Веб-сервисы на страже безопасности

Сторчак Сергей

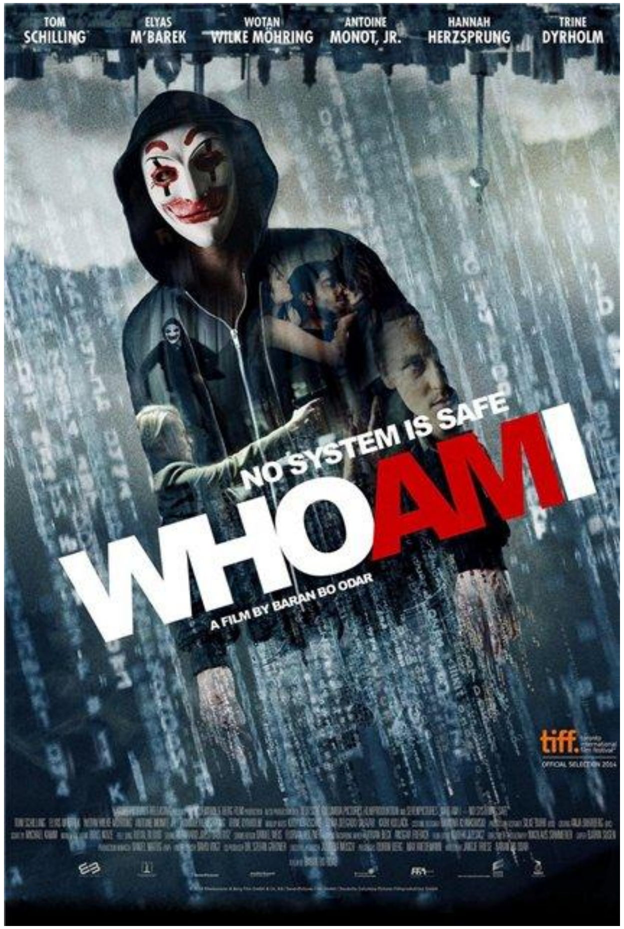
ser-storchak@mail.ru

Обо мне

аспирант ИКТИБ ИТА ЮФУ

специалист по защите информации ПАО «Таганрогбанк»

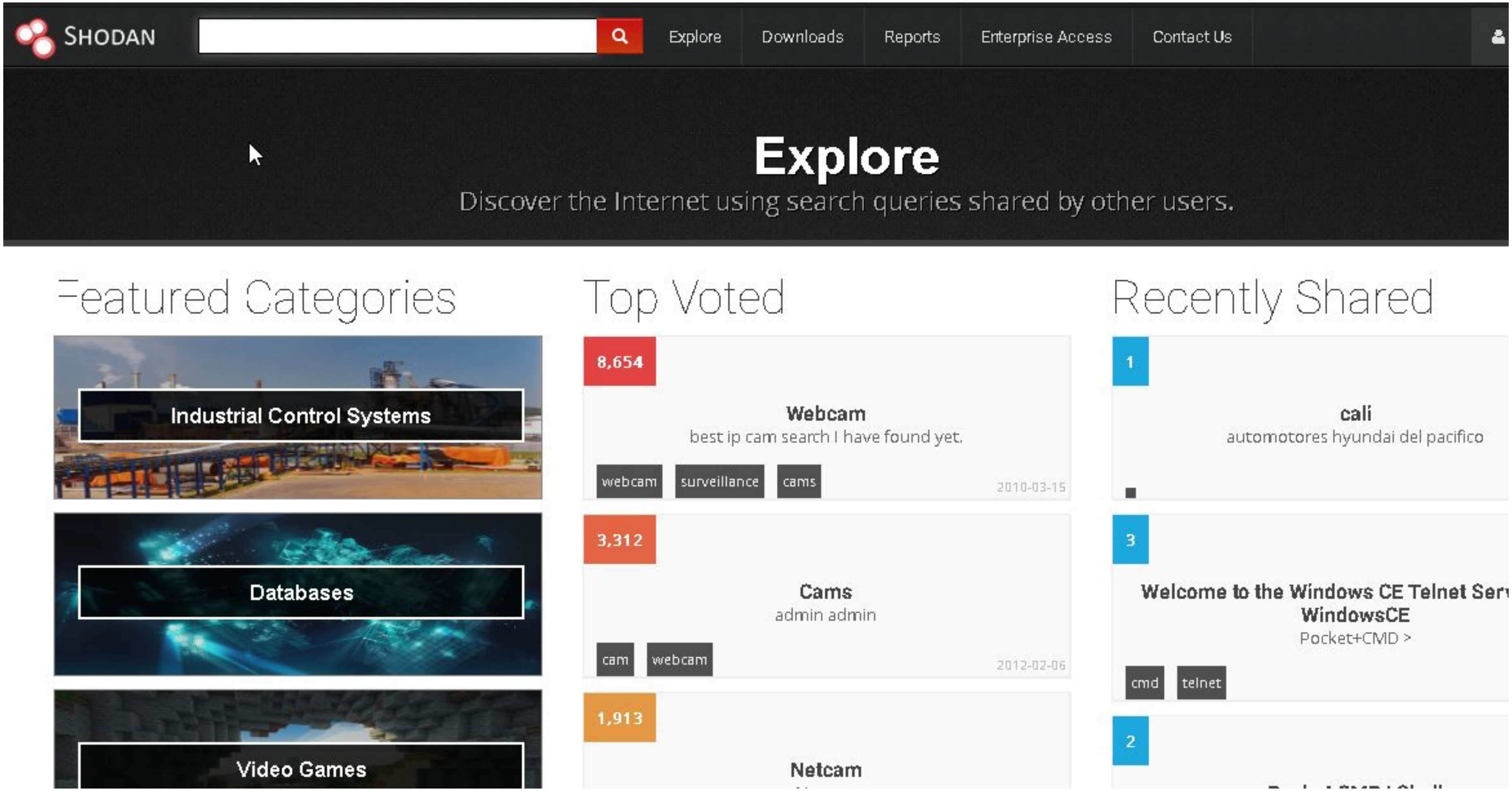
- ser-storchak.blogspot.ru
- vk.com/pentestnoob
- forum.pentestnoob.ru



Содержание

- Поисковые системы
  - Shodan, Censys, Vulners, Google
- Веб-сканеры
  - One button scan, SecurityHeaders.io, CSP Evaluator, SSL Server Test, Observatory, MageReport, ASafaWeb, Snyk, hackapp
- Агрегаторы утечек данных
  - Zone-H, Have I been pwned?, Leakedsource, Leakbase, 3WiFi: Карта точек доступа
- Проверка на вредоносность
  - ReScan.pro, VirusTotal, Koodous, No More Ransom, ID Ransomware, Virusinfo
- и прочее
  - Surfpatrol, Qualys BrowserCheck, Let's Encrypt, Is It Down Right Now?

Shodan



Explore

Discover the Internet using search queries shared by other users.

Featured Categories

Industrial Control Systems

Databases

Video Games

Top Voted

8,654

Webcam

best ip cam search I have found yet.

webcam surveillance cams 2010-03-15

3,312

Cams

admin admin

cam webcam 2012-02-06

1,913

Netcam

Recently Shared

1

cali

automotores hyundai del pacifico

3

Welcome to the Windows CE Telnet Serv

WindowsCE

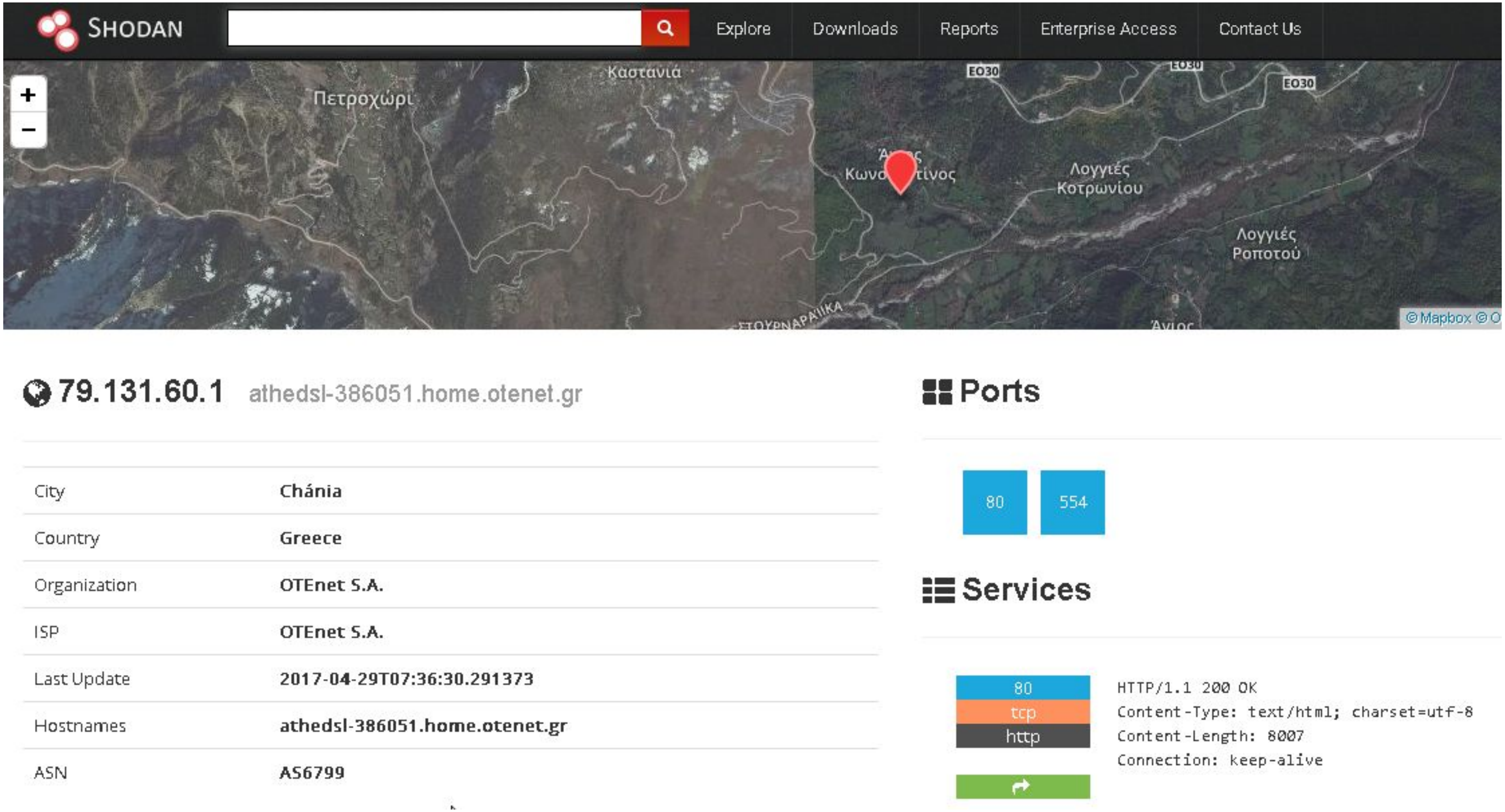
Pocket+CMD >

cmd telnet

2

https://www.shodan.io/

Shodan



79.131.60.1 athedsl-386051.home.otenet.gr

City	Chánia
Country	Greece
Organization	OTEnet S.A.
ISP	OTEnet S.A.
Last Update	2017-04-29T07:36:30.291373
Hostnames	athedsl-386051.home.otenet.gr
ASN	AS6799

Ports

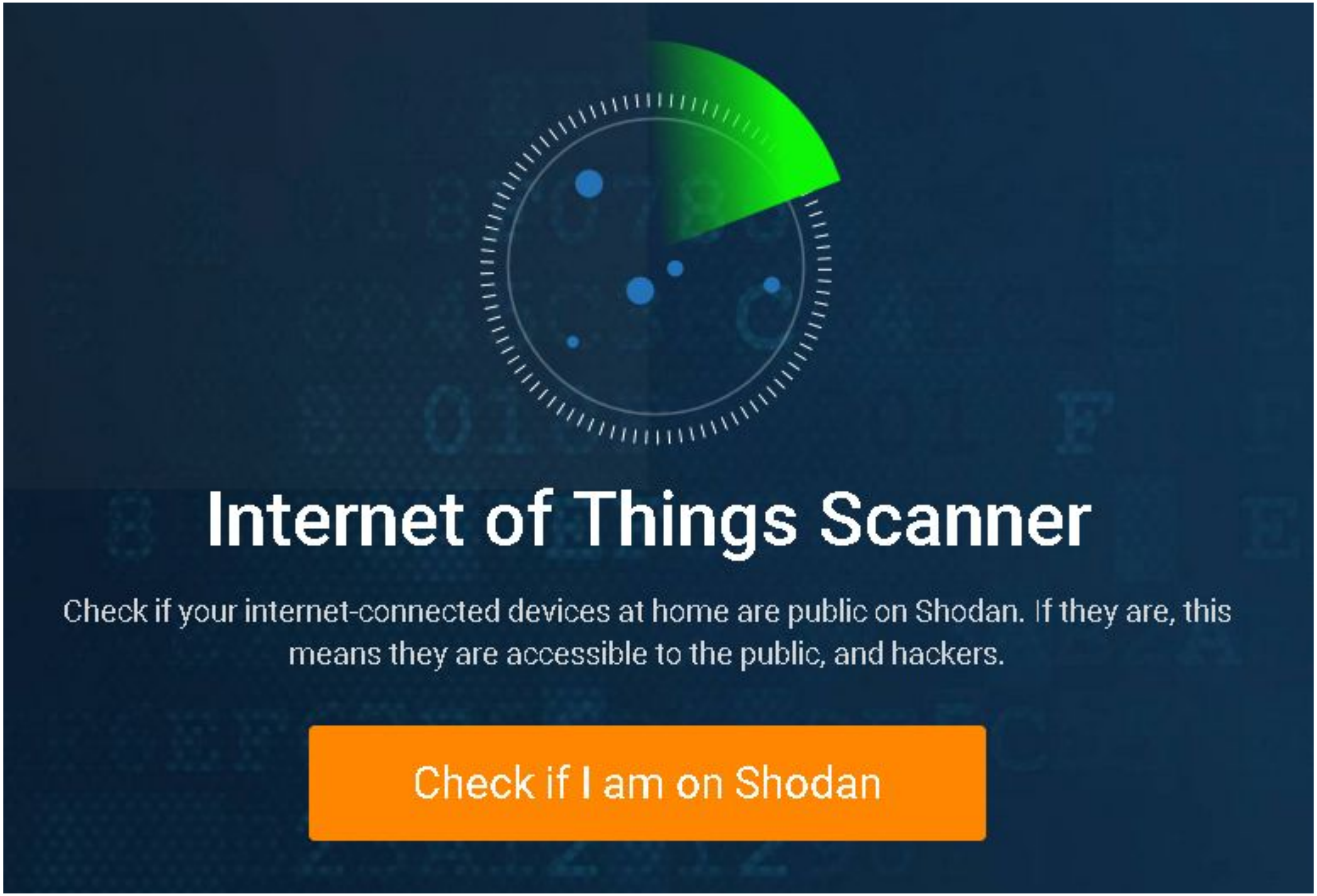
80 554

Services

80
tcp
http

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 8007
Connection: keep-alive
```

Internet of Things Scanner

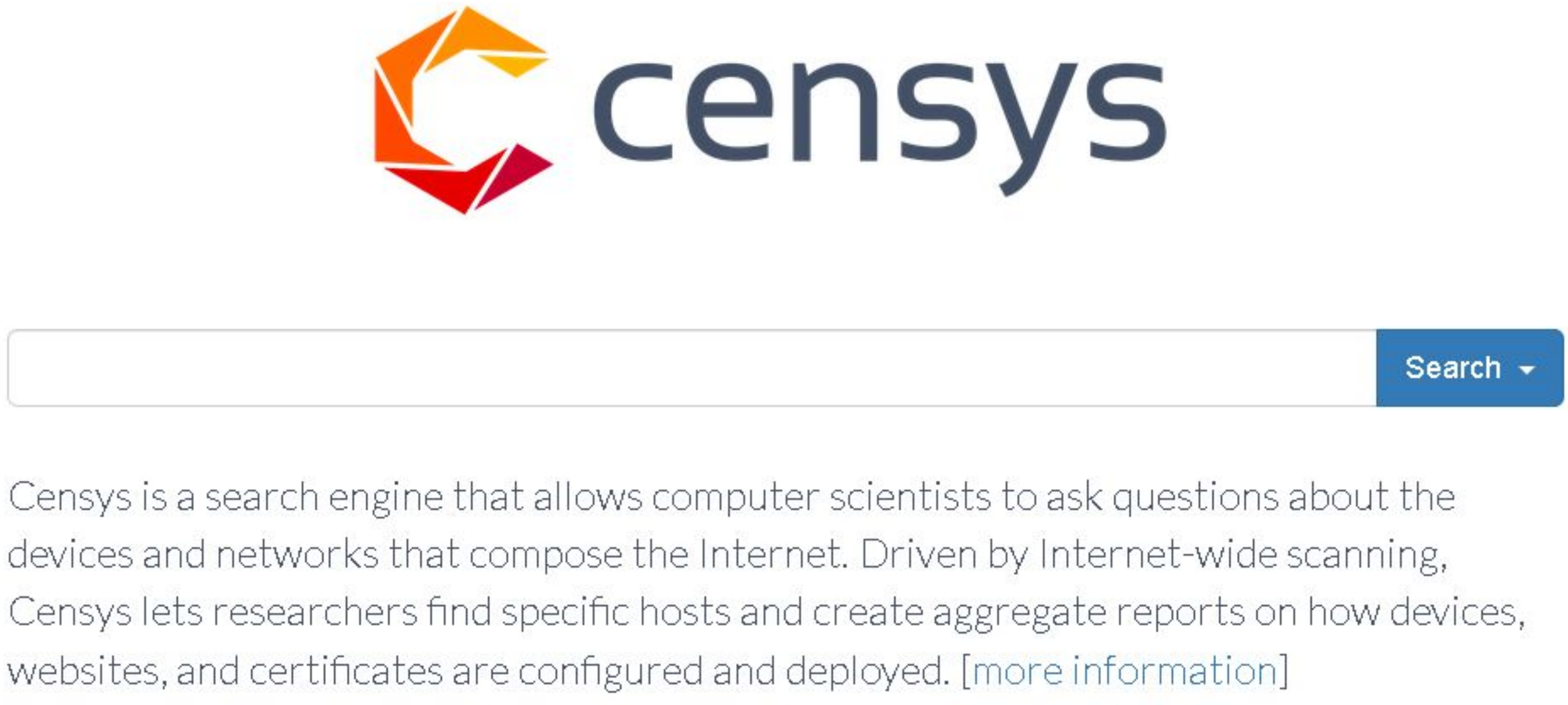


Internet of Things Scanner

Check if your internet-connected devices at home are public on Shodan. If they are, this means they are accessible to the public, and hackers.

http://iotscanner.bullguard.com/

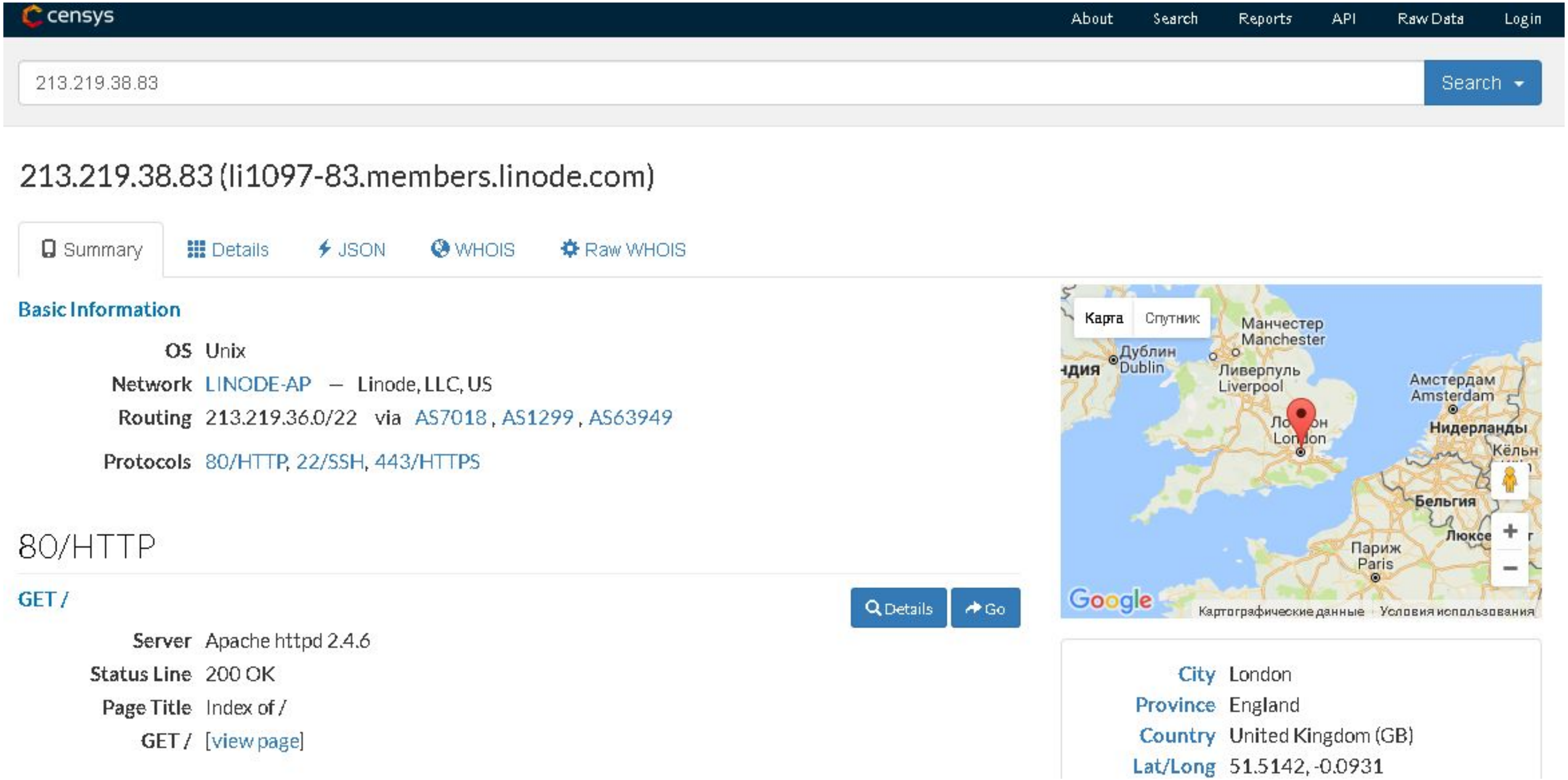
Censys



Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed. [more information]

https://censys.io/

Censys



213.219.38.83

213.219.38.83 (li1097-83.members.linode.com)

Basic Information

OS	Unix
Network	LINODE-AP — Linode, LLC, US
Routing	213.219.36.0/22 via AS7018 , AS1299 , AS63949
Protocols	80/HTTP, 22/SSH, 443/HTTPS

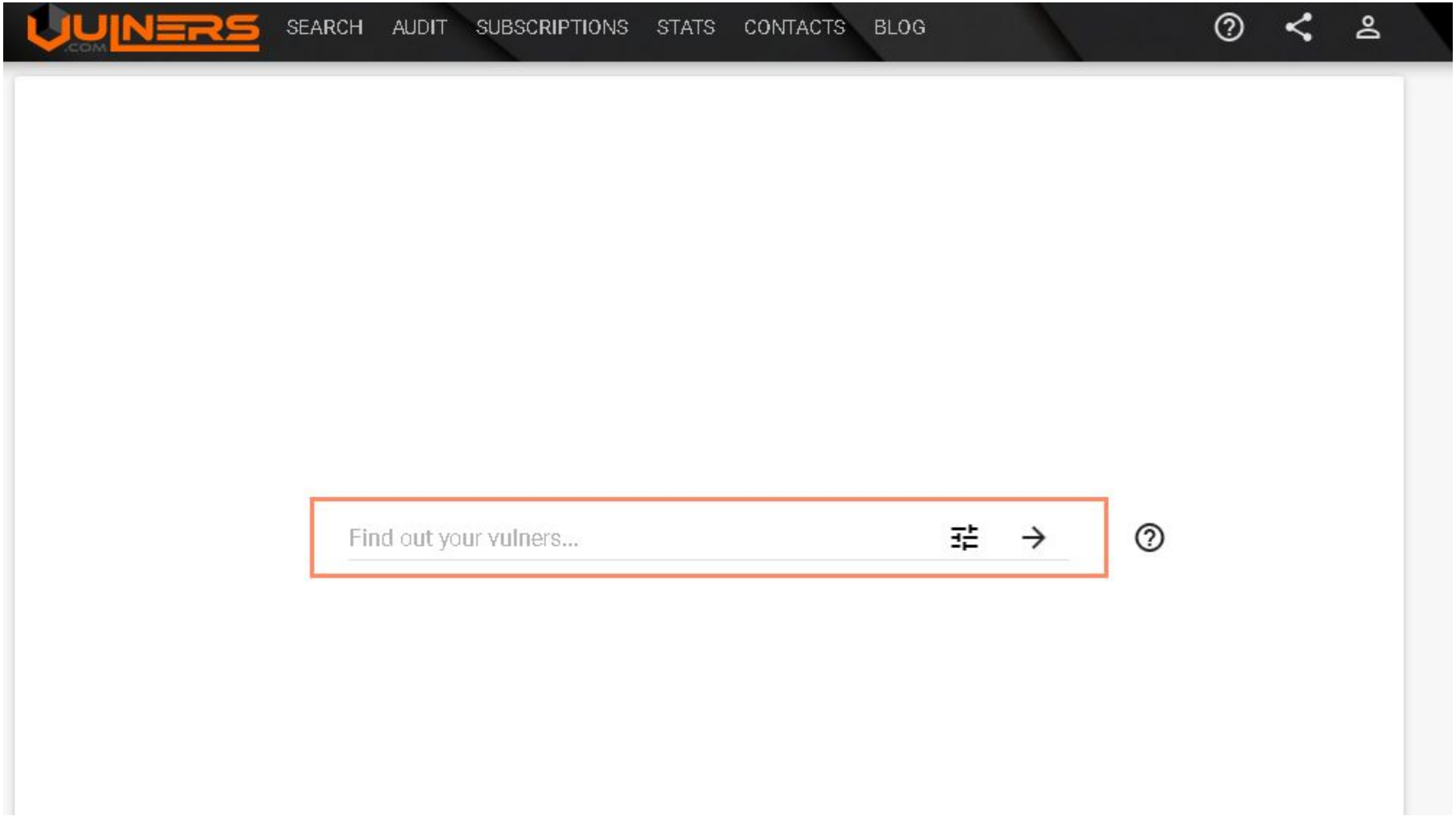
80/HTTP

GET /

Server	Apache httpd 2.4.6
Status Line	200 OK
Page Title	Index of /
GET /	[view page]

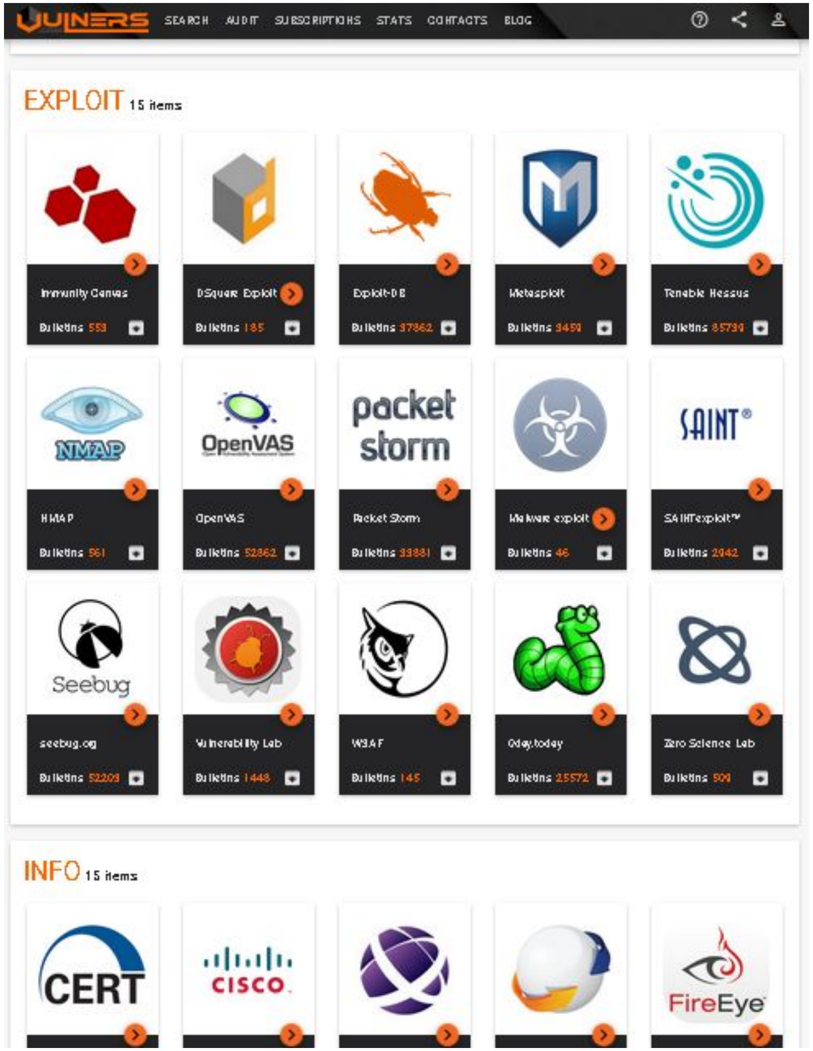
City	London
Province	England
Country	United Kingdom (GB)
Lat/Long	51.5142, -0.0931

Vulners



https://vulners.com/

Vulners



EXPLOIT 15 items

Immunity Canvas
Bulletins 553

DSquare Exploit
Bulletins 185

Exploit-DB
Bulletins 37862

Metasploit
Bulletins 3459

Tenable Nessus
Bulletins 85739

NMAP
Bulletins 561

OpenVAS
Bulletins 52862

Packet Storm
Bulletins 33881

Malware exploit
Bulletins 46

SAINTexploit™
Bulletins 2942

seebug.org
Bulletins 52209

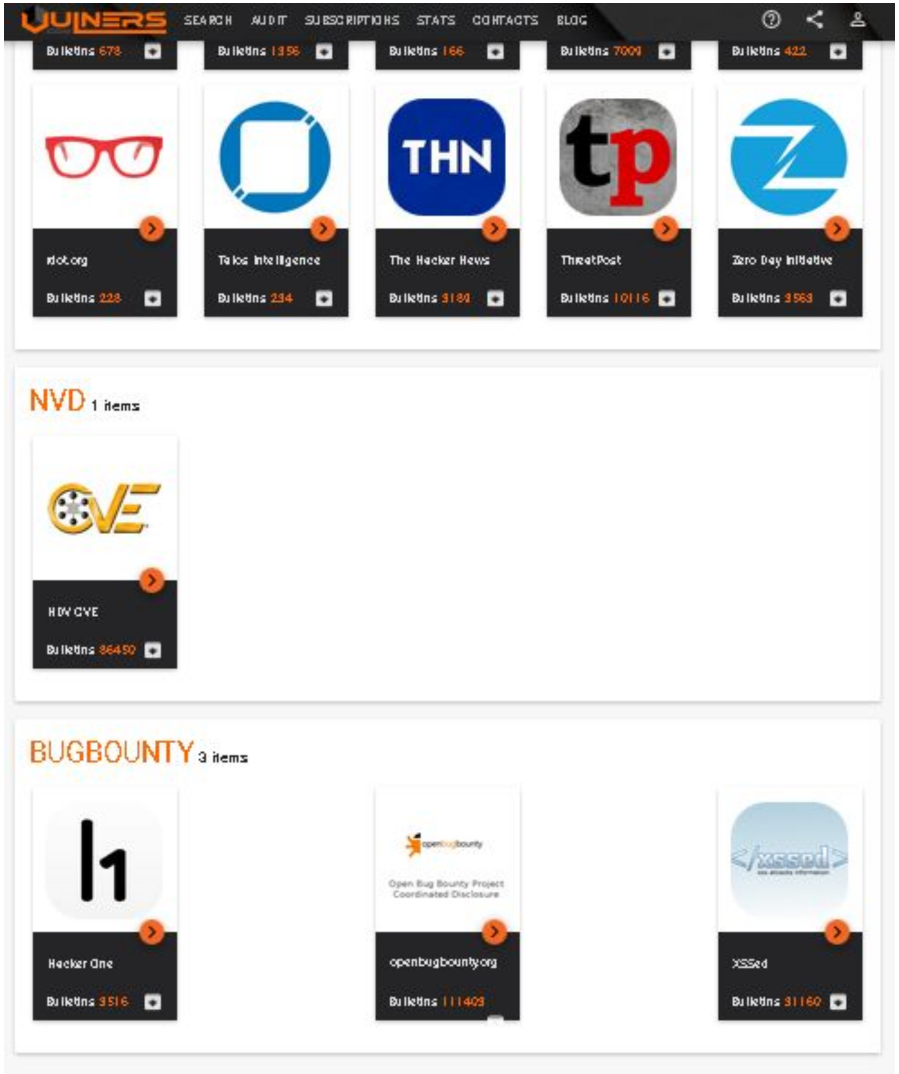
Vulnerability Lab
Bulletins 1448

W3AF
Bulletins 145

0day.today
Bulletins 25572

Zero Science Lab
Bulletins 509

INFO 15 items



Bulletins 678

Bulletins 1356

Bulletins 166

Bulletins 7009

Bulletins 422

rdot.org
Bulletins 228

Talos Intelligence
Bulletins 234

The Hacker News
Bulletins 3189

ThreatPost
Bulletins 10116

Zero Day Initiative
Bulletins 3563

NVD 1 items

NVD CVE
Bulletins 86450

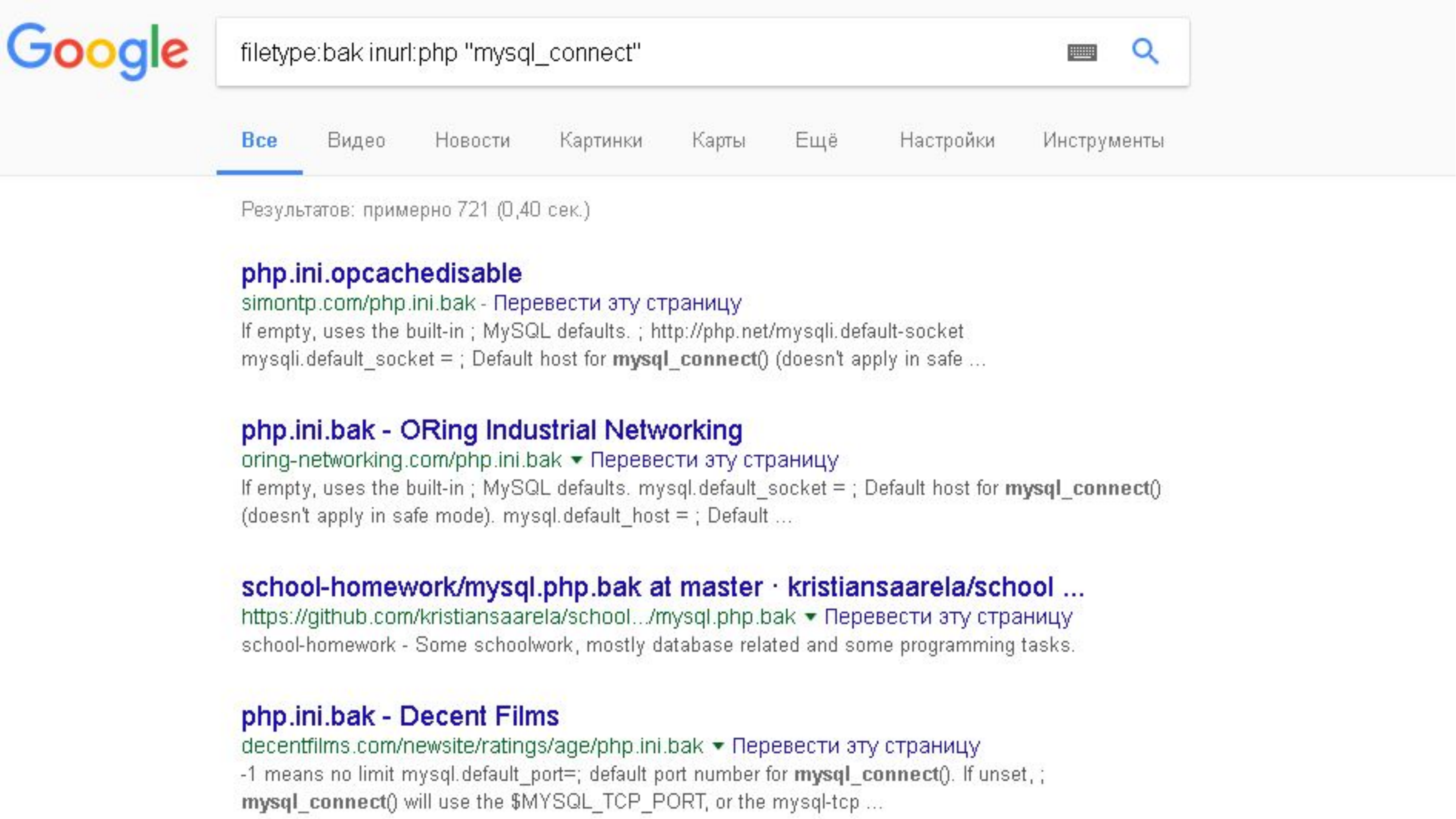
BUGBOUNTY 3 items

Hacker One
Bulletins 3516

openbugbounty.org
Bulletins 111409

XSSed
Bulletins 31160

Резервные копии PHP, которые содержат пароли для подключения к MySQL



filetype:bak inurl:php "mysql_connect"

Результатов: примерно 721 (0,40 сек.)

php.ini.opcachedisable
simontp.com/php.ini.bak - Перевести эту страницу
If empty, uses the built-in ; MySQL defaults. ; http://php.net/mysqli.default-socket mysqli.default_socket = ; Default host for **mysql_connect**() (doesn't apply in safe ...

php.ini.bak - ORing Industrial Networking
oring-networking.com/php.ini.bak ▾ Перевести эту страницу
If empty, uses the built-in ; MySQL defaults. mysql.default_socket = ; Default host for **mysql_connect**() (doesn't apply in safe mode). mysql.default_host = ; Default ...

school-homework/mysql.php.bak at master · kristiansaarela/school ...
https://github.com/kristiansaarela/school.../mysql.php.bak ▾ Перевести эту страницу
school-homework - Some schoolwork, mostly database related and some programming tasks.

php.ini.bak - Decent Films
decentfilms.com/newsite/ratings/age/php.ini.bak ▾ Перевести эту страницу
-1 means no limit mysql.default_port=; default port number for **mysql_connect**(). If unset, ; **mysql_connect**() will use the $MYSQL_TCP_PORT, or the mysql-tcp ...

https://www.google.ru/

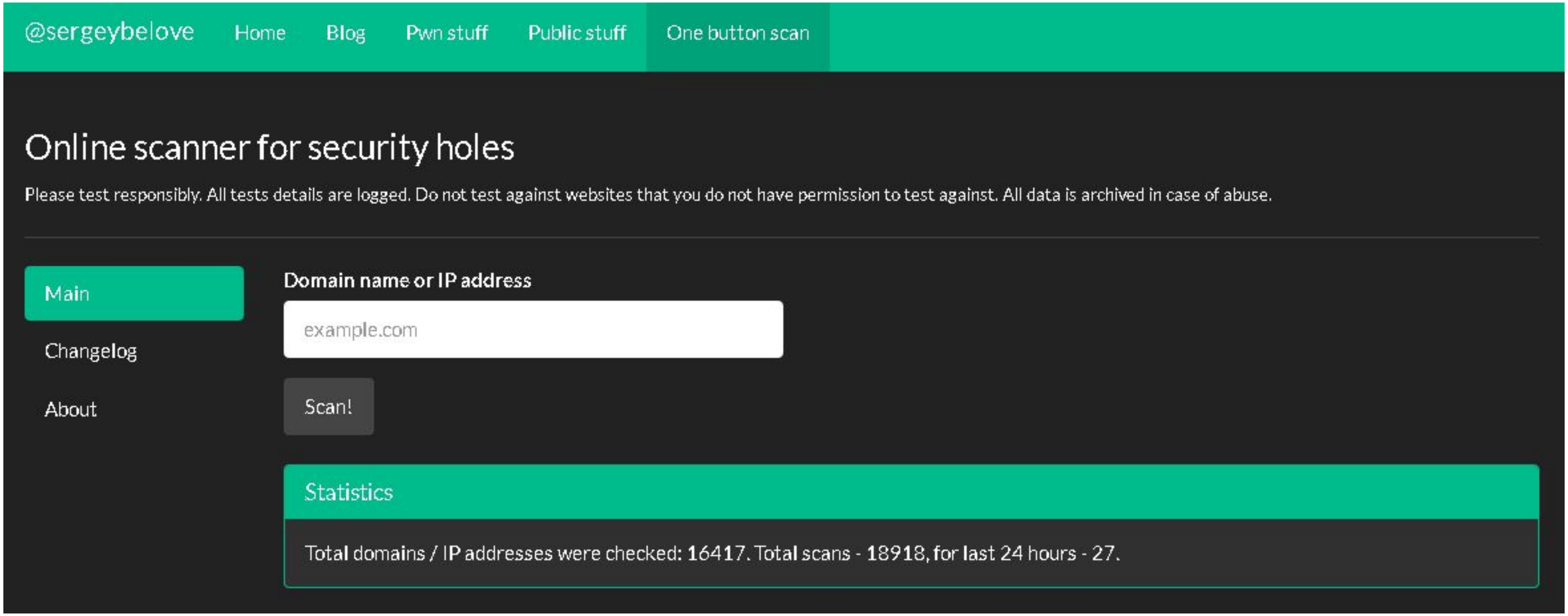
https://www.exploit-db.com/google-hacking-database/

Поисковые запросы Google

Google Hacking - сбор информации с использование расширенных поисковых запросов Google

site:название_сайта - поиск в пределах сайта или домена
filetype:расширение_файла – находит файлы с заданным расширением
ext:расширение_файла – ищет необычные расширения (например, DMP, KS, key…) передает более точные результаты, чем оператор filetype.
link:название_сайта - кто ссылается на сайт
cache:название_сайта - вывести кэшированную версию для указанного сайта.
intitle:ключевое_слово - найти страницы, содержащие ключевое слово или фразу в заголовке,
allintitle:ключевые_слова – вывести результаты, содержащие все перечисленные элементы в заголовке страницы.
inurl:ключевое_слово - найти страницы, содержащие ключевое_слово в своем адресе
allinurl:ключевые_слова - найти страницы, содержащие все ключевые_слова в своем адресе
intext:слово - ищет указанное слово только в теле страницы, игнорируя заголовки, тексты ссылок и прочее.
allintext:ключевые_слова - найти все слова в тексте страницы

One button scan от Сергея Белова



Online scanner for security holes

Please test responsibly. All tests details are logged. Do not test against websites that you do not have permission to test against. All data is archived in case of abuse.

Domain name or IP address

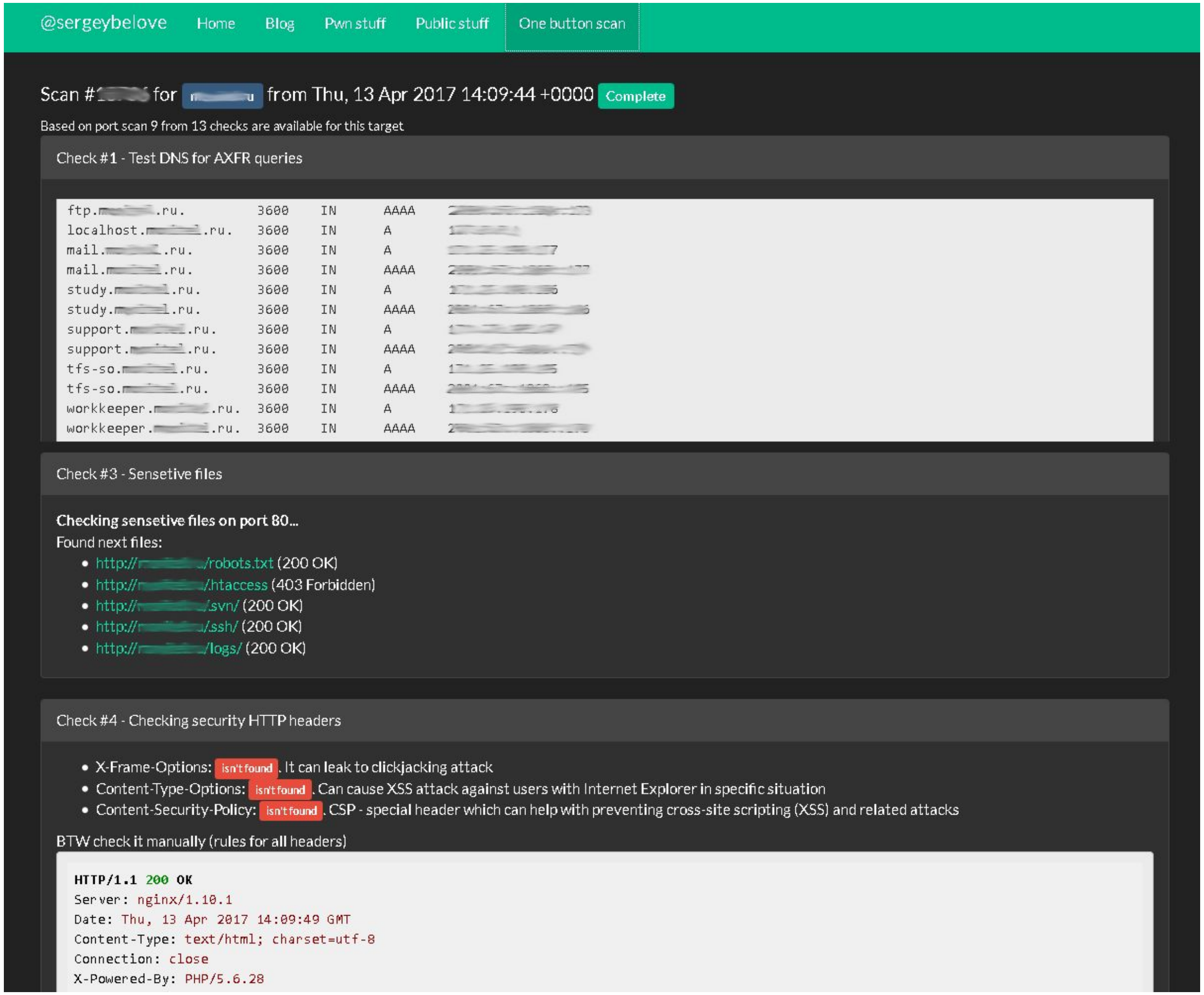
example.com

Statistics

Total domains / IP addresses were checked: 16417. Total scans - 18918, for last 24 hours - 27.

https://www.sergeybelove.ru/one-button-scan/

One button scan



Scan #[redacted] for [redacted] from Thu, 13 Apr 2017 14:09:44 +0000 Complete

Based on port scan 9 from 13 checks are available for this target

Check #1 - Test DNS for AXFR queries

```
ftp.[redacted].ru.          3600   IN   AAAA   [redacted]
localhost.[redacted].ru.    3600   IN   A      [redacted]
mail.[redacted].ru.         3600   IN   A      [redacted]
mail.[redacted].ru.         3600   IN   AAAA   [redacted]
study.[redacted].ru.        3600   IN   A      [redacted]
study.[redacted].ru.        3600   IN   AAAA   [redacted]
support.[redacted].ru.      3600   IN   A      [redacted]
support.[redacted].ru.      3600   IN   AAAA   [redacted]
tfs-so.[redacted].ru.       3600   IN   A      [redacted]
tfs-so.[redacted].ru.       3600   IN   AAAA   [redacted]
workkeeper.[redacted].ru.   3600   IN   A      [redacted]
workkeeper.[redacted].ru.   3600   IN   AAAA   [redacted]
```

Check #3 - Sensetive files

Checking sensetive files on port 80...

Found next files:

- http://[redacted]/robots.txt (200 OK)
- http://[redacted]/.htaccess (403 Forbidden)
- http://[redacted]/.svn/ (200 OK)
- http://[redacted]/.ssh/ (200 OK)
- http://[redacted]/logs/ (200 OK)

Check #4 - Checking security HTTP headers

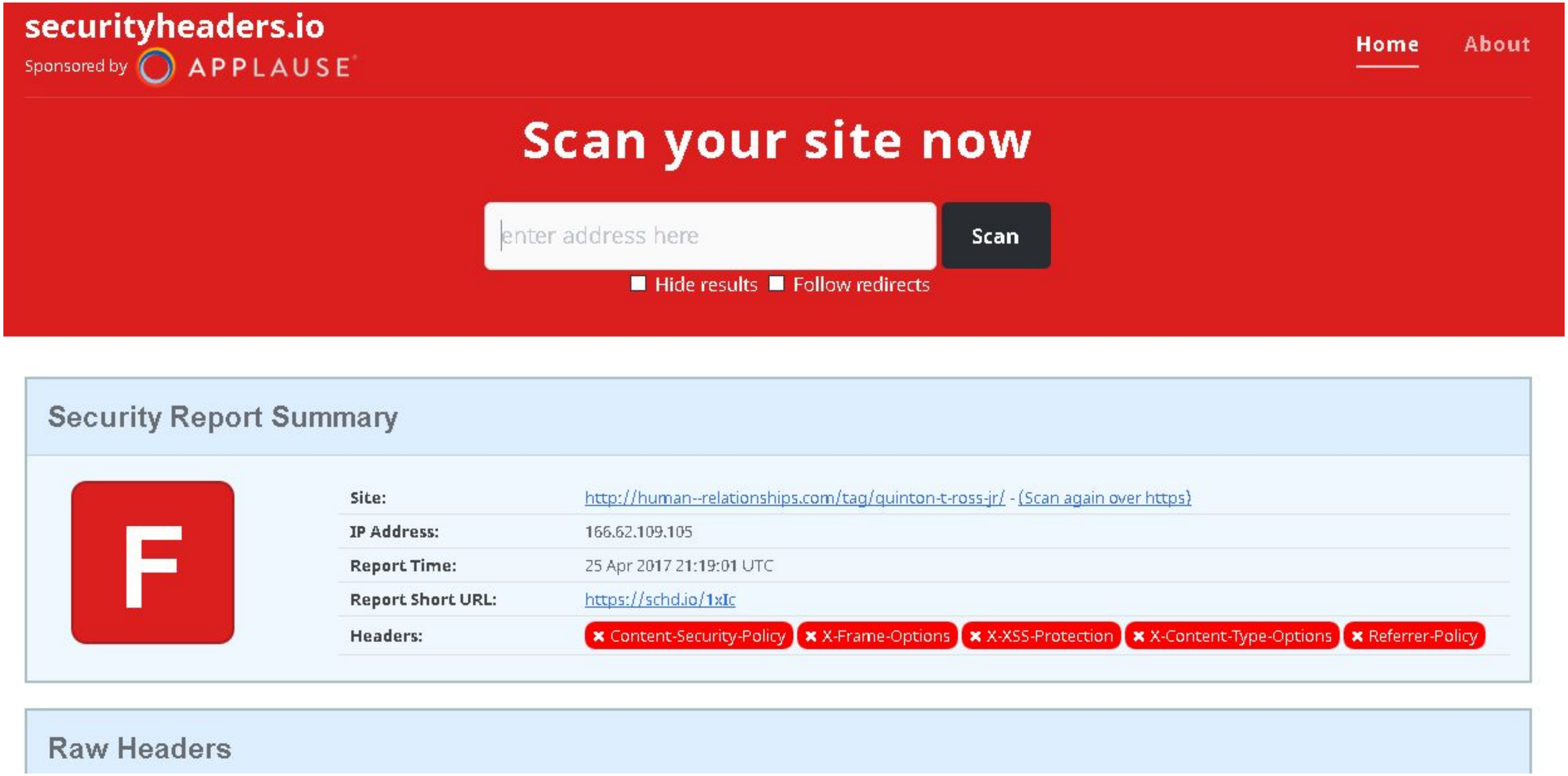
- X-Frame-Options: isn't found . It can leak to clickjacking attack
- Content-Type-Options: isn't found . Can cause XSS attack against users with Internet Explorer in specific situation
- Content-Security-Policy: isn't found . CSP - special header which can help with preventing cross-site scripting (XSS) and related attacks

BTW check it manually (rules for all headers)

```
HTTP/1.1 200 OK
Server: nginx/1.10.1
Date: Thu, 13 Apr 2017 14:09:49 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: PHP/5.6.28
```

https://www.sergeybelove.ru/one-button-scan/

SecurityHeaders.io



Scan your site now

□ Hide results □ Follow redirects

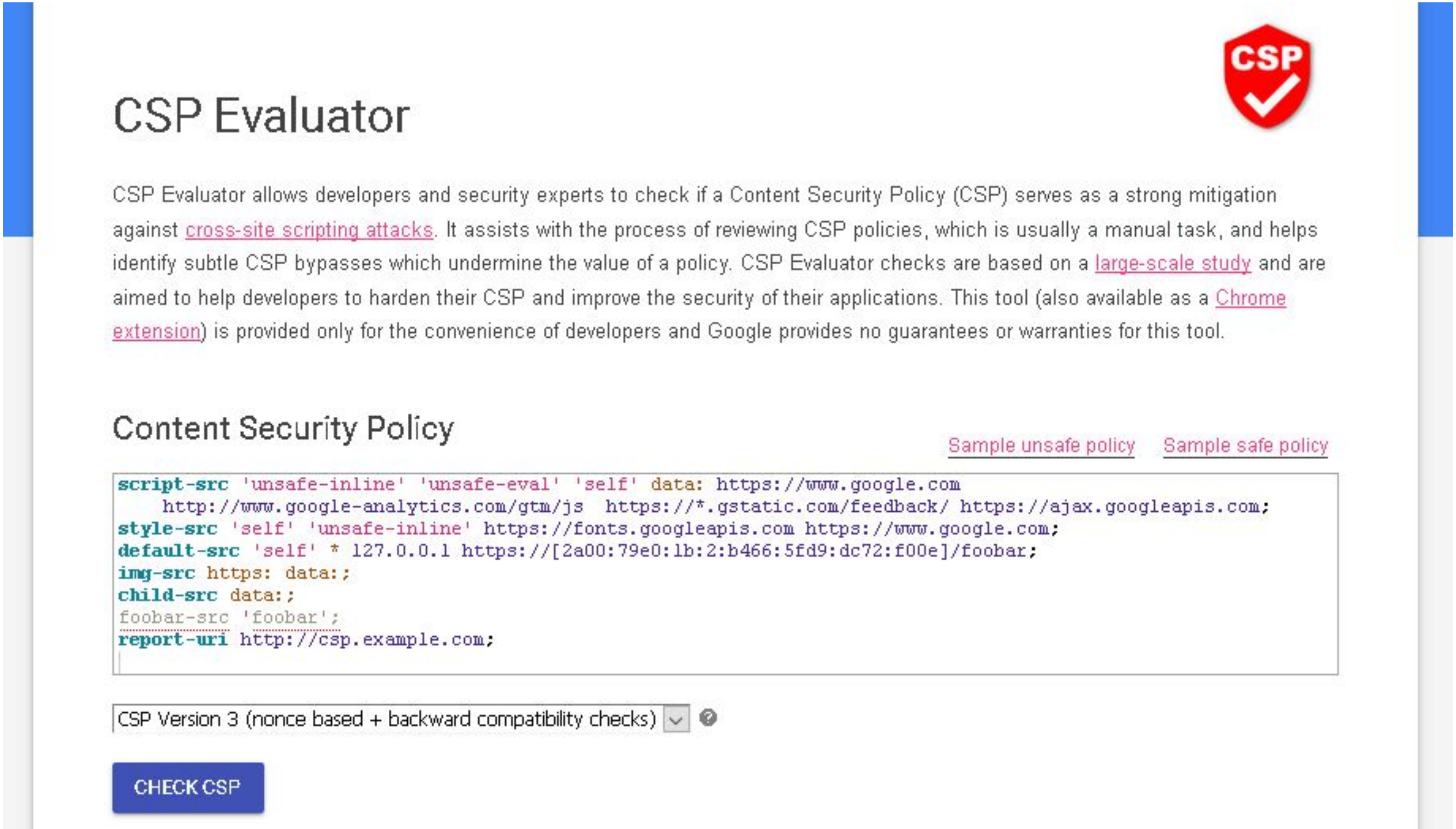
Security Report Summary

Site:	http://human--relationships.com/tag/quinton-t-ross-jr/ - (Scan again over https)
IP Address:	166.62.109.105
Report Time:	25 Apr 2017 21:19:01 UTC
Report Short URL:	https://schd.io/1xIc
Headers:	✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-XSS-Protection ✖ X-Content-Type-Options ✖ Referrer-Policy

Raw Headers

https://securityheaders.io/

CSP Evaluator



CSP Evaluator

CSP Evaluator allows developers and security experts to check if a Content Security Policy (CSP) serves as a strong mitigation against cross-site scripting attacks. It assists with the process of reviewing CSP policies, which is usually a manual task, and helps identify subtle CSP bypasses which undermine the value of a policy. CSP Evaluator checks are based on a large-scale study and are aimed to help developers to harden their CSP and improve the security of their applications. This tool (also available as a Chrome extension) is provided only for the convenience of developers and Google provides no guarantees or warranties for this tool.

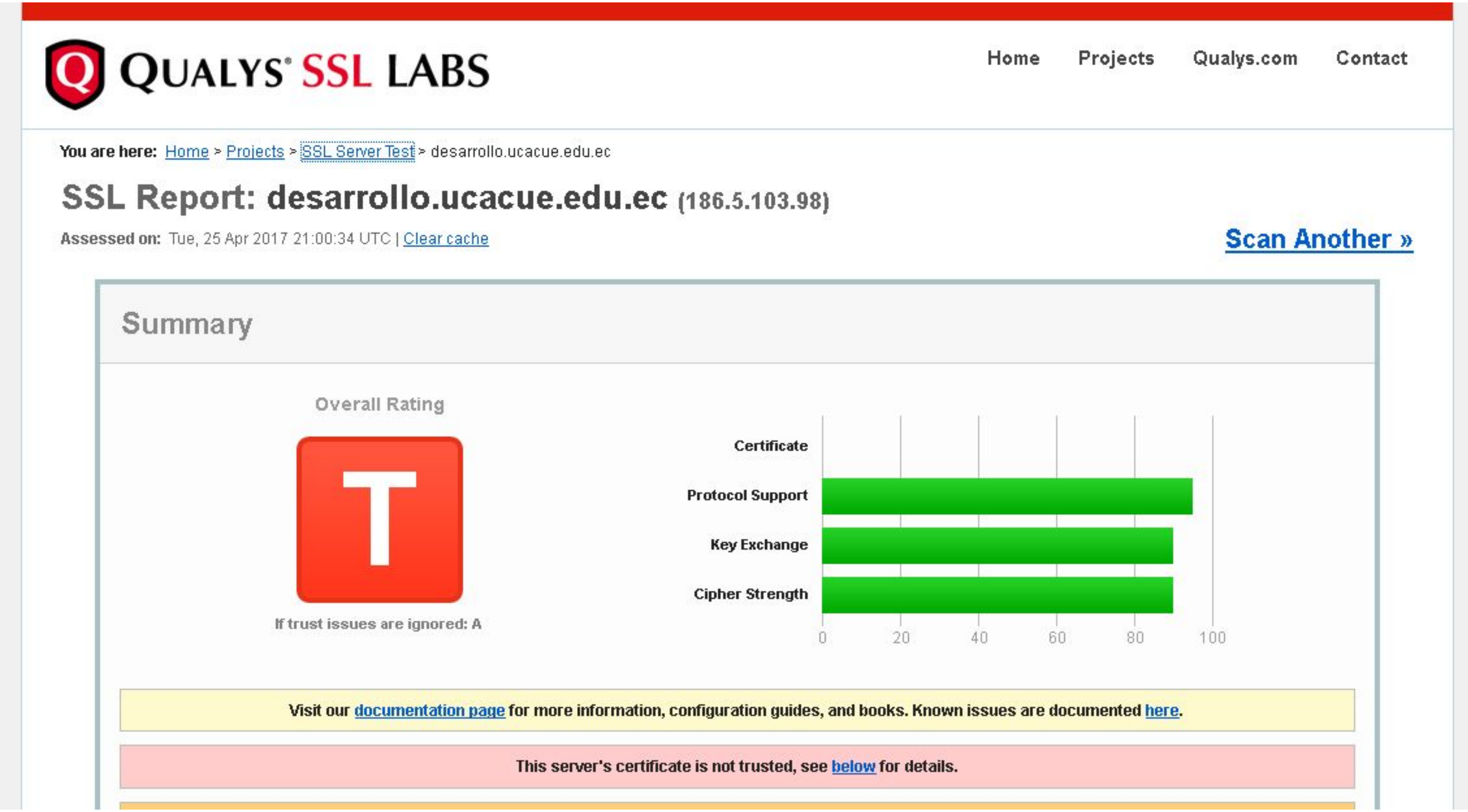
Content Security Policy

```
script-src 'unsafe-inline' 'unsafe-eval' 'self' data: https://www.google.com
    http://www.google-analytics.com/gtm/js  https://*.gstatic.com/feedback/ https://ajax.googleapis.com;
style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://www.google.com;
default-src 'self' * 127.0.0.1 https://[2a00:79e0:1b:2:b466:5fd9:dc72:f00e]/foobar;
img-src https: data:;
child-src data:;
foobar-src 'foobar';
report-uri http://csp.example.com;
```

CSP Version 3 (nonce based + backward compatibility checks)

https://csp-evaluator.withgoogle.com/

SSL Server Test от Qualys



You are here: Home > Projects > SSL Server Test > desarrollo.ucacue.edu.ec

SSL Report: desarrollo.ucacue.edu.ec (186.5.103.98)

Assessed on: Tue, 25 Apr 2017 21:00:34 UTC | Clear cache

Scan Another »

Summary

Overall Rating

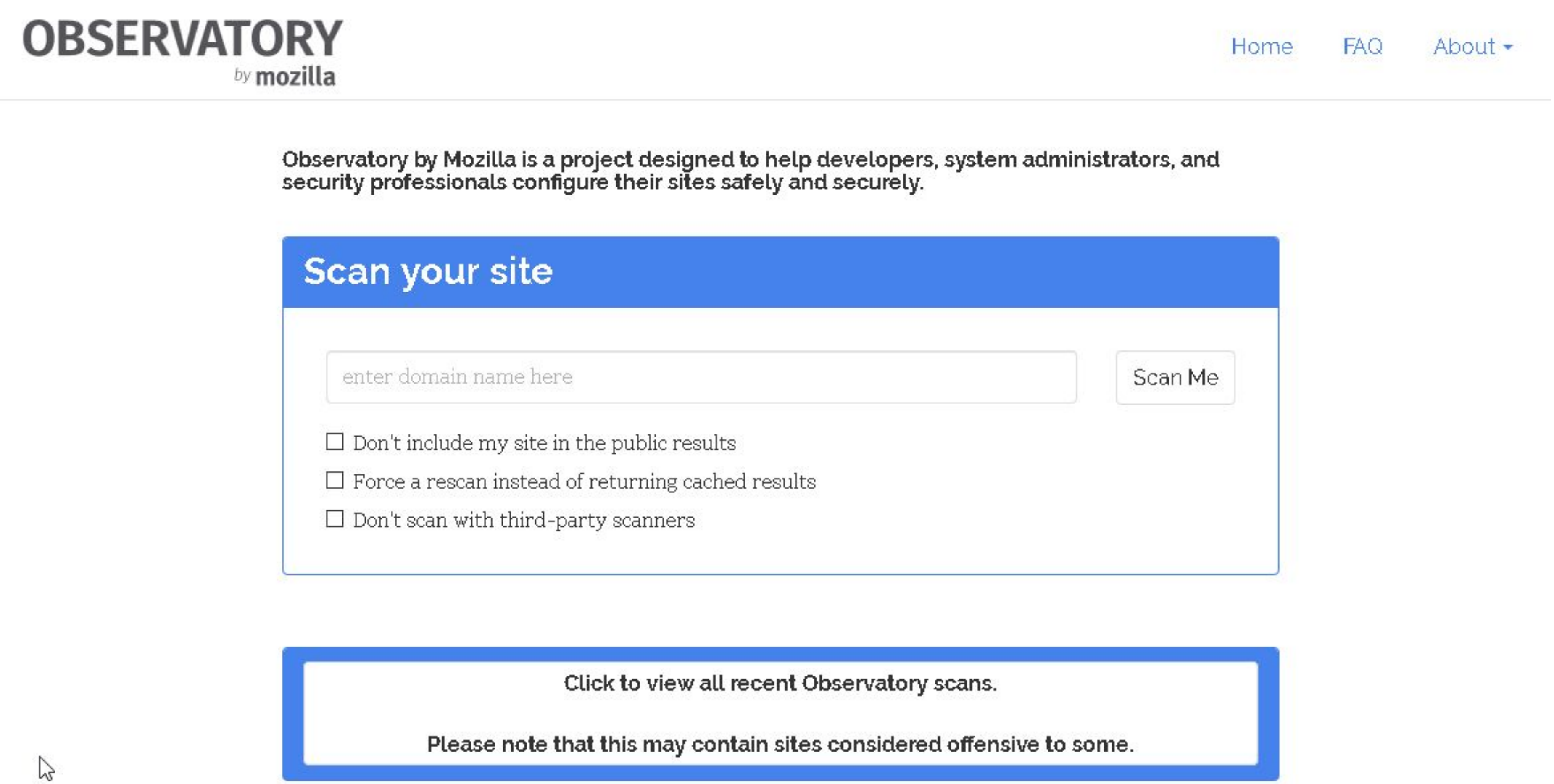
T

If trust issues are ignored: A

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

This server's certificate is not trusted, see below for details.

https://www.ssllabs.com/ssltest/



Observatory by Mozilla is a project designed to help developers, system administrators, and security professionals configure their sites safely and securely.

Scan your site

☐ Don't include my site in the public results

☐ Force a rescan instead of returning cached results

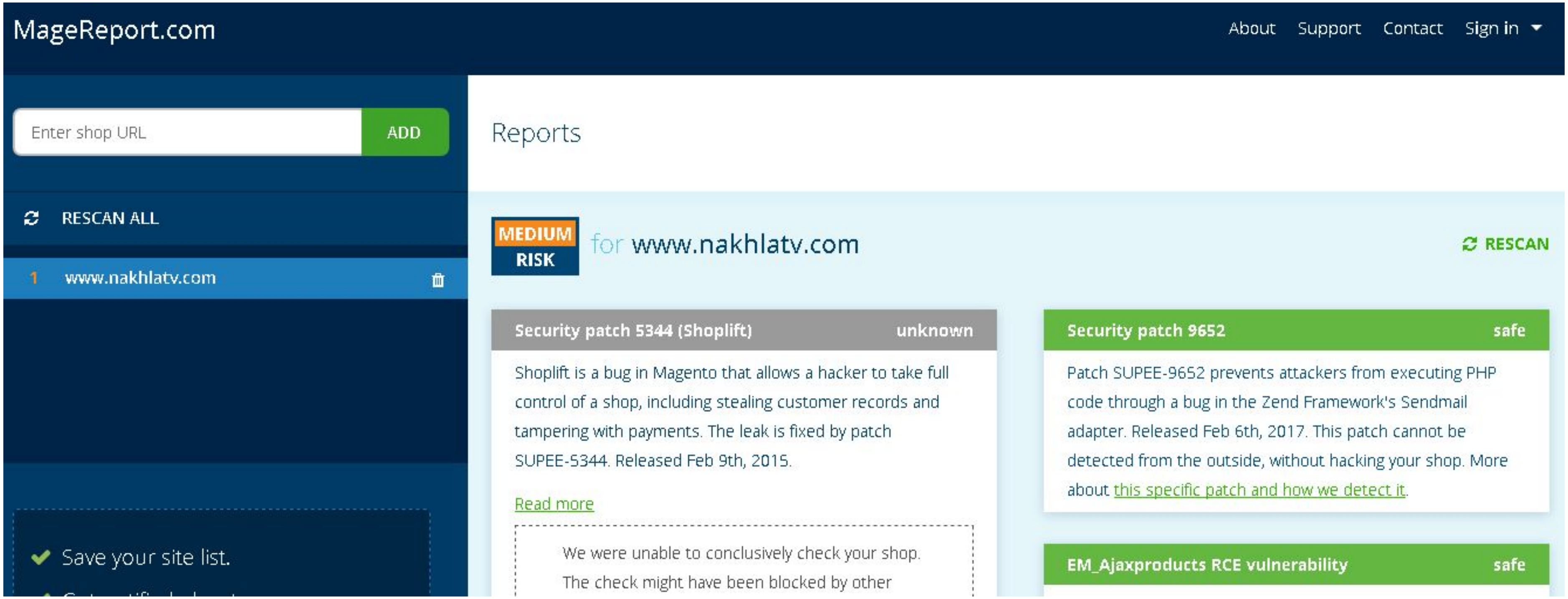
☐ Don't scan with third-party scanners

Click to view all recent Observatory scans.

Please note that this may contain sites considered offensive to some.

https://observatory.mozilla.org/

MageReport



Reports

MEDIUM RISK for www.nakhlatv.com

Security patch 5344 (Shoplift) unknown

Shoplift is a bug in Magento that allows a hacker to take full control of a shop, including stealing customer records and tampering with payments. The leak is fixed by patch SUPEE-5344. Released Feb 9th, 2015.

Read more

We were unable to conclusively check your shop. The check might have been blocked by other

Security patch 9652 safe

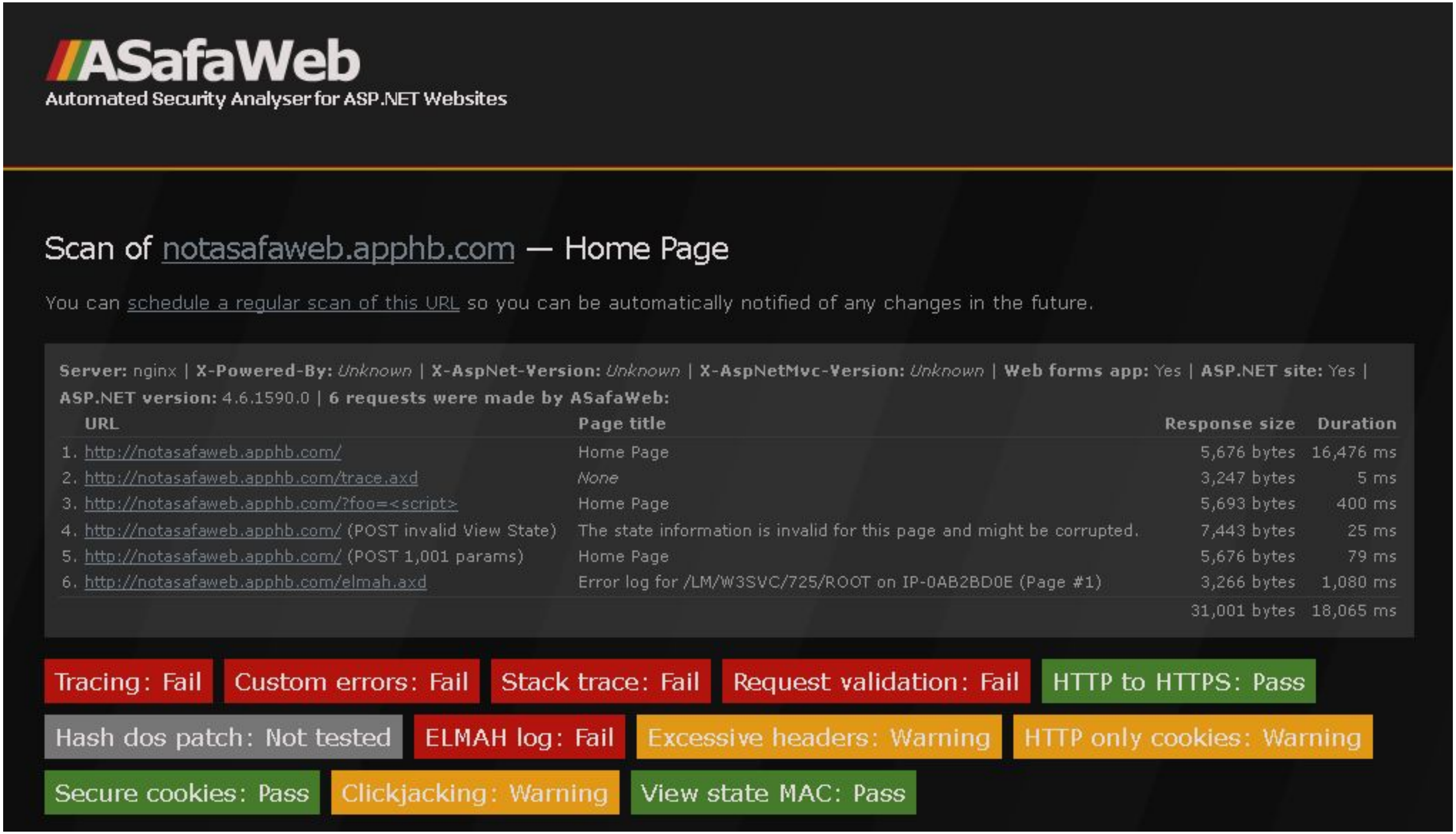
Patch SUPEE-9652 prevents attackers from executing PHP code through a bug in the Zend Framework's Sendmail adapter. Released Feb 6th, 2017. This patch cannot be detected from the outside, without hacking your shop. More about this specific patch and how we detect it.

EM_Ajaxproducts RCE vulnerability safe

✓ Save your site list.

https://www.magereport.com/

ASafaWeb



ASafaWeb
Automated Security Analyser for ASP.NET Websites

Scan of notasafaweb.apphb.com — Home Page

You can schedule a regular scan of this URL so you can be automatically notified of any changes in the future.

Server: nginx | **X-Powered-By:** *Unknown* | **X-AspNet-Version:** *Unknown* | **X-AspNetMvc-Version:** *Unknown* | **Web forms app:** Yes | **ASP.NET site:** Yes | **ASP.NET version:** 4.6.1590.0 | **6 requests were made by ASafaWeb:**

	URL	Page title	Response size	Duration
1.	http://notasafaweb.apphb.com/	Home Page	5,676 bytes	16,476 ms
2.	http://notasafaweb.apphb.com/trace.axd	*None*	3,247 bytes	5 ms
3.	http://notasafaweb.apphb.com/?foo=<script>	Home Page	5,693 bytes	400 ms
4.	http://notasafaweb.apphb.com/ (POST invalid View State)	The state information is invalid for this page and might be corrupted.	7,443 bytes	25 ms
5.	http://notasafaweb.apphb.com/ (POST 1,001 params)	Home Page	5,676 bytes	79 ms
6.	http://notasafaweb.apphb.com/elmah.axd	Error log for /LM/W3SVC/725/ROOT on IP-0AB2BD0E (Page #1)	3,266 bytes	1,080 ms
			31,001 bytes	18,065 ms

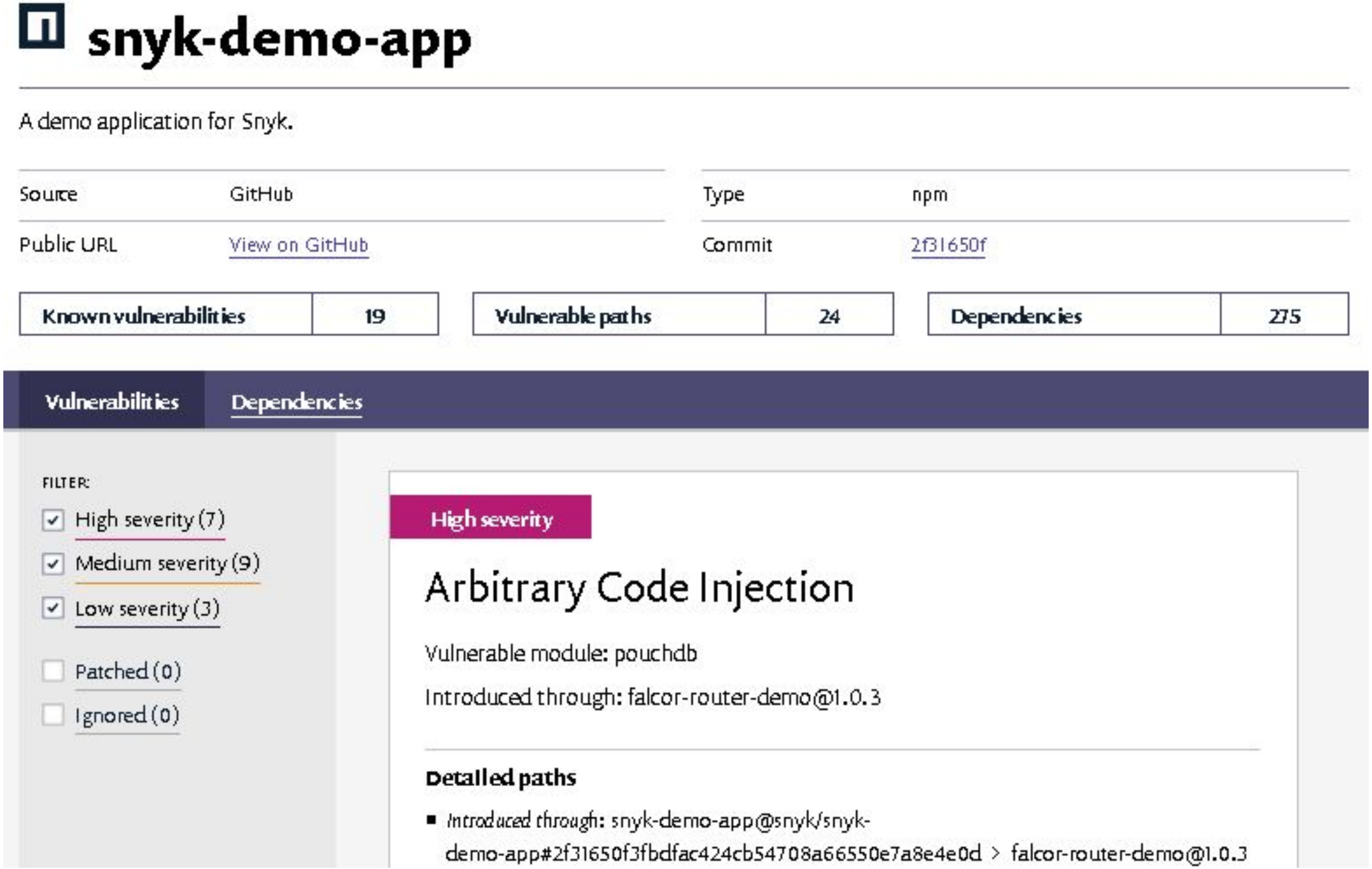
Tracing: Fail | Custom errors: Fail | Stack trace: Fail | Request validation: Fail | HTTP to HTTPS: Pass

Hash dos patch: Not tested | ELMAH log: Fail | Excessive headers: Warning | HTTP only cookies: Warning

Secure cookies: Pass | Clickjacking: Warning | View state MAC: Pass

https://asafaweb.com/

Snyk



snyk-demo-app

A demo application for Snyk.

Source	GitHub	Type	npm
Public URL	View on GitHub	Commit	2f31650f

Known vulnerabilities	19	Vulnerable paths	24	Dependencies	275

FILTER:

☑ High severity (7)
☑ Medium severity (9)
☑ Low severity (3)

□ Patched (0)
□ Ignored (0)

High severity

Arbitrary Code Injection

Vulnerable module: pouchdb

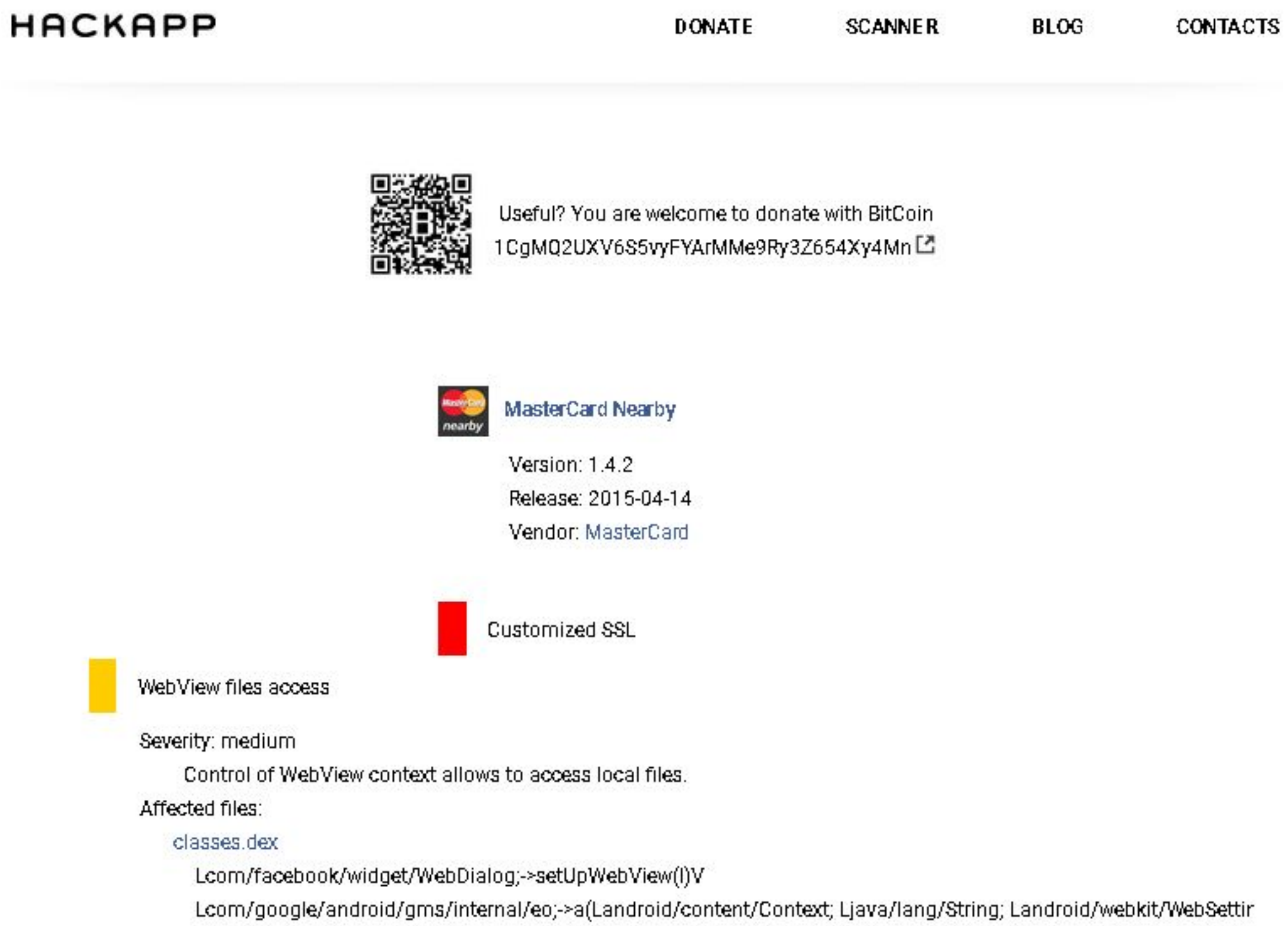
Introduced through: falcor-router-demo@1.0.3

Detailed paths

- *Introduced through*: snyk-demo-app@snyk/snyk-demo-app#2f31650f3fbdfac424cb54708a66550e7a8e4e0d > falcor-router-demo@1.0.3

https://snyk.io/test

Hackapp



Useful? You are welcome to donate with BitCoin
1CgMQ2UXV6S5vyFYArMMe9Ry3Z654Xy4Mn

MasterCard Nearby

Version: 1.4.2
Release: 2015-04-14
Vendor: MasterCard

🟥 Customized SSL

🟨 WebView files access

Severity: medium

Control of WebView context allows to access local files.

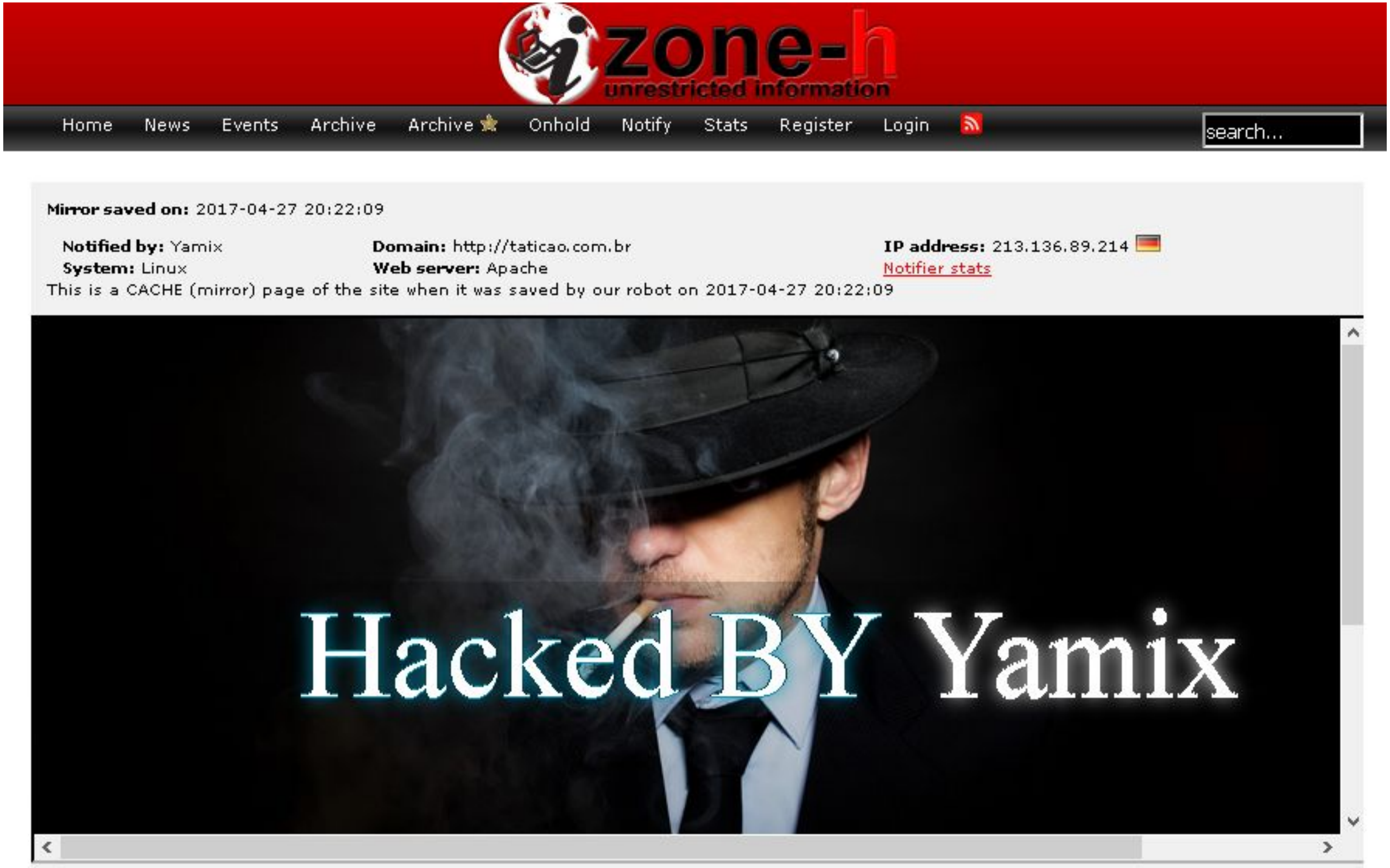
Affected files:

classes.dex

```
Lcom/facebook/widget/WebDialog;->setUpWebView(I)V
Lcom/google/android/gms/internal/eo;->a(Landroid/content/Context; Ljava/lang/String; Landroid/webkit/WebSettir
```

https://hackapp.com/list

Zone-H



Mirror saved on: 2017-04-27 20:22:09

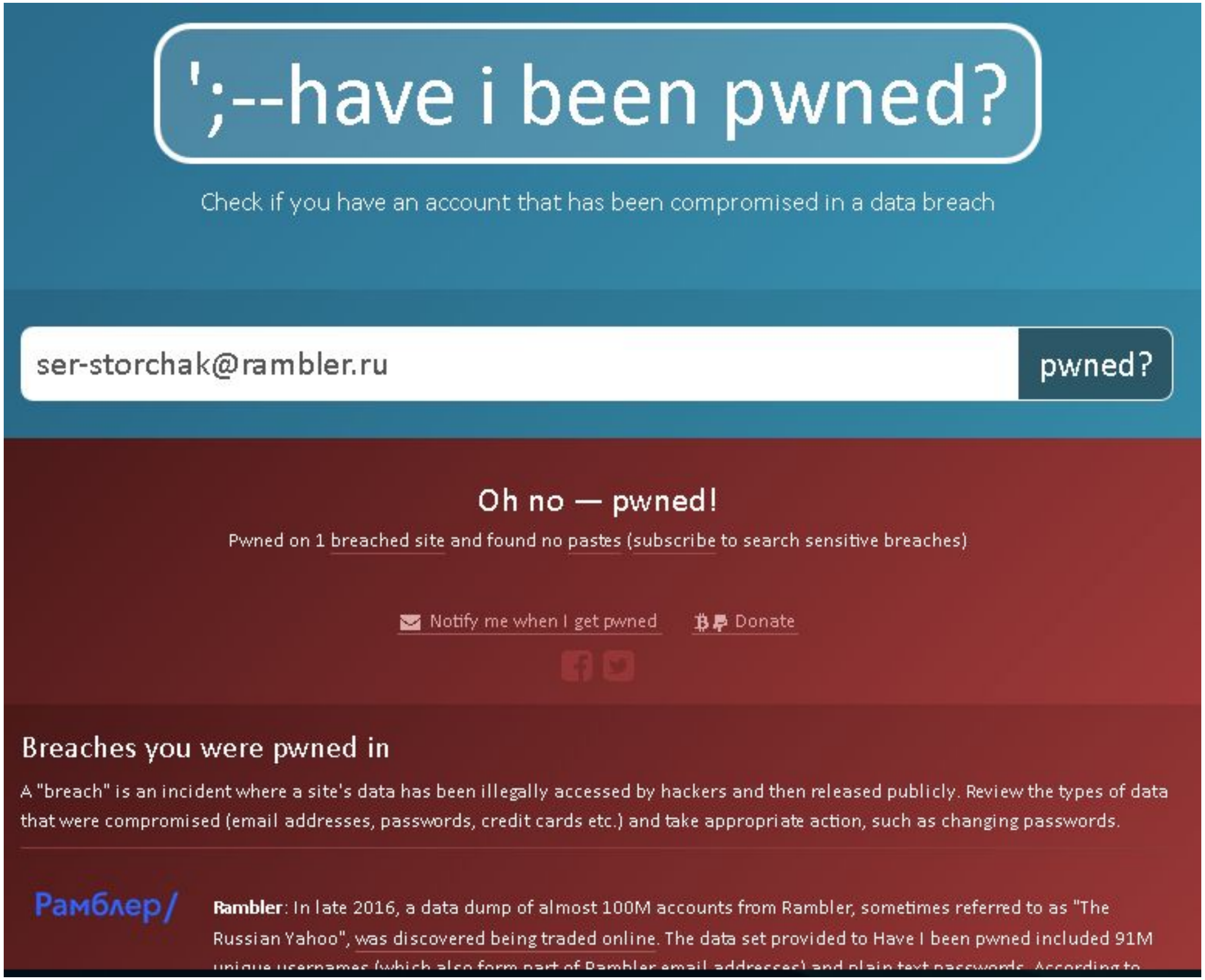
Notified by: Yamix **Domain:** http://taticao.com.br **IP address:** 213.136.89.214

System: Linux **Web server:** Apache Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2017-04-27 20:22:09

http://www.zone-h.org/archive

Have I been pwned?



Check if you have an account that has been compromised in a data breach

ser-storchak@rambler.ru

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

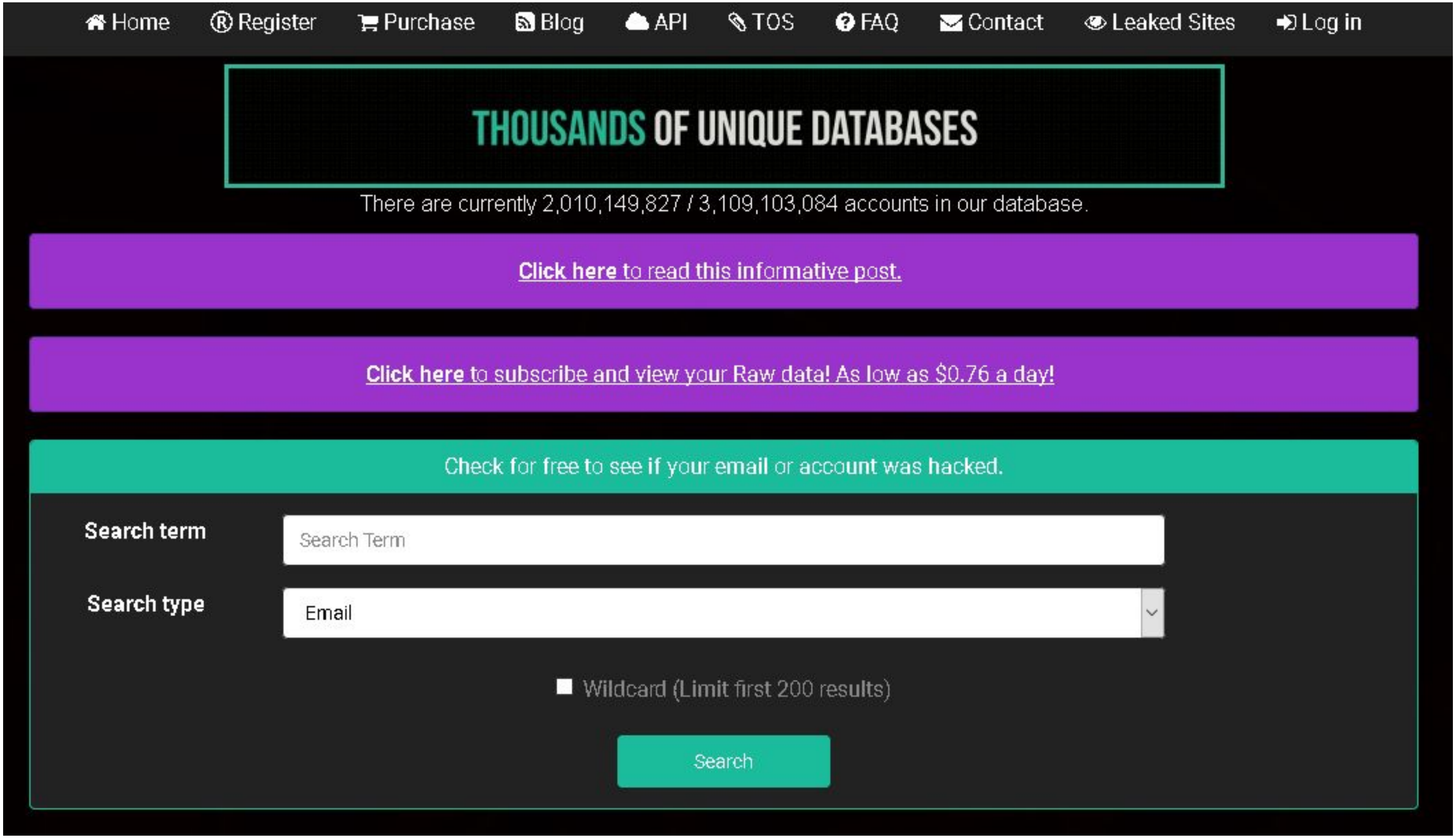
Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Rambler: In late 2016, a data dump of almost 100M accounts from Rambler, sometimes referred to as "The Russian Yahoo", was discovered being traded online. The data set provided to Have I been pwned included 91M unique usernames (which also form part of Rambler email addresses) and plain text passwords. According to

https://haveibeenpwned.com/

Leakedsource



THOUSANDS OF UNIQUE DATABASES

There are currently 2,010,149,827 / 3,109,103,084 accounts in our database.

Click here to read this informative post.

Click here to subscribe and view your Raw data! As low as $0.76 a day!

Check for free to see if your email or account was hacked.

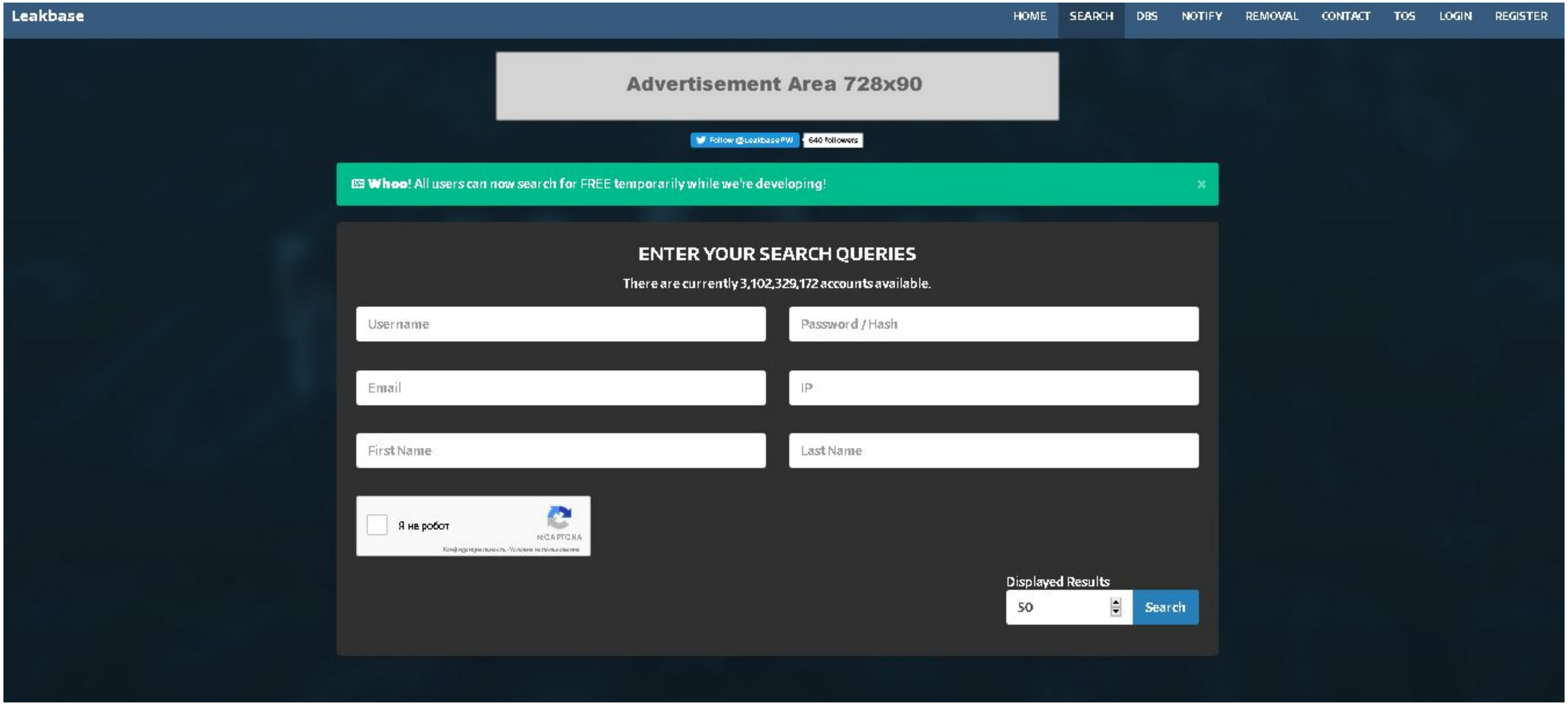
Search term: Search Term

Search type: Email

□ Wildcard (Limit first 200 results)

https://leakedsource.ru/

Leakbase



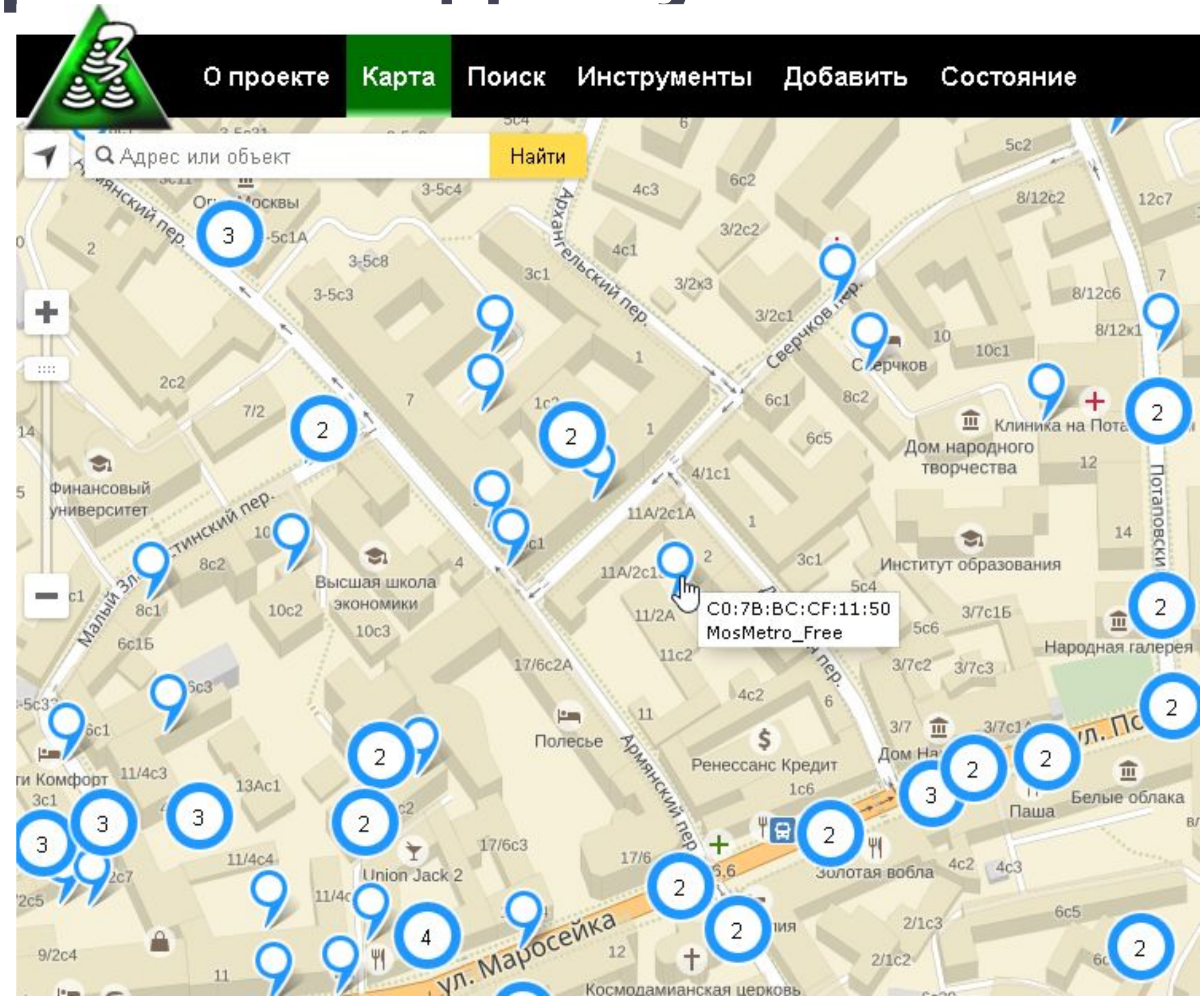
Whoo! All users can now search for FREE temporarily while we're developing!

ENTER YOUR SEARCH QUERIES

There are currently 3,102,329,172 accounts available.

https://leakbase.pw/landing.php

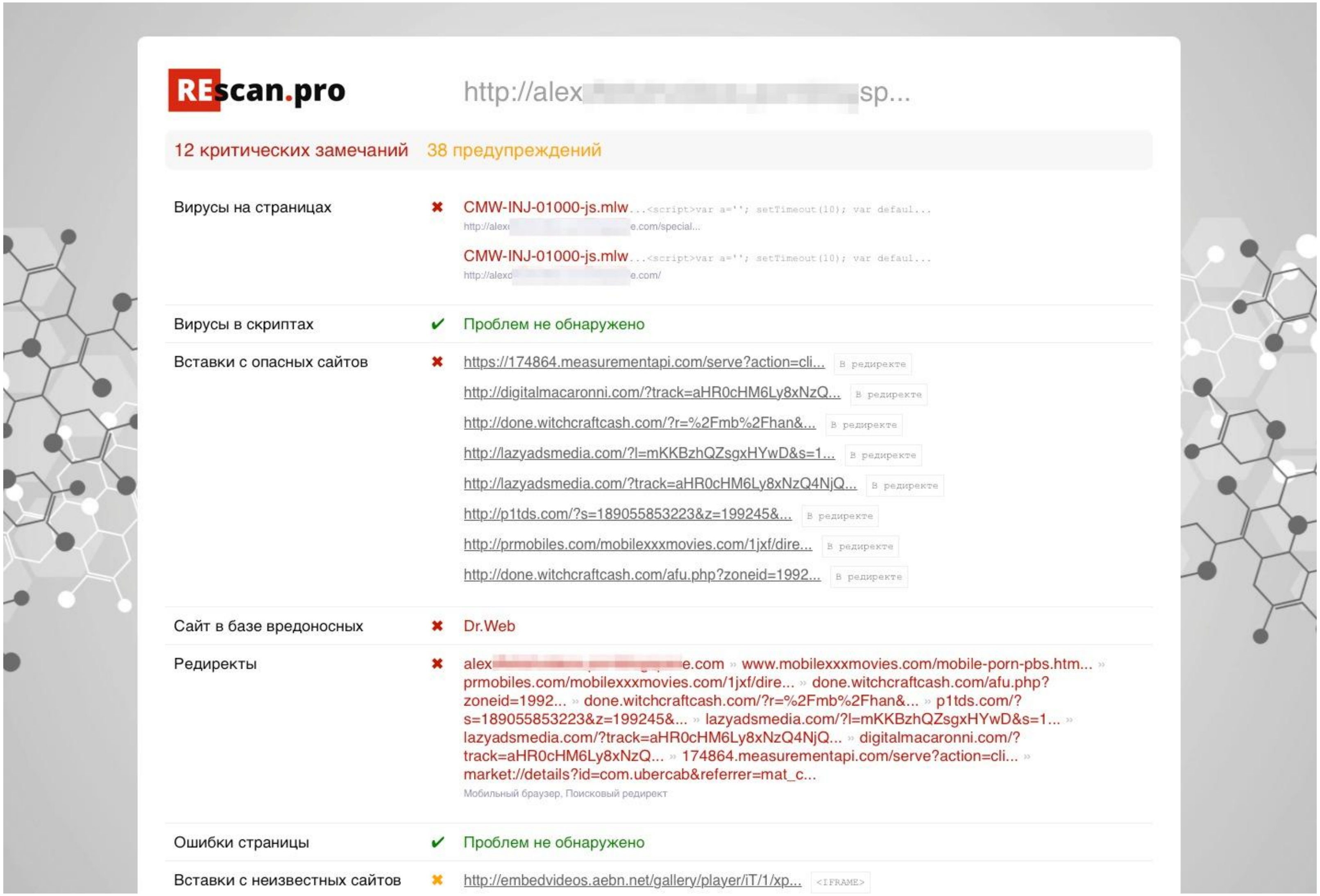
3WiFi: Карта точек доступа



C0:7B:BC:CF:11:50
MosMetro_Free

http://3wifi.stascorp.com/

ReScan.pro



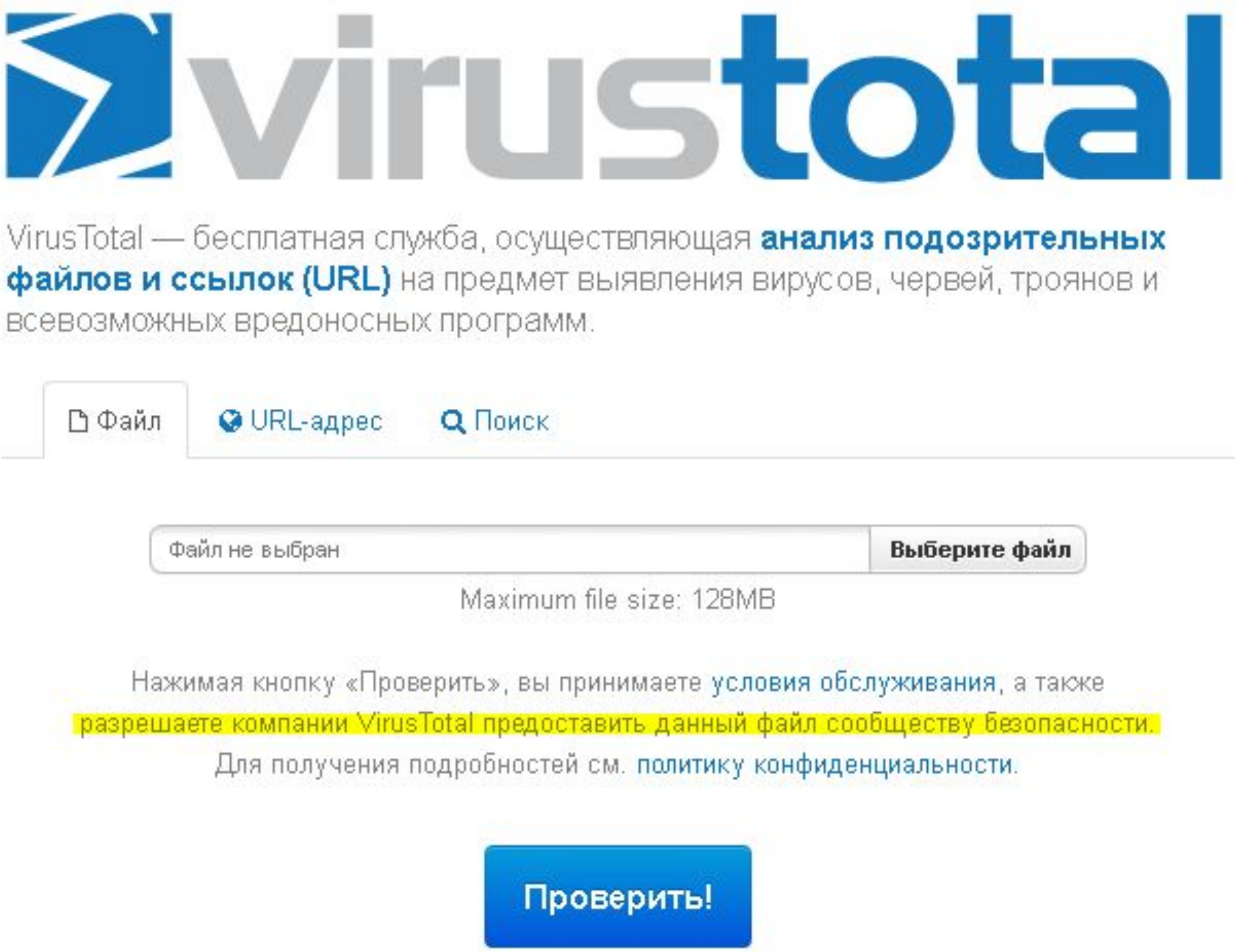
REscan.pro http://alex[redacted]sp...

12 критических замечаний 38 предупреждений

Вирусы на страницах	✖	CMW-INJ-01000-js.mlw...<script>var a=''; setTimeout(10); var defaul... http://alex[redacted]e.com/special... CMW-INJ-01000-js.mlw...<script>var a=''; setTimeout(10); var defaul... http://alex[redacted]e.com/
Вирусы в скриптах	✔	Проблем не обнаружено
Вставки с опасных сайтов	✖	https://174864.measurementapi.com/serve?action=cli... В редиректе http://digitalmacaronni.com/?track=aHR0cHM6Ly8xNzQ... В редиректе http://done.witchcraftcash.com/?r=%2Fmb%2Fhan&... В редиректе http://lazyadsmedia.com/?l=mKKBzhQZsgxHYwD&s=1... В редиректе http://lazyadsmedia.com/?track=aHR0cHM6Ly8xNzQ4NjQ... В редиректе http://p1tds.com/?s=189055853223&z=199245&... В редиректе http://prmobiles.com/mobilexxxmovies.com/1jxf/dire... В редиректе http://done.witchcraftcash.com/afu.php?zoneid=1992... В редиректе
Сайт в базе вредоносных	✖	Dr.Web
Редиректы	✖	alex[redacted]e.com » www.mobilexxxmovies.com/mobile-porn-pbs.htm... » prmobiles.com/mobilexxxmovies.com/1jxf/dire... » done.witchcraftcash.com/afu.php?zoneid=1992... » done.witchcraftcash.com/?r=%2Fmb%2Fhan&... » p1tds.com/?s=189055853223&z=199245&... » lazyadsmedia.com/?l=mKKBzhQZsgxHYwD&s=1... » lazyadsmedia.com/?track=aHR0cHM6Ly8xNzQ4NjQ... » digitalmacaronni.com/?track=aHR0cHM6Ly8xNzQ... » 174864.measurementapi.com/serve?action=cli... » market://details?id=com.ubercab&referrer=mat_c... Мобильный браузер, Поисковый редирект
Ошибки страницы	✔	Проблем не обнаружено
Вставки с неизвестных сайтов	✖	http://embedvideos.aebn.net/gallery/player/iT/1/xp... <IFRAME>

https://rescan.pro/

VirusTotal



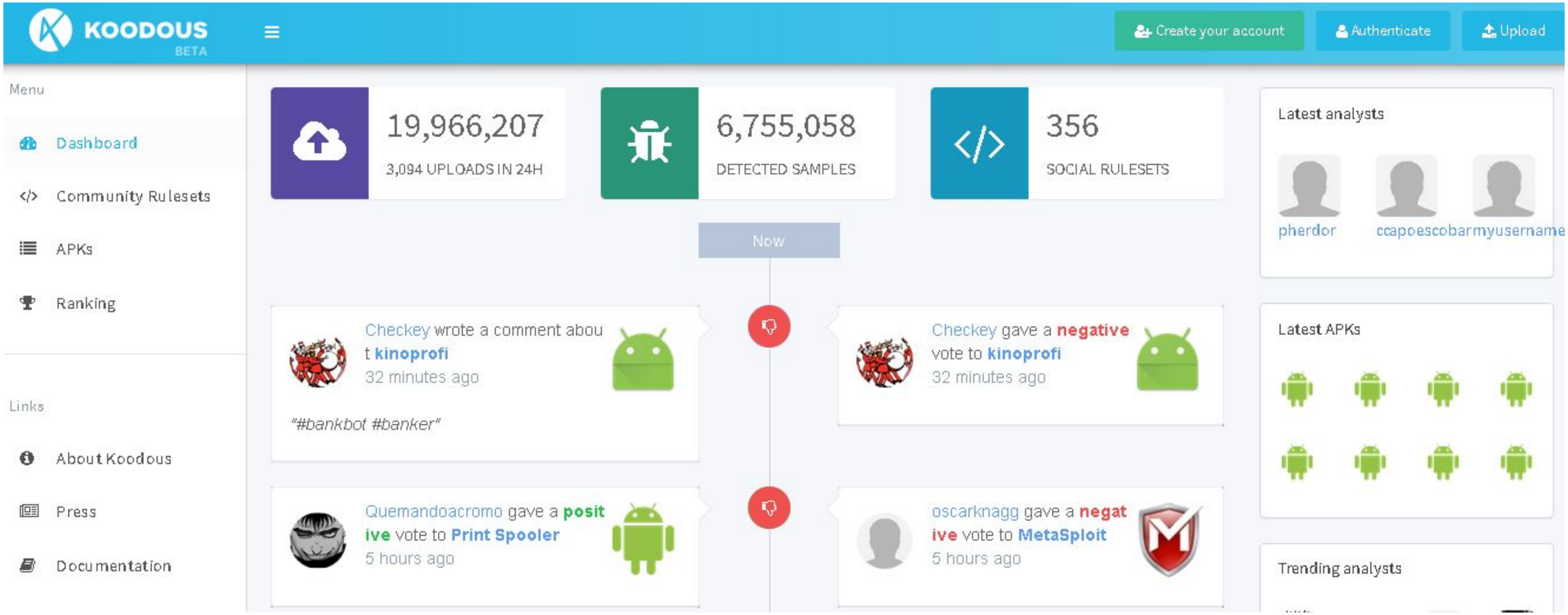
VirusTotal — бесплатная служба, осуществляющая **анализ подозрительных файлов и ссылок (URL)** на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ.

Maximum file size: 128MB

Нажимая кнопку «Проверить», вы принимаете условия обслуживания, а также разрешаете компании VirusTotal предоставить данный файл сообществу безопасности. Для получения подробностей см. политику конфиденциальности.

https://virustotal.com/

Koodous



19,966,207
3,094 UPLOADS IN 24H

6,755,058
DETECTED SAMPLES

356
SOCIAL RULESETS

Checkey wrote a comment about kinoprofi
32 minutes ago

"#bankbot #banker"

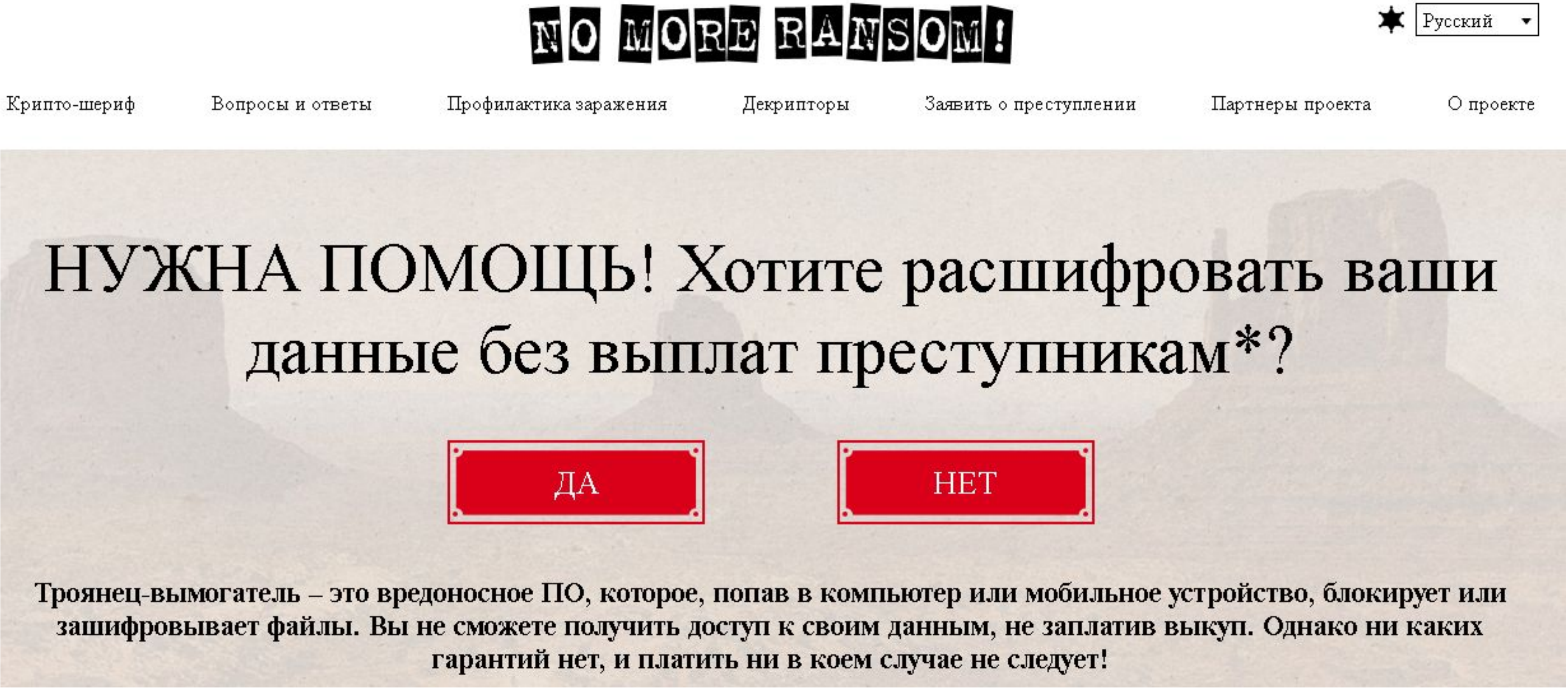
Checkey gave a **negative** vote to **kinoprofi**
32 minutes ago

Quemandoacromo gave a **positive** vote to **Print Spooler**
5 hours ago

oscarknagg gave a **negative** vote to **MetaSploit**
5 hours ago

https://koodous.com/

No More Ransom



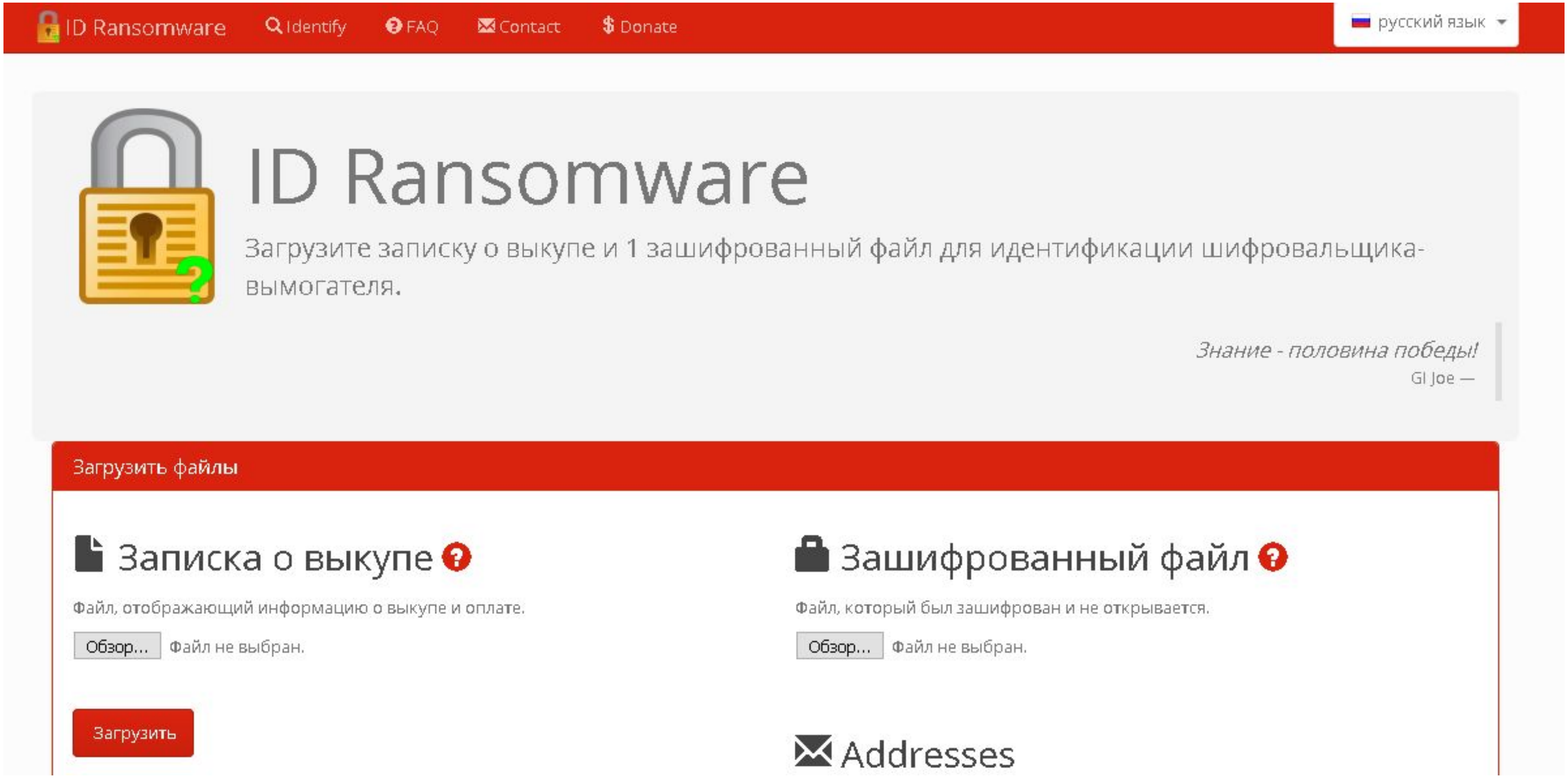
NO MORE RANSOM!

НУЖНА ПОМОЩЬ! Хотите расшифровать ваши данные без выплат преступникам*?

Троянец-вымогатель – это вредоносное ПО, которое, попав в компьютер или мобильное устройство, блокирует или зашифровывает файлы. Вы не сможете получить доступ к своим данным, не заплатив выкуп. Однако ни каких гарантий нет, и платить ни в коем случае не следует!

https://www.nomoreransom.org/

ID Ransomware



ID Ransomware

Загрузите записку о выкупе и 1 зашифрованный файл для идентификации шифровальщика-вымогателя.

Знание - половина победы!
GI Joe —

Загрузить файлы

Записка о выкупе

Файл, отображающий информацию о выкупе и оплате.

Обзор... Файл не выбран.

Зашифрованный файл

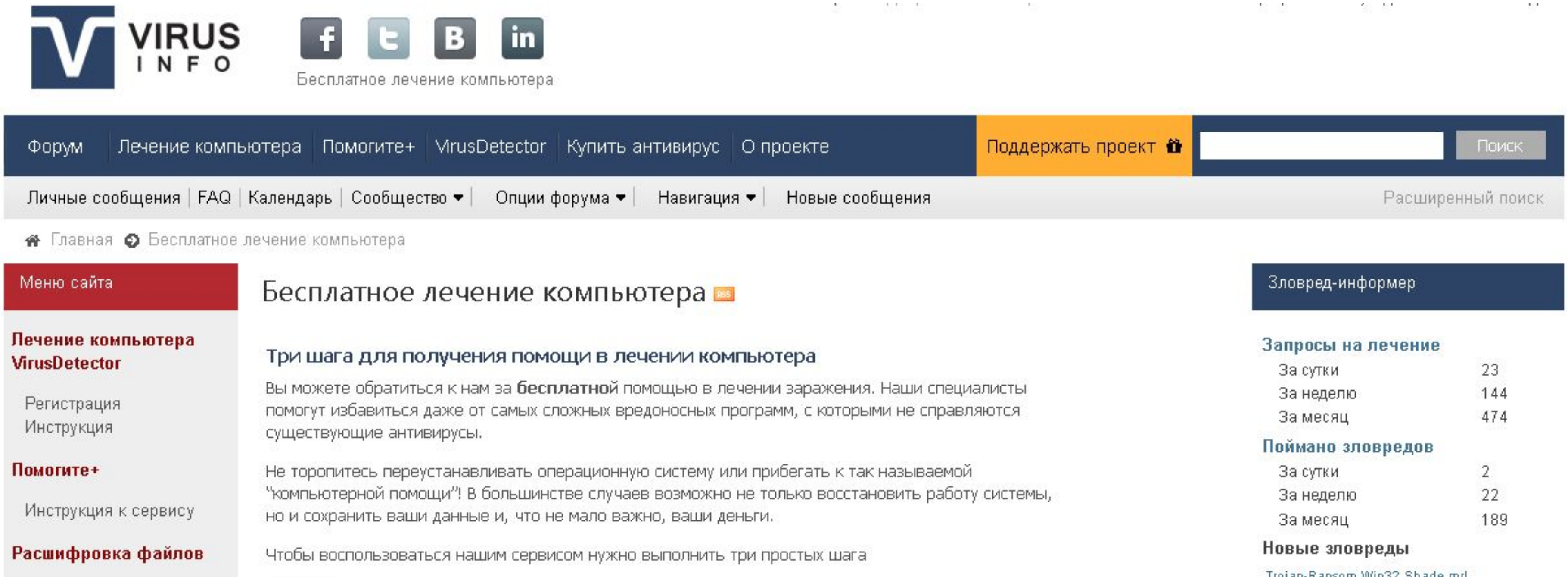
Файл, который был зашифрован и не открывается.

Обзор... Файл не выбран.

Addresses

https://id-ransomware.malwarehunterteam.com/

Virusinfo



Бесплатное лечение компьютера

Три шага для получения помощи в лечении компьютера

Вы можете обратиться к нам за **бесплатной** помощью в лечении заражения. Наши специалисты помогут избавиться даже от самых сложных вредоносных программ, с которыми не справляются существующие антивирусы.

Не торопитесь переустанавливать операционную систему или прибегать к так называемой "компьютерной помощи"! В большинстве случаев возможно не только восстановить работу системы, но и сохранить ваши данные и, что не мало важно, ваши деньги.

Чтобы воспользоваться нашим сервисом нужно выполнить три простых шага

Запросы на лечение	
За сутки	23
За неделю	144
За месяц	474
Поймано зловредов	
За сутки	2
За неделю	22
За месяц	189

Новые зловреды

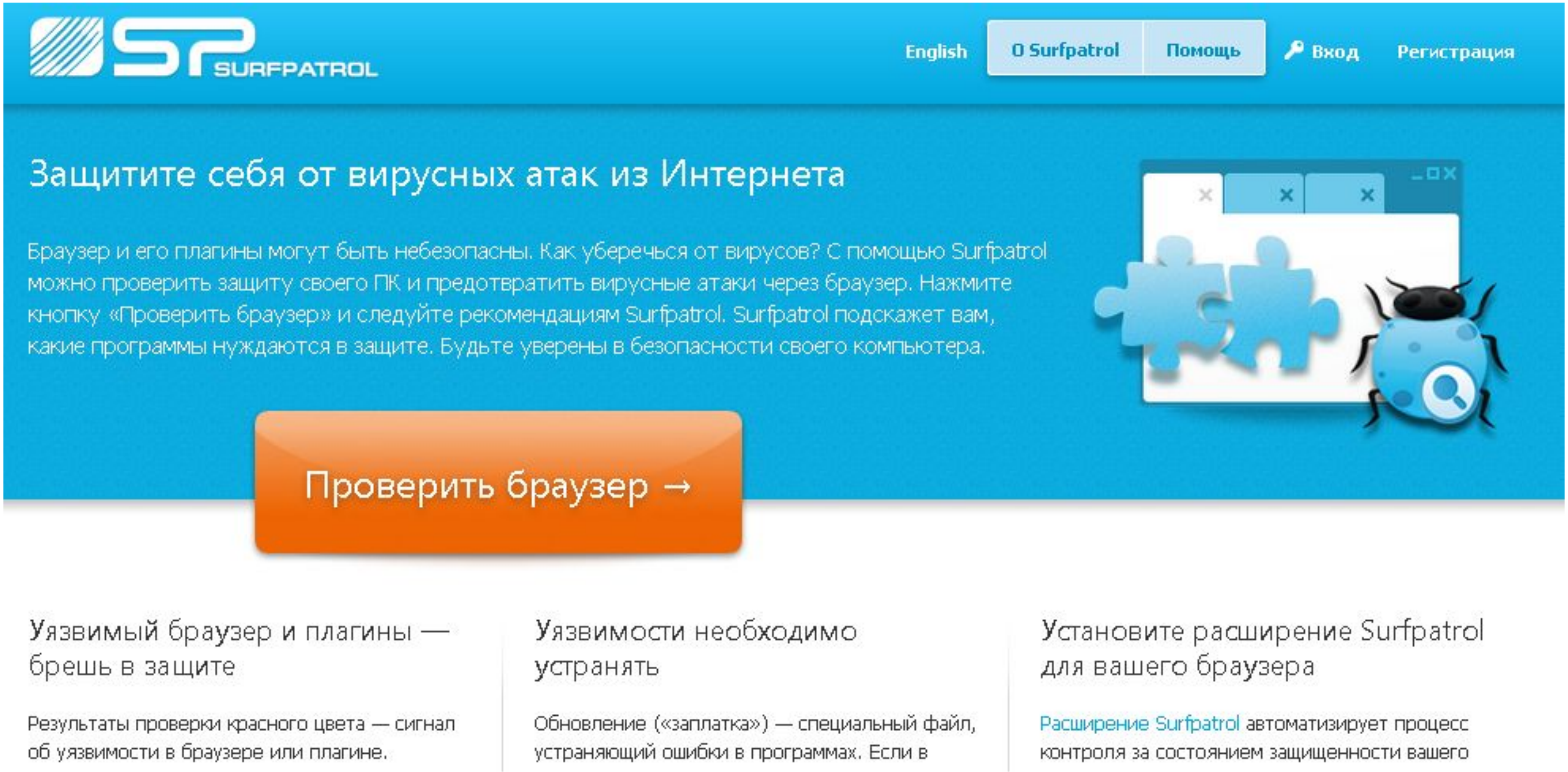
Trojan-Ransom.Win32.Shade.mrl

https://virusinfo.info/content.php

Бесплатные онлайн-сервисы для поиска потенциально опасных сайтов, https://zeltser.com/lookup-malicious-websites/

Бесплатные песочницы и сервисы для анализа вредоносов, https://zeltser.com/automated-malware-analysis/

Surfpatrol



Защитите себя от вирусных атак из Интернета

Браузер и его плагины могут быть небезопасны. Как уберечься от вирусов? С помощью Surfpatrol можно проверить защиту своего ПК и предотвратить вирусные атаки через браузер. Нажмите кнопку «Проверить браузер» и следуйте рекомендациям Surfpatrol. Surfpatrol подскажет вам, какие программы нуждаются в защите. Будьте уверены в безопасности своего компьютера.

Уязвимый браузер и плагины — брешь в защите

Результаты проверки красного цвета — сигнал об уязвимости в браузере или плагине.

Уязвимости необходимо устранять

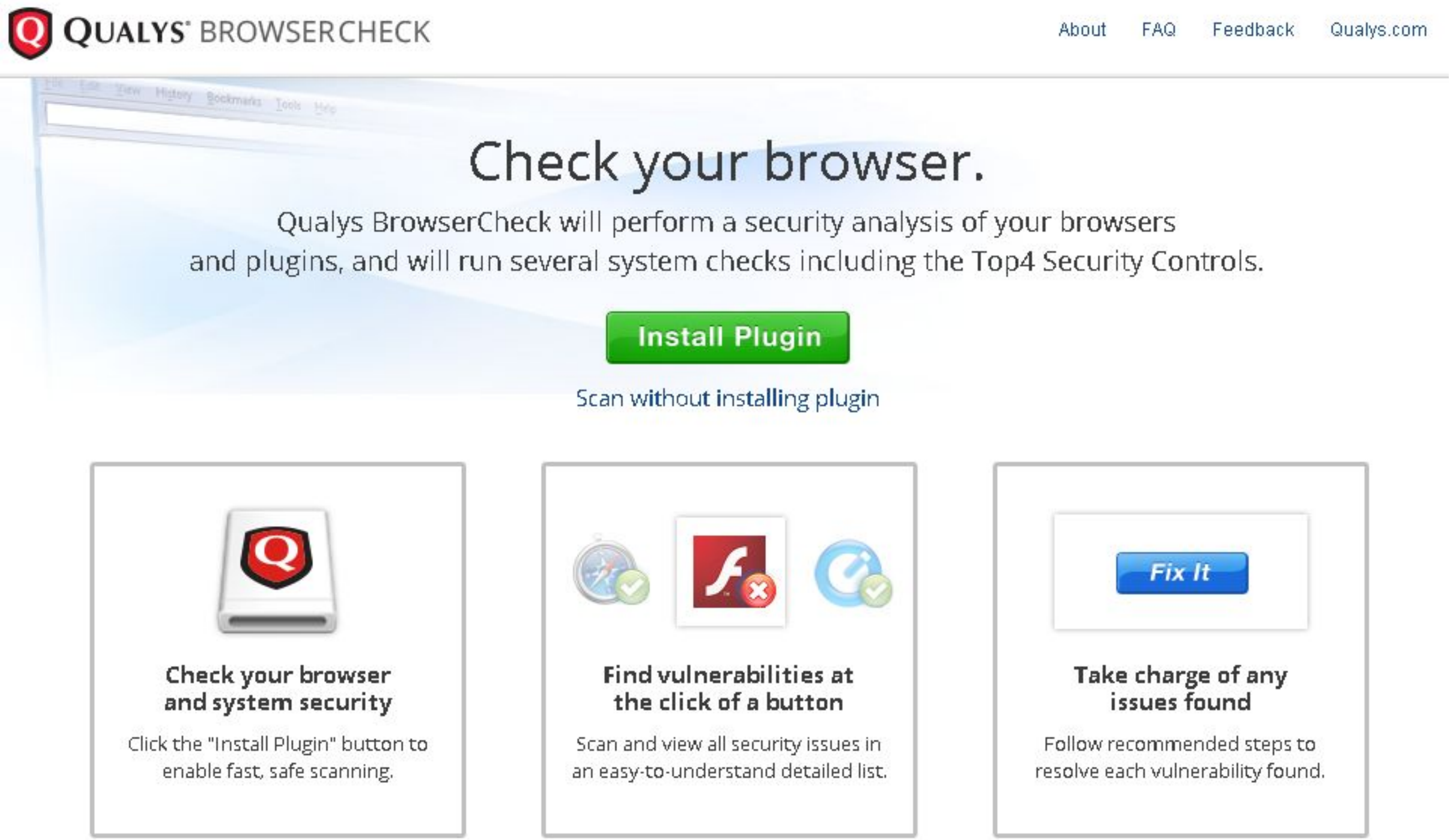
Обновление («заплатка») — специальный файл, устраняющий ошибки в программах. Если в

Установите расширение Surfpatrol для вашего браузера

Расширение Surfpatrol автоматизирует процесс контроля за состоянием защищенности вашего

http://www.surfpatrol.ru/

Qualys BrowserCheck



QUALYS BROWSERCHECK

About FAQ Feedback Qualys.com

Check your browser.

Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.

Install Plugin

Scan without installing plugin

Check your browser and system security

Click the "Install Plugin" button to enable fast, safe scanning.

Find vulnerabilities at the click of a button

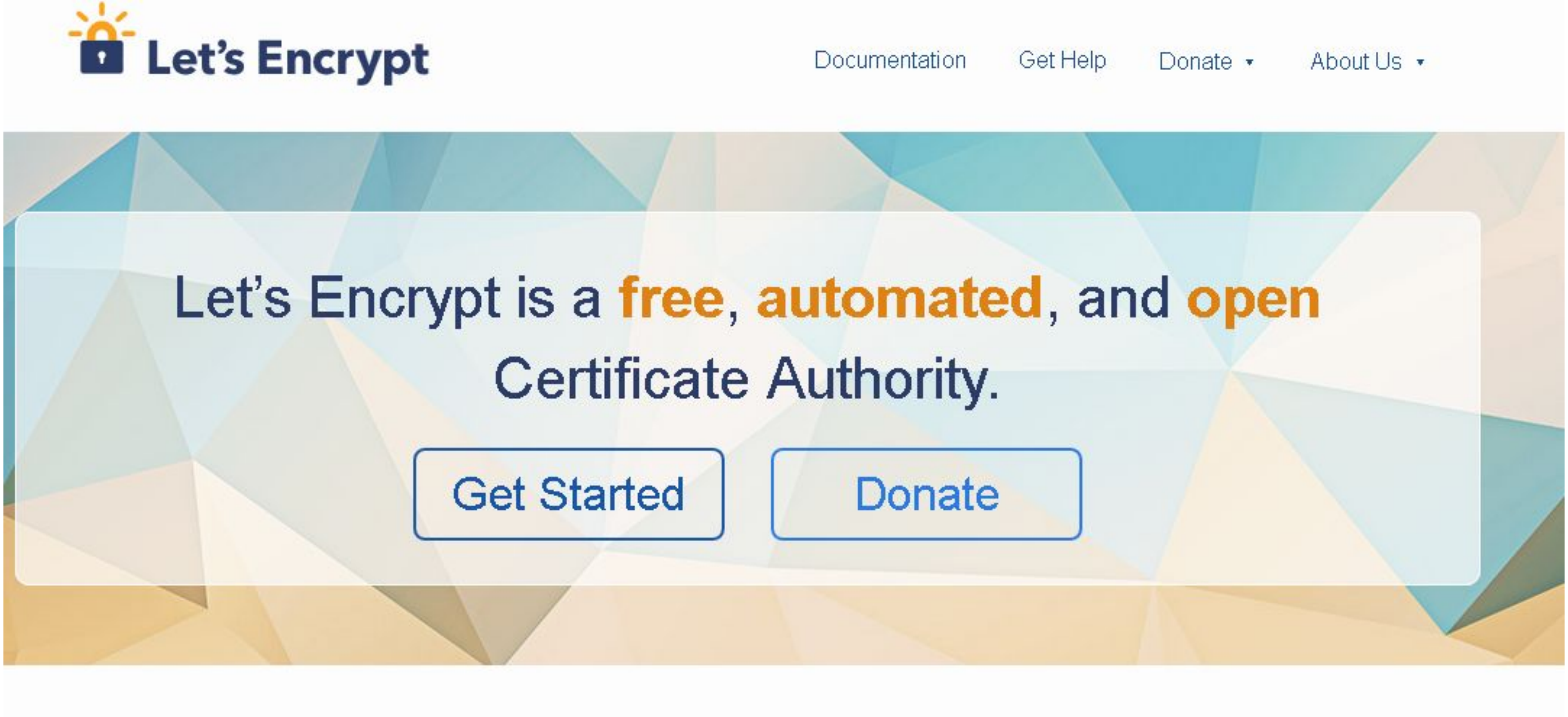
Scan and view all security issues in an easy-to-understand detailed list.

Take charge of any issues found

Follow recommended steps to resolve each vulnerability found.

https://browsercheck.qualys.com/

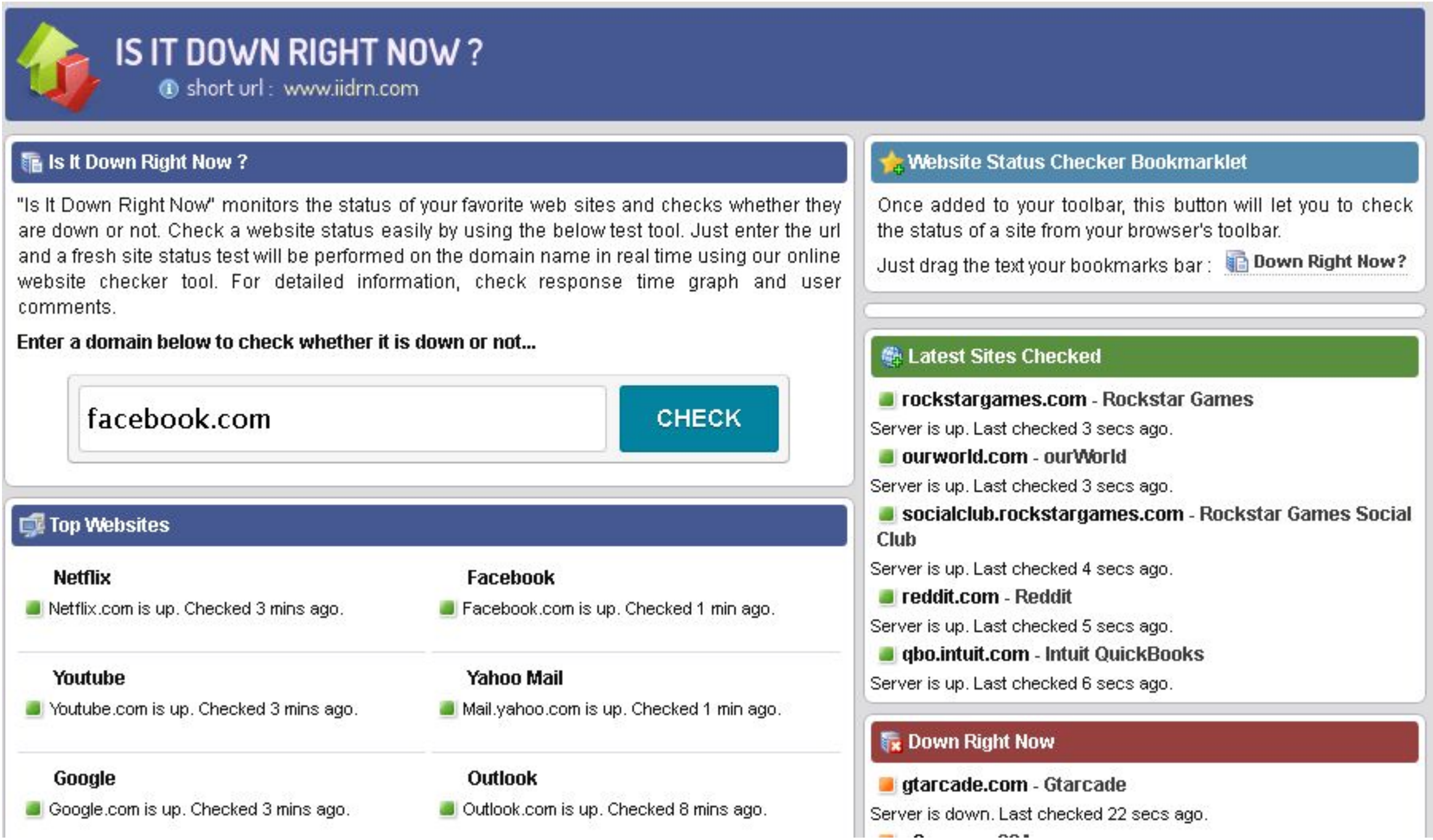
Let's Encrypt



Let's Encrypt is a **free**, **automated**, and **open** Certificate Authority.

https://letsencrypt.org/

Is It Down Right Now?



IS IT DOWN RIGHT NOW ?

short url : www.iidrn.com

Is It Down Right Now ?

"Is It Down Right Now" monitors the status of your favorite web sites and checks whether they are down or not. Check a website status easily by using the below test tool. Just enter the url and a fresh site status test will be performed on the domain name in real time using our online website checker tool. For detailed information, check response time graph and user comments.

Enter a domain below to check whether it is down or not...

facebook.com

CHECK

Top Websites

Netflix
🟩 Netflix.com is up. Checked 3 mins ago.

Facebook
🟩 Facebook.com is up. Checked 1 min ago.

Youtube
🟩 Youtube.com is up. Checked 3 mins ago.

Yahoo Mail
🟩 Mail.yahoo.com is up. Checked 1 min ago.

Google
🟩 Google.com is up. Checked 3 mins ago.

Outlook
🟩 Outlook.com is up. Checked 8 mins ago.

Website Status Checker Bookmarklet

Once added to your toolbar, this button will let you to check the status of a site from your browser's toolbar.

Just drag the text your bookmarks bar : Down Right Now?

Latest Sites Checked

🟩 **rockstargames.com** - Rockstar Games
Server is up. Last checked 3 secs ago.

🟩 **ourworld.com** - ourWorld
Server is up. Last checked 3 secs ago.

🟩 **socialclub.rockstargames.com** - Rockstar Games Social Club
Server is up. Last checked 4 secs ago.

🟩 **reddit.com** - Reddit
Server is up. Last checked 5 secs ago.

🟩 **qbo.intuit.com** - Intuit QuickBooks
Server is up. Last checked 6 secs ago.

Down Right Now

🟧 **gtarcade.com** - Gtarcade
Server is down. Last checked 22 secs ago.

http://www.isitdownrightnow.com/

Спасибо за внимание!