Cybersecurity 701

Typo squatting Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Typosquatting

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

- Software tool used
  - **`wget`** (Linux Command Line Tool)
  - Leafpad (Linux application)

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.2 - Explain common threat vectors and attack surfaces.
    - Human vectors/ social engineering
      - Typo squatting

What is Typosquatting?

- Typosquatting is exploiting a user’s misspelling
  - Could type www.facbook.com instead of www.facebook.com
  - What if a user goes to www.waether.com instead of www.weather.com
  - This is also known as cybersquatting
- A malicious user will buy one of these domain names in the hope that someone will visit this website accidentally

Typosquatting Lab Overview

1. Set up Environments
2. Find Kali’s IP Address
3. Copy Taylor’s Blog Site
4. Access Website
5. Create Typosquatting Website
6. Create Malicious File
7. Edit the Typosquatting Website
8. Access Typosquatting Website

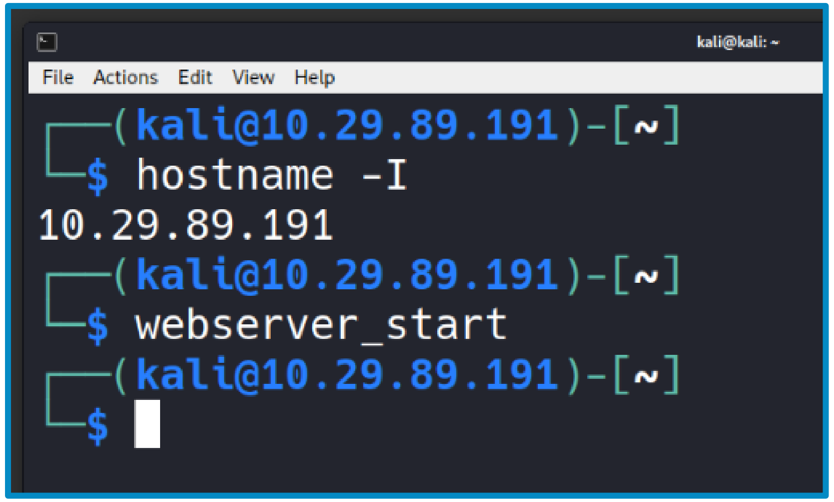
Set up Environments

- Log into your range.
- Duplicate the browser tab for the range.
- Open the Kali Linux in one tab and Windows 7 in the second tab.
  - You should start on your Kali Linux Desktop.
  - You can leave your Windows 7 Desktop running on the second tab.

Find the Kali IP Address and Start the Server

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Kali VM, open the Terminal and type the following command:

  `hostname -I`
- This will display the IP Address
  - Write down the Kali VM IP address
- Use the command **`webserver_start`** to start hosting the page we will exploit.



```
┌──(kali@10.29.89.191)-[~]
└─$ hostname -I
10.29.89.191
┌──(kali@10.29.89.191)-[~]
└─$ webserver_start
┌──(kali@10.29.89.191)-[~]
└─$ 
```

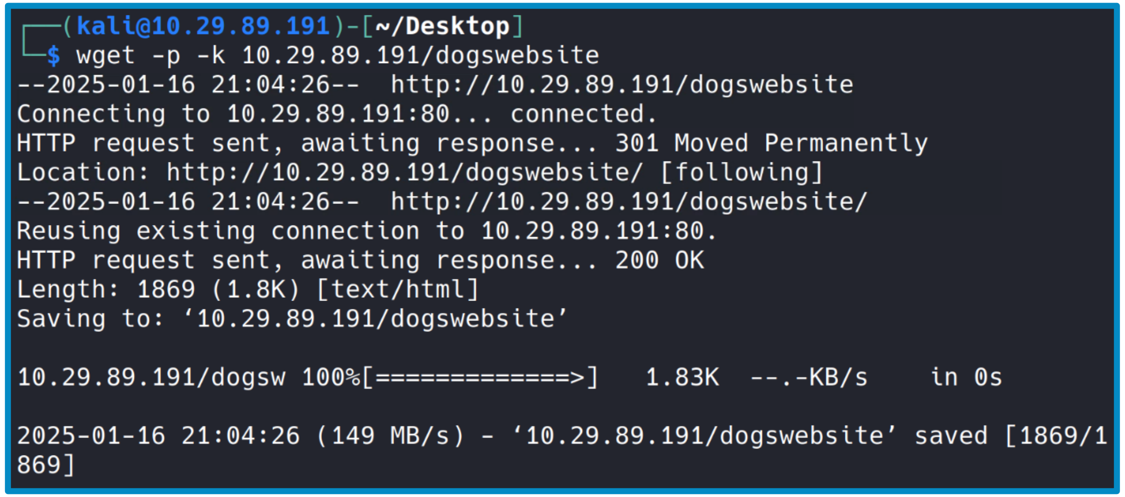
Copy Taylor’s Blog

- Navigate to the Desktop

```
cd Desktop
```

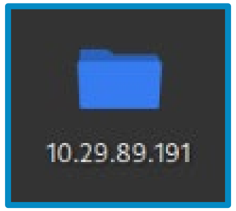
- Copy Taylor’s Blog page

```
wget -p -k <kali-IP-address>/dogswebsite
```



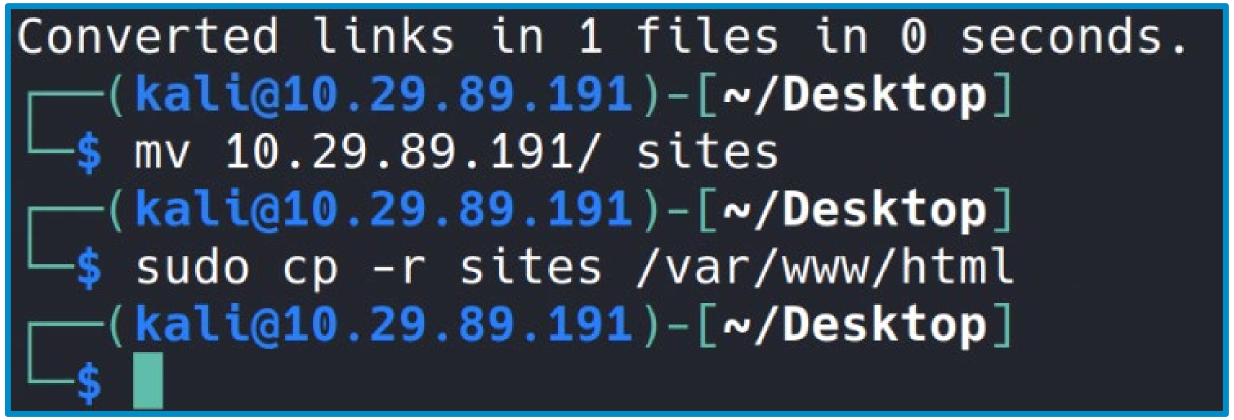
```
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ wget -p -k 10.29.89.191/dogswebsite
--2025-01-16 21:04:26--  http://10.29.89.191/dogswebsite
Connecting to 10.29.89.191:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://10.29.89.191/dogswebsite/ [following]
--2025-01-16 21:04:26--  http://10.29.89.191/dogswebsite/
Reusing existing connection to 10.29.89.191:80.
HTTP request sent, awaiting response... 200 OK
Length: 1869 (1.8K) [text/html]
Saving to: ‘10.29.89.191/dogswebsite’

10.29.89.191/dogsw 100%[=============>]   1.83K  --.-KB/s    in 0s

2025-01-16 21:04:26 (149 MB/s) - ‘10.29.89.191/dogswebsite’ saved [1869/1
869]
```

You should see this folder appear on the Desktop that contains the website’s index page. The IP address will match yours. →



Access Website

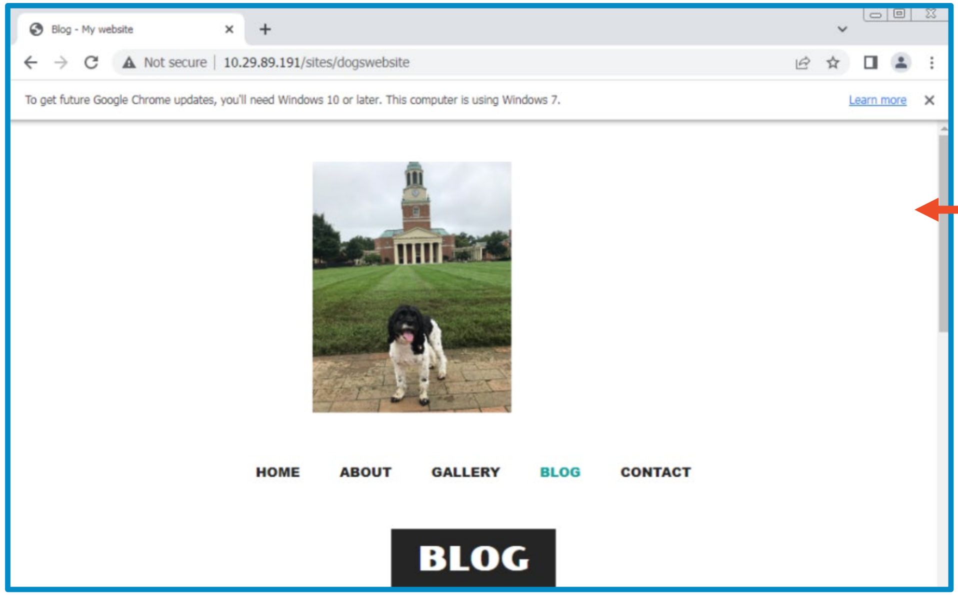
- Rename the directory
  - **`mv <Kali-IP-address> sites`**
- Copy the cyber.org file to the Apache server
  - **`sudo cp -r sites /var/www/html`**



```
Converted links in 1 files in 0 seconds.
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ mv 10.29.89.191/ sites
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ sudo cp -r sites /var/www/html
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ 
```

Access Website on Windows 7

- Go to the Windows 7 Environment
- Open Google Chrome
- Go to the following URL
  - <Your-Kali-IP-Address>/sites/dogswebsite
- Click on the HOME tab and note it simply reloads the page



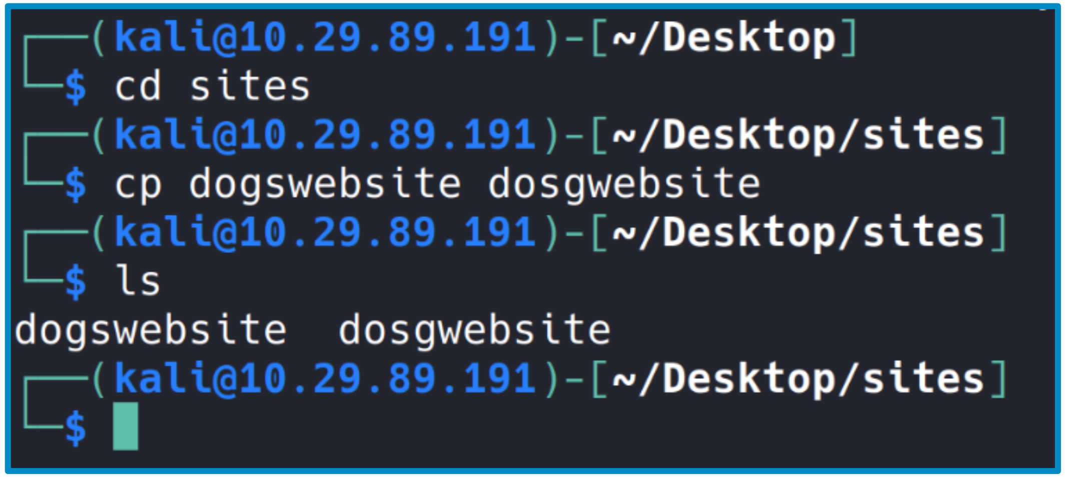
To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

You should see this website load as shown

Create Typosquatting Website

- Now, create a malicious website.
- Go back to the Kali machine.
- Navigate into the sites directory with
  `cd sites`
- Create an altered copy of the blog page.
  `cp dogswebsite dosgwebsite`
- Use **`ls`** to view the files.

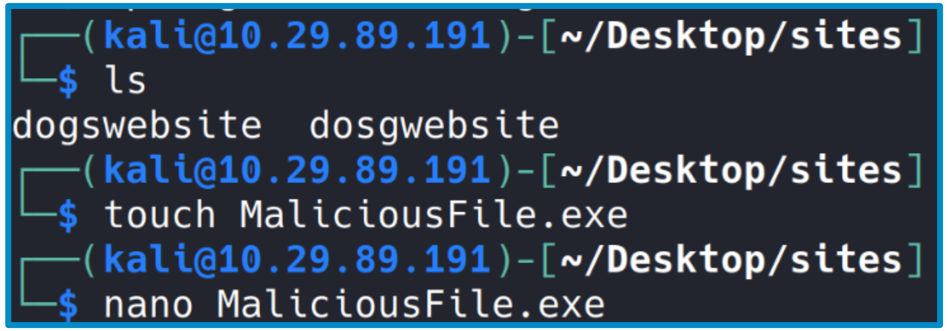
Note the misspelling of “dogswebsite” to “dosgwebsite”



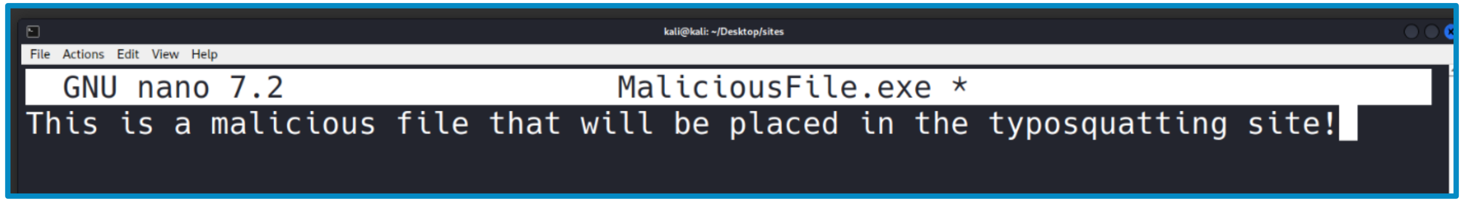
```
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ cd sites
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ cp dogswebsite dosgwebsite
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ ls
dogswebsite  dosgwebsite
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ 
```

Create Malicious File

- Create a malicious file
  - **`touch MaliciousFile.exe`**
- Add some text to the MaliciousFile.exe
  - **`nano MaliciousFile.exe`**
  - Add some text
  - CTRL+X, y, ENTER to exit



```
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ ls
dogswebsite  dosgwebsite
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ touch MaliciousFile.exe
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ nano MaliciousFile.exe
```

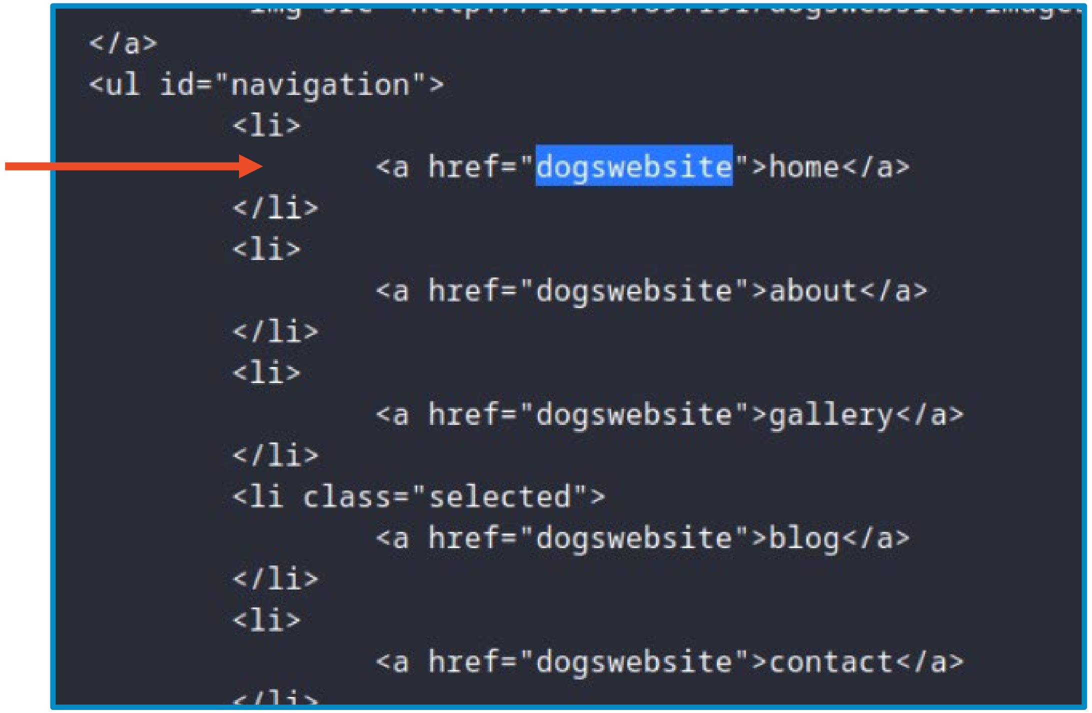


```
  GNU nano 7.2                    MaliciousFile.exe *
This is a malicious file that will be placed in the typosquatting site!
```

Edit the Typosquatting Website

- Open the cybre.org HTML file in Leafpad
  - **`leafpad dosgwebsite`**
- Find the code that controls the home link
  - You could change any of the links for about, gallery, blog, etc. if desired.

The line of code will start with <a href.



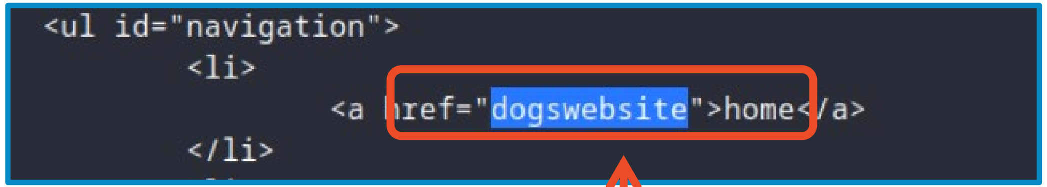
```
          img src="http://10.29.69.191/dogswebsite/image
</a>
<ul id="navigation">
        <li>
                <a href="dogswebsite">home</a>
        </li>
        <li>
                <a href="dogswebsite">about</a>
        </li>
        <li>
                <a href="dogswebsite">gallery</a>
        </li>
        <li class="selected">
                <a href="dogswebsite">blog</a>
        </li>
        <li>
                <a href="dogswebsite">contact</a>
        </li>
```

Edit the Typosquatting Website Home Link

- Change the “home” link to the following:

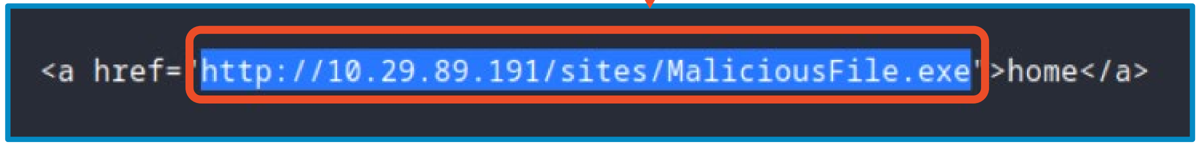
  `http://<Your-Kali-IP-Address>/sites/MaliciousFile.exe`

- Click File, Save, and exit when you are finished



```
<ul id="navigation">
        <li>
                <a href="dogswebsite">home</a>
        </li>
```

Change this link and be sure to add http and use your Kali IP address

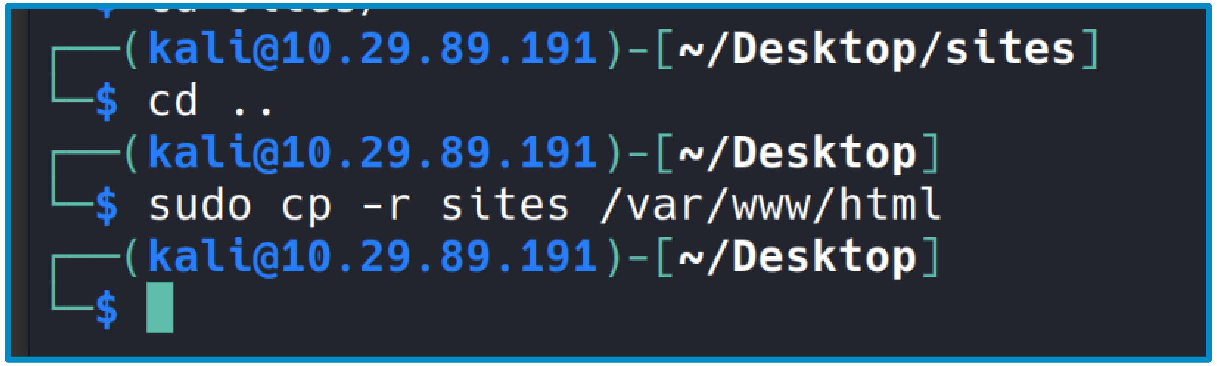


```
<a href="http://10.29.89.191/sites/MaliciousFile.exe">home</a>
```

Move Typosquatting Website

- Navigate out of the directory with **`cd ..`**
- Copy the files to the Apache server which will overwrite the one we copied earlier

```
  sudo cp -r sites /var/www/html
```

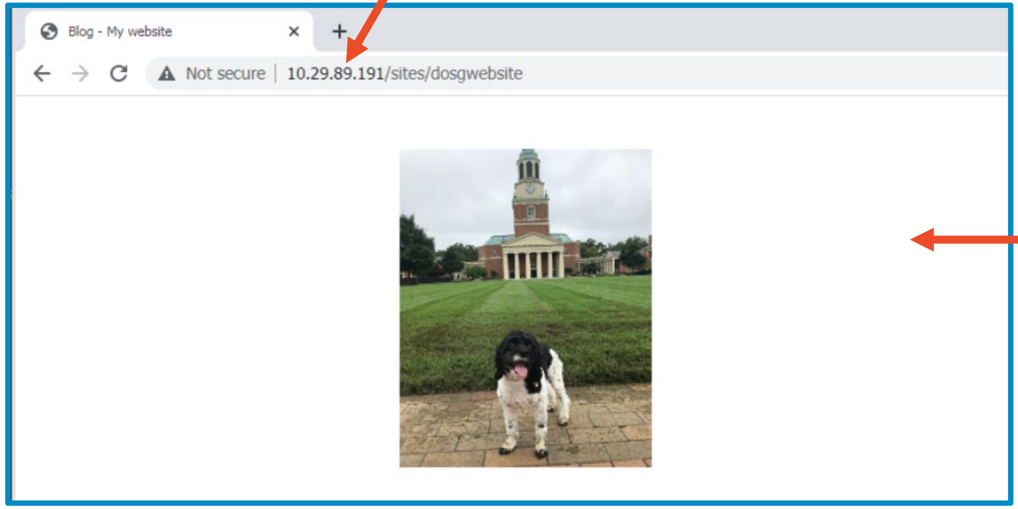


```
└─$ cd sites/
┌──(kali@10.29.89.191)-[~/Desktop/sites]
└─$ cd ..
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ sudo cp -r sites /var/www/html
┌──(kali@10.29.89.191)-[~/Desktop]
└─$ 
```

Access Typosquatting Website

- Go to the Windows 7 Environment
- Return to Google Chrome
- Go to the following URL
  - <Your-Kali-IP-Address>/sites/dosgwebsite

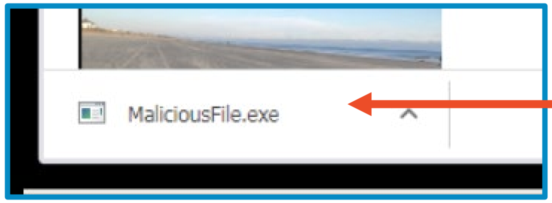
Here, the user misspells dog



You should see this website load, which looks just like the original website.

Downloading the Malicious File

- On the website, click on the “Home” option
- You should see the MaliciousFile.exe download
- Obviously this MaliciousFile.exe is not harmful, but an unsuspecting user might trust this website because it looks exactly like the original blog page.
- In the real world, this file is probably going to be harmful to your system!



MaliciousFile.exe downloaded

Defend Against Typosquatting

- Always check your domain names!
- Companies will actually purchase the domains of common typos to protect users
  - For example, go to www.gooogle.com
    - It will re-direct you to Google
  - Go to www.facbook.com
    - It will re-direct you to Facebook
  - Go to mikerowesoft.com
    - It will re-direct you to Microsoft’s website