

**Advanced Security**

**Assignment 1**

**DT211C**

**BSc in Computer Science**

**Tim Browning**

**C14519547**

School of Computing

Dublin Institute of Technology

****

Table of Contents

[Part A 3](#_Toc506815224)

[Part B 6](#_Toc506815225)

[Part C 8](#_Toc506815226)

[Part D 8](#_Toc506815227)

[References 11](#_Toc506815228)

Figure 1 - Filetype operator 3

Figure 2 - Info Operator 4

Figure 3 - Filetype Operator (google) 4

Figure 4 - filetype operator (Bing) 5

Figure 5 - Database Rollback 8

Figure 6 - Buffer-flow 9

Figure 7 - SQL Injection 10

Figure 8 -Deleting Logs 10

# Part A

**Basic Operators**

The AND Searches for results that include both the term before and the term after the operator. This operator can be used alone. The operator wont work the the OR operator. It is normally used with two key words e.g. Dublin AND Cork. There are more results if you use the AND operator.

The OR operator Searches for results that include either the term before or the term after the operator (or both). This operator can be used alone. The operator wont work the the AND operator. It is normally used with two key words e.g. Dublin AND Cork. There are less results if you use the OR operator.

- operator = Manchester –united will just return Manchester.

~ operator = ~set will bring back synonyms.

\* operator - I’ve got a brand new pair of \*

Don’t work with Bing

related

cache

info

allinurl

allintitle

link:

\*

~

**Advanced Operators**

Filetype – searches google for more then just web pages. Searches google for different types of files(including PDF and word documents). An example of doing this is writing security filetype:pdf. Using this operator narrowed my search from 35,700,000 to 1,060,000 results. My results only consisted of pdf documents. The file extension typically has to be listed in the URL

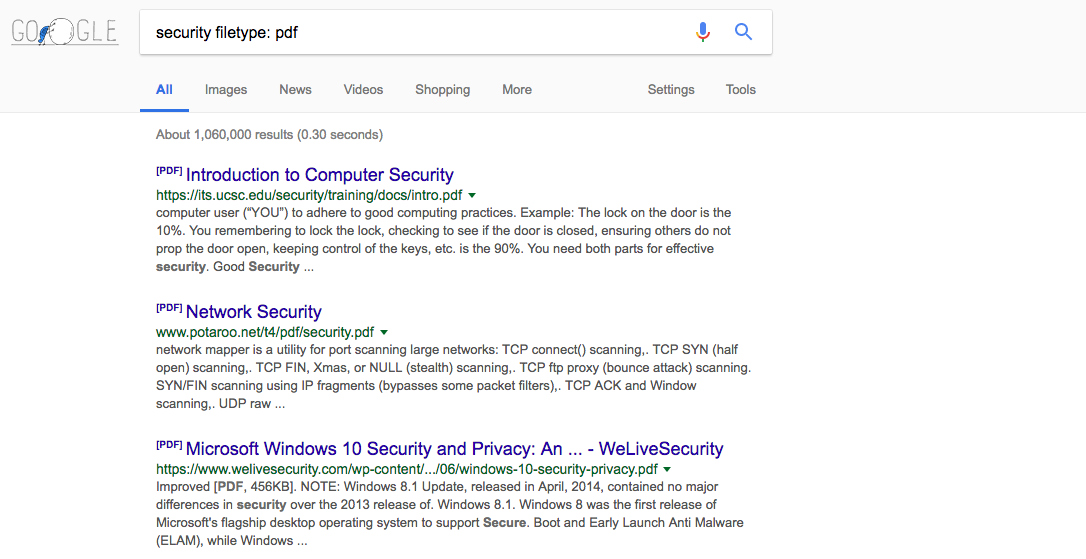


Figure 1 - Filetype operator

info:website – This operator will bring back information about a certain domain. It reveals

* Pages that are similar to the one you searched for
* Pages that link to the domain you searched for
* Other pages on the same domain
* Pages that contain the domain text on their page
* Google’s cache of the site

A regular search for [www.dit.ie](http://www.dit.ie) will give you 21,000,000 results where as info:www.dit.ie gives you back 1 result. This operator is generally not used with other operators.

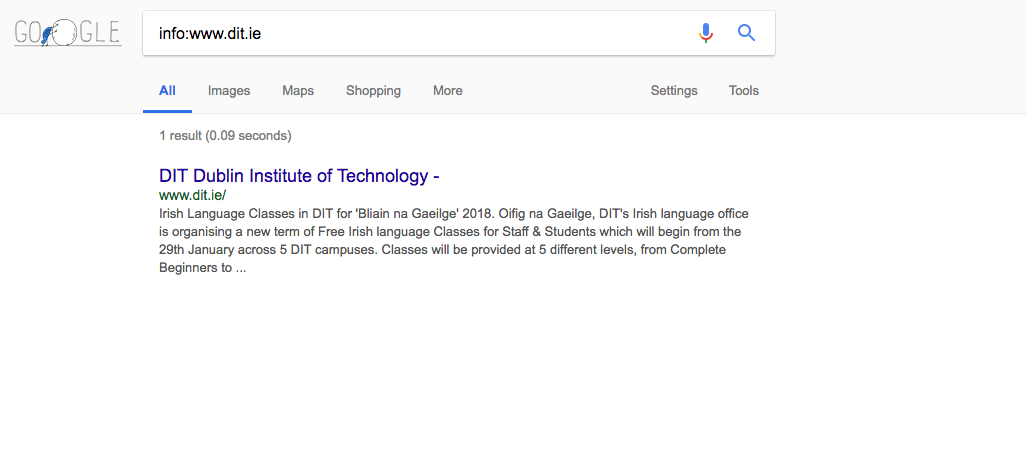


Figure 2 - Info Operator

Bing has ‘filetype,’ ‘AND’ and ‘OR’ operators. Bing does not have the ‘info’ operator. Google and Bing return different results. I searched security filetype:pdf in both search engines and bing returned 4,670,000 Results where as google returned 1,060,000 results. Also the two search engines displayed different top results.

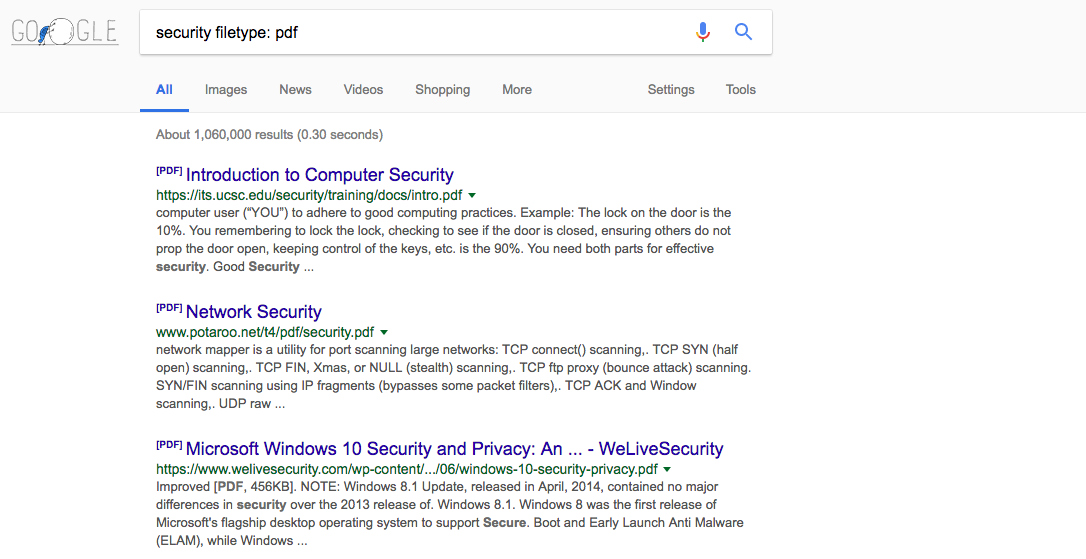


Figure 3 - Filetype Operator (google)

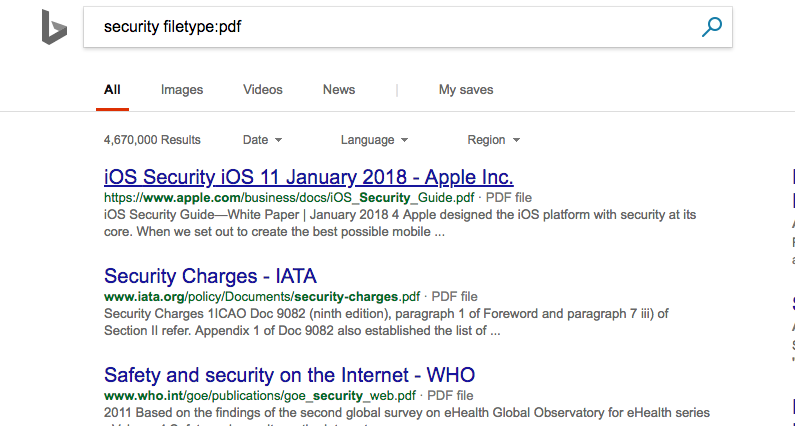


Figure 4 - filetype operator (Bing)

**1. Yahoo**

Advantages:

* Mail (1Tb) as opposed to googles 15GB

Disadvantages:

* Doesn’t have a book search
* No Google hangouts alternative
* No google maps alternative

**2. AOL**

Advantages:

* The AOL network includes many popular web sites like engadget.com, techchrunch.com and the huffingtonpost.com.

**3. ask.com**

google ranks their search results based on popularity but ask.com ranks their results based on a expertRank formula. The top results are determined by expertise.

Anyone can edit the search engines results.

**4. Baidu**

Advantages:

* Has the upper hand in China
* Baidu is [reported](http://www.chinainternetwatch.com/12678/search-engine-market-overview-2014/) to control around 80% of Chinese online search market

Disadvantages:

* Not an international search engine

**5. Wolframalpha**

Advantages:

* Does calulations. for example if you enter “mortgage 2000” as input it will calculate your loan amount, interest paid etc.

**6. DuckDuckGo**

Advantages:

* it is not fully loaded with ads
* DuckDuckGo(DDG) does not collect any information about the user, no search history, IP address or cookies

**7. Internet Archive**

Advantages:

* It is very useful tool if you want to trace the history of a domain.

**8. Yandex.ru**

Advantages:

* Yandex is a portal.
* Yandex is better for Russian language search
* It is popular on android

**9. Firefox**

Advantages:

* Tweakable interface and settings
* User-friendly features
* Open Source

**10. Opera**

Advantages:

* Hackers spend less time trying to infiltrate Opera

# Part B

**1. E-mail**

Messages can be easily misused. Confidential information can be leaked and nasty viruses can be sent between devices. One targeted e-mail could phish for access credentials from an employee. To reduce vulnerability, Identify the sender using technology such as PGP, or a simple array of questions before sending sensitive information.

**2. Smartphones and other digital devices**

A user is able to take a high-resolution picture of a computer screen, and then e-mail it over its 3G network? Implement a security system which checks what device goes in and out of a building

**3. USB thumb drives:**

Is the most common way a network is hacked into. The advantages of thumb drives are that they are small and hold a lot of data. Conficker worm can automatically execute upon connecting with a live USB port. Changing the computers autorun policy can reduce potential threats.

**3. Laptop and netbooks:**

Laptops are small and discrete and carry a full operating system with an Ethernet port. Employees may infect the device which can result in the stealing of personal, company and financial information. The laptop needs advanced encryption so data isn’t lost. Important information should not be stored on laptops.

**4. Wireless access points**

Wireless access points can be accessed by anyone with the correct key. Security protocols such as WPA are still prone to dictionary attacks. A common method of hacking into a access point is camping out in a van in proximity of the access point. The attackers use programs like Aircrack which picks up networking packets. Strong passwords are recommended to reduce dictionary attacks.

**5. Miscellaneous USB devices**

Devices such as cameras and mp3 players fall under this category. These devices can store information just like USBs. They are not commonly expected to hold viruses. But they are able to store them and have the potential are infecting an entire system.

Enforce asset control so no devices can enter the environment. Banning removable media will get rid of any threats.

**6. Inside connections:**

An employee may borrow a co-worker’ pc and unintentionally access areas of the network which are forbidden. This can give the employee confidential information such as usernames and passwords. Passwords should be strong and changed regularly. Access levels must be put in place by the workplace.

**7. The Trojan human:**

A Trojan human is a thief who dresses up as a normal worker and comes into the workplace. This person steals information from places such as server rooms and pc labs. They may ask a employee for a key or a swipe card to grant him access to unauthorised locations within the workplace.

Reminders for employees should be made constantly to reminder them to be wary if someone asks for your key card.

**8. LDAP Injection**

Injections occur when a malicious user enters in data that is not properly screened. The malicious data is sent to the app and gives you unauthorised access. LDAP contains applications that our email systems, network printers, encryption certificates use to get information from the local server. Poor coding can allow for attackers to manipulate parameters in the search function. The attacker can input a malicious query or code.

**9. Stored Cross-Site Scripting(XSS)**

XSS attacks occur when an attacker is able to inject a bit of malicious JavaScript into a site. The attacker is able to send malicious content and in return receive data from the victim. The end user does not know about this. XSS attackers can enable every user to be redirected to the attackers’ website.

**10. Optical Media**

CDs can store information much like USBs. They can be used like thumb drives. They can be mistaken for CDs which contain music. A asset control system would prevent this.

# Part C

Demonstrate the use of Fingerprinting Organizations with Collected Archives (FOCA)

Setup:

https://null-byte.wonderhowto.com/how-to/hack-like-pro-extract-metadata-from-websites-using-foca-for-windows-0155076/

# Part D

**1. Deployment Failures**

The most common cause of database failure is a lack of care at the moment a database is deployed. There is very little error checking occurring. Database teams five insufficient thought in how they are to deploy the database. The consequences of this mean the database becomes too fragile and it is impossible to do a rollback. The database is in an unreliable state.

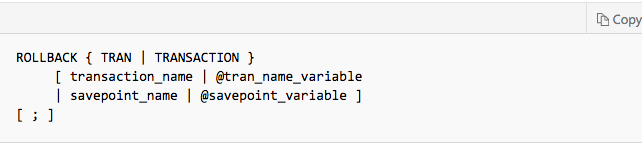


Figure - Database Rollback

**2. Broken databases**

A bug called slammer worm went around in 2003 and infected 90% of vulnerable computers. This broke thousands of databases. The worm was discovered in Microsoft SQL server. The database administrators had to install a fix. This exploited buffer-flow vulnerability.

And example of a buffer-flow is demonstrated in this video:

<https://www.youtube.com/user/marcelocarvalho0910>

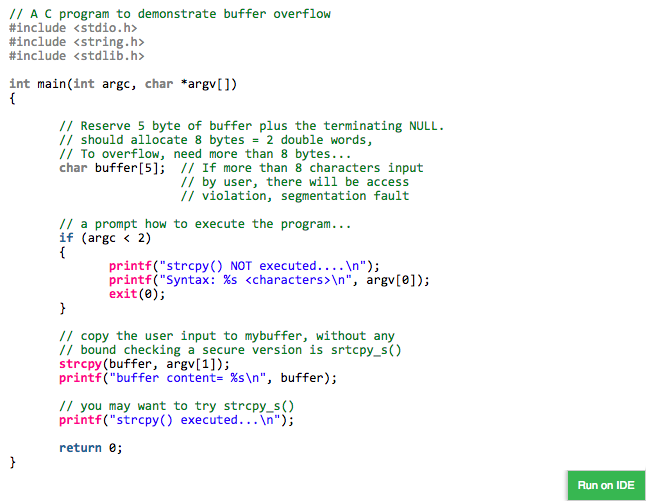


Figure - Buffer-flow

**3. Data leaks**

Databases contain a networking interface. This means they are accessible to hackers are able to capture traffic to exploit it. To avoid this pitfall, administrators use SSL or TLS encryptions. This video tutorial shows you how to get information from a database

<https://www.youtube.com/watch?v=X9sClw-wXqM>

**4.  SQL injections**

Is an injection attack where an attacker can execute malicious SQL statements. An SQL injection can effect any website that’s uses SQL based database. An attacker can use it to bypass a web application’s authentication and authorization mechanisms and retrieve the contents of an entire database. For a SQL injection to occur, the vulnerable website needs to allow for a user input.

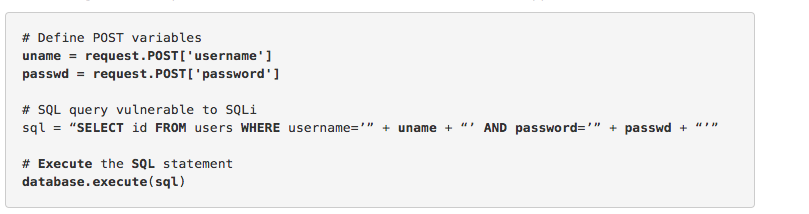


Figure - SQL Injection

<https://www.youtube.com/watch?v=PB7hWlqTSqs>

**5. The abuse of database features**

Programs which use SQL have many different tools. Getting rid of the unnecessary tools can reduce the risk of being attacked. Logs also store important information which could exploit information

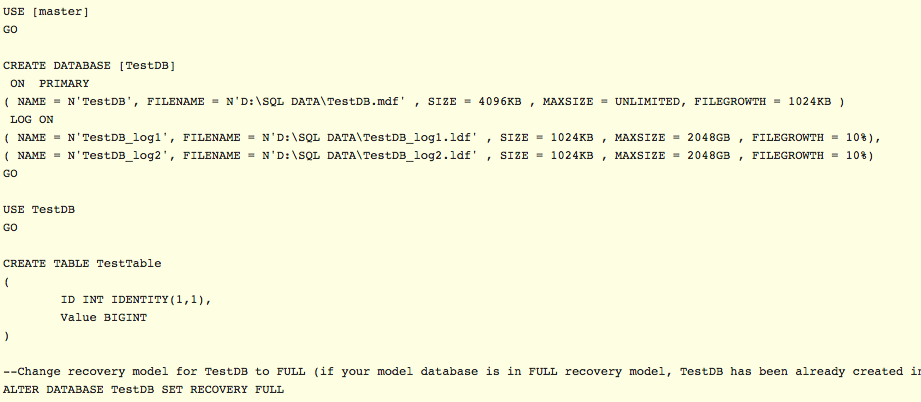


Figure -Deleting Logs

**6. Hopscotch**

Hopscotch is when an attacker tries to Find weakness within the infrastructure of a database system. The attacker can see the credit card processing area. Each department should have different access control.

# References

<https://www.acunetix.com/websitesecurity/sql-injection/>

<http://www.zdnet.com/article/the-top-ten-most-common-database-security-vulnerabilities/>