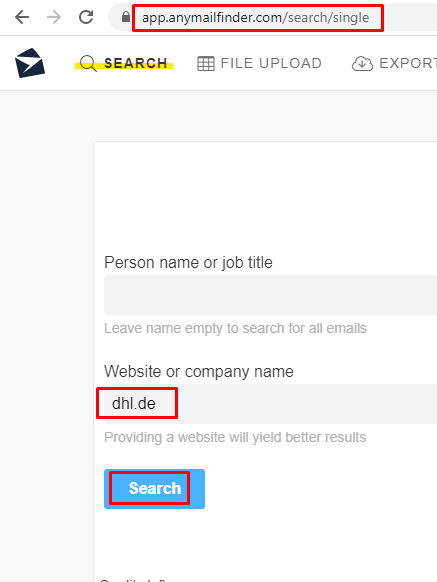
**INFO LEAK MONITOR**

1. **VIP Leaks**

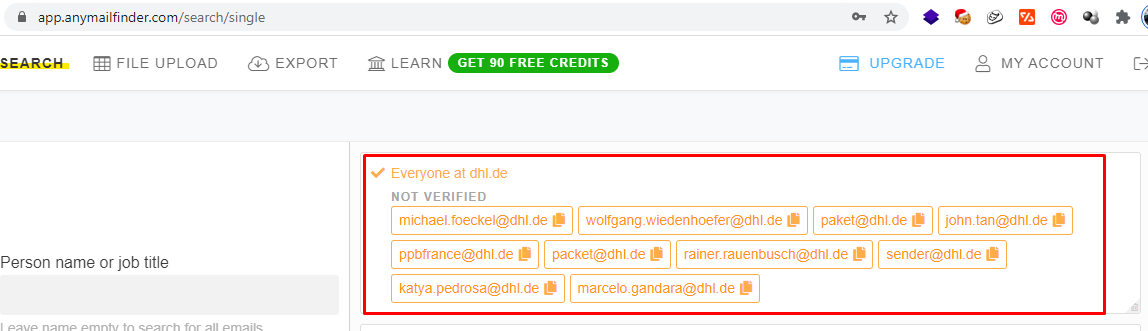
Tool to check email harvesting **https://app.anymailfinder.com/search/**

1. **VIP Email harvesting:**

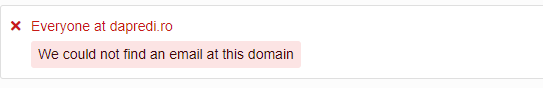
**Step 1:** Enter the domain name in search field, click on search and consider domain name as input.



**Step 2:** If the output shows the emails consider alert severity **INFORMATIONAL** with alert score **0**.



**Step 3:** If output shows could not find any emails at this domain consider as **IGNORE**



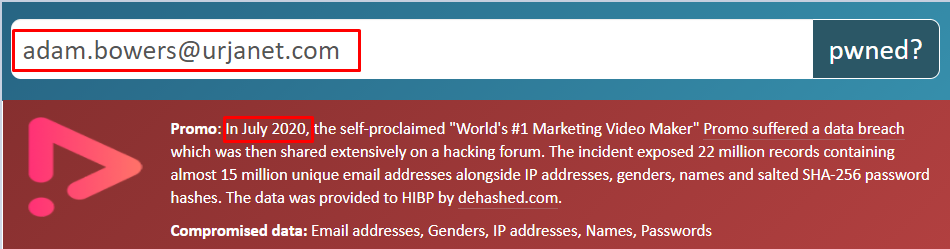
1. **VIP Email Breach**

Tool to check VIP Email Breach **https://haveibeenpwned.com/**

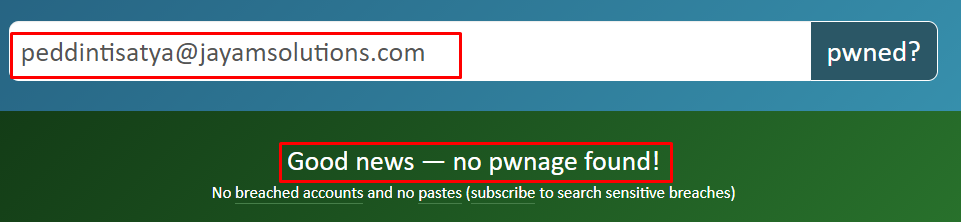
**Step 1:** Enter the email id and consider email id as Input

* **VIP Email ID Breach < 6 Months:**

**Step-1:** If the email breaches < = 6 months consider alert severity as **MEDIUM** with alert score **5**

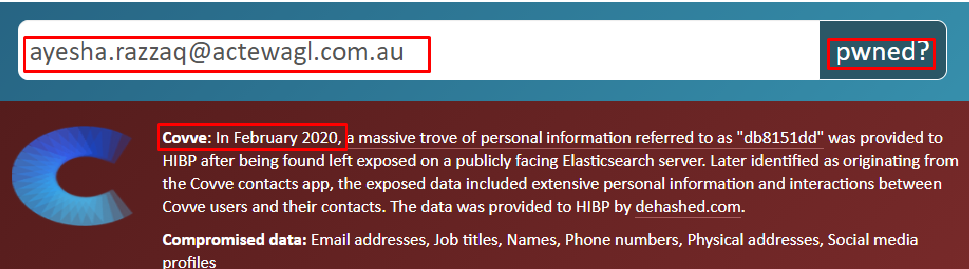


**Step-2:** If no VIP email breaches consider as **IGNORE**



* **VIP Email ID Breach 6-12 months:**

**Step-1:** If the email breaches 6-12 months consider alert severity as **LOW** with alert score **3**

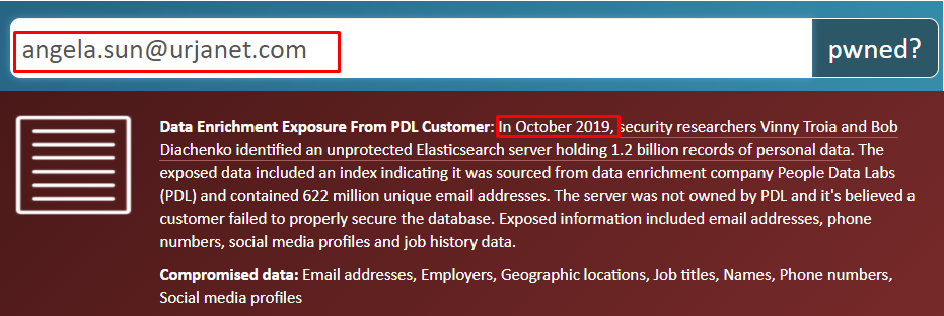


**Step-2:** If no VIP email breaches consider as **IGNORE**

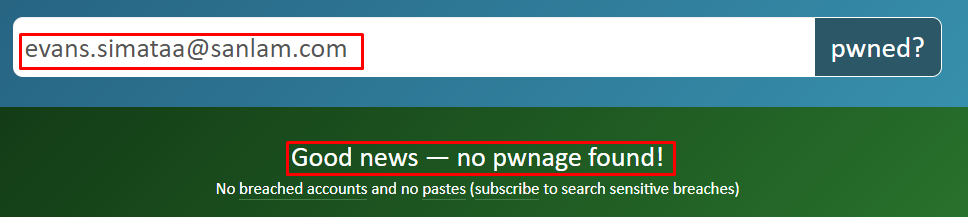


* **VIP Email ID Breach >12 Months:**

**Step-1:** If the email breaches > 12 months consider alert severity as **INFORMATIONAL** with alert score **0**



**Step-2:** If no VIP email breaches consider as **IGNORE**



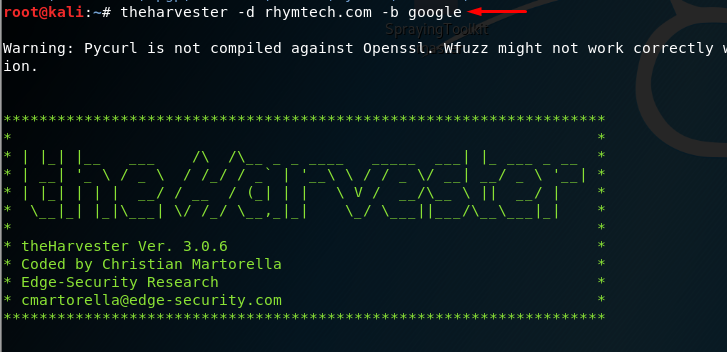
**VIP Name Defamation:**

**Manual Check**

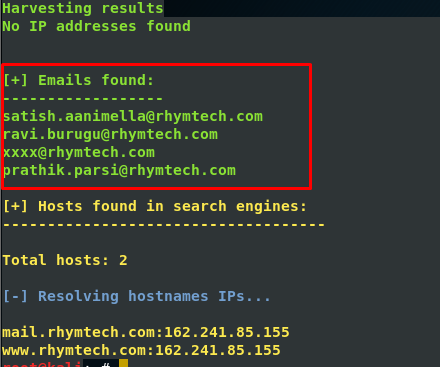
1. **Credential Leaks:**
2. **Employee login credentials detection**

Tool to check Employee Login Credential detection theharvester Kali Linux 2019 default tool

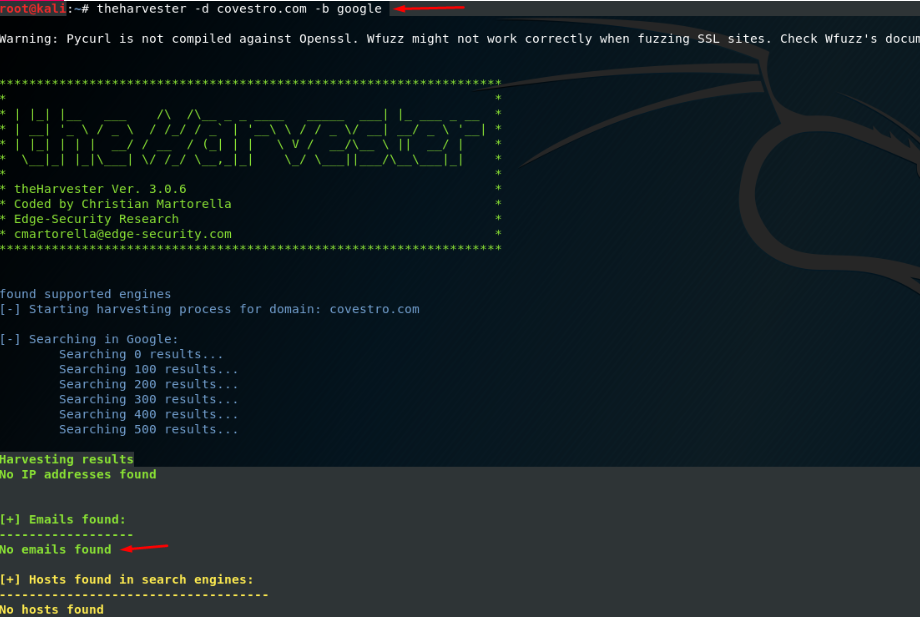
**Step 1:** Enter the domain name using the command theharvester –d domain name -b google



**Step 2:** If the output display any email ids consider alert severity as **LOW** with alert score **3**



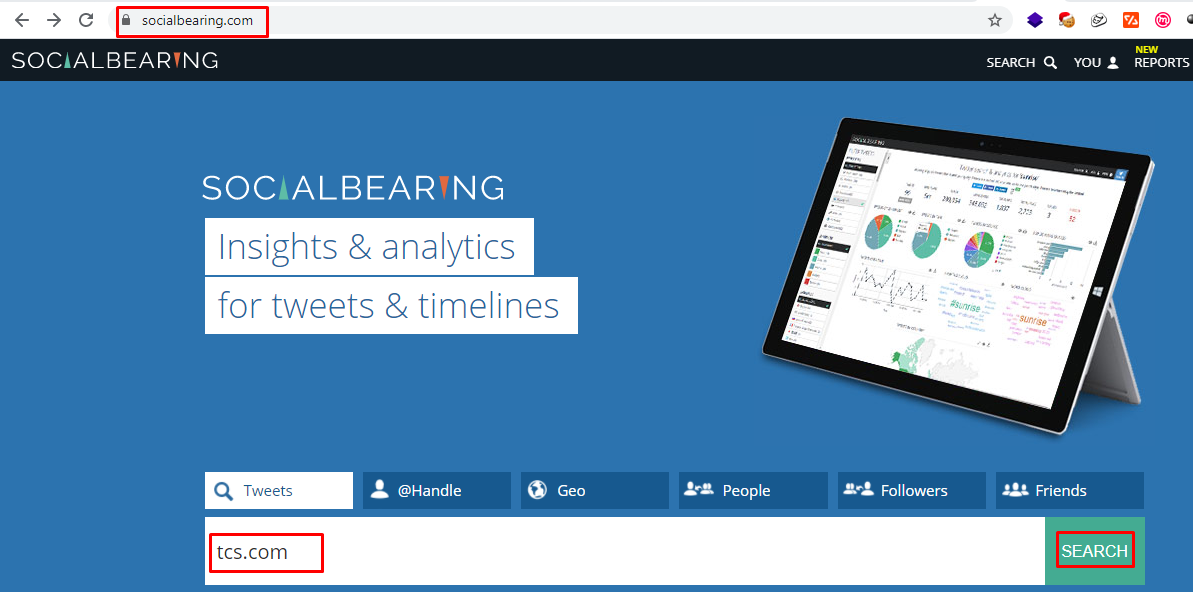
**Step-3:** If Output doesn’t sh ow any email ids consider as **IGNORE**



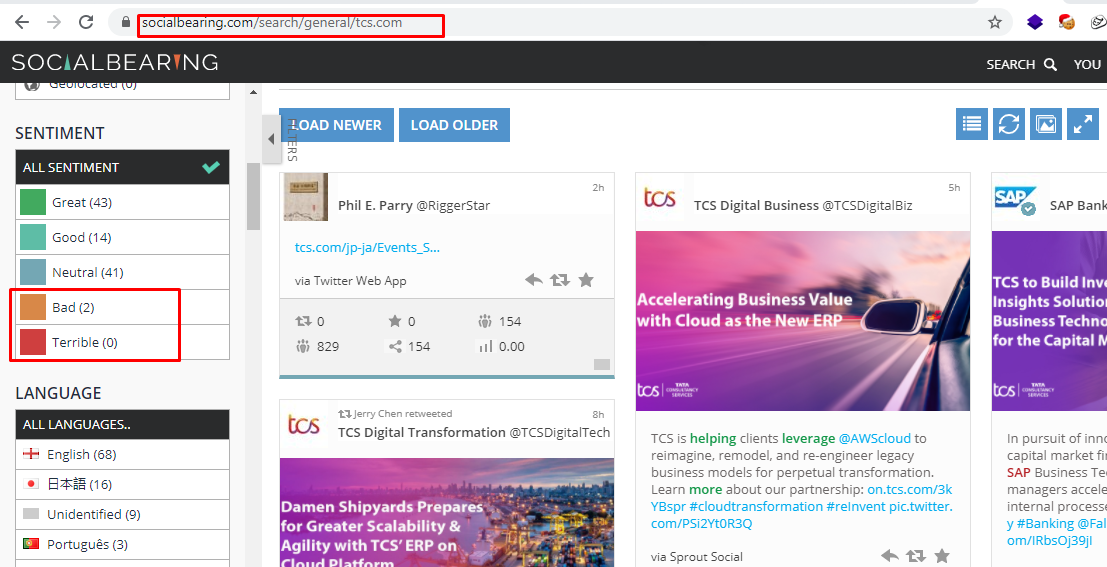
1. **Social Media Leaks**

URL to check Social Media Leaks **https://socialbearing.com/**

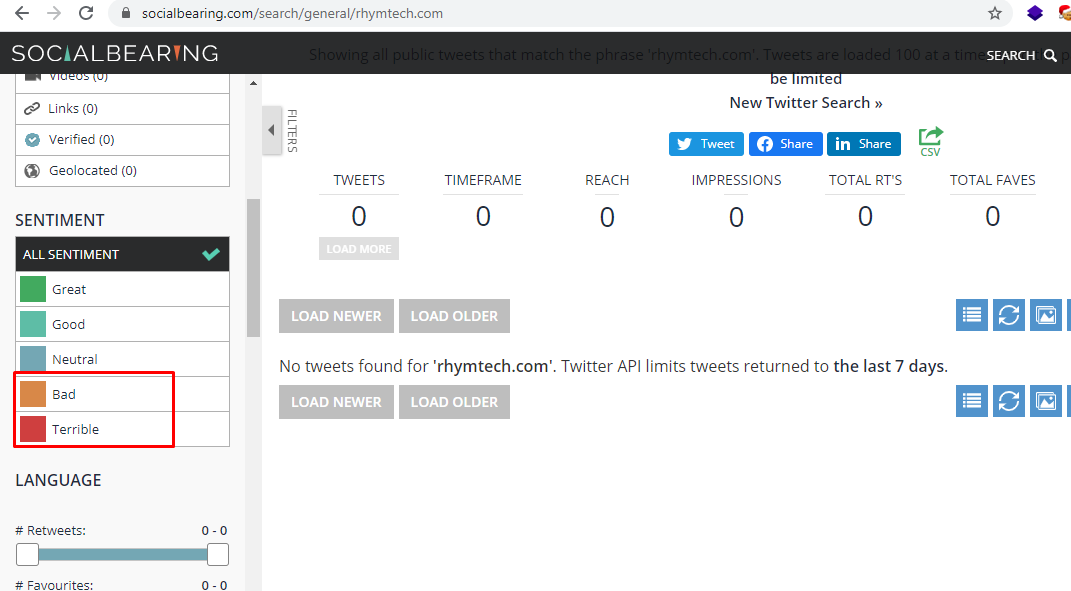
**Step 1:** Enter the Domain name in search field and click on search and consider domain name as input.



**Step 2:**In the output consider only bad and terrible sentiment .If any sensitive information disclose consider alert as **MEDIUM** with alert score **5**



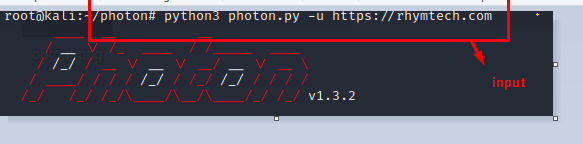
**Step-3:** If the output doesn’t show any Confidential/Sensitive Information Leaked In Social Media consider as **IGNORE**



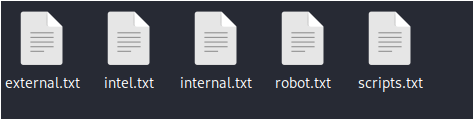
1. **Web Surface Leaks:**

Tool to check web surface leaks **https://github.com/s0md3v/photon.git**

**Step-1:** Enter the domain name using the command python3 photon.py -u domain name consider domain name as Input



**Step 3:** Afterrunning the tool it will create a .txt files within the photon folders



**Step 5:** Open the each text file and check if any sensitive information is present or not

If the output txt file contains IP Address consider alert as **INFORMATIONAL** with alert score **0**

If the output txt file does not contain IP Address consider as **IGNORE.**

If the output txt file contains Sensitive URLs consider alert as **LOW** with alert score **3**

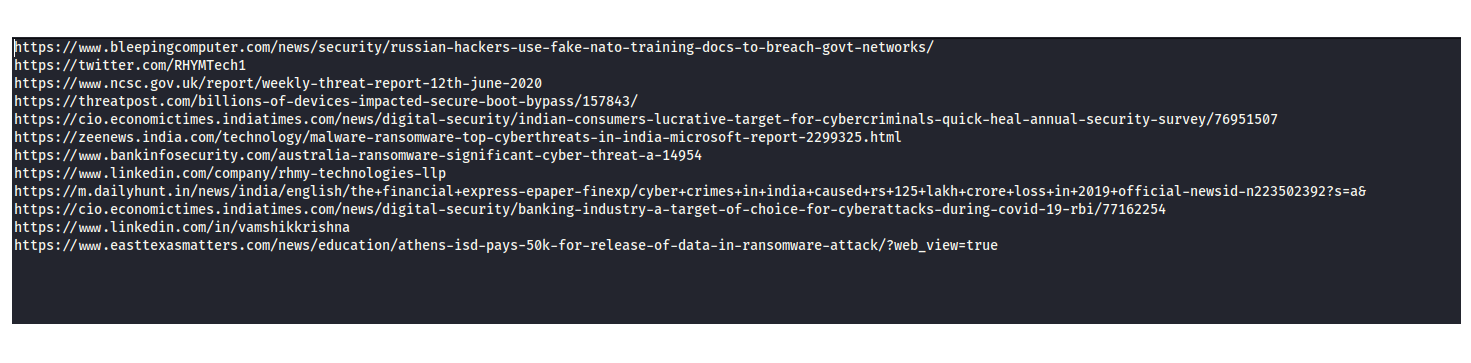
If the output txt file does not contain sensitive URLs consider as **IGNORE**

If the output txt file contains API Keys consider alert as **LOW** with alert score **3**

If the output txt file does not contain API Keys consider as **IGNORE.**

If the output txt file found Hardcoded User Names and Passwords consider alert as **HIGH** with alert score **7**

If the output txt file does not contain any Hardcoded User Names and Passwords consider as **IGNORE**

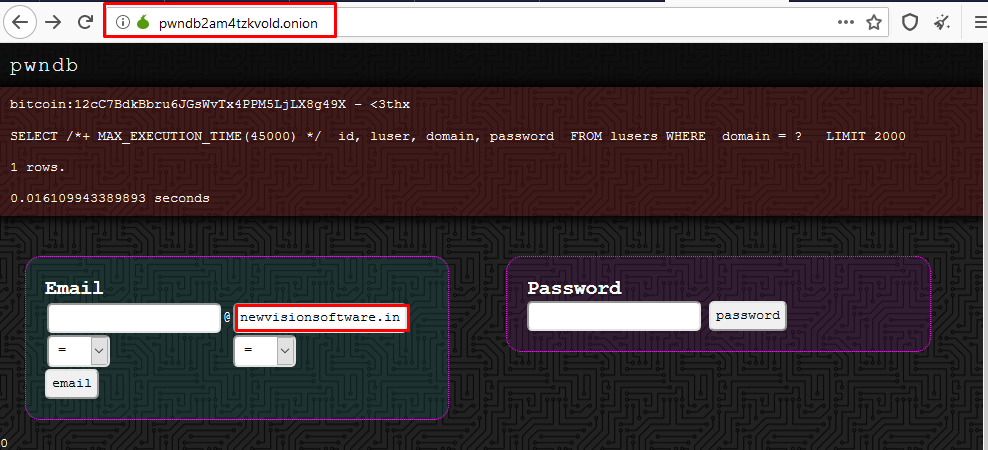


1. **Dark web Leaks:**

URL to check dark web leaks **http://pwndb2am4tzkvold.onion/**

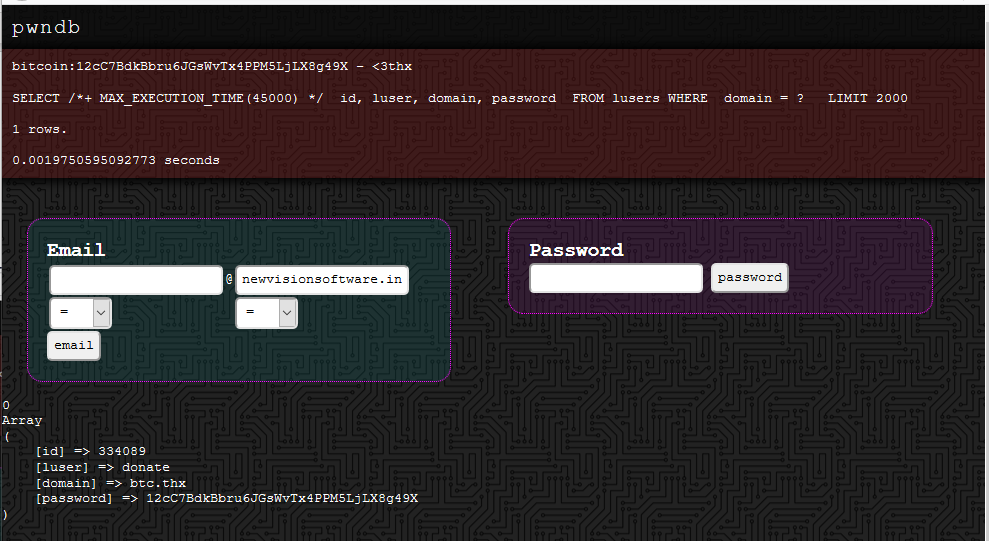
1. **Sensitive information leaks**

**Step-1:** Enter the @email extension of the testing domain and consider this as Input



**Step-2:** If the output shows any usernames and passwords in plain text consider alert severity as **HIGH** with alert score **7**

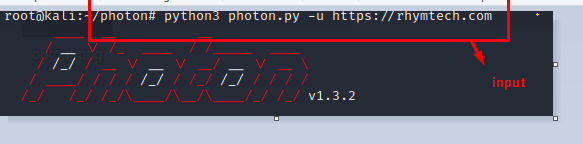
**Step-3:** Or else if the output does not show any sensitive info leaks about usernames and passwords consider as **IGNORE**



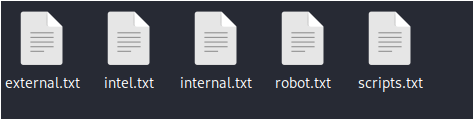
1. **Unprotected Files:**
2. **Sensitive data exposure(pdf, xlsx, csv):**

Tool to check web surface leaks **https://github.com/s0md3v/photon.git**

**Step-1:** Enter the domain name using the command python3 photon.py -u domain name consider domain name as Input

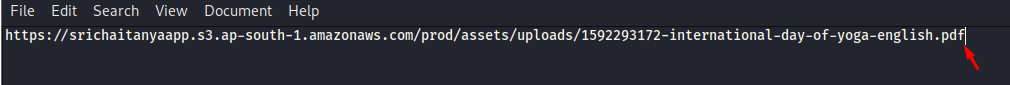


**Step 2:** Afterrunning the tool it will create a .txt files within the photon folders



**Step-3:** So we need to check each and every txt files and search for the pdf, xlsx and csv files

If sensitive Files or Information Found in that pdf, xlsx and csv files consider alert as **MEDIUM** with alert score **5**



**Step-4:** If the output doesn’t show any sensitive files consider **IGNORE**