

Fakulta elektrotechniky a informatiky
Vysoká škola báňská - Technická univerzita Ostrava

Cvičení 6

POČÍTAČOVÁ OBRANA A ÚTOK - POU




Google hacking – úvod, historie

- v roce 2002 John Long začal sbírat zajímavé dotazy pro vyhledávač google, které označoval jako **googleDorks**
- z **googleDorks** se později stala Google Hackng Databáze (GHDB)
- Google hacking je technika využívající (poměrně agresivní) vyhledávače – především Google
- slouží k nalezení (zaindexovaných) bezpečnostních děr webů


Google hacking database (GHDB)

- <http://www.hackersforcharity.org/ghdb/>
- <https://www.offensive-security.com/community-projects/google-hacking-database/>
- <https://www.exploit-db.com/google-hacking-database/>
- <https://pentest-tools.com/information-gathering/google-hacking#>

Target domain 

This field is required.

- Q Directory listing vulnerabilities
- Q Configuration files exposed
- Q Database files exposed
- Q Log files exposed
- Q Backup and old files
- Q Login pages
- Q SQL errors
- Q Publicly exposed documents
- Q phpinfo()

EXPLOIT DATABASE 

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category **SEARCH**

Date	Title	Category
2017-03-27	(ext:php) (inurl:/wp-content/uploads/AAPL/loaders/)	Footholds
2017-03-27	inurl:"/irclogs/" ext:log	Files Containing Juicy Info
2017-03-27	"Below is a rendering of the page up to the first error." ext:xml	Error Messages
2017-03-27	inurl:"/attachment/" ext:log	Files Containing Juicy Info
2017-03-21	filetype:pcmcfg	Files Containing Juicy Info
2017-03-08	inurl:cgi-bin/!spores_web?node	Various Online Devices

Google hacking - operátory

<https://www.google.com/help/cheatsheet.html>

<http://www.vyhledavace.net/jak-pouzivat-parametry-pri-vyhledavani/>

<https://www.sans.org/security-resources/GoogleCheatSheet.pdf>

site: (hledání výrazů v zadané síti)

filetype: (hledání uvnitř souborů daného typu)

link: (hledání stránek obsahujících odkaz)

cache: (Zobrazí stránku z cache Google)

intitle: (vyhledává výraz v titulku dokumentu)

allintitle: (vyhledává výraz v titulku dokumentu)

inurl: (vyhledává výraz v URL stránek)

allinurl: (vyhledává výraz v URL stránek)

@, -, "", OR, .., related, ...

Google hacking - nástroje

- Search Diggity
- Goolag Scanner

The screenshot displays the Search Diggity application window. The 'Google' search engine is selected. The 'Settings' dialog is open, showing options for 'Sites/Domains/IP Ranges' and 'Proxies'. The 'Simple' scan mode is active. The 'Queries' list on the left includes 'SLDB' with a 'Custom' query selected. The search results table shows the following data:

Categc	Search String	Page Title	URL
SLDB	"phpMyAdmin" "running on localhost - phpMyAdmin 2.2.4	running on localhost - phpMyAdmin 2.2.4	http://www.ppt-us.com/phpMyAdmin/main.php?lang:
SLDB	"phpMyAdmin" "running on 195.128.235.43 - ph	phpMyAdmin running on 195.128.235.43 - ph	http://www.nbtv.info/ml/main.php
SLDB	"phpMyAdmin" "running on rdbms.strato.de - ph	phpMyAdmin running on rdbms.strato.de - ph	http://www.nothofer.de/phpMyAdmin/main.php
SLDB	"phpMyAdmin" "running on rdbms.strato.de - ph	phpMyAdmin running on rdbms.strato.de - ph	http://www.realcreation.com/survey/main.php?lang=

The 'Output' pane shows the following log:

```
Simple Scan started. [8/4/2012 4:10:45 PM]
Found 85 result(s) for query: `phpMyAdmin" "running on" inurl:"main.php"`.
Total Results: 85.
Scan Complete. [8/4/2012 4:10:51 PM]
```

The Google Diggity logo is visible in the bottom right corner of the application window.

Google hacking - příklady

- Stránky admin.php

<http://www.google.com/search?q=inurl:admin.php&start=10>

- emailové adresy

<https://www.google.cz/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=inurl%3A%22email.xls%22>

- bezpečnostní kamery

https://www.google.cz/?gfe_rd=cr&ei=WqAsVd6hHOmk8wfm6YCgBw&gws_rd=ssl#q=inurl:%22viewerframe%3Fmode%3Dmotion%22

intitle:liveapplet inurl:LvAppl nebo “powered by webcamXP“

<http://www.opentopia.com/hiddencam.php>

- hesla:

inurl:passlist.txt

inurl:password.txt

inurl:config.php

Google hacking - protokol



Počítačová obrana a útok Protokol z předmětu



Tématická oblast: Google hacking

Přednášející: prof. Ing. Ivan Zelinka, Ph.D., Ing. Jan Plucar
Cvičící: Ing. Jiří Znoj

Jméno a číslo studenta:

Datum vypracování:

Zadání:

- 1) Seznamte se s problematikou Google hacking.
- 2) Vyzkoušejte si základní řetězce pro vyhledání obsahu.
- 3) Nalezněte a popište 5 zajímavých vyhledávacích termínů, zkuste k těmto termínům najít přes Google obsah, který je zajímavý z pohledu počítačové bezpečnosti.

Postup řešení:

- 1) Seznamte se s technikou Google hackingu, dále také s operátory (argumenty) vyhledávání přes Google službu
- 2) Pomocí operátorů sestrojte alespoň 5 složitějších vyhledávacích termínů
- 3) Odkoušejte vámi sestrojené dotazy – z každého dotazu vyberte nejzajímavější obsah, alespoň 3 dotazy musí vrátit obsah zajímavý z pohledu bezpečnosti.
- 4) Pro každý z těchto 5ti dotazů do protokolu запиšte:
 - Hledaný výraz (Search query)
 - Ukázka nalezeného obsahu (nejlépe screenshot)
 - Popis možného zneužití výsledku

Závěr:

- Napište, s jakým dalším zajímavým obsahem (z pohledu bezpečnosti) jste se při plnění protokolu setkali.
- Blíže popište, jak funguje indexování a vyhledávání Google. Jaké mohou být důvody, že vyhledávač dokáže vrátit potenciálně zneužitelné výsledky?
- Jak se chránit?

vícenapř. zde: <http://www.lukasnovak.net/skolni-prace/kib-google-hacking/>