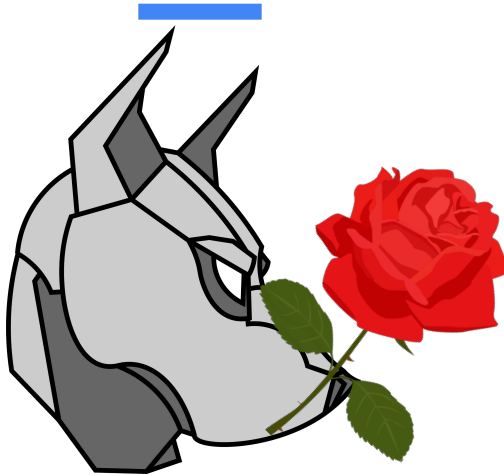


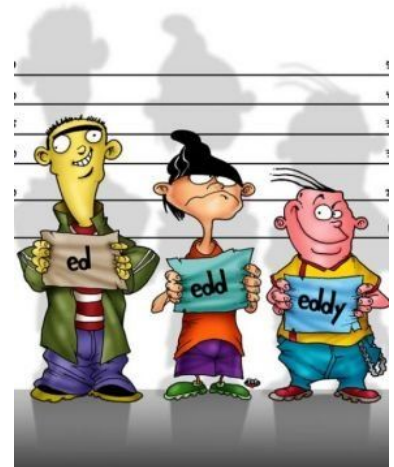
# Cyber Defense Organization

Spring 2020 - Google Dorking



# Disclaimer

- Please do not use this to log into websites/ databases/ etc or download files you find that you don't have permission to. That is illegal and CDO is not responsible for what happens to you.
- You could be prosecuted under CFAA



# OSINT - Open Source Intelligence

- Definition: Using basic internet searching to find information on the target. This information must be Publicly Available to be considered OSINT
- Used by: Pen-Testers, Red Team, malicious hackers
- Why is it used: Because it's easy, and a good way to find information about your target



Penetration  
Test

Reconnaissance

Threat Modeling

Vulnerability  
Analysis

Exploitation

Post Exploitation

# What is Google Dorking?!?

- If you work at Google are you a dork?
- A form of OSINT
- Obviously we are using Google for this but how/ why?



# What does googling actually mean?

- You are querying a database
- But google is “smart” so it doesn’t need the extra junk

## Example

```
SELECT CustomerName, City FROM Customers;
```

Try it Yourself »

## SELECT \* Example

The following SQL statement selects all the columns from the "Customers" table:

## Example

```
SELECT * FROM Customers;
```

Try it Yourself »


^ Mega simplification... but it worky for our case




# How does this work?

- You might have heard of ways to make your google search better
- Examples...
  - Adding quotes around the word you're searching
    - puppy dog sweaters vs "puppy dog sweaters"
  - Using the hyphen to exclude words
    - Mustang -car -cars
- Google dorking uses more advanced operators to find things



# How most people use this

"ACFE" OR site:www.acfe.com trends of fraud accounting  

 All  News  Images  Videos  Shopping  More Settings Tools

---

About 48,500 results (0.57 seconds)

www.acfe.com › report-to-the-nations ▼

**2018 ACFE Report to the Nations - ACFE.com**

Discover **trends**. Learn how **fraud** is committed and the most effective ways to detect it. Identify **fraud** losses at global, industry and organizational levels. Discover ...

www.acfe.com › the-fraud-examiner ▼

**The Fraud Examiner Archives | ACFE - ACFE.com**

Learn recent **trends** and techniques from CFEs and subject matter experts. ... Auditing U.S. Companies in China: Symptomatic of Bigger **Accounting Fraud** ...

site:www.acfe.com type:pdf



All

News

Images

Shopping

Videos

More

Settings

Tools

About 707 results (0.43 seconds)

www.acfe.com › rttn › images › cost-of-fraud-infographic ▼ PDF

## Median Loss By Scheme Type When collusion is ... - ACFE.com

of FRAUD. Median Loss By Scheme **Type**. Financial statement fraud. Asset misappropriation. Corruption. \$200,000. \$1,000,000. \$130,000. Revenues the typical.

www.acfe.com › Shared\_Content › Products › Self-Study\_CPE ▼ PDF

## I. Introduction to Fraud Examination - ACFE.com

while a **type** of internal fraud, will be covered in a separate section. Asset Misappropriation Schemes. Asset misappropriation schemes include both the theft of ...

**type:pdf lets you find official stuff**



# What are WE looking for??

- Misconfigured devices that are pointing out to the internet
- Examples of these things
  - FTP servers
  - Webcams
- Files that made their way out to the internet (probably on accident)
  - Log files
  - Excel sheets
  - Config Files
  - Frankly any file of importance
- Fun stuff



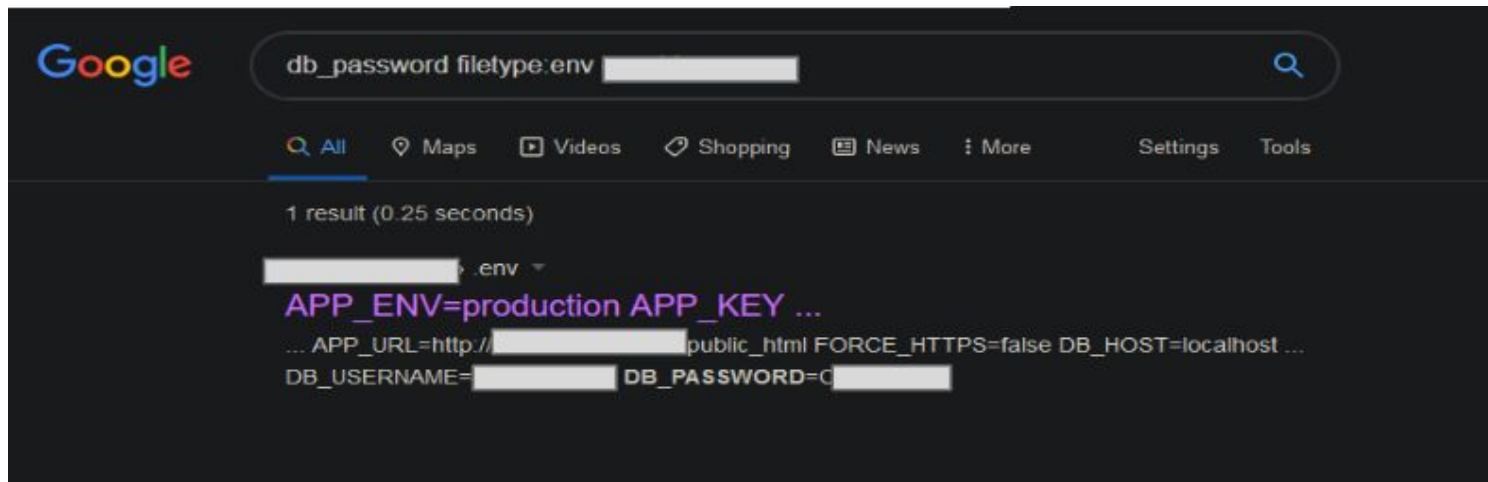
# What are some of the operators?

- **allintext:**
  - Searches for specific text string
- **allintitle:**
  - Same as all in text but for the title
- **site:**
  - Looks for specific sites
- **inurl:**
  - Looks for things in the url
- **filetype:**
  - Looks for file types



# A fun example

- db\_password filetype:env WEBSITE.COM
- Why does this work?
  - It is looking for the variable db\_password
  - A common variable in an environment file



# Another example

- allintext: "WebcamXP 5"
- Searches for the WebcamXP 5

**webcamXP**

webcamXP is the most popular webcam and network camera software for Windows.

It allows you to monitor your belongings from any location with access to Internet by turning your computer into a security system.

Connect remotely by using other computers or your mobile phone. Broadcast live video to your website. Schedule automatic captures or recordings. Trig specific actions using the motion detector. You can easily use those features among others with webcamXP.

It supports a large selection of [Network Cameras](#) (1500+) and is used in multiple industries including national security (police, army), aerospace and defense, museums, hotels, shops, zoos and many others.

Most important for us is to provide a stable and high-performance software. webcamXP is designed to be online 24/7 while using reasonable resources on your computer.



**webcamXP 5.9.8.7**  
Updated on 09/06/2016

**webcam 7 1.5.3.0**  
Updated on 09/06/2016

**Moonware Universal Source Filter 4.6**



Compatible with Windows XP, Vista, 7, 8, 10\*  
Server 2003, 2008 and 2012

**[Download Now](#)**

\* Windows 10 is supported by webcam 7.



Date Added 

Dork

2019-08-02

s3 site:amazonaws.com filetype:log

2019-07-31

s3 site:amazonaws.com intext:dhcp filetype:txt inurl:apollo

2019-07-31

site:amazonaws.com inurl:login.php

2019-06-04

s3 site:amazonaws.com filetype:sql

2019-05-31

s3 site:amazonaws.com filetype:xls login

2019-05-31

s3 site:amazonaws.com filetype:xls password

**What might these be looking for?**

# In Scope: Bug Bounties

<https://www.bugcrowd.com/bug-bounty-list/>



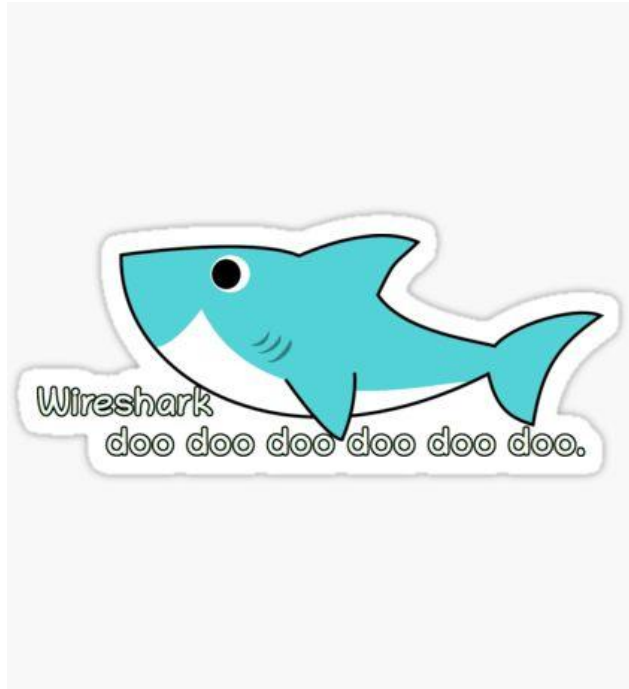
# Hands on time

- Go to this link for a full list of operators and some example searches
- <https://tinyurl.com/GoogleDorking>





# Next Time... Wireshark!





# Add us on Social Media!

Twitter: **@ualbanyCDO** 

Instagram: **ualbany\_cdo** 

Website: **uacyber.org** 

Myinvolvement: **Cyber Defense Org**

**We have a new discord!**

