLabs
Red Team Simulation Labs

IPPSEC

[Twitter](#) • [Patreon](#) • [Youtube](#)

metasp|

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>

GET MORE PWK

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

REGISTER



COURSE OVERVIEW

<https://www.offensive-security.com/pwk-oscip/>



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

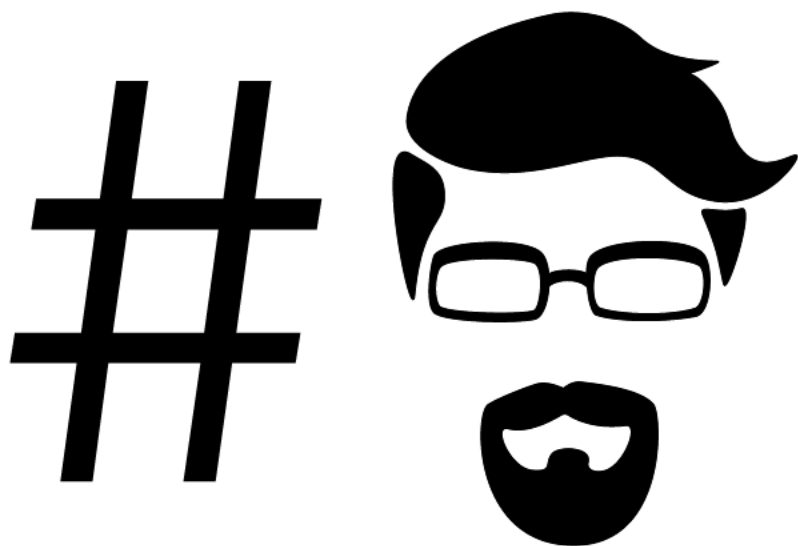
- Nie hakuj **bez pozwolenia**
- Nie żądaj pieniędzy
- Nie hejtuj



Bug Bounty

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





bug bounty

Szukanie błędów.

Jak zacząć?

pentester

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

Program	Launch date ↓	Reports resolved	Bounties minimum	Bounties average
 Culture.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 |



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

Reports resolved
8

Assets in scope
1

Average bounty
\$250-\$300

[Submit report](#)

Bug Bounty Program

Launched on Oct 2019

Managed by HackerOne

[Policy](#) [Hacktivity](#) [Thanks](#) [Updates \(0\)](#)

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 wolno a czego nie)

- 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"

http://www.



Security Hall of Fame

The following researchers have taken the time to identify and report security concerns with Selffy. 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](#)

Waqeesh 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



The image features two halves of a pineapple, cut lengthwise, positioned symmetrically on a solid yellow background. The pineapple halves are oriented vertically, with their green, spiky crowns at the top. The cut surfaces of the fruit are visible, showing the characteristic diamond-patterned texture of the pineapple flesh. A semi-transparent white rectangular box is centered over the middle of the image, containing the text "Szukanie to połowa pracy: raport".

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



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	cryptography	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

A hand holding a smartphone is the central focus, with a semi-transparent text box overlaid on the left. The background shows a blurred office environment with a laptop, a magnifying glass, and several potted plants on a desk.

Android/Iphone

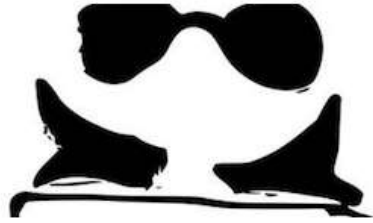
1. OWASP Mobile Security Testing Guide
2. Bezpieczeństwo API
3. Dekompilacja aplikacji
4. Jailbreak/root
5. SSL Pinning

The image features a solid teal background. In the top-left corner, there is a large white cloud. To its right, a smaller white cloud is positioned. In the top-right corner, there are two more white clouds of varying sizes. Along the bottom edge, there is a dense, layered row of white clouds, creating a horizon-like effect.

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>



Exploring the Power of Phished Persistent Cookies in AWS

Spencer Gietzen

AWS

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



CloudGoat Official
Walkthrough Series:
"rce_web_app"

AWS



Phishing Users with MFA on
AWS

AWS



CloudGoat 2: The New &
Improved "Vulnerable by
Design"
AWS Deployment Tool

AWS

<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/juliocezarfort/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 model¹. 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.

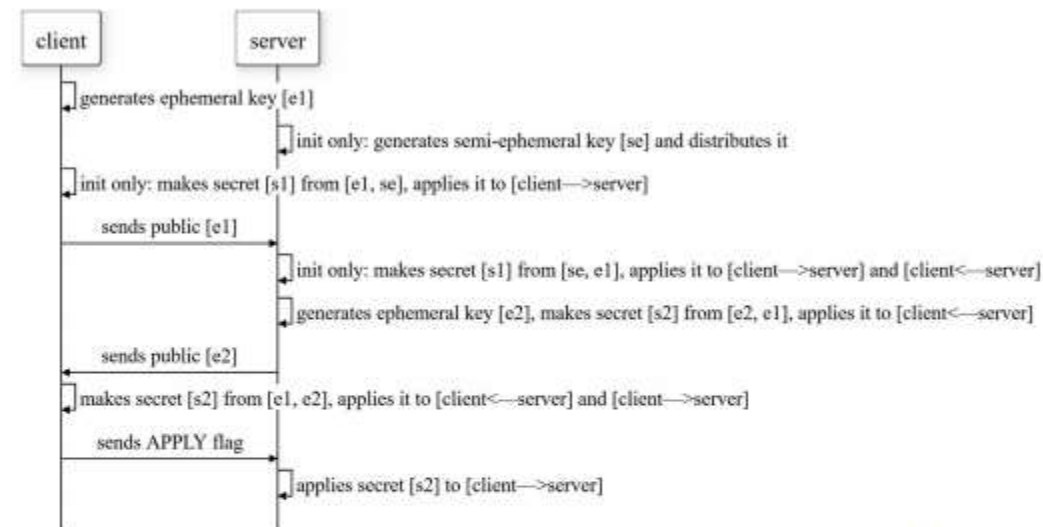


Fig.: Jess’ Diffie-Hellman secure channel protocol, based on the NK⁶ Noise Protocol Framework Handshake Pattern.

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 software⁷. The results were the following:

Result • authentication? Client -> Server: enc1: When the following values are mutated by the attacker:

$g_{e1} \rightarrow G^{nil}$ (originally G^{e1})
 enc1, sent by Client and resolving to $AEAD_ENC(G^{se^{e1}}, msg1, nil)$, is successfully used in primitive $AEAD_DEC(G^{nil^{se}}, AEAD_ENC(G^{se^{e1}},$

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



- 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



MALWARE UWAGA!!!

Możesz
stracić
dane



Public submissions

Significant tasks

Q Type hash or tag to search

Nie musisz uruchamiać
plików
na swoim komputerze

Windows 7 Professional 32bit 23 March 2020, 18:59	Malicious activity	Prepare your workforce for COVID - 19 Challenge.msg CDFV2 Microsoft Outlook Message covid19	MD5: 4BAC708197E1FA44AB881730A37D2A32 SHA1: 3E413022D990CEC3A745C7DF6F2CCCD4033EDC86 SHA256: 095C8D3BEA2ADEF05C1E1380E276FCFA06A5752093A86F510ADB33A818DC24
Windows 7 Professional 32bit 23 March 2020, 18:59	No threats detected	https://threatinsight.proofpoint.com/27c97bbb-955b-44e6-9040-6e282973b045/threat/email/de23261... Open in browser	MD5: DA7525256D4CCEB7CE88100AFF98C041 SHA1: D2912FDCE57D5018AD71049E7A4DAFB06414AA6D SHA256: 4369E602FDFB8FFC0C1F11214CCCA4599957A8CB73A9C53F98AE5601FC7AED49
Windows 7 Professional 32bit 23 March 2020, 18:59	Malicious activity	ZoomOutlookPluginSetup.msi Zoom V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 949, Title: Zoom Ou...	MD5: 753D6E66A881479873113292731FD882 SHA1: 1F700B516105B4E6932213DB18563F20F07300E5 SHA256: 021473E1C583362E2D5832B5539C162B81CC9DEBE1D05D0AFC471A84C74339C4
Windows 7 Professional 32bit 23 March 2020, 18:58	No threats detected	https://www2.wesnet.com/redirect?p=aaqqg61394 HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators	MD5: E6F00EDF3360D9E50A83E2914260C254 SHA1: 368C7C75C8A1135DE91C38087C492F87ED63CE15 SHA256: E39DF6FD9C8A1AC43B26DB3800AF8CA038C3986A85A857F1414FC21737E9A4C
Windows 7 Professional 32bit 23 March 2020, 18:58	No threats detected	http://23.95.132.48/~main/.lsuoxiso/w.php/lSeKTE1ZsfI3A Open in browser	MD5: 556D9CAAA785C1B0FF16367040DF9B83 SHA1: 0FE2C7B775A20262FC08E3B1463024AC95C18E7F SHA256: 4231280C94FC89743545CB418FAA081228890DB91D53867C133A82A96BC75C3A
Windows 7 Professional 32bit 23 March 2020, 18:58	No threats detected	https://uksouthr-notifyp.svc.ms:443/api/v2/tracking/method/Click?mi=dLGdS0x02EG_G1NCnxqtfg&tc=... Open in browser	MD5: 1F7FEC8C68B46E5AD66A8292B0368073 SHA1: B6A3F7C77370901810DFA39DDA25F50ABC5CF57B SHA256: E16F8E46490A00C6E85378276156E0633EB3DDAD2577AA39B5C16EC684DCD7E7
Windows 7 Professional 32bit 23 March 2020, 18:58	No threats detected	https://ulachu.com/event ASCII text	MD5: 3F979A2309A0EB82D68AA67288797039 SHA1: F63553E9410459D0FE3503EA707246EE2DC65F54 SHA256: F13C500F9F77E9BCE9C5AD514CD5EB9A657A7FFF1F60FF7A816441BFF02856CE
Windows 7 Professional 32bit 23 March 2020, 18:57	No threats detected	https://... Open in browser	MD5: 289BE6D062B320BC4B1E1FD06E0F0B7E SHA1: 32F85540B56D5971B3696D38E60E4947B862505B SHA256: E4030A66EFD0B72B00BAF66848A3C5F6CFF5D24E24EBC58464F1A41968583D66
Windows 7 Professional 32bit 23 March 2020, 18:57	No threats detected	https://... Open in browser	MD5: 74231CC58BF4E1072B0258D8958F8BD8 SHA1: 82AEAC8610B755350859DDCDD59F866434069175 SHA256: 3AD8CC29E7605FC69EC7EAA6FF25FD53008A57C0EDB80C13769944ACAF00824
Windows 7 Professional 32bit 23 March 2020, 18:57	No threats detected	... PE32 executable (DLL) (GUI) Intel x86_64, for MS Windows	MD5: 62CB6A2A517351472698F669A845F91C SHA1: 31C2E2B490C944308A18675DA73B00E39F6FA626 SHA256: C25812F5C186F74EC606A928461601C305DA29E6C36B80CE0637CC44030F2C19
Windows 7 Professional 32bit 23 March 2020, 18:57	Malicious activity	http://loginhelper.co Open in browser	MD5: 0731BD8C9A01CE630BE97C46EC51B303 SHA1: 6AAD220276CCC89A53D5CE63EE5905E22E06FB1B SHA256: 62515EA29C8F641A88E978D063634A6D08FF94531EE3B4C1489AC0DB17963479
Windows 7 Professional 32bit 23 March 2020, 18:56	No threats detected	https://p0rddd1101.godaddy.com/ Open in browser	MD5: B88BAA463C7C38E6C10D826256DC1DEC SHA1: 9E441CCCA9C568AC8B1FC134A8765807EAF74DB2



1 OF 25527



Podszywanie się pod witryny



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:

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-unlockserves.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/>

Jak próbują Cię oszukać

OpenPhish

/ [Phishing Feeds](#) / [Global Phishing Activity](#)

Timely. Accurate. Relevant Threat Intelligence.

5,000+

active phishing URLs
discovered daily

1,000+

online accounts
at risk monthly

400+

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.jackchallen.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

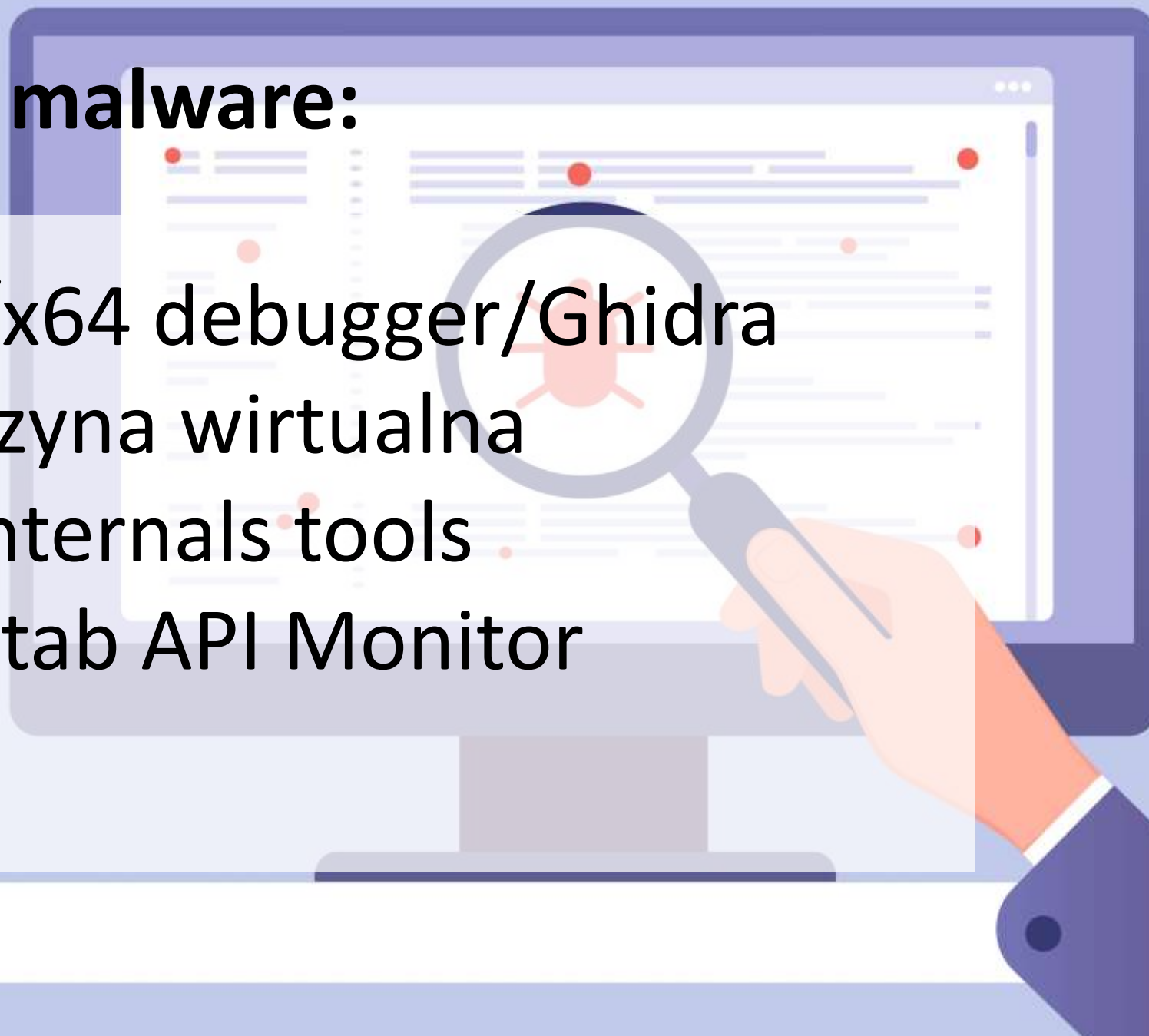
lista wystawionych certyfikatów SSL



Macro/JS/VBS

Analiza malware:

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



Asembler vs dekompilacja

wndproc proc near ; DATA XREF: sub_4010E0+210

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, 80h
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+3Cj
mov     ecx, [esp+0A4h+wParam]
mov     eax, ecx
and     eax, 0FFFFh
sub     eax, 68h
jz      short loc_40138A
dec     eax
jz      short loc_401371
```

```
HRESULT __stdcall wndproc(HWND hWnd, UINT Msg, WPARAM wParam, LPARAM lParam)
{
    HRESULT 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, 0x004u, &Buffer, 100);

    case 20:
        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;
```

Co robi aplikacja

API Capture Filter

All Modules

- [-] Messaging and Collaboration
- [-] Monitor Configuration
- [-] Netscape Portable Runtime
- [+] Network Security Services (NSS)
- [-] Networking
- [+] NT Native
- [-] Office Development
- [-] Security
- [+] System Services
 - [-] Device Services
 - [-] DLLs, Processes, and Threads
 - [+] File Services
 - [-] Backup
 - [-] Local File Systems
 - [-] Directory Management
 - [-] Disk Management
 - [+] File Management
 - [-] Advapi32.dll
 - [+] AddUsersToEncryptedFile
 - [-] CloseEncryptedFileRaw
 - [+] DecryptFileA
 - [-] DecryptFileW
 - [-] DuplicateEncryptionInfoFile
 - [-] EncryptFileA

Summary: 2375 Calls

#	TID	Module	API	Return	Error
1745	6716	kernel32.dll	NtQueryInformationProcess (GetCurrentProcess(), ProcessDefaultHa...	STATUS_SUCCESS	
1746	6716	kernel32.dll	NtSetInformationProcess (GetCurrentProcess(), ProcessDefaultHardE...	STATUS_SUCCESS	
1747	6716	kernel32.dll	NtQueryInformationProcess (GetCurrentProcess(), ProcessDefaultHa...	STATUS_SUCCESS	
1748	6716	kernel32.dll	NtSetInformationProcess (GetCurrentProcess(), ProcessDefaultHardE...	STATUS_SUCCESS	
1749	6716	VERSION.dll	CreateFileW ("C:\Programming\TortoiseSVN\Languages\TortoisePro...	INVALID_HANDLE_VALUE	2 = T
1750	6716	kernel32.dll	NtCreateFile (0x00000000000028b4b8, GENERIC_READ, SYNCHRON...	STATUS_OBJECT_NAME_NOT_F...	0xc00
1751	6716	kernel32.dll	CreateFileW (		0xc00
1752	6716	kernel32.dll	0x00000000000028b830 "C:\Programming\TortoiseSVN\Languages\TortoiseProc1033.dll",		
1753	6716	kernel32.dll	GENERIC_READ,		
1754	6716	kernel32.dll	FILE_SHARE_READ,		
1755	6716	kernel32.dll	NULL,		
1756	6716	kernel32.dll	OPEN_EXISTING,		
1757	6716	kernel32.dll	FILE_ATTRIBUTE_NORMAL,		
1758	6716	kernel32.dll	NULL		
1759	6716	kernel32.dll	NtClose (0x000000000000001a0)	STATUS_SUCCESS	
1760	6716	kernel32.dll	LdrGetDllHandle (NULL, NULL, 0x00000000000028da80, 0x000000000002...	STATUS_SUCCESS	
1761	6716	kernel32.dll	NtQueryKey (0x000000000000001a0, KeyNameInformation, NULL, 0, 0x...	STATUS_BUFFER_TOO_SMALL	0xc00
1762	6716	kernel32.dll	NtQueryKey (0x000000000000001a0, KeyNameInformation, 0x00000000...	STATUS_SUCCESS	

```
CreateFileW (  
0x00000000000028b830 "C:\Programming\TortoiseSVN\Languages\TortoiseProc1033.dll",  
GENERIC_READ,  
FILE_SHARE_READ,  
NULL,  
OPEN_EXISTING,  
FILE_ATTRIBUTE_NORMAL,  
NULL  
);
```

- [-] Direct3D 9
- [+] DirectX Audio
 - [-] DirectSound
 - [-] Functions
 - [-] Interfaces
 - [+] IDirectSound
 - [-] IDirectSound3DBuffer
 - [-] IDirectSound3DListener
 - [-] IDirectSound8
 - [-] IDirectSoundBuffer
 - [+] IDirectSoundBuffer8
 - [+] AcquireResources
 - [-] AddRef
 - [-] GetCaps
 - [-] GetCurrentPosition
 - [-] GetFormat

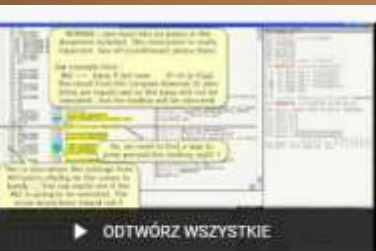
Reverse Engineering for Beginners



CONTENTS

1.12	Pointers	110
1.12.1	Swap input values	110
1.12.2	Returning values	111
1.13	GOTO operator	121
1.13.1	Dead code	124
1.13.2	Exercise	125
1.14	Conditional jumps	125
1.14.1	Simple example	125
1.14.2	Calculating absolute value	142
1.14.3	Ternary conditional operator	144
1.14.4	Getting minimal and maximal values	147
1.14.5	Conclusion	152
1.14.6	Exercise	153
1.15	switch()/case/default	154
1.15.1	Small number of cases	154
1.15.2	A lot of cases	167
1.15.3	When there are several case statements in one block	179
1.15.4	Fall-through	183
1.15.5	Exercises	184
1.16	Loops	185
1.16.1	Simple example	185
1.16.2	Memory blocks copying routine	196
1.16.3	Conclusion	199
1.16.4	Exercises	200
1.17	More about strings	201
1.17.1	strlen()	201
1.17.2	Boundaries of strings	212
1.18	Replacing arithmetic instructions to other ones	212
1.18.1	Multiplication	212
1.18.2	Division	217
1.18.3	Exercise	218
1.19	Floating-point unit	218
1.19.1	IEEE 754	218
1.19.2	x86	218
1.19.3	ARM, MIPS, x86/x64 SIMD	219
1.19.4	C/C++	219
1.19.5	Simple example	219
1.19.6	Passing floating point numbers via arguments	230
1.19.7	Comparison example	233
1.19.8	Some constants	267
1.19.9	Copying	267
1.19.10	tack, calculators and reverse Polish notation	267
1.19.11	x64	267
1.19.12	Exercises	267
1.20	Arrays	268
1.20.1	Simple example	268
1.20.2	Buffer overflow	275
1.20.3	Buffer overflow protection methods	283
1.20.4	One more word about arrays	286
1.20.5	Array of pointers to strings	287
1.20.6	Multidimensional arrays	293
1.20.7	Pack of strings as a two-dimensional array	300
1.20.8	Conclusion	304
1.21	By the way	304
1.21.1	Exercises	304

„Wypakowywanie” aplikacji (mniejszy rozmiar – dłuższe wykonywanie)



Reversing Tutorial For
newbies by lena151 all 40
videos in HD

26 105 wyświetleń • Ostatnia aktualizacja:
2019



Download All original files including Exercise files

Size - 139.59 Mb

Download Link - <http://bit.ly/1D14FRT>

If you can't Download from above link visit -

<http://bit.ly/1aHfodz>

- 1  A reversing tutorial for newbies by lena151 Part01.avi
Ranjeet Mewada 40:34
- 2  A reversing tutorial for newbies by lena151 Part02.avi
Ranjeet Mewada 26:42
- 3  A reversing tutorial for newbies by lena151 Part03.avi
Ranjeet Mewada 38:15
- 4  A reversing tutorial for newbies by lena151 Part04.avi
Ranjeet Mewada 24:48
- 5  A reversing tutorial for newbies by lena151 Part05.avi
Ranjeet Mewada 36:22
- 6  A reversing tutorial for newbies by lena151 Part06.avi
Ranjeet Mewada 31:49
- 7  A reversing tutorial for newbies by lena151 Part07.avi

<https://www.youtube.com/playlist?list=PLcFU5WYCxVYeR7AgsmjzGW6PjamaY6JO>

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
WhatD0youLove	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

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

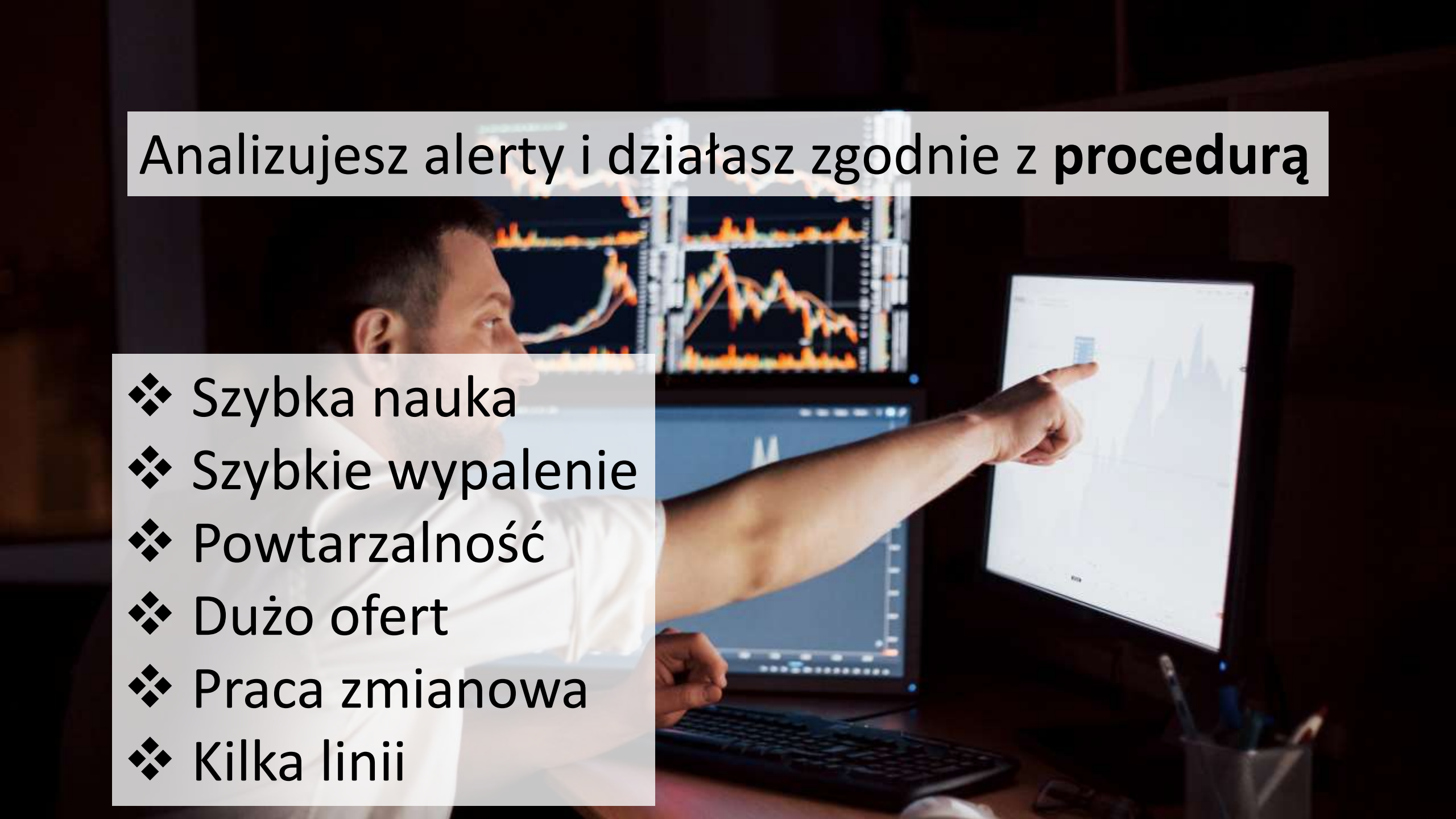
2.Windows

3.Iphone





soc

A man in a white shirt is sitting at a desk, pointing his right index finger at a computer monitor. The monitor displays a financial chart with a white background and blue lines. In the background, another monitor shows multiple colorful line charts (orange, yellow, green) on a dark background. The scene is dimly lit, with the primary light source being the computer screens.

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-vlfB4>





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

Getting started

Writing YARA rules

Modules

Writing your own modules

Running YARA from the command-line

Using YARA from Python

The C API

Support Read the Docs!

Please help keep us sustainable
by allowing our Ethical Ads in your ad
blocker or go ad-free by
subscribing.

Thank you! ❤️

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/>

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	Account Manipulation	Jak działają przestępcy					Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	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	Applnit 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	Applnit 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
			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

Brute Force

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

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

Adversaries may attempt to brute force logins without knowledge of password. This is a riskier option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies. [2]

A related technique called password spraying uses one password (e.g. a single password from a list of passwords, that matches the complexity policy of the domain and the user's used password. Logins are attempted with that password and many different users on the network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [3]

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

Procedure Examples

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

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

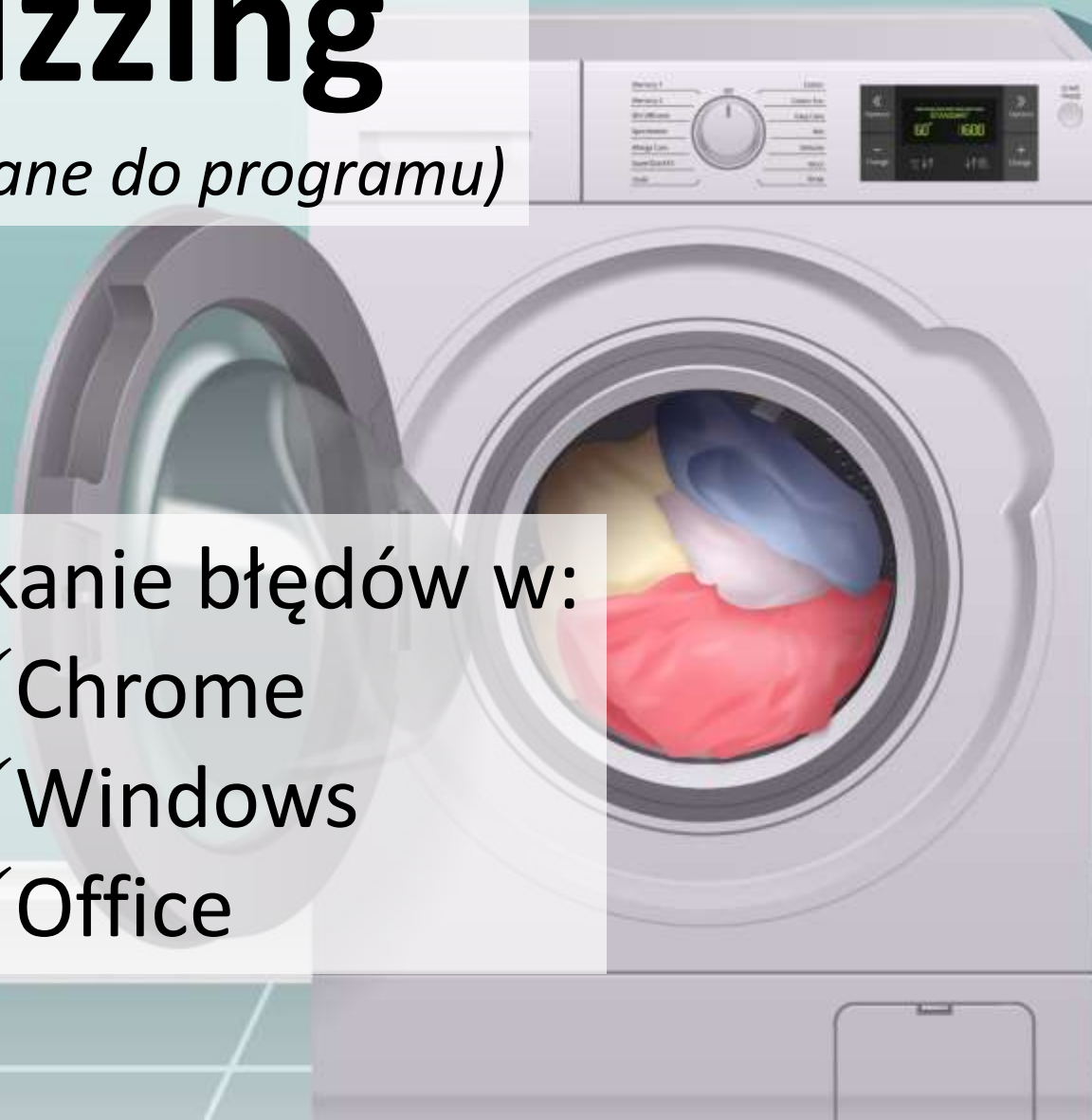


Fuzzing

(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 I

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);



The background is a detailed architectural floor plan of a house, featuring rooms like Kitchen, Bed 1, Bed 2, Bath, Spa, Sauna, and Deck. Various drafting tools are scattered around: a laptop keyboard in the top left, a pair of glasses in the top center, a compass and a pencil in the top right, a pencil and a calculator in the bottom left, and a rolled-up blueprint in the bottom right. A north arrow is also visible in the bottom right area.

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.

16-03-2020 8 MINUT



BadWPAD

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

16-03-2020 8 MINUT



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



Problematiczne 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



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 nie znacząca klasa podatności. Ale czy aby na pewno?

17-02-2020 9 MINUT