



[GoogleHacking]

ДОКЛАДЧИК: [l1th1um]

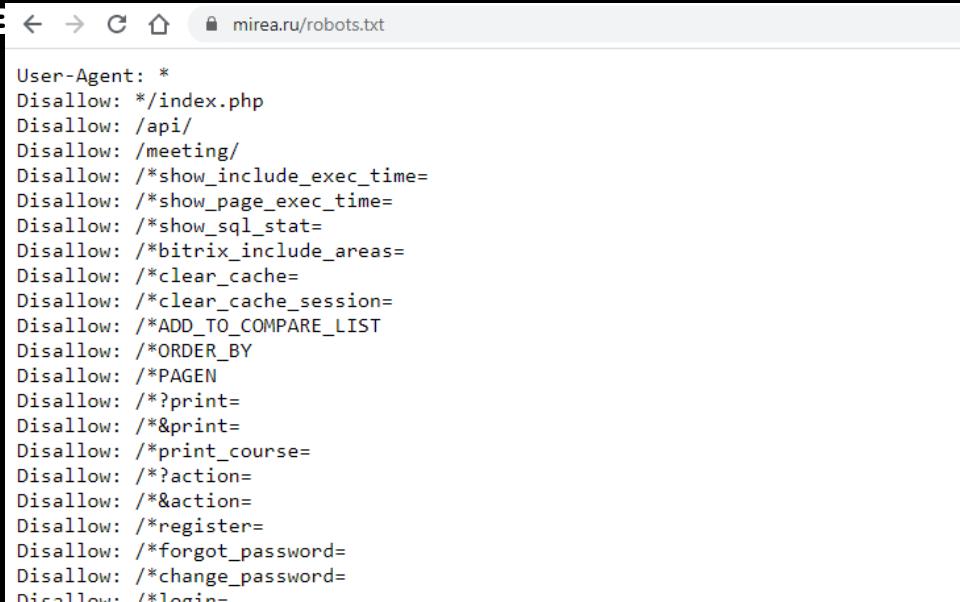
Определения



- **Google Dork или Google Dork Queries (GDQ) — это набор запросов для выявления грубейших ошибок в безопасности (всего, что должным образом не спрятано от поисковых роботов).**
- **Для краткости такие запросы называют гугл дорки или просто дорками.**
- **Поисковые роботы, безостановочно сканирующие интернет, помимо информации, полезной обычному пользователю, часто фиксируют то, что может быть использовано злоумышленниками при атаке на веб-ресурс. Например, ошибки скриптов и файлы с важной информацией (начиная от конфигурационных файлов и логов, заканчивая файлами с аутентификационными данными и бэкапами баз данных).**



- Для того, чтобы поисковые роботы не могли индексировать страницы веб приложения используется файл robots.txt
- Как правило, он хранится в корне сайта и может содержать интересную информацию, в том числе ту, которую администратор хотел спрятать от поисковых систем



User-Agent: *
Disallow: */index.php
Disallow: /api/
Disallow: /meeting/
Disallow: /*show_include_exec_time=
Disallow: /*show_page_exec_time=
Disallow: /*show_sql_stat=
Disallow: /*bitrix_include_areas=
Disallow: /*clear_cache=
Disallow: /*clear_cache_session=
Disallow: /*ADD_TO_COMPARE_LIST
Disallow: /*ORDER_BY
Disallow: /*PAGEN
Disallow: /*?print=
Disallow: /*&print=
Disallow: /*print_course=
Disallow: /*?action=
Disallow: /*&action=
Disallow: /*register=
Disallow: /*forgot_password=
Disallow: /*change_password=
Disallow: /*login=

Применение



- 1. Поиск учебных материалов, улучшение способностей поиска информации в целом.**
- 2. Поиск закрытой информации, индексированной поисковыми роботами – поиск утечек информации.**
- 3. Поиск информации о системе при проведении тестирования на проникновение на основе проиндексированной информации (баз данных, файлов конфигурации).**
- 4. Поиск проиндексированных веб-интерфейсов интернета вещей (камер, систем управления).**
- 5. И многое другое.**

Основные операторы

DC7495
[GoogleHacking]
dc7495.org



INURL:

Поиск будет проводиться только в адресе страницы.

SITE:

Поиск только на определенном сайте включая его поддомены.

INTEXT:

Поиск только в тексте документа.

FILETYPE: или EXT:

Поиск по расширению файла. Можно искать фото, архивы, текстовые файлы, базы данных и прочее.



Основные операторы

INTITLE:

Поиск по сайтам между тегами (<title>Найдем этот текст</title>)

SIZE:

Поиск по размеру файлов\страниц.

size:512000 найдёт контент, больше, чем 500 кбайт.

CACHE:

Находит копию страницы, даже если эта страница уже недоступна по адресу в интернете или изменила свое содержание. Эта команда ищет в кэше Google.

Основные операторы

DC7495
[GoogleHacking]
dc7495.org



INFO:

Покажет страницу, содержащую ссылки на варианты поиска: поиск по похожим страницам, обратные ссылки, и страницы, содержащие такую же ссылку.

LINK:

Возвращает список страниц, которые ссылаются на заданный сайт.

RELATED:

Поиск страниц похожих на эту.

DEFINE:

Показать определение слова.

Основные операторы

DC7495
[GoogleHacking]
dc7495.org



"	Точная фраза	intitle:«RouterOS router configuration page» — поиск роутеров
*	Любой текст	inurl:«bitrix*mcart» — поиск сайтов на bitrix с уязвимым модулем mcart
.	(точка) Любой символ	Index.of — аналогично запросу index of
-	Исключить слово	error -warning — показать все страницы, где есть error, но нет warning
..	(две точки) Диапазон	cve 2006..2016 — показать уязвимости по годам начиная с 2006
	Логическое «или»	linux windows — показать страницы, где встречается либо первое либо второе слово



Различия в поисковой выдаче

цифровая схемотехника и архитектура компьютера

Все Картинки Видео Новости Покупки Ещё Настройки Инструменты

Результатов: примерно 174 000 (0,31 сек.)

www.ozon.ru › context › detail ▾

Книга "Цифровая схемотехника и архитектура компьютера ..."

OZON предлагает выгодные цены и отличный сервис. Книга "Цифровая схемотехника и архитектура компьютера" - характеристики, фото и отзывы ...

Результаты по запросу "цифровая схемотехника и архитектура компьютера"

(0+) Цифровая схемотехника и архитектура компьютера

3 059 ₽

БУ

цифровая схемотехника и архитектура компьютера filetype:pdf

Все Картинки Видео Новости Покупки Ещё Настройки Инструменты

Результатов: примерно 21 500 (0,61 сек.)

easyelectronics.ru › files › Book › digital-design-and-computer-archit... ▾ PDF

Цифровая схемотехника и архитектура компьютера ...

31 дек. 2014 г. - Это издание книги Дэвида Мани Харриса и Сары Л. Харрис "Цифровая схемотехника и архитектура компьютера" публикуется по.

Похожие запросы

таненбаум архитектура компьютера hennessy computer architecture pdf

mips паттерсон хеннесси архитектура компьютера pdf

схемотехника pdf



Данный ресурс постоянно пополняется дорками, которые категоризируются следующим образом:

Category
Any
Footholds
Files Containing Usernames
Sensitive Directories
Web Server Detection
Vulnerable Files
Vulnerable Servers
Error Messages



FOOTHOLDS:

Позволяет найти веб-шеллы, публичные файловые менеджеры,

все сайты где существует вебшелл phremoteview :

intitle:"phremoteview" filetype:php "Name, Size, Type, Modify»

Дорк: <https://www.exploit-db.com/ghdb/615>

ⓘ Not Secure | gittaklotz.de/info.php?&c=l&d=%2Fmnt%2Fweb118%2Fc1%2F38%2F51071138%2Fht

		DIR	1
	4euro		
	admin		2
	Altern		1
	Angst		0
	Bankomat		1
	blog		2



FILES CONTAINING USERNAMES:

Такие дорки служат для того, чтобы искать файлы реестра, конфигурационные файлы, логи, файлы, содержащие историю введенных команд.

Найти все сайты, где существует файл sms.log:

intitle:"index of" "sms.log"

Дорк:

<https://www.exploit-db.com/ghdb/5717>

← → C ⌂ Not Secure adcom.it/public/sms.log			
19.02.20	18:02:58	+393355900721	
20.02.20	09:02:01	+393474310240	
20.02.20	09:02:35	+393386061097	
20.02.20	09:02:52	+393318107699	
20.02.20	09:02:37	+393318107699	
20.02.20	09:02:12	+393318107699	
20.02.20	10:02:36	+393386061097	
20.02.20	10:02:08	+393284611075	
20.02.20	10:02:01	+393284611075	
20.02.20	11:02:15	+393294984752	
20.02.20	11:02:18	+393383145085	
20.02.20	11:02:03	+393479106855	
20.02.20	11:02:03	+393662556904	
20.02.20	12:02:58	+393458892487	
20.02.20	12:02:37	+393284611075	
20.02.20	12:02:27	+393479106855	
20.02.20	15:02:25	+393662556907	



FILES CONTAINING USERNAMES:

Найти все сайты, где существует файл .xls, содержащий
емейлы и/или пароли: email password filetype:xls

Google email password filetype:xls

Все Картинки Видео Новости Карты Ещё Настройки Инструменты

На всех языках За год Все результаты Сбросить настройки

SP001 Certified Tank Inspectors List.xls [Compatibility Mode]

Office Update To keep up to date with security updates, fixes and improvements, choose Check for Updates.

Check for Updates

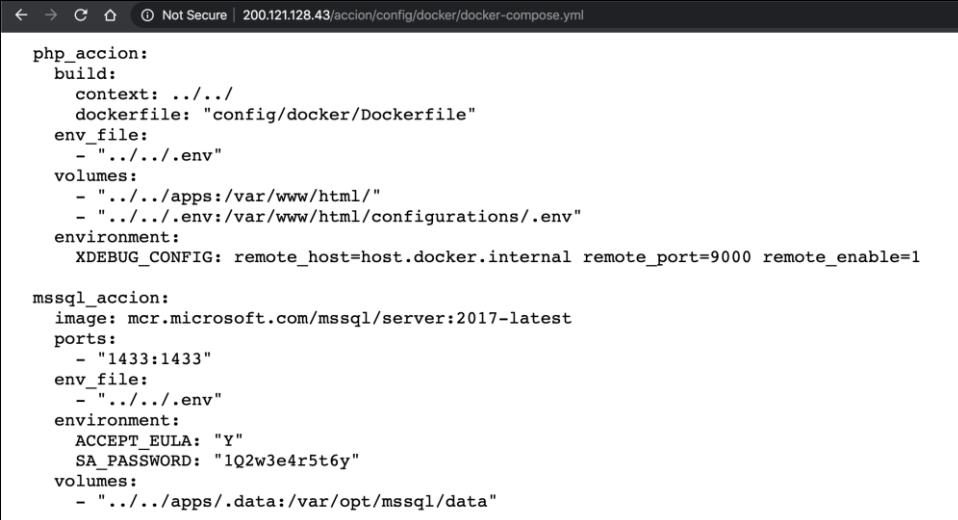
L1837	A	B	C	E	F	G	H	I	J	K
1	LAST	FIRST	ID#	ADDRESS	CITY	ST	ZIP	PHONE	FAX/CC EMAIL	EMAIL
1450	Wright	Shain	AST 12184	90 CES/CEAN	300 Vesle Drive, FE Warren AFB	WY	82005	307-773-4357	307-773-4153	shain.wright@us.af.mil
1451	Wright	William	AST-990124	424 Newmans Cardington Rd E	Marion	OH	43302	740-389-2076	740-389-2076	dine@rrrohi.com
1452	Yang	Jenna	AST-110404	1131 S Street	Sacramento	CA	95811	916/322-3028		jenna.yang@fire.ca.gov
1453	Yanko	Joseph	AST-42710	286 Houses Corner Road	Sparta	NJ	07871	800-440-8265		jyanko@atsenvironmental.com
1454	Yencsik	Peter	AST-990420	Technolog 225 Schilling Circle #400	Hunt Valley	MD	21031	410-771-4950		pyencsik@east.com
1455	Yilmaz	Ertugrul	AC 34112	İ. Sti.	Eskişehir Yolu 17. Km. Fatih Sult Etimesgut - Ankara	Turkey	06790	011-90 (533) 633 54 45		Ertugrul YILMAZ-ertugrul@alkalite.com
1456	Yoo	Thomas	AST-990125	1800 Washington Blvd	Baltimore	MD	21230	410-537-4403		thomas.yoo@maryland.gov
1457	York	Michael J.	AST-1164	1595 S Hwy 150 Suite F	Evanson	WY	82390	307-789-3540		mikey@eatnmetal.com
1458	Yorke	William J.	AST-1748	7916 Maryland St	Hammond	IN	46323	219-616-3090		John.Yorke@insndt.com
1459	Young	Michael	AST-1749	PO Box 1964	La Porte	TX	77572	361-813-0114		msy0072000@yahoo.com
1460	Young	Ric	AST-1623	11000 N Mopac Expressway Ste Austin		TX	78759	614-805-1394		ryoung@tanknology.com
1461	Young	Thomas D.	AST-1750	3170 Bood Rd	Courtenay	BC, CAN	V9N 1L8	250-334-9990		tom.young2@forces.gc.ca
1462	Zabik	Matthew	AST-990450	6296 Fly Road	East Syracuse	NY	13057	(315) 800-1801	n/a	matthew.zabik@gza.com
1463	Zimmerman	Michael J.	AST R1205	1277 Treat Blvd., Suite 500	Walnut Creek	CA	94597	925-946-0455		zippyeng@comcast.net
1464	Zwara	Nicholas David	AC 44244	2745 Broadway Ave	Buffalo	NY	14227	716-908-4792		Nzwarra@encorus.com
1465	Zwick	Thomas Charles	AST-1968	Altants LLC 7333 Palmleaf Lane	Columbus	OH	43235	614-314-4446		tzwick@zec.cc



SENSITIVE DIRECTORIES:

Поиск каталогов с различной информацией (личные документы, конфиги vrp, скрытые репозитории и т.д.)

Найти все сайты, где существует директория docker и файл config:



```
php_accion:
    build:
        context: ../../
        dockerfile: "config/docker/Dockerfile"
    env_file:
        - "../../.env"
    volumes:
        - "../../apps:/var/www/html/"
        - "../../.env:/var/www/html/configurations/.env"
    environment:
        XDEBUG_CONFIG: remote_host=host.docker.internal remote_port=9000 remote_enable=1

mssql_accion:
    image: mcr.microsoft.com/mssql/server:2017-latest
    ports:
        - "1433:1433"
    env_file:
        - "../../.env"
    environment:
        ACCEPT_EULA: "Y"
        SA_PASSWORD: "1Q2w3e4r5t6y"
    volumes:
        - "../../apps/.data:/var/opt/mssql/data"
```

intitle:"docker" intitle:"index of" config

Дорк: <https://www.exploit-db.com/ghdb/5000>



WEB SERVER DETECTION:

Поиск версии и иной информации о веб-сервере.

Найти все сайты, где существует раздел server-status:

Apache Server Status for azbyka.ru (via 192.168.3.122)

Server Version: Apache/2.4.39 (Unix) PHP7/7.2.23 mpm-itk/2.4.7-01
Server MPM: prefork
Server Built: Apr 3 2019 07:57:09

Current Time: Monday, 24-Feb-2020 15:15:45 MSK
Restart Time: Monday, 24-Feb-2020 02:06:02 MSK
Parent Server Config: Generation: 8
Parent Server MPM: Generation: 42
Server uptime: 13 hours 9 minutes 42 seconds
Server load: 0.04 0.10 0.09
Total accesses: 61371 - Total Traffic: 8.4 GB - Total Duration: 24467174
CPU Usage: u:0.74 s:0.04 q:0.0376.3 c:39960.3 - 275% CPU load
1.3 requests/sec - 184.9 kB/second - 442.8 kB/request - 398.676 ms/request
1 requests currently being processed, 4 idle workers

N

Scoreboard Key:
" " Waiting for Connection, "s" Starting up, "r" Reading Request,
"w" Sending Reply, "k" Keepalive (read), "p" DNS Lookup,
"c" Closing connection, "l" Logging, "e" Gracefully finishing,
"z" Idle cleanup of worker, " " Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Dur	Conn	Child	Slot	Client	Protocol	VHost	Request
0-7	4270	0/2735/0/0338_-	0.21	1	272	4093315	0.0	402.23	1470.76	94.181.100.38	http/1.1	azbyka.ru:80	GET /molitvoslov/wp-json/nycomment/v1/comments?post=122&parent	
1-7	18017	0/148/9846	W	0.00	0	3763239	0.0	21.25	1367.53	109.252.50.180	http/1.1	azbyka.ru:80	GET /molitvoslov/server-status/ HTTP/1.0	
2-7	-	0/0/8453	-	0.00	615	0	3441339	0.0	0.00	1207.71	127.0.0.1	http/1.1	azbyka.ru:80	OPTIONS * HTTP/1.0
3-7	12116	0/1258/9234	-	0.00	1	10	3682191	0.0	172.48	1301.68	217.107.124.181	http/1.1	azbyka.ru:80	GET /molitvoslov/ HTTP/1.0
4-7	17135	0/3/12/8683	-	0.28	0	420	3645209	0.0	49.44	1197.22	80.245.114.232	http/1.1	azbyka.ru:80	GET /molitvoslov/1/kanony-i-molitvy-dlya-podgotovki-k-tainstvam
5-7	-	0/0/7941	-	0.00	1268	0	3224878	0.0	0.00	1074.28	127.0.0.1	http/1.1	azbyka.ru:80	OPTIONS * HTTP/1.0
6-7	11948	0/1293/6876	-	0.00	0	11	2617000	0.0	174.50	936.50	188.170.82.56	http/1.1	azbyka.ru:80	GET /molitvoslov/molitva-poslednix-optinskikh-starcev-na-nachalo

Srv Child Server number - generation
PID OS process ID

inurl:/server-status + "Server MPM:"

Дорк: <https://www.exploit-db.com/ghdb/5294>



VULNERABLE FILES:

Поиск скриптов, содержащих известные уязвимости.

Найти сайты, использующие скрипт, позволяющий выгрузить произвольный файл с сервера:

allinurl:forcedownload.php?file=

www.pharmakeez.com › forcedownload › fil... ▾ Перевести эту страницу
官方授权 - 10bet十博体育网
最可能的原因: 指定的目录或文件在Web服务器上不存在。URL拼写错误。某个自定义筛选器或模块(如URLScan)限制了对该文件的访问。

www.lyon.biz › forcedownload › filename=... ▾ PDF Перевести эту страницу
Untitled - lyon.biz
Page 1.

www.cash.com.ar › forcedownload.php?file='.. ▾ Перевести эту страницу
Resultados de Búsqueda para 'ejplode/feed/rss2/wpadmin ...
Información de 'ejplode/feed/rss2/wpadmin/wpcontent/plugins/revslider/temp/
update_extract/revslider/forcedownload.php?file='..//index.php » ...

allinurl:forcedownload.php?file=

Дорк: <https://www.exploit-db.com/ghdb/3738>



VULNERABLE SERVERS:

Поиск инсталляционных скриптов, веб-шеллов, открытых административных консолей и т.д.

Данный дork может быть использован для поиска уязвимых или взломанных серверов которые позволяют обратиться к /proc/self cwd/.

inurl:/proc/self cwd

inurl:/proc/self cwd

Результатов: примерно 3 620 000 (0,44 сек.)

агри eco ku ac th › admin › cwd › var › www › [Перевести эту страницу](#)
Index of /admin/fileupload/ciprut/root/proc/self cwd/var/www
Index of /admin/fileupload/ciprut/root/proc/self cwd/var/www. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - [DIR] ...

www.euroskiclub.com › public › lib › exim › [Перевести эту страницу](#)
of /public/uploads/config/shu/proc/self cwd/usr/lib/exim
Index of /public/uploads/config/shu/proc/self cwd/usr/lib/exim. Parent Directory · bin/

stuff.mit.edu › lib › python3 › dist-packages › [Перевести эту страницу](#)
of /afs/sipb/user/mkgray/bar/proc/self cwd/usr/lib/python3 ... - Mit
Name · Last modified · Size. [PARENTDIR], Parent Directory, - [DIR], CommandNotFound/, 2015-09-19 23:53, - [DIR], DistUpgrade/, 2019-05-28 23:16, - [DIR] ...



Дорк для поиска уязвимых веб-серверов на RPi:
GOOGLE: intitle:RPi Cam Control inurl:preview.php
SHODAN: RPi cam

intitle:RPi Cam Control inurl:preview.php

Все Картинки Видео Новости Покупки Ещё Настройки Инструменты

Результатов: примерно 67 (0,44 сек.)

projectbee.ddns.net › html › preview ▾ Перевести эту страницу

RPi Cam Control v6.4.21: mycam@raspberrypi Download

Files Select None Select All Get Zip Delete Sel Delete All. Used:26.4% Total:14648(MB).

Preview Thumb Update Sort. Ascending, Descending. Types. Images & ...

81.161.252.52 › preview ▾ Перевести эту страницу

mycam@raspberrypi Download - RPi Cam Control v6.0.22

Files Select None Select All Get Zip Delete Sel Delete All. Used:0% Total:0(MB). No videos/images saved.

Preview Thumb Sort Order. Ascending, Descending.

RPiCam 02/25/2020 15:39:14

record video start record image timelapse start motion detection start stop camera

Download Videos and Images Edit schedule settings

Camera Settings Motion Settings System Help



RCE!

```
connect to ssh://192.36.31.221:22 - Timeout co
[*] Returning prompt!
/18.21.227.53:22/ does not support password
connect to ssh://209.19.16.129:22 - Timeout co
/www-data@raspberrypi:/var/www/html$ █
/143.215.130.193:22/ does not support passwo
```



<https://blog.reigningshells.com/2018/09/hacking-rpi-cam-web-interface.html>
<https://www.exploit-db.com/exploits/45361>



ERROR MESSAGES:

Поиск ошибок и предупреждений которые, могут раскрывать важную информацию, начиная от версии CMS до паролей.

intitle:"Error log for /LM/"

Дорк: <https://www.exploit-db.com/ghdb/5644>

← → ⌂ ⌄ Не защищено intranet.sailife.com/easyPay/view/errorlog.axd/detail?id=24379	
HTTP_USER_AGENT	Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.186 Mobile Safari/537.36 +http://www.google.com/bot.html
HTTPS	on
HTTPS_KEYSIZE	256
HTTPS_SECRETKEYSIZE	2048
HTTPS_SERVER_ISSUER	C=US, O="Entrust, Inc.", OU=See www.entrust.net/lega
HTTPS_SERVER_SUBJECT	C=IN, S=Telangana, L=Hyderabad, O=Sai Life Sciences
INSTANCE_ID	3
INSTANCE_META_PATH	/LM/W3SVC/3
LOCAL_ADDR	10.0.0.106
LOGON_USER	
PATH_INFO	/easyPay/view/errorlog.axd/detail
PATH_TRANSLATED	C:\inetpub\wwwroot\EasyPAY\view\errorlog.axd
QUERY_STRING	id=100%27A=0
REMOTE_ADDR	66.249.68.15
REMOTE_HOST	66.249.68.15
REMOTE_PORT	46506
REMOTE_USER	
REQUEST_METHOD	GET
SCRIPT_NAME	/easyPay/view/errorlog.axd
SERVER_NAME	intranet.sailife.com
SERVER_PORT	443
SERVER_PORT_SECURE	1
SERVER_PROTOCOL	HTTP/1.1
SERVER_SOFTWARE	Microsoft-IIS/7.5
URL	/easyPay/view/errorlog.axd



Files containing juicy info:

Сертификаты, бэкапы, электронные письма, логи.

```
← → C ⌂ ⓘ Не защищено | netsellsit.com/Download/Bitsum%20Software%20License%20-%20License%20Keys.txt

From: Bitsum Technologies <sales@bitsum.com>
Sent: Wednesday, February 01, 2017 8:17 AM
To: mark.byrd@netsellsit.com
Subject: Your Bitsum Software License - License Keys

Your activation code(s):
Process Lasso Pro Entire Home - Entire Home /w Yearly Updates:
639945524984bf8a62813a436f14d8b2
Installation: If you have not already, download the public version of the
software and use your activation code to enable your license.
Note that if this is a full install, it will take up to 30 minutes to activate.
```

```
← → C ⌂ ⓘ essienarthur.net/keys.txt

MG48D-6Q38K-AZKX8-AV9N2-3ACHD
NC2F3-DFH97-3Z2N8-9T054-92N4D
4U2MU-D2J4J-KZT79-YK0XX-9AYHE
1F68L-AF3DN-LZTF0-793X6-CC7QW
HZ4W9-A32D6-KZFJ9-H98EM-ACQ5J
```

intitle:index.of "keys.txt"

Дорк: <https://www.exploit-db.com/ghdb/5733>



Files containing passwords:

Дорки для поиска логинов и паролей

```
← → C ⌂ jira.mariadb.org/secure/attachment/48063/slow.log
# Rows_affected: 1
SET timestamp=1557759154;
INSERT INTO `api_logs`(`uri`, `method`, `params`, `api_key`, `ip_address`)
VALUES('{"username":\admin@ciosa.com", "password":BUZZqNm0saMbLz14Ex7\00000000000000000000000000000000}', 'PUT', 'application/json', null, '192.168.1.56');
# User@Host: CD.com[CD.com] @ [192.168.1.56]
# Thread_id: 1152 Schema: ciosa_productivo QC_hit: No
# Query_time: 1.085387 Lock_time: 0.000030 Rows_sent: 0 Rows_examined: 0
# Rows_affected: 1
SET timestamp=1557759154;
INSERT INTO `api_logs`(`uri`, `method`, `params`, `api_key`, `ip_address`)
VALUES('{"username":\admin@ciosa.com", "password":BUZZqNm0saMbLz14Ex7\00000000000000000000000000000000}', 'PUT', 'application/json', null, '192.168.1.141');
# User@Host: CD.com[CD.com] @ [192.168.1.141]
# Thread_id: 1153 Schema: ciosa_productivo QC_hit: No
# Query_time: 1.078652 Lock_time: 0.000018 Rows_sent: 0 Rows_examined: 0
# Rows_affected: 1
SET timestamp=1557759154;
UPDATE `ci_sessions` SET `last_activity` = 1557759144, `user_data` = 'a:1:{s:9:\"user_data\";s:0:\"\";s:5:\"clase\";s:11:\"webservices\";s:7:\"dyna...{i:0;s:10:\"0030000014\";i:1;s:10:\"0030000190\";i:2;s:10:\"0030000027\";i:3;s:10:\"0aa80133fd51f0baf18b0ed5b79b9b8b\";}' WHERE `session_id` = '0aa80133fd51f0baf18b0ed5b79b9b8b';
```

intext:"username=" AND "password=" ext:log

Дорк: <https://www.exploit-db.com/ghdb/5747>



Sensitive Online Shopping Info:

Дорки для поиска информации, связанной с онлайн шоппингом.

```
← → C ⌂ 🔍 snk.id/uploads/1/2019-05/c267fe795c60cf4f1b8fec89731195eb.sql
INSERT INTO `login` VALUES (1, 'jsihom', 'df62231efbea819b13e01042336486d2', NULL, 1, '2019-02-20 10:36:24', 'pdQdJKXugk5RbXFkBkkv2Pm1v0mp2Twh1550817810_juliver.jpeg');
INSERT INTO `login` VALUES (2, 'erwin', 'df62231efbea819b13e01042336486d2', NULL, 1, '2019-03-08 14:03:23', 'f287SElayDUGSfVdWAYgcpjhVC3sFSDSB1550817836_erwin.png');
INSERT INTO `login` VALUES (3, 'admin', 'df62231efbea819b13e01042336486d2', NULL, 1, '2019-03-09 16:52:51', 'Kqd0r9V5mwfak11ndpAuKZrXiW9LebusX
```

intext:"Dumping data for table `orders`"

Все Новости Картинки Видео Карты Ещё Настройки Инструменты

Результатов: примерно 830 (0,31 сек.)

desklib.com › document › 12-set-sql_mode-... ▾ Перевести эту страницу

Dumping data for table 'ORDER' - mysql dump

21 сент. 2019 г. - ... NULL, `orderStatus` varchar(55) DEFAULT NULL ENGINE=InnoDB DEFAULT CHARSET=latin1;--- Dumping data for table `orders`.

rextester.com › DSLK3533 ▾ Перевести эту страницу

test, Sql Server - rextester

... ENGINE=InnoDB DEFAULT CHARSET=latin1; -- -- Dumping data for table `orders` --
INSERT INTO `orders` ('order_id', 'cart_id', 'order_status') VALUES (1, ...)

www.homeworkmarket.com › ... › DB Report ▾ Перевести эту страницу

Db report | Information Systems homework help

27 апр. 2019 г. - ... Dumping data for table `orders` -- INSERT INTO `orders` ('order_id', 'user_id', 'order_date', 'shipped_date', 'employee_id') VALUES (19, ...)



Sensitive Online Shopping Info - на GHDB подобные дорки – все ПАЖИЛЫЕ, поэтому мы можем прибегнуть к следующему:



ОВЕН

Google carding dorks 2020

Все Новости Картинки Видео Карты Ещё Настройки Инструменты

Результатов: примерно 142 000 (0,51 сек.)

[itechhacks.com › latest-fresh-carding-dorks-... ▾ Перевести эту страницу](#)

Google And Carding Dorks 2020 - iTech Hacks

Fresh Google Dorks List 2019, Fresh Google SEO Dorks, 2500+ Google Dorks of 2020. Use these dorks to search like a pro and itechhacks.

[www.compsmag.com › Tips ▾ Перевести эту страницу](#)

Best Google Dorks list for SQL Injection - Compsmag

A lot of Hackers & Crackers use Google Dorks to Take a look at Website Vulnerabilities. At the Different Hand, Google Dorks is also used by Hackers and Crackers to deface Susceptible Web sites. Today we are on Darknet websites people are normally looking for Google carding dorks or Google dorks for carding.

[phishers.net › google-dorks-list ▾ Перевести эту страницу](#)

Google Dorks List 2019 | Fresh Google Dorks 【2020】 for SQLI

19 / 20 Google Dorks List 2020 | Fresh Google Dorks for SQLi ... Most of the time I saw google dork is used for credit card dorks aka carding dorks or ...

[latesttechnews.com › carding-dorks ▾ Перевести эту страницу](#)

Latest Fresh Carding dorks for SQL injection and getting credit ...

4 апр. 2019 г. - Carding dorks are the easiest method to get carding details of random people. After getting the ... Ultimate List of Fresh Google Carding Dorks.

What is Google Dorking? · What are search operators? · Carding Dorks List 2018





Дорки в открытом доступе зачастую быстро становятся ПАЖИЛЫМИ и сайты, на которых они были упомянуты, в свою очередь мешают нормальному поиску так же, как и оперативное удаление гуглом выдачи по таким доркам и баг фиксингу веб движков и конфигов (решается с помощью просмостра сохраненной копии страницы).



Network or vulnerability data:

Ищем информацию о сети проиндексированную на веб ресурсах.

Last Refresh : 10:10:01 pm

rp0sgw1.redparra.int	rp0shost1.redparra.int	rp0shost2.redparra.int	rp1ipcam1.redparra.int	rp1ipcam2.redparra.int	rp1nas1.redparra.int	rp1router1.redparra.int	rp1ssw1.redparra.int	rp1ups1.redparra.int	rp1xen1.redparra.int
rp1v1app1.redparra.int	rp1v1app2.redparra.int	rp1v1app3.redparra.int	rp1v1app4.redparra.int	rp1v1app5.redparra.int	rp1v1bd1.redparra.int	rp1v1bkp1.redparra.int	rp1v1descargas1.redparra.int	rp1v1dev1.redparra.int	rp1v1front1.redparra.int
rp1v1fw1.redparra.int	rp1v1grafana1.redparra.int	rp1v1ids1.redparra.int	rp1v1log1.redparra.int	rp1v1monitor1.redparra.int	rp1v1pihole1.redparra.int	rp1v1unifi1.redparra.int	rp1v1vpn1.redparra.int	rp2sfireserver2.redparra.int	rp2snas1.redparra.int
rp2srouter1.redparra.int	rp3snas1.redparra.int	rp3srouter1.redparra.int	rp5sap5.redparra.int	rp5snas1.redparra.int	rp5ssw1.redparra.int	rp5xen1.redparra.int	rp5v1app1.redparra.int	rp5v1bkp1.redparra.int	rp5v1front1.redparra.int
rp5v1front1t1.redparra.int	rp5v1fw1.redparra.int	rp5v1fw1t1.redparra.int	rp5v1ids1.redparra.int	rp5vinas1.redparra.int	rp5v1pihole1.redparra.int	rp5v1vpn1.redparra.int			

intitle:"Cacti" AND inurl:"/monitor/monitor.php"

Дорк: <https://www.exploit-db.com/ghdb/5600>



Pages containing login portals:

Ищем формы авторизации.

site:*/AdminPanel.php

Dra. Astrid Ochoa Lovino
Dra. Astrid Ochoa Lovino
Dra. Astrid Ochoa De lovino Médico cirujano UCV. Medicina Biorreguladora, Neuralterapeuta, Biorresonancia. Practitioner Bach. Medicina Integrativa.

zambranohugo.com › adminpanel ▾ Перевести эту страницу
Area restringida - Panel de Control - Hugo Abel Zambrano ...
Corredor de seguros en Barquisimeto, Estado Lara, Somos corredores de seguros, somos intermediario de entre el asegurado y la compañías aseguradoras, ...

tequefrench.com › adminpanel ▾ Перевести эту страницу
Bienvenidos TequeFrench, C.A.
Fabricación, comercialización y distribución de tequeños y franquicia de comidas.

simcardmundi.com › adminpanel ▾ Перевести эту страницу
Sim Card Mundi Corp.
En la era de las comunicaciones Máquina a Máquina Sim Card Mundi ofrece Conectividad Global M2M abarcando más de 185 países con Romaing ...

www.foodexpressbqto.com › adminpanel ▾ Перевести эту страницу
Area de Administrador - Food Express Barquisimeto
FoodExpress, Cortes de carne seleccionados, Viveres, venta de licores nacionales e importados, para todo tipo de evento en Barquisimeto, Venezuela.

site:*/AdminPanel.php

Дорк: <https://www.exploit-db.com/ghdb/5697>



Advisories and Vulnerabilities: Сайты на уязвимых версиях CMS и всякое такое

universal-sompo.net.in/USGISGSProd/cmsinstall/install.aspx?checkpermission=0

Step 1 - SQL Server and Authentication Mode

SQL Settings → Database → Starter Site → Finish

SQL server

SQL Server name or IP address: INDC-RECIPTWEB1

Use SQL Server account

Login name:

Password:

Use integrated Windows authentication
(ASP.NET account: NT AUTHORITY\NETWORK SERVICE)

Next

Do you need help with installation? Please contact our support.

Version: 9.0 Build: 9.0.5802

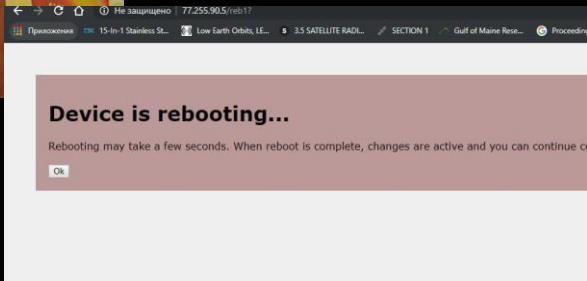


inurl:/cmsinstall/install ext:aspx
<https://www.exploit-db.com/ghdb/5695>



Various Online Devices:

Принтеры, роутеры, системы мониторинга и т.д





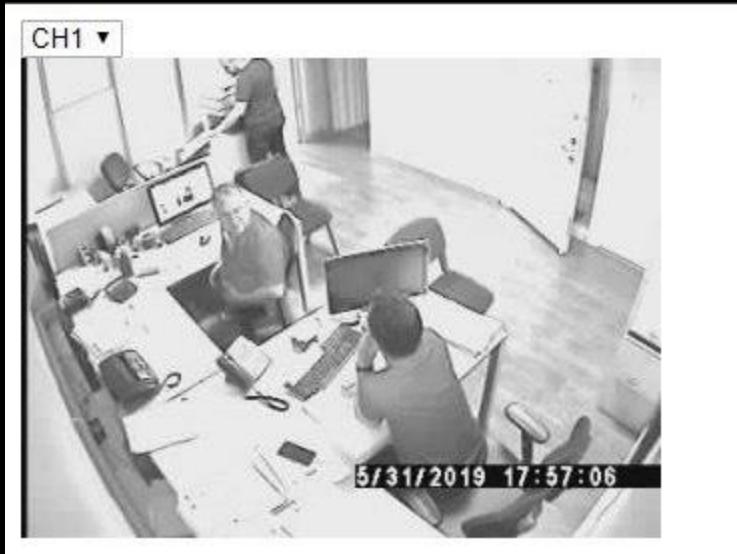
Камеры:

Существует множество ресурсов с дорками, написанными непосредственно для камер и систем видеонаблюдения. Для того, чтобы написать свой дорк, необходимо изучить веб приложение, предоставляемое с оборудованием и выписать все уникальные урлы и/или заголовки.

Например: `inurl:ViewerFrame?Mode=Refresh`

`intitle:"Live View / - AXIS«`

Дорк: <https://www.exploit-db.com/ghdb/342>





Various Online Devices:

Принтеры – освежаем дork.

1. Заходим на устройство.
2. Жмем по кнопкам, ходим по директориям.
3. Выписываем уникальные словосочетания и урлы.
4. Проверяем обновленный дork.

Device Status - Refresh

Toner Status:
Black Toner ~70%

Paper Input Tray:	Status:	Capacity:	Size:	Type:
Tray 1	OK	500	Letter	Plain Paper
MP Feeder	First	100		

Paper Output Bin:	Status:	Capacity:
Standard Bin	OK	500

Device Type: Monochrome Laser
Speed: Up to 45 Pages/Minute
Toner Cartridge Capacity: Approximately 21,000 Pages at approximately 5% coverage
Maintenance Kit Life Remaining: 100%

Dell 2330dn Device Status - Refresh Tray 1

Все Картинки Карты Покупки Ещё Настройки Инструменты

На всех языках ▾ За всё время ▾ Точное соответствие ▾ Сбросить настройки

164.67.82.67 ▾ Перевести эту страницу

Dell 2330dn Laser Printer

Device Status - Refresh ... Paper Input **Tray: Status: Capacity: Size: Type: Tray 1 ... 50. Letter. Custom Type 6. Paper Output Bin: Status: Capacity: Standard Bin ...**

164.67.82.36 ▾ Перевести эту страницу

Dell 2330dn Laser Printer

Device Status - Refresh ... Paper Input **Tray: Status: Capacity: Size: Type: Tray 1 ... 50. Letter. Plain Paper. Paper Output Bin: Status: Capacity: Standard Bin ...**

inurl:"cgi-bin/dynamic/" intitle:"Printer Status"

Дорк: <https://www.exploit-db.com/ghdb/4220>



Роутеры-сделай сам:

1. Берем свой роутер.
2. Ищем “кривые” урлы.
3. Проверяем.

The screenshot shows a web browser displaying two search results for "inurl:general_stats.htm?".

Result 1: Address bar: 192.168.1.254/general_stats.htm?l0=0&l1=0&l2=-1&l3=-1. The page is for MTS (МТС) and shows the "Общая информация" tab selected. It displays the "Общая информация" section, which includes the "Устройство" tab. The device information is as follows:

Model: AnywhereUSB/2. Ethernet MAC Address: 00:40:9D:8C:C4:E2. Firmware Version: 1.82.16.41 (build 82002116_L2 awusb2 eos 6/16/2015 9:19:40a).

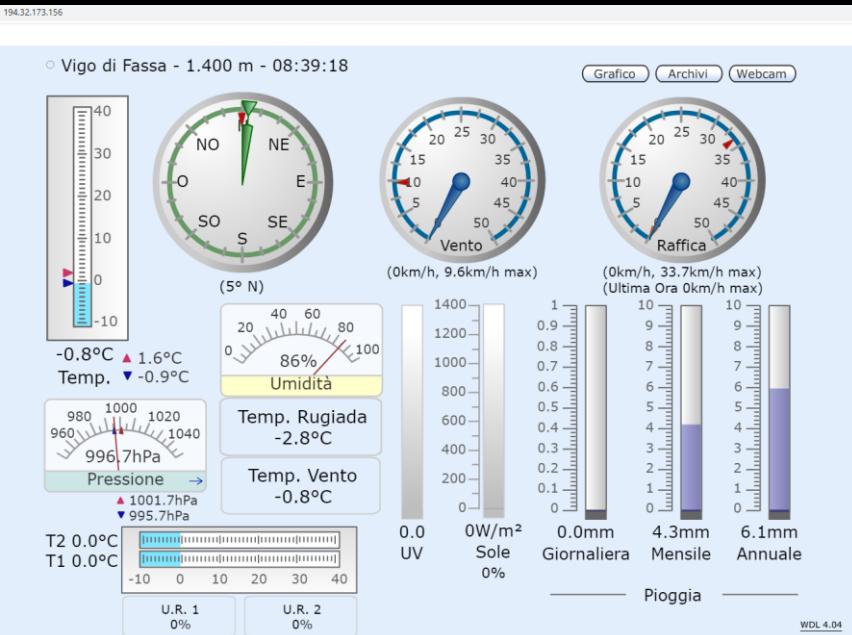
Result 2: Address bar: 75.208.61.16/admin/sysinfo/general_stats-. The page is for ConnectPort WAN VPN and shows the "General - ConnectPort WAN VPN Configuration and ..." section. The device information is as follows:

Model: ConnectPort WAN VPN. Ethernet MAC Address: 00:40:9D:37:D9:8B. Firmware Version: 2.7.2.7 (Version 82001350_G 04/14/2008). Boot Version: 1.1.3 ...



Various Online Devices: IOT девайсы

Погодная станция
intitle:"Weather Wing WS-2"





GHDB

Various Online Devices:

ИОТ девайсы - делаем дорки из выдачи Шодана!

1. Берем контроллеры со встроенными веб – серверами, например Corigo
2. Изучаем

REGIN
THE CHALLENGER IN BUILDING AUTOMATION

Regulator värmesystem

Your browser is not Java enabled.

Corrido E Web

Controller with integrated webserver

R&B Regin. All rights reserved.
WARNING: This computer program is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil or criminal penalties.

REGIN

SHODAN corigo

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS: 127

TOP COUNTRIES:

Country	Count
Sweden	65
Lithuania	39
Norway	5
Netherlands	5
Estonia	3

TOP SERVICES:

Service	Count
HTTP	77
	10
	9
	9
	7

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

92.111.40.189

Ziggo
Added on 2020-02-26 07:08:26 GMT
Netherlands, Amsterdam

```
HTTP/1.0 200 OK\nDate: Tue, 15 July 2014 10:09:09\nServer: Corigo Webserver\nLast-Modified: \nContent-Type: text/html\n\n
```

85.229.200.97

Bredbandsbolaget AB
Added on 2020-02-25 20:07:35 GMT
Sweden, Stockholm

```
HTTP/1.0 200 OK\nDate: Wed, 18 July 2012 09:42:15\nServer: Corigo Webserver\nLast-Modified: Fri, 11 March 2011 09:10:44\nAccept-Ranges: bytes\nContent-Length: 3122\nContent-Type: text/html\n\n
```

82.135.245.166

Telia Lietuva
Added on 2020-02-25 22:39:29 GMT
Lithuania, Kaunas

```
HTTP/1.0 200 OK\nDate: Tue, 31 March 2015 11:31:04\nServer: Corigo Webserver\nLast-Modified: Fri, 08 October 2016 09:41:10\nAccept-Ranges: bytes\nContent-Length: 2764\nContent-Type: text/html\n\n
```



GHDB

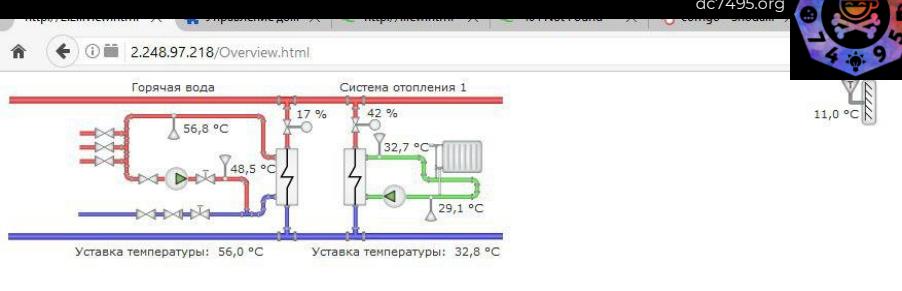
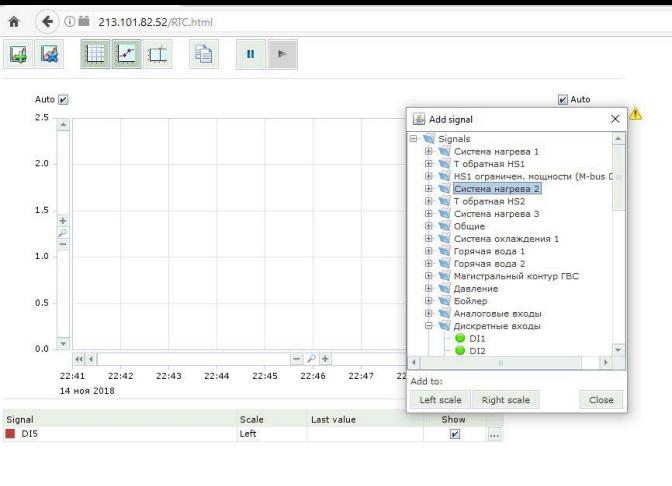
Various Online Devices:

ИОТ девайсы - делаем дorkи из выдачи Шодана!

3. Проваливаемся внутрь (спс, Java)

4. Изучаем

5. Пишем свой дork (выдача может отличаться от выдачи Шодана, а может-нет).



intext:Regulator värmesystem intitle:corigo e

Result	Description
90.236.102.80	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
217.209.92.169	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
81.225.235.94	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
81.224.80.94	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
81.225.235.90	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
81.228.46.67	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
46.230.233.47	Перевести эту страницу Regulator värmesystem, Corrigo E AB Regn. Regulator värmesystem. Login. Your browser is not Java enabled. Corrigo E Web.
155.4.76.157	Перевести эту страницу Regulator värmesystem, Corrigo E



FTP

inurl:ftp://ftp

Дорк: <https://www.exploit-db.com/ghdb/5358>

← → ⌂ ⌄ Не защищено | ftp://epncb.oma.be/pub/station/

Содержание /pub/station/

[родительский каталог]

Название	Размер	Последнее изменение
coord/		12.09.2019, 09:31:00
densification/		07.02.2019, 03:00:00
frequencies/		01.01.2020, 10:16:00
general/		26.02.2020, 07:10:00
log/		25.02.2020, 16:45:00
log_9char/		25.02.2020, 16:45:00
new/		20.02.2020, 18:00:00
new_9char/		20.02.2020, 18:00:00
old/		25.02.2020, 16:45:00
old_9char/		25.02.2020, 16:45:00
real_time/		25.02.2020, 16:24:00
skl/		14.02.2020, 12:45:00
tie/		22.01.2007, 03:00:00
xml/		25.02.2020, 16:45:00

EUREF Permanent GNSS Network

The EUREF Permanent GNSS Network consists of

- a network of continuously operating GNSS (Global Navigation Satellite Systems, such as GPS, GLONASS, Galileo, BeiDou, ...) reference stations;
- data centres providing access to the station data;
- analysis centres that analyze the GNSS data;
- product centres or coordinators that generate the EPN products;
- and a Central Bureau that is responsible for the daily monitoring and management of the EPN.

The network is operated under the umbrella of the IAG (International Association of Geodesy) Regional Reference Frame sub-commission for Europe, EUREF.

All contributions to the EPN are provided on a voluntary basis, with more than 100 European agencies/universities involved. The EPN operates under well-defined international standards and guidelines which are subscribed by its contributors. These guidelines guarantee the long-term quality of the EPN products.

The primary purpose of the EPN is to provide access to the European



MP3, Movie, PDF
intitle: index of mp3
intitle: index of pdf intext: .mp4

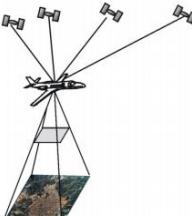
Directory Listing For /geova/erva/

Filename	Size
Diaric30seg/	
Horari1seg/	2005/
Horari5seg/	2006/
Apache click/5.5.23	2007/
Apache tomcat/5.5.23	2007/
20070101/	
20070102/	
20070103/	
20070104/	
20070105/	
20070106/	
20070107/	
20070108/	
20070109/	
20070110/	
20070111/	
20070112/	

Directory Listing To /geova/erva/

click

click



И множество другой информации для размышления.



Например, можно найти дистрибутивы Безопасного города...

← → ⌂ ⌂ ⌂ Не защищено | <ftp://ftp.integra-s.com/Intstructions/>

Содержание /Intstructions/

Название	Размер	Последнее обновление
[родительский каталог]		
E3Workstation/		30.03.
Eily.Net/		30.03.
English/		30.03.
Integra_Video_5_Service/		30.03.
Integra-4D/		30.03.
Integra-ACS/		30.03.
Integra-Auto/		30.03.
Integra-Control/		30.03.
IntegraVideo_5/		30.03.
IntegraVideo2xx-3xx/		30.03.
IntegraVideo7/		30.03.
IntegraVideo-Retranslator/		30.03.
readme.txt	493 B	04.06.
recommendations.doc	741 kB	04.06.
Traffic_control/		30.03.
Инструкции Интегра-распознавание ЖД/		30.03.
Инструкции к КДД (безопасное движение)/		30.03.
Интегра Видео 7/		30.03.
Интегра-Web/		30.03.
Интегра-СКД/		30.03.

Файл Редактирование Инструменты Расширения Окно Справка Дополнительно
Куделькин

Интегра планета Земля 4Б 1.6.123 - Просмотр

Основная панель АРМ СУДС

Не в сети

53°13'2.87" С.Ш., 45°0'43.97" В.Д.
148.3 м. над уровнем моря

Интегра-С © 2019
Участники OpenStreetMap

Обзор с высоты: 988.4 м



Honeypots

We highly recommend to check out the Glastopf successor [SNARE](#) and [TANNER](#).

Glastopf build failing

ABOUT

Glastopf is a Python web application honeypot founded by Lukas Rist.

General approach:

Выдержка: Злоумышленники используют поисковые системы и специальные поисковые запросы, чтобы найти уязвимые сервисы. Чтобы привлечь их, Glastopf предоставляет необходимые ключевые слова (АКА "dork") и дополнительно извлекает их из запросов, автоматически расширяя область атаки. В результате ханипот становится все более «привлекательным».

Вкратце: для ханипотов используются скрипты, которые генерируют на веб странице текст, соответствующий запросам через дorkи. После индексации таких веб-страниц, запросы к таким ханипотам агрегируются и превращаются в статистику.



Ботнеты

Существует два стула (пруфов не будет)

Для Exploit.in
Android bot
by maza-in

SELECT * FROM klients limit 0,30										
IMEI/ID	Номер	Версия OS	Версия apk	Страна	Банк	Модель	ROOT	Экран	оп/off	Date
015437438851433	88005553535	1.1	1.2	Франция	по	HTC	×	×	●	2015
015437438851433	88005553535	1.1	1.2	Франция	по	HTC	×	×	●	2015
015437438851433	88005553535	1.1	1.2	Франция	по	HTC	×	×	●	2019-
015437438851433	88005553535	1.1	1.2	Франция	по	HTC	×	●	●	2019-
015437438851433	88005553535	1.1	1						●	2019-
015437438851433	88005553535	1.1	1						●	2019-
015437438851433	88005553535	1.1	1						●	2019-
015437438851433	88005553535	1.1	1						●	2019-
015437438851433	88005553535	1.1	1						●	2019-
015437438851433	88005553535	1.2							●	2015
015437438851433	88005553535	1.1							●	2015
015437438851433	88005553535	1.1							●	2015
015437438851433	88005553535	1.2							●	2015
015437438851433	88005553535	1.1							●	2015
015437438851433	88005553535	1.1							●	2015
015437438851433	88005553535	1.2							●	2015
015437438851433	88005553535	1.2							●	2015
015437438851433	88005553535	1.2							●	2015

Стул 3

Качаем известные админ-панели,
делаем дорки, забираем ботнеты
себе.

(З.Ы. Изучаем стойки Кробы,
чтобы знать, какие админ панели
как можно лАМАт)

Автоматизация!

DC7495
[GoogleHacking]
dc7495.org



Теперь, мой дорогой друг, ты
научился пользоваться
поисковиком гугол.

Для использования дорков есть
ТРИЛЛИАРДы скриптов всех
цветов и оттенков.

Но теперь ты можешь САМ найти
и выбрать тулзу по душе.

Помни, что не бывает идеальных
утилит, лучшие дорки –
написанные самостоятельно под
твои цели.

Zeus-Scanner

What is Zeus?

Zeus is an advanced rec... with a powerful built-in and webcache URLs, the... captchas.

github google dorks

Результатов: примерно 154 000 (0,31 сек.)

github.com › topics › google-dorks ▾ Перевести эту страницу

google-dorks · GitHub Topics · GitHub

This toolkit comprises of two options first one is to use existing word press exploits to find vulnerable websites or the second one to use custom google dork to ...

github.com › BullsEye0 › google_dork_list ▾ Перевести эту страницу

BullsEye0/google_dork_list: Google Dorks | Google ... - GitHub

Google Dorks | Google helps you to find Vulnerable Websites that Indexed in Google Search Results. Here is the latest collection of Google Dorks. A collection ...

github.com › opsdisk › pagodo ▾ Перевести эту страницу

opsdisk/pagodo: pagodo (Passive Google Dork ... - GitHub

PaGoDo. Introduction. The goal of this project was to develop a passive Google dork script to collect potentially vulnerable web pages and applications on the ...

github.com › moriarity9211 › Google-Dorks... ▾ Перевести эту страницу

moriarity9211/Google-Dorks-2019 - GitHub

Contribute to moriarity9211/Google-Dorks-2019 development by creating an account on GitHub.

github.com › ZephxFish ▾ Перевести эту страницу

ZephxFish/GoogDOrker: GoogDOrker is a tool for firing ... - GitHub

GoogDOrker is a tool for firing off google dorks against a target domain, it is purely for OSINT against a specific target domain. READ the readme before ...

ATSCAN SCANNER

Initiation Scanner

Required Platform All Facebook Follow Youtube Follow



Contact me: Telegram: @N3M351DA

Read more: Telegram : @in51d3



Материалы

DC7495
[GoogleHacking]
dc7495.org



1. [Статья] Google Dorks \ Гугл Дорки <https://forum.antichat.ru/threads/425255>
2. Ищем уязвимости с помощью google <https://habr.com/ru/post/283210/>
3. Exploring Google Hacking Techniques <https://securitytrails.com/blog/google-hacking-techniques>
4. <https://ufonet.03c8.net/>
5. <https://github.com/Ekultek/Zeus-Scanner>
6. <https://github.com/AlisamTechnology/ATSCAN>