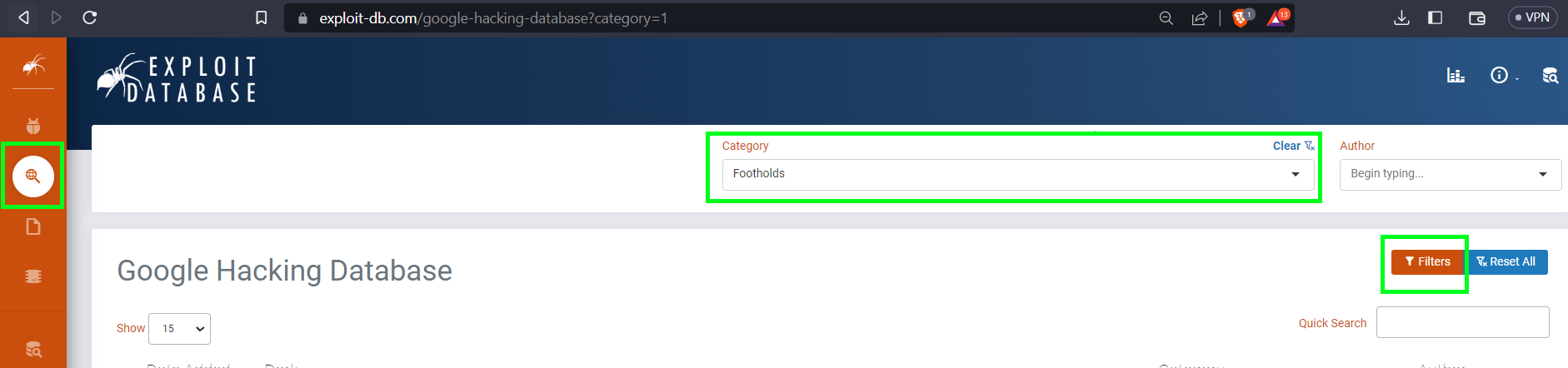
|  |  |  |  |
| --- | --- | --- | --- |
| **MODALIDADE:** | Curso de Especialização Tecnológica (CET) | **Ficha 10: Exploit-DB – Google Hacking** | |
| **CURSO:** | Técnico especialista em cibersegurança | | |
| **UFCD:** | Wargamming | **CÓDIGO UFCD:** | 9197 |
| **FORMADOR/A:** | Ricardo Lobo | **DATA:** | 05/05/2023 |
|  |  |  |  |
| **OBJETIVOS** | | | |
| * A utilização do *Google Hacking* para a obtenção de informações que se encontram disponíveis na Internet, mas que não se encontram indexadas no Google. * Compreender a importância do *Exploit-DB* e como pode ser utilizado na cibersegurança. | | | |

# Exercício 1: Exploit-DB: Google Hacking

No site Exploit-DB, na área dedicada ao Google *Hacking* (<https://www.exploit-db.com/google-hacking-database>), **escolha um “*Dorks*” de cada categoria** e faça capturas de ecrã das informações obtidas com esses *dorks*.



De seguida, apresenta-se um exemplo do que se pretende que os formandos realizem.

### EXEMPLO Categoria 1 – Footholds

|  |
| --- |
| **Google Hacking *- Query*** |
| intitle:"Index of /" +.htaccess |

|  |
| --- |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
|  |

### Categoria 1 – Footholds

* <https://www.exploit-db.com/google-hacking-database?category=1>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| inurl:/Dashboard.xhtml intitle:"Dashboard" |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-1** |

### Categoria 2 - Files Containing Usernames

* <https://www.exploit-db.com/google-hacking-database?category=2>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| intext:"-----BEGIN CERTIFICATE-----" ext:txt |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-2** |

### Categoria 3 - Sensitive Directories

* <https://www.exploit-db.com/google-hacking-database?category=3>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| intitle:"index of /" "sqlite.db" |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-3** |

### Categoria 4 - Web Server Detection

* <https://www.exploit-db.com/google-hacking-database?category=4>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| inurl \*:8080/login.php |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-4** |

### Categoria 5 - Vulnerable Files

* <https://www.exploit-db.com/google-hacking-database?category=5>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| allintext:wp-includes/rest-api |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-5** |

### Categoria 6 - Vulnerable Servers

* <https://www.exploit-db.com/google-hacking-database?category=6>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| intitle:"index of" "/views/auth/passwords" |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-6** |

### Categoria 7 - Error Messages

* <https://www.exploit-db.com/google-hacking-database?category=7>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| intitle:"index of" errors.log |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-7** |

### Categoria 8 - Files Containing Juicy Info

* <https://www.exploit-db.com/google-hacking-database?category=8>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| inurl: "/wp-content/uploads" |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-8** |

### Categoria 9 - Files Containing Passwords

* <https://www.exploit-db.com/google-hacking-database?category=9>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| intitle:"Index of" pwd.db |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-9** |

### Categoria 10 - Sensitive Online Shopping Info

* <https://www.exploit-db.com/google-hacking-database?category=10>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| site:mail.\* intitle:Dashboard |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-10** |

### Categoria 11 - Network or Vulnerability Data

* <https://www.exploit-db.com/google-hacking-database?category=11>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| -site:"pentest-tools.com" intext:"Scan coverage information" AND "List of tests" ext:PDF |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-11** |

### Categoria 12 - Pages Containing Login Portals

* <https://www.exploit-db.com/google-hacking-database?category=12>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| inurl: "/admin" intitle:"Admin Login" |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-12** |

### Categoria 13 - Various Online Devices

* <https://www.exploit-db.com/google-hacking-database?category=13>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| inurl:"device.rsp" -in |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-13** |

### Categoria 14 - Advisories and Vulnerabilities

* <https://www.exploit-db.com/google-hacking-database?category=14>

|  |
| --- |
| **Google Hacking *- Query* 1** |
| intext:"Powered by Virtual Airlines Manager [v2.6.2]" |
| ***Print screens* das informações recolhidas com a *query* escolhida** |
| **images/Rodrigo\_Dorking-14** |

Depois de realizada a ficha de trabalho, submeta este ficheiro na tarefa criada para o efeito.

**Bom trabalho**