Немного про тестирование безопасности с точки зрения QA

Как укрепить защиту периметра своей компании
с помощью open source инструментов

www.internetlivestats.com/watch/websites/

internet live stats live 1 second watch trends & more

Total number of Websites

1,933,898,772

All on this page, one by one

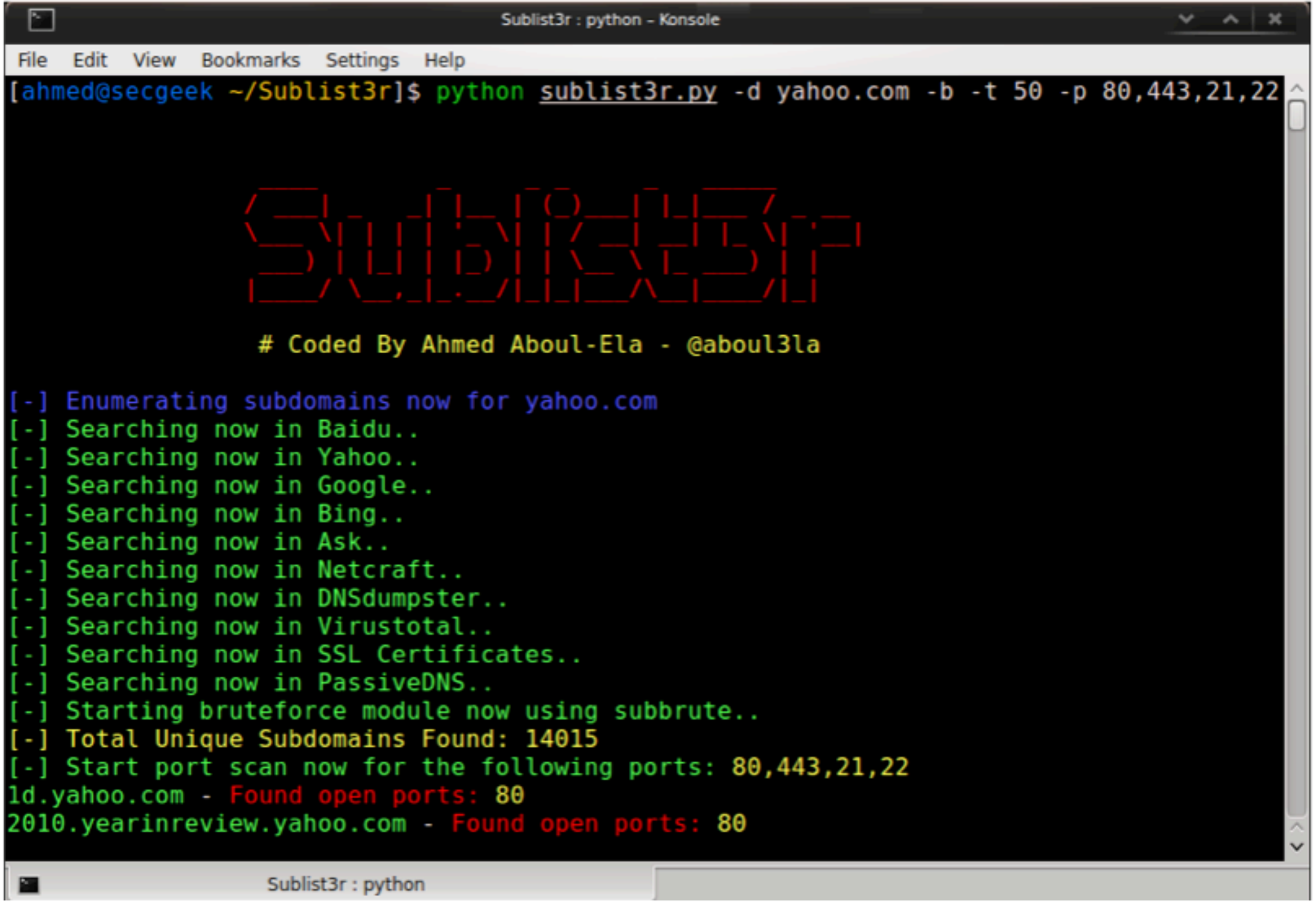
watch as they increase

http://www.internetlivestats.com/watch/websites/

OWASP Top 10 Application Security Risks - 2017

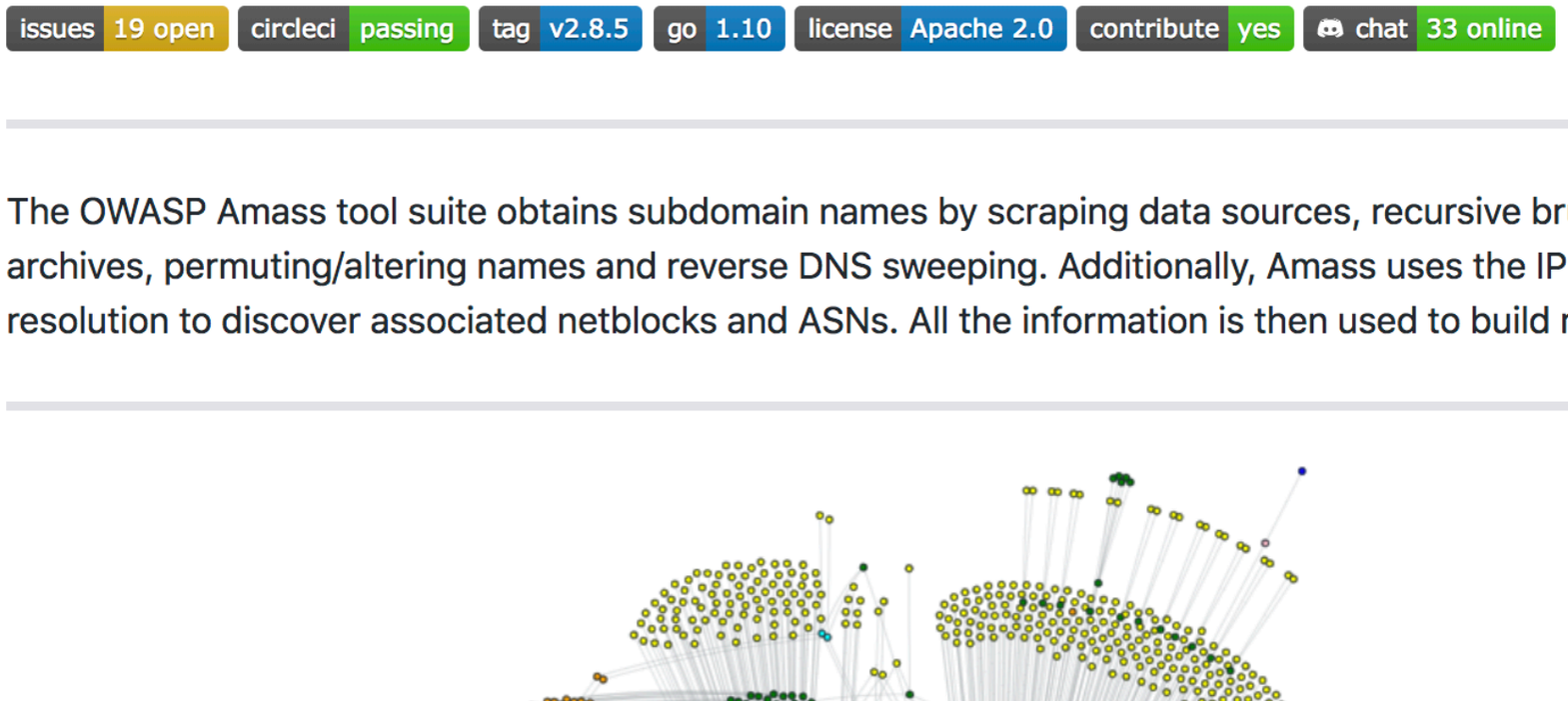
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Google	
Facebook	
Yahoo	$3,000,000
Uber	$1,661,094
Twitter	$1,039,240
GitHub	$345,900
Snapchat	$260,367
Pornhub	$215,495

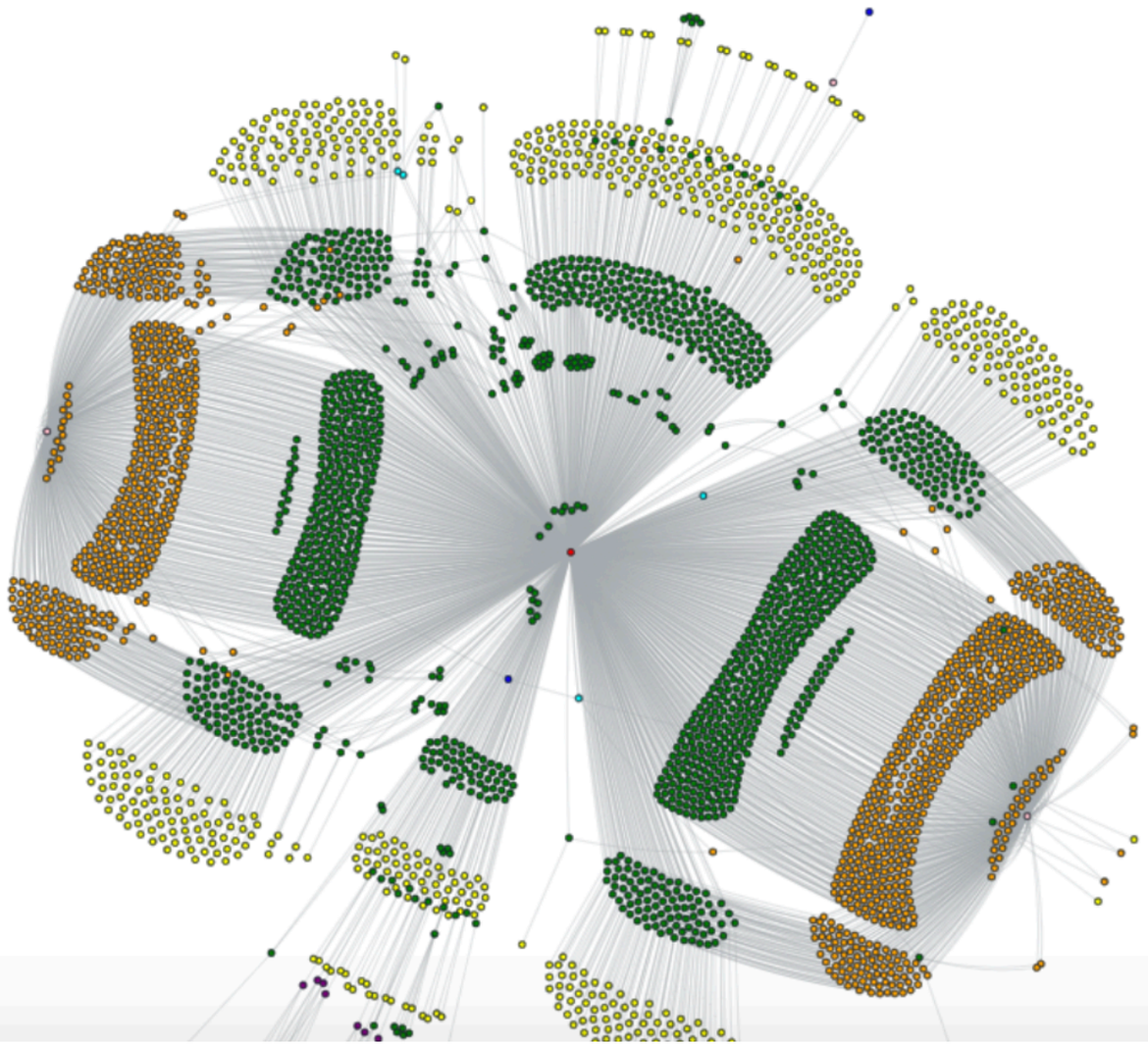


https://github.com/aboul3la/Sublist3r

OWASP Amass



The OWASP Amass tool suite obtains subdomain names by scraping data sources, recursive brute forcing, crawling web archives, permuting/altering names and reverse DNS sweeping. Additionally, Amass uses the IP addresses obtained during resolution to discover associated netblocks and ASNs. All the information is then used to build maps of the target networks.



https://github.com/OWASP/Amass

https://tns-2161-www.k.avito.ru/
http://admin5.hh.ru/
https://bgr1-itdep-office.hh.ru
http://git.dev.us-south.continuous-delivery.cloud.ibm.com
https://webmaster-2036-teamcity.trusty-sas.webmaster.dev.yandex.com

Hi, I'm Michael. Security engineer, internet sleuth and builder of tools.

© 2018 Michael Henriksen | about | blog | projects

Buy me a coffee

AQUATONE: A tool for domain flyovers

Posted June 17, 2017

The Lockheed U-2 reconnaissance aircraft was given the codename Aquatone.

Knowing the attack surface of something is critical for both defending and attacking it. When it comes to domain names, a very common approach for uncovering the attack surface is to discover its subdomains. Subdomains will increase the number of potential target sites as well as uncover IP ranges to probe further.

https://github.com/michenriksen/aquatone

200 OK

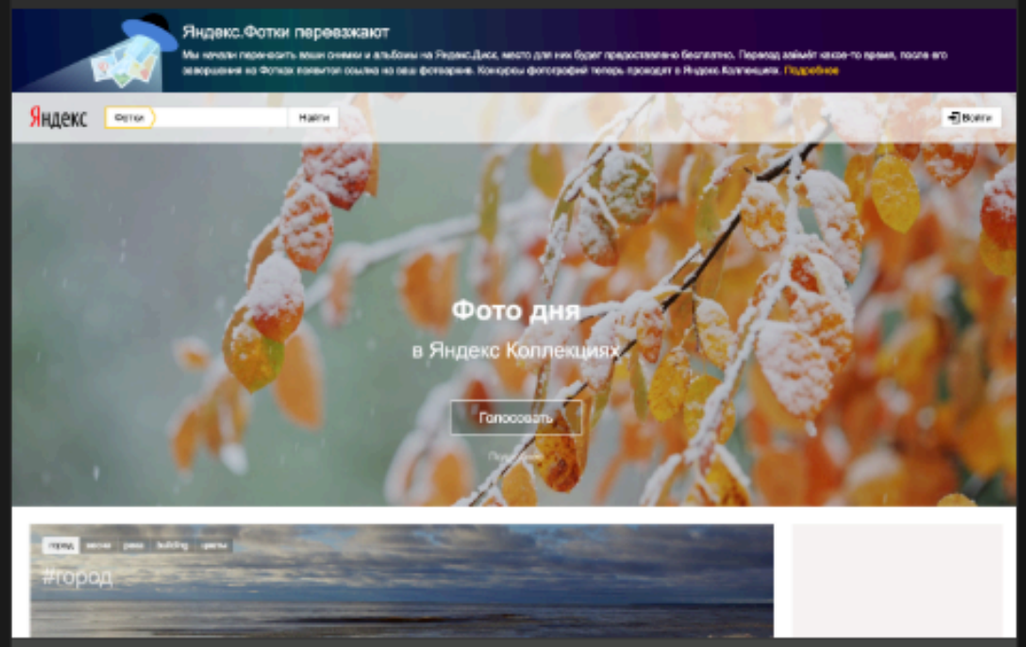
Nginx React jQuery

NO SCREENSHOT AVAILABLE

Details Visit

200 OK

Nginx React jQuery



Details Visit

200 OK

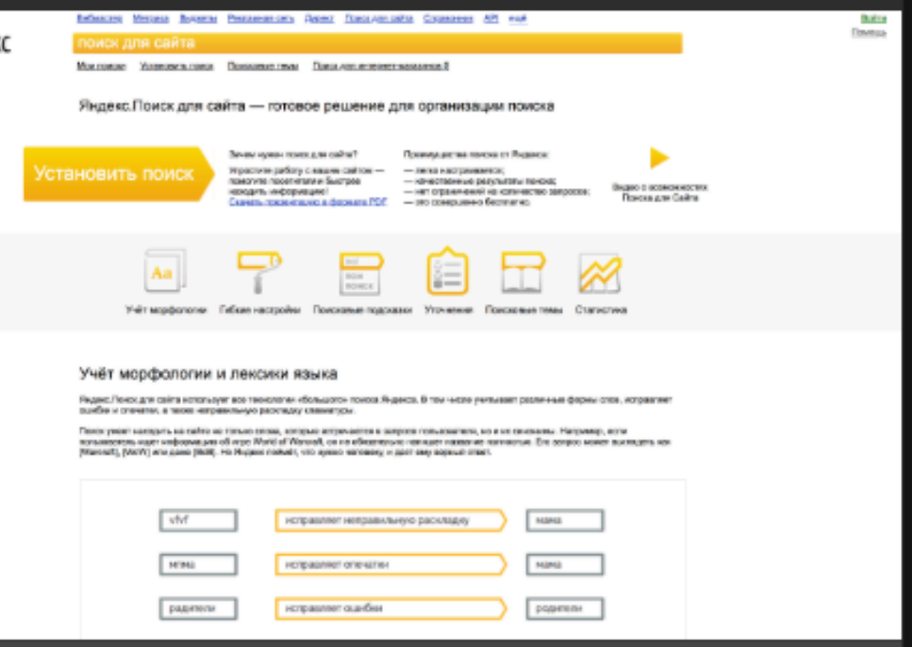
Nginx React

Details Visi

p://site.ya.ru/

Internal Server Error

nx



http://travel.ya.ru/

404 Not Found

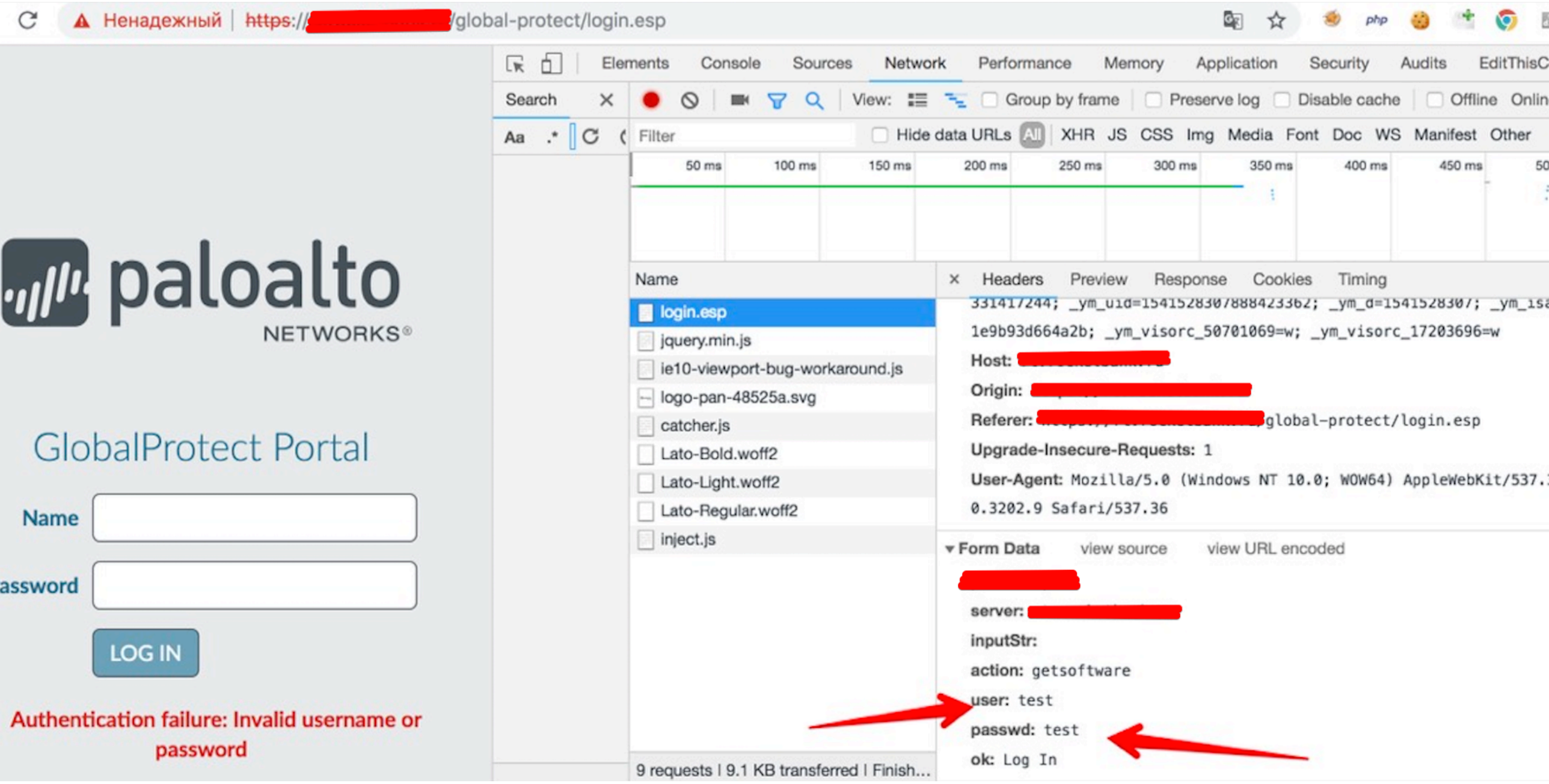
Nginx

http://pda.wc.ya.ru/

404 Not Found

Nginx

Вот так в 2018 году не должно быть ни на одном из ваших доменов:



Ненадежный | https:/[redacted]

```
INSTALLED_APPS                  [ 'django.contrib.staticfiles',
                                 'django.contrib.humanize',
                                 'raven.contrib.django.raven_compat',
                                 'backupdb',
                                 'django_extensions',
                                 'compressor',
                                 [redacted]mozilla']
INTERNAL_IPS                    []
INXPO_PARAMETERS                {'AUTH_CODE': '[redacted]',
                                 'SHOW_KEY': '**********',
                                 'SHOW_PACKAGE_KEY': '**********',
                                 'USER_CREDENTIALS': '[redacted]'}
```

Основная страница давно забытого сайта..

dirsearch — Python dirsearch.py -e CHANGELOG.md README.md allpaths.txt db default.conf dirsearch.py lib logs nginx reports thirdparty yandex yandexbig

```
[14:50:19] Starting:
[14:50:19] 301 -  178B  - /CHANGELOG.md  ->  https://fotki.yandex.ru/CHANGELOG.md
[14:50:23] 301 -  178B  - /CHANGELOG.md  ->  https://fotki.yandex.ru/CHANGELOG.md
[14:50:36] 301 -  178B  - /adminCHANGELOG.md  ->  https://fotki.yandex.ru/adminCHANGELOG.md
[14:50:44] 301 -  178B  - /myadminCHANGELOG.md  ->  https://fotki.yandex.ru/myadminCHANGELOG.md

Target: https://www.vogino.photos.yandex.ru/

[14:50:48] Starting:
[14:50:49] 301 -  178B  - /CHANGELOG.md  ->  https://fotki.yandex.ru/CHANGELOG.md
[14:50:52] 301 -  178B  - /CHANGELOG.md  ->  https://fotki.yandex.ru/CHANGELOG.md
[14:51:04] 301 -  178B  - /adminCHANGELOG.md  ->  https://fotki.yandex.ru/adminCHANGELOG.md
[14:51:13] 301 -  178B  - /myadminCHANGELOG.md  ->  https://fotki.yandex.ru/myadminCHANGELOG.md

Target: https://www.validator-api.semweb.yandex.ru/

Couldn't resolve DNS

Target: https://www.validator-rc.yandex.ru/

Couldn't resolve DNS

Target: https://www.validator.yandex.ru/

[14:51:18] Starting:

Target: https://www.vendor.market.yandex.ru/

Couldn't resolve DNS

Target: https://www.vesna.yandex.ru/

[14:53:10] Starting:

Target: https://www.video.yandex.ru/

[14:54:40] Starting:
[14:55:09] 200 -  610B  - /index.html
[14:55:23] 301 -  178B  - /upload/  ->  https://disk.yandex./
[14:55:33] 301 -  178B  - /_  ->  https://localhost/_/
[14:55:51] 200 -    1KB - /crossdomain.xml
[14:55:55] 301 -  178B  - /favicon.ico  ->  https://yastatic.net/islands-icons/_/ScXmk_CH9cCtdXl0GzdpgxSQjdI.ico
[14:55:56] 301 -  178B  - /help  ->  https://yandex./support/video/
[14:55:56] 301 -  178B  - /help/  ->  https://yandex./support/video/
[14:55:58] 200 -  610B  - /index.html
[14:56:07] 301 -  178B  - /partners  ->  https://yandex./support/video/partners/partner-program.xml
[14:56:10] 200 -    0B  - /ping
[14:56:13] 200 -  388B  - /robots.txt
[14:56:13] 301 -  178B  - /search  ->  https://yandex./video/search
[14:56:19] 301 -  178B  - /tags  ->  https://yandex./video/search?text=
[14:56:21] 301 -  178B  - /upload  ->  https://disk.yandex./
[14:56:21] 301 -  178B  - /upload/  ->  https://disk.yandex./

Target: https://www.visit-monitor.yandex.ru/
```

https://github.com/maurosoria/dirsearch

https://github.com/maurosoria/dirsearch

Dismiss

Join GitHub today

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

Sign up

Fetch many paths for many hosts - without killing the hosts

77 commits | 4 branches | 9 releases | 3 contributors | MIT

Branch: master | New pull request | Find file | Clone or download

tomnomnom Adds some tweaks to http.Transport to keep file descriptors under con... | Latest commit 2507780 18 days ago

lists	Adds lists, disables Opaque suffix	a year ago
script	Adds contrib, licence, release script	11 months ago
.gitignore	Switches prefix/suffix teminology to host/path; breaking change; fixes ...	11 months ago
CONTRIBUTING.mkd	Adds contrib, licence, release script	11 months ago
LICENSE	Adds contrib, licence, release script	11 months ago
README.mkd	Adds install help to readme	9 months ago
args.go	Adds --no-headers option	2 months ago
gohttp.go	Adds some tweaks to http.Transport to keep file descriptors under con...	18 days ago

equest failed: Get https://et17-1.fab2-1-gdc.gq2.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://gops.usm113.mobstor.vip.ne1.yahoo.com/pi.php: dial tcp 98.136.97.52:443: connect: connection refused
equest failed: Get https://lg-optimus-sol.en.9apps.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://ironic-reserved-ipv6-53431-124.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:2401::2:a0f1]:443: connect: no route to host
equest failed: Get https://mail225-150.mail.alibaba.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://mapi-wrapper2.mall.vip.tw1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://ca104.progrss.bf1.yahoo.com/pi.php: dial tcp 98.139.136.172:443: connect: connection refused
equest failed: Get https://mail139-49.mail.alibaba.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://oxy-oxygen-2001-4998-58-5864--4088.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:5864::4088]:443: connect: no route to host
equest failed: Get https://mta5.email.sel.sony.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://vengate.pok.ibm.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://13306081.ostk.bm2.prod.bf1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://out210-92.dm.aliyun.com/pi.php: dial tcp 140.205.210.92:443: connect: connection refused
equest failed: Get https://out25-139.mail.alibaba.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://1046519.ostk.bm2.prod.bf1.yahoo.com/pi.php: dial tcp 72.30.41.107:443: connect: connection refused
equest failed: Get https://ozone.gs.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://sync700056.mail.ir2.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://ironic-reserved-ipv6-52992-342.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:1800::1155]:443: connect: no route to host
equest failed: Get https://hz-network-migration-75121-236.tw1.yahoo.com/pi.php: dial tcp [2406:2000:fc:c10::10eb]:443: connect: no route to host
equest failed: Get https://out211-50.dm.aliyun.com/pi.php: dial tcp 140.205.211.50:443: connect: connection refused
equest failed: Get https://as1501.access.mail.vip.gq1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://out3135-131.mail.aliyun.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://oxy-oxygen-4a0633ea.bf1.yahoo.com/pi.php: dial tcp 74.6.51.234:443: connect: network is unreachable
equest failed: Get https://stg-jpst002.ysl.corp.gq1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://hz-network-migration-82544-423.tp2.yahoo.com/pi.php: dial tcp [2406:2000:ec:c10::11a6]:443: connect: no route to host
equest failed: Get https://code-morning-ntranslator.ar.9apps.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://hz-network-migration-75126-220.tw1.yahoo.com/pi.php: dial tcp [2406:2000:fc:c15::10dd]:443: connect: no route to host
equest failed: Get https://ironic-reserved-ipv6-52992-346.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:1800::1159]:443: connect: no route to host
equest failed: Get https://71.195.43.202.aprez.ostk.prod.tw1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://56712-v6-bucket-5637105-52997-180.flakey.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:1805::10b6]:443: connect: no route to host
equest failed: Get https://ironic-reserved-ipv6-98905-232.gq1.yahoo.com/pi.php: dial tcp [2001:4998:c:1026::70e8]:443: connect: no route to host
equest failed: Get https://tw56069-v6-ostk-1691057-50093-401.prod.tw1.yahoo.com/pi.php: dial tcp [2406:2000:fc:b::2:a193]:443: connect: no route to host
equest failed: Get https://ironic-reserved-ipv6-101122-153.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:5852::1098]:443: connect: no route to host
equest failed: Get https://vl-224.bas1-1-flk.gq1.yahoo.com/pi.php: dial tcp 67.195.16.131:443: connect: connection refused
equest failed: Get https://as11.access.mail.vip.gq1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://out29-167.mail.aliyun.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://out29-254.mail.aliyun.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://oxy-oxygen-4a06336d.bf1.yahoo.com/pi.php: dial tcp 74.6.51.109:443: connect: network is unreachable
equest failed: Get https://bos-k026a-rdr1.blue.icq.net/pi.php: tls: first record does not look like a TLS handshake
equest failed: Get https://hz-network-migration-75199-216.ir2.yahoo.com/pi.php: dial tcp [2a00:1288:110:81e::10d7]:443: connect: no route to host
equest failed: Get https://b22.f59.ymdb.tw1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://hz-network-migration-82542-82.tp2.yahoo.com/pi.php: dial tcp [2406:2000:ec:c0f::1051]:443: connect: no route to host
equest failed: Get https://ironic-reserved-ipv6-101461-276.bf1.yahoo.com/pi.php: dial tcp [2001:4998:58:5868::1115]:443: connect: no route to host
equest failed: Get https://gi-1-19.bas5-1-grd.gq1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://out21-16.dm.aliyun.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://ha19-mta.dns.gq1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://ironic-reserved-ipv4-98060-48.ir2.yahoo.com/pi.php: dial tcp 87.248.96.118:443: connect: network is unreachable
equest failed: Get https://247.237.139.98.aprez.ostk.prod.bf1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://ra2-mail.dns.ne1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://dcwxpphesa002.imr.gm.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://xe-7-1-0.msr2.bf1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://gpiecjp.partner.boulder.ibm.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://out210-204.dm.aliyun.com/pi.php: dial tcp 140.205.210.204:443: connect: connection refused
equest failed: Get https://lo0.usw6-57-pdc.bf1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://pcdash1-vm1.stage.cp.bf1.yahoo.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
equest failed: Get https://dr-safety-data-security-free.en.9apps.com/pi.php: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)

Sensitive data exposure

[redacted].microsoft.com/info.php

_SERVER["APPSETTING_KeyVault_Secret_AZURE_STORAGE_KEY"]	[redacted]

_SERVER["KeyVault_Secret_AZURE_STORAGE_KEY"]	[redacted]
_SERVER["APPSETTING_KeyVault_Secret_AZURE_STORAGE_KEY"]	[redacted]
_SERVER["KeyVault_Secret_DB_HOST"]	[redacted]
_SERVER["APPSETTING_KeyVault_Secret_DB_HOST"]	[redacted]
_SERVER["KeyVault_Secret_DB_NAME"]	[redacted]
_SERVER["APPSETTING_KeyVault_Secret_DB_NAME"]	[redacted]
_SERVER["KeyVault_Secret_DB_PASSWORD"]	[redacted]
_SERVER["APPSETTING_KeyVault_Secret_DB_PASSWORD"]	[redacted]
_SERVER["KeyVault_Secret_DB_USER"]	[redacted]
_SERVER["APPSETTING_KeyVault_Secret_DB_USER"]	[redacted]
_SERVER["KeyVault_Secret_EMAIL_ENCRYPTION_KEY"]	[redacted]

Ненадежный [redacted]yahoo.com/server-status

Apache Server Status for [redacted]

Server Version: Apache/2.2.31 (Unix)
Server Built: Jul 20 2016 04:08:52

Current Time: Tuesday, 27-Nov-2018 13:48:40 UTC
Restart Time: Friday, 20-Jul-2018 15:33:35 UTC
Parent Server Generation: 0
Server uptime: 129 days 22 hours 15 minutes 5 seconds
Total accesses: 3354101 - Total Traffic: 45.2 MB
CPU Usage: u822.38 s620.6 cu0 cs0 - .0129% CPU load
.299 requests/sec - 4 B/second - 14 B/request
1 requests currently being processed, 299 idle workers

_____
_____
_____
_____
_____W_____
_____
_____
_____
_____
_____

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	34847	0/2976/11180	_	4.67	462	1	0.0	0.01	0.12	127.0.0.1	[redacted]	GET /status.html HTTP/1.1
1-0	39584	0/2425/11182	_	3.83	444	1	0.0	0.02	0.13	127.0.0.1	[redacted]	GET /status.html HTTP/1.1

Server Settings, Startup Hooks, Request Hooks

Loaded Modules:
mod_appdynamics.cpp, mod_ssl.c, mod_proxy_ajp.c, mod_jk.c, mod_cgi.c, mod_disk_cache.c, mod_suexec.c, mod_cache.c, mod_proxy_connect.c, mod_proxy_http.c, mod_proxy_ftp.c, mod_proxy_balancer.c, mod_proxy.c, mod_rewrite.c, mod_alias.c, mod_userdir.c, mod_speling.c, mod_actions.c, mod_dir.c, mod_negotiation.c, mod_vhost_alias.c, mod_dav_fs.c, mod_in
mod_autoindex.c, mod_status.c, mod_dav.c, mod_mime.c, mod_setenvif.c, mod_usertrack.c, mod_headers.c, mod_deflate.c, mod_expires.c, mod_mime_magic.c, mod_ext_filter.c, mod_env.c
mod_logio.c, mod_log_config.c, mod_include.c, mod_authnz_ldap.c, util_ldap.c, mod_authz_default.c, mod_authz_dbm.c, mod_authz_groupfile.c, mod_authz_owner.c, mod_authz_user.c,
mod_authz_host.c, mod_authn_default.c, mod_authn_dbm.c, mod_authn_anon.c, mod_authn_alias.c, mod_authn_file.c, mod_auth_digest.c, mod_auth_basic.c, mod_so.c, http_core.c, worker
core.c

Server Settings

Server Version: Apache/2.2.17 (Unix) DAV/2 mod_jk/1.2.31 mod_ssl/2.2.17 OpenSSL/1.0.0-fips
Server Built: Feb 9 2012 12:02:07
Server loaded APR Version: 1.3.9
Compiled with APR Version: 1.3.9
Server loaded APU Version: 1.3.9
Compiled with APU Version: 1.3.9
Module Magic Number: 20051115:25
Hostname/port [redacted]toyota.com:80
Timeouts: connection: 120 keep-alive: 15
MPM Name: Worker
MPM Information: Max Daemons: 10 Threaded: yes Forked: yes
Server Architecture: 64-bit
Server Root: /www/httpd.access-2
Config File: /www/httpd.access-2/conf/httpd.conf
Server Built With:

```
 -D APACHE_MPM_DIR="server/mpm/prefork"
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
 -D APR_USE_SYSVSEM_SERIALIZE
 -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
 -D APR_HAS_OTHER_CHILD
 -D AP_HAVE_RELIABLE_PIPED_LOGS
 -D HTTPD_ROOT="/etc/httpd"
 -D SUEXEC_BIN="/usr/sbin/suexec"
 -D DEFAULT_ERRORLOG="logs/error_log"
 -D AP_TYPES_CONFIG_FILE="conf/mime.types"
 -D SERVER_CONFIG_FILE="conf/httpd.conf"
```

w9w 11 октября 2018 в 17:28

[Bug bounty | mail.ru] Доступ к админ панели партнерского сайта и раскрытие данных 2 млн пользователей

IT-компании, Информационная безопасность, Разработка веб-сайтов, Тестирование IT-систем, Тестирование веб-сервисов

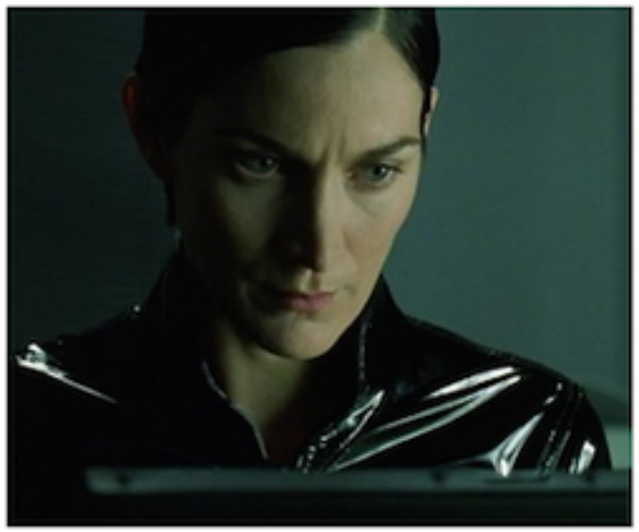
https://habr.com/post/416835/comments/

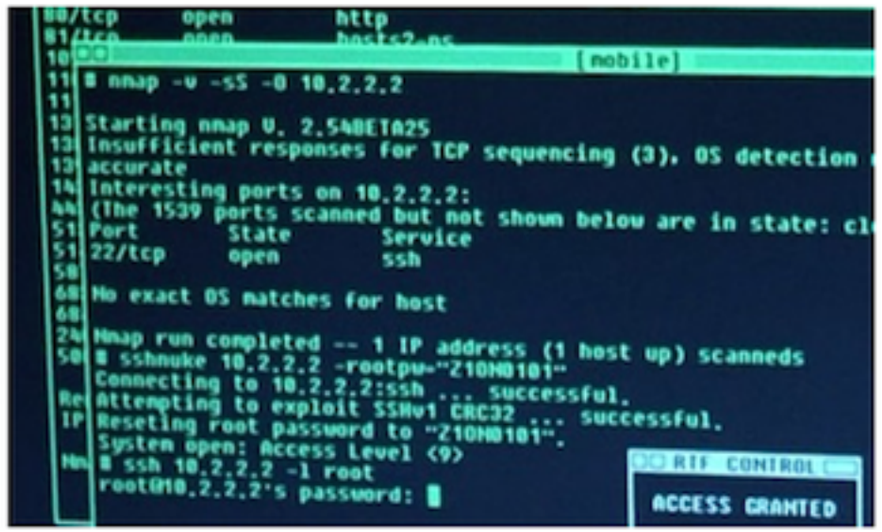
Комментарии 9

nikitasius 11 октября 2018 в 17:38 +1

Я бы поискал тут [redacted]mail.ru/Новая папка (3)/пароли.txt, да уже потерли все :/

Nmap



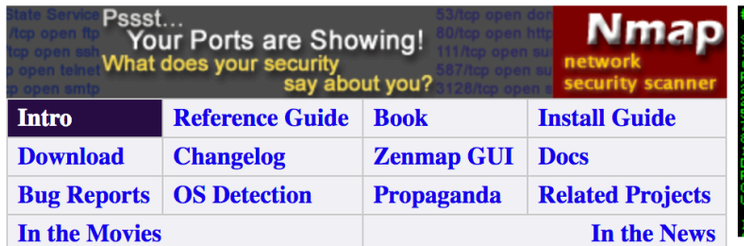


https://nmap.org

Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More



Intro	**Reference Guide**	**Book**	**Install Guide**
Download	**Changelog**	**Zenmap GUI**	**Docs**
Bug Reports	**OS Detection**	**Propaganda**	**Related Projects**
In the Movies			**In the News**

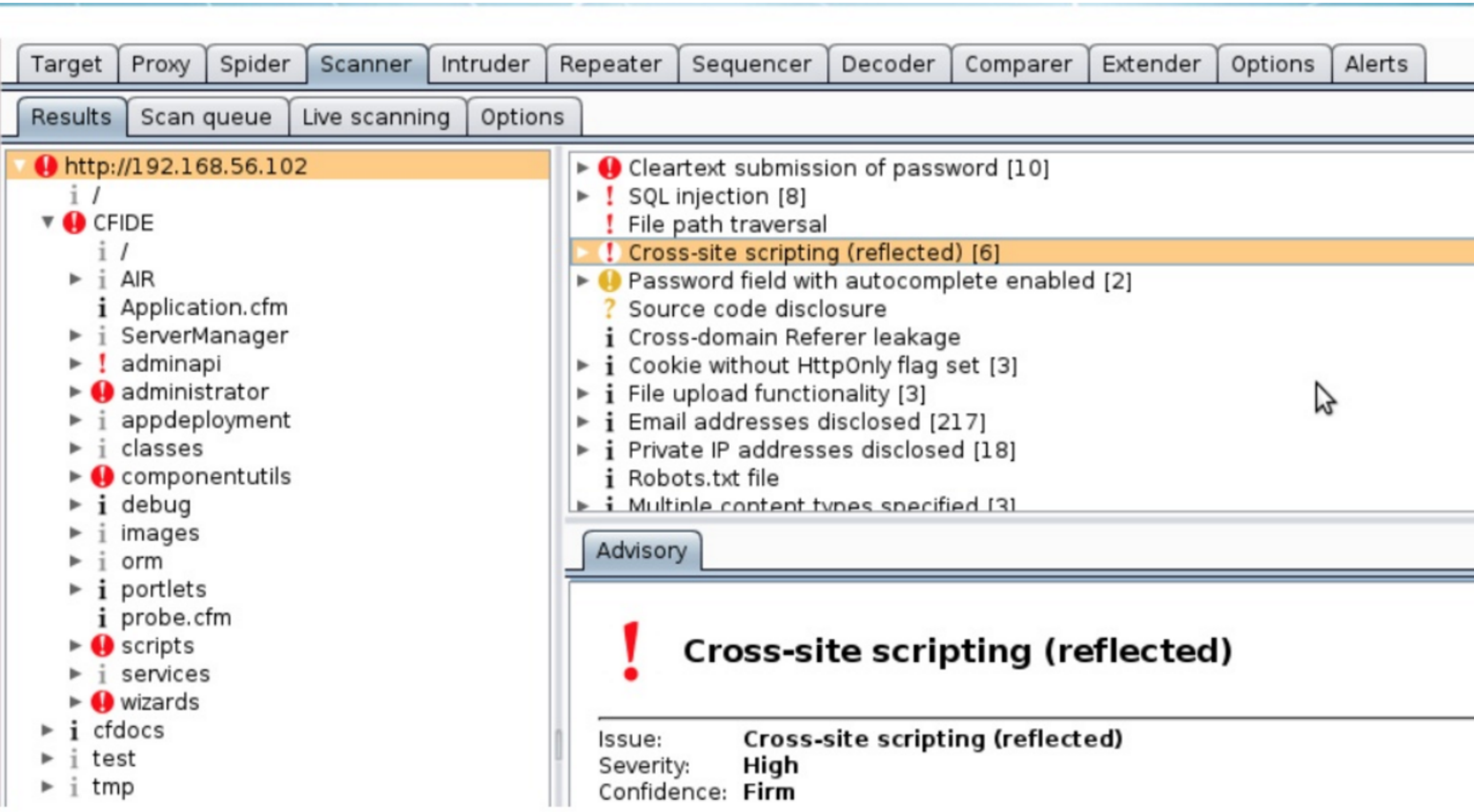
News

- Nmap 7.70 is now available! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.60 is now available! [release notes | download]
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on th
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in C
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many grea Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcem
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerpri

```
[mbp323msk:~ vpolyakov$ sudo nmap -Pn --script vuln [redacted] -vv
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-27 17:13 MSK
NSE: Loaded 103 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 17:13
NSE Timing: About 83.33% done; ETC: 17:13 (0:00:06 remaining)
Completed NSE at 17:13, 34.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 17:13
Completed NSE at 17:13, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     [redacted]
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
[redacted]
Initiating Parallel DNS resolution of 1 host. at 17:13
Completed Parallel DNS resolution of 1 host. at 17:13, 0.01s elapsed
Initiating SYN Stealth Scan at 17:13
Scanning edu.ozon.ru [redacted] [1000 ports]
Discovered open port 80/tcp on [redacted]
Discovered open port 445/tcp on [redacted]
Discovered open port 139/tcp on [redacted]
Discovered open port 22/tcp on [redacted]
Discovered open port 443/tcp on [redacted]
Discovered open port 50000/tcp on [redacted]
Discovered open port 9100/tcp on [redacted]
Discovered open port 9101/tcp on [redacted]
Discovered open port 9000/tcp on [redacted]
Discovered open port 636/tcp on [redacted]
Completed SYN Stealth Scan at 17:13, 0.42s elapsed (1000 total ports)
NSE: Script scanning [redacted]
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 17:13
NSE Timing: About 99.12% done; ETC: 17:14 (0:00:00 remaining)
NSE Timing: About 99.12% done; ETC: 17:14 (0:00:01 remaining)
NSE Timing: About 99.78% done; ETC: 17:15 (0:00:00 remaining)
NSE Timing: About 99.78% done; ETC: 17:15 (0:00:00 remaining)
NSE Timing: About 99.78% done; ETC: 17:16 (0:00:00 remaining)
Completed NSE at 17:16, 162.99s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 17:16
Completed NSE at 17:16, 0.00s elapsed
Nmap scan report for [redacted]
Host is up, received user-set (0.0098s latency).
Other addresses for [redacted]
Scanned at 2018-11-27 17:13:38 MSK for 163s
Not shown: 990 closed ports
Reason: 990 resets
PORT    STATE SERVICE     REASON
22/tcp  open  ssh         syn-ack ttl 59
80/tcp  open  http        syn-ack ttl 59
| http-aspnet-debug:
|_  status: DEBUG is enabled
| http-csrf:
```

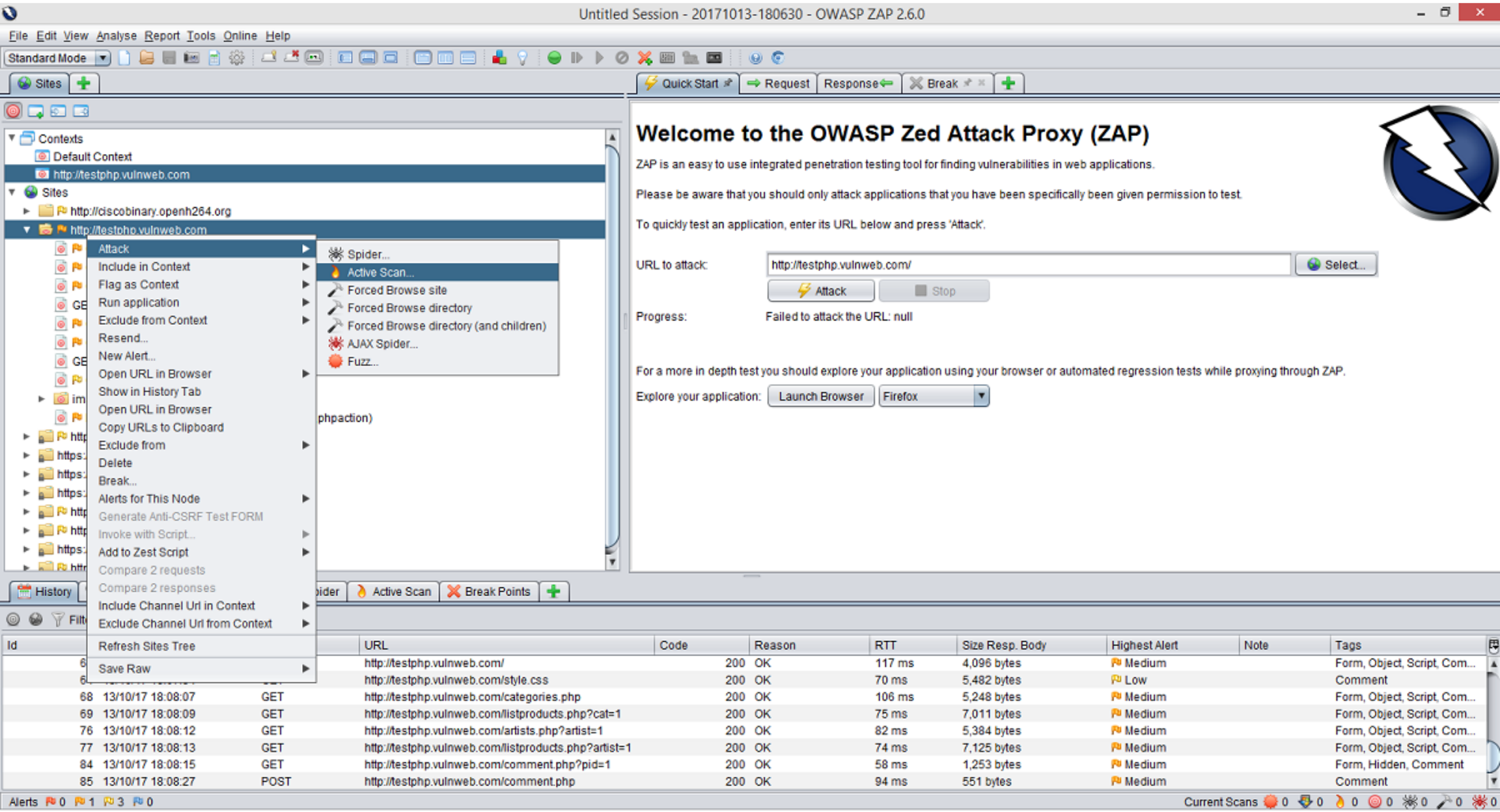
```
Scanned at 2018-11-27 17:13:38 MSK for 163s
Not shown: 990 closed ports
Reason: 990 resets
PORT    STATE SERVICE     REASON
22/tcp  open  ssh         syn-ack ttl 59
80/tcp  open  http        syn-ack ttl 59
| http-aspnet-debug:
|_  status: DEBUG is enabled
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=[redacted]
|   Found the following possible CSRF vulnerabilities:
|
|     Path: [redacted]
|     Form id: user_remember_frm
|     Form action: /?login=yes
|
|     Path: [redacted]
|     Form id: user_remember
|     Form action: /?login=yes
|
|     Path: [redacted]
|     Form id: user_remember_frm
|     Form action: /?login=yes&print_course=Y
|
|     Path: [redacted]
|     Form id: user_remember
|     Form action: /?login=yes&print_course=Y
|
|     Path: [redacted]
|     Form id: user_remember_frm
|     Form action: /?login=yes
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /login/: Login page
|   /mail/: Mail folder
|   /info.php: Possible information file
|   /errors/: Potentially interesting folder
|   /form/: Potentially interesting folder
|   /help/: Potentially interesting folder
|   /news/: Potentially interesting folder
|   /search/: Potentially interesting folder
|   /stat/: Potentially interesting folder
|   /tests/: Potentially interesting folder
|_  /xml/: Potentially interesting folder
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
|_sslv2-drown:
445/tcp   open  microsoft-ds syn-ack ttl 59
636/tcp   open  ldapssl      syn-ack ttl 59
| ssl-poodle:
|   VULNERABLE:
```

Burp Suite


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Results
Scan queue
Live scanning
Options
http://192.168.56.102
/
CFIDE
AIR
Application.cfm
ServerManager
adminapi
administrator
appdeployment
classes
componentutils
debug
images
orm
portlets
probe.cfm
scripts
services
wizards
cfdocs
test
tmp
Cleartext submission of password [10]
SQL injection [8]
File path traversal
Cross-site scripting (reflected) [6]
Password field with autocomplete enabled [2]
Source code disclosure
Cross-domain Referer leakage
Cookie without HttpOnly flag set [3]
File upload functionality [3]
Email addresses disclosed [217]
Private IP addresses disclosed [18]
Robots.txt file
Advisory
Cross-site scripting (reflected)
Issue: Cross-site scripting (reflected)
Severity: High
Confidence: Firm

OWASP ZAP

(если нет денег на BURP SUITE)



light reading

https://medium.com/@niruragu/so-you-want-to-be-a-security-engineer-d8775976afb7

https://medium.freecodecamp.org/so-you-want-to-work-in-security-bc6c10157d23

https://medium.com/@Nick_Jenkins/the-hitchhikers-guide-to-bug-bounty-hunting-throughout-the-galaxy-474ddb87ae15

P.S.

Для поиска секретов в репозиториях(токены, пароли, итд): gitrob
https://github.com/michenriksen/gitrob

Если есть вопросы-мой email johndoe1492@yandex.ru