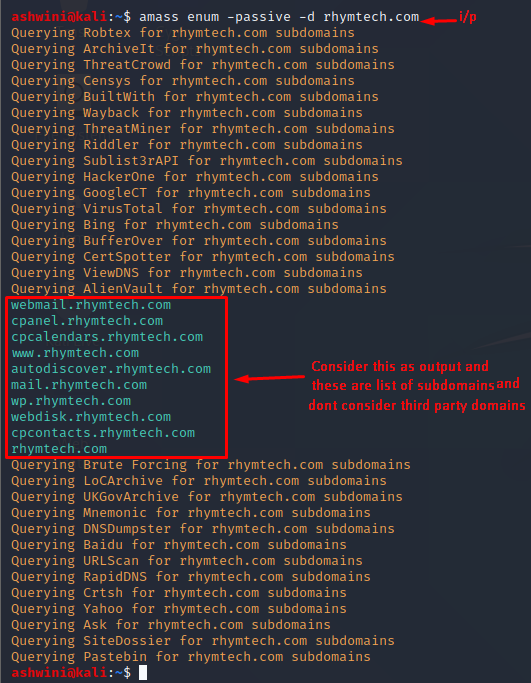
**DOMAIN STRENGTH**

1. **Sub Domain Enumeration**
2. **Check for Sub Domains**

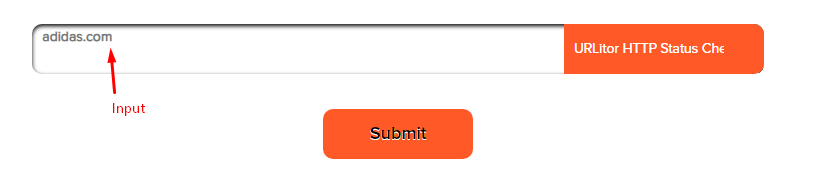
Tool to check Sub Domain EnumerationAmass: **https://github.com/OWASP/Amass.git**



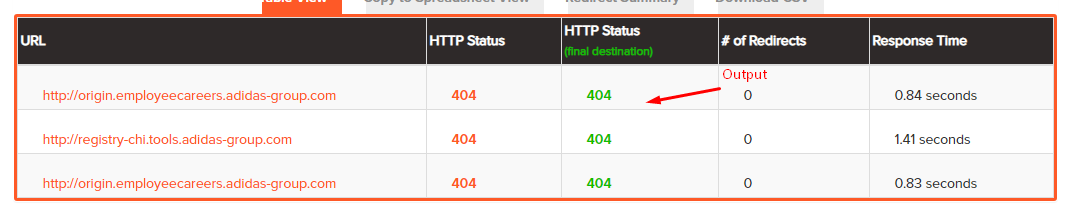
1. **Invalid Subdomains**
2. **Check http Response code**

URL to check Invalid Subdomains urlitor **http://www.urlitor.com/**

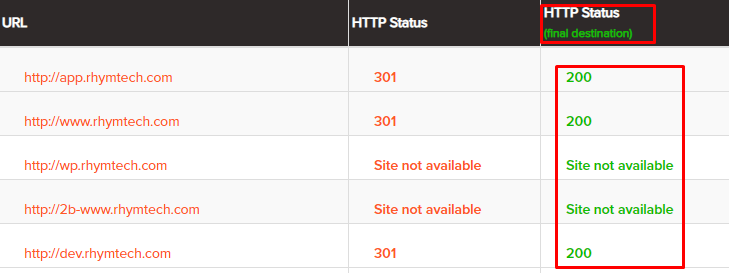
**Step-1:** Enter domain name in search field and click on URLitor HTTP Status Check and take Domain Name as Input



**Step-2:**In Output we will get the 404 status code and report it 404 status code found and alert as **LOW** with alert score 2**.**

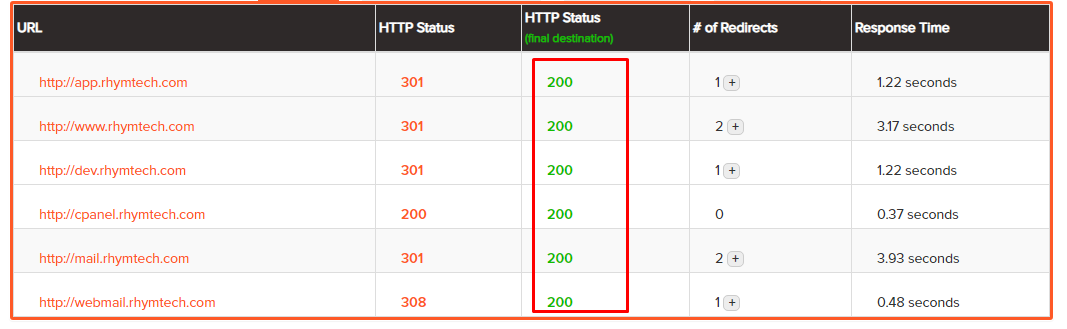


**Step-3:** Or else in output if we not find any 404 status code report it as **IGNORE.**

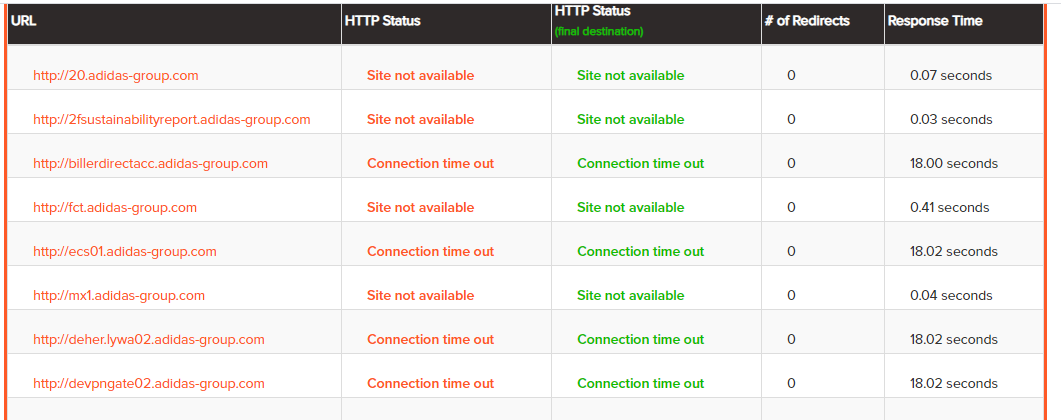


**3. Valid Subdomains:**

**Step-1:** If we found 200 status code as output report it 200 status code found and alert as **INFORMATIONAL** with alert score 0



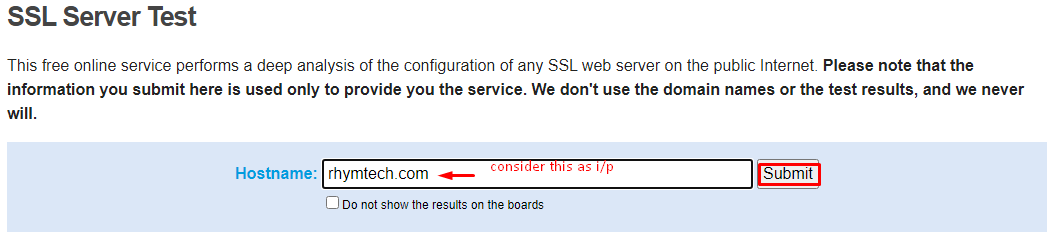
**Step2:** Or else in output if we not find any 200 status code report it as **IGNORE.**



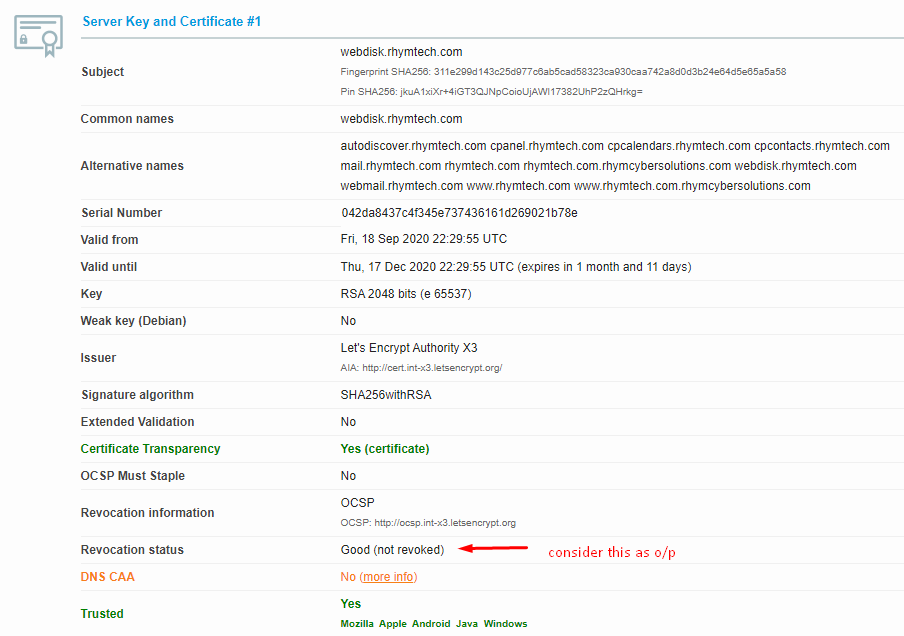
1. **SSL Status**
2. **SSL Certificate Revocation Status**

URL to check SSL Certificate Revocation Status ssllabs **https://www.ssllabs.com/ssltest//index.html**

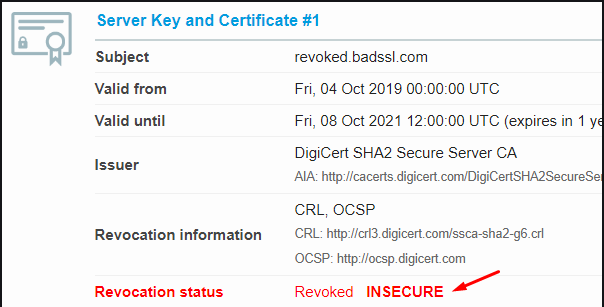
**Step-1:** Enter the domain name in search field and click on submit and consider Domain Name as Input.



**Step-2:**The output will be displayed as Revocation status is good and report it SSL revocation status good and alert as **INFORMATIONAL** with an alert score **0.**



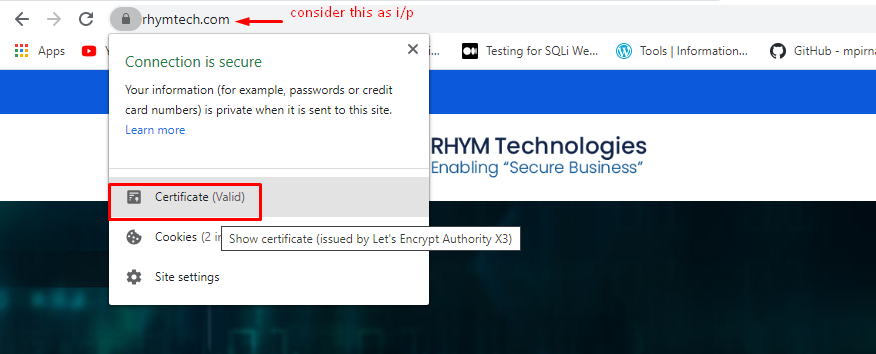
**Step-3:** Also if the Revocation status is bad Consider alert as **INFORMATIONAL** with alert score **0** even



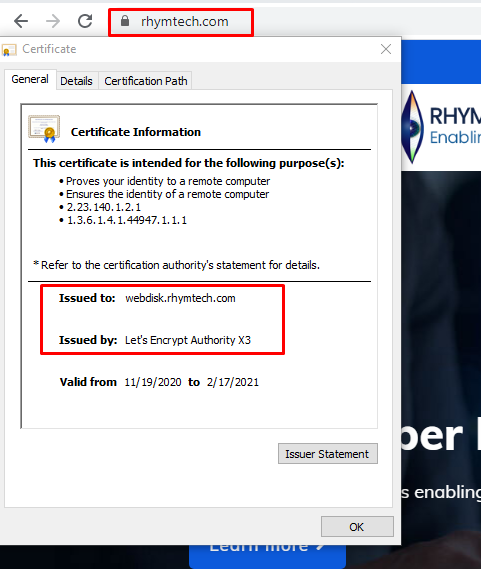
1. **SSL certificate is self-signed:**

**Manual check:**

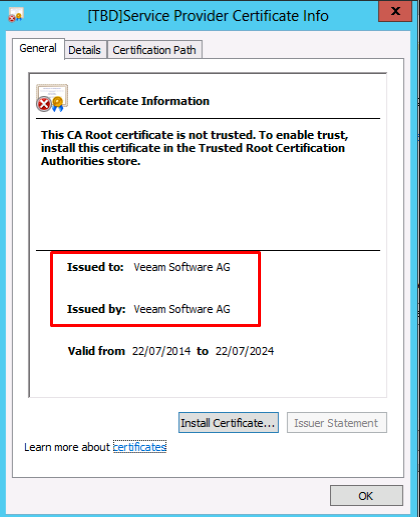
**Step-1:** Enter the URL and click on the lock symbol and consider that URL as Input.



**Step-2**: If the output issued to and issued by is not same alert as **IGNORE**

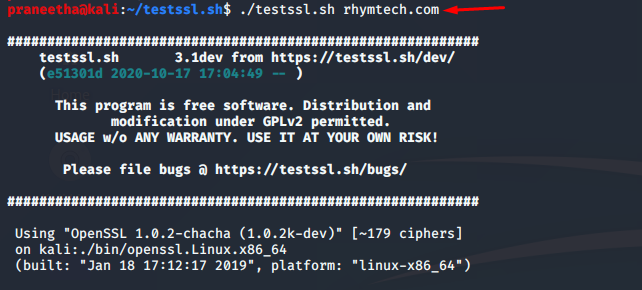


**Step-3:** If the output issued to and issued by is same consider alert as **HIGH** with alert score **7**

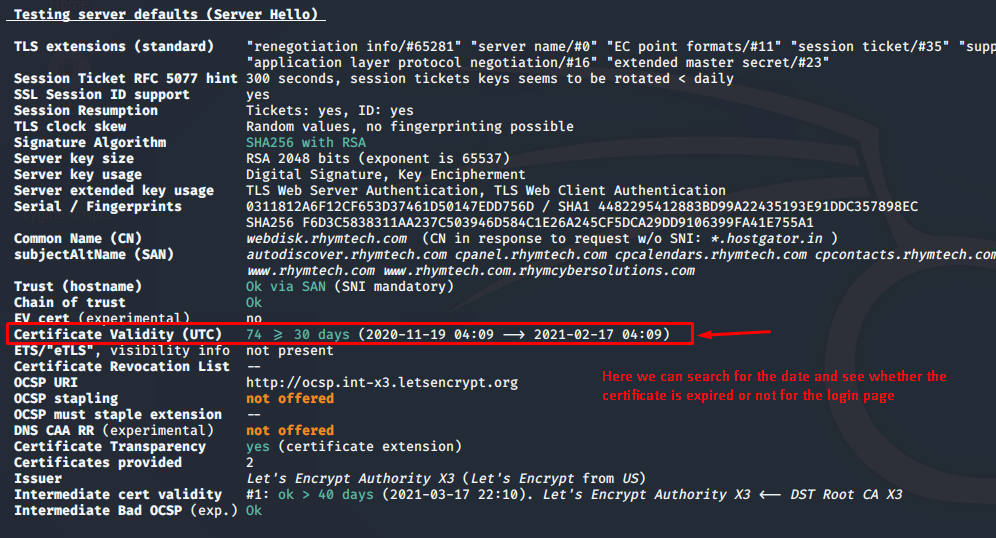


1. **Expired SSL certificate on login page**

**Step-1:** Enter the domain name which is having Login Page using command ./testssl.sh domain name and consider that domain name as Input



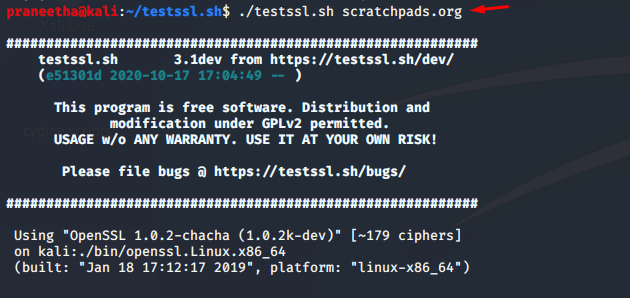
**Step-2:** If the Output shows Expired SSL certificate on Login Page Consider alert as **CRITICAL** with alert severity score **9.8**



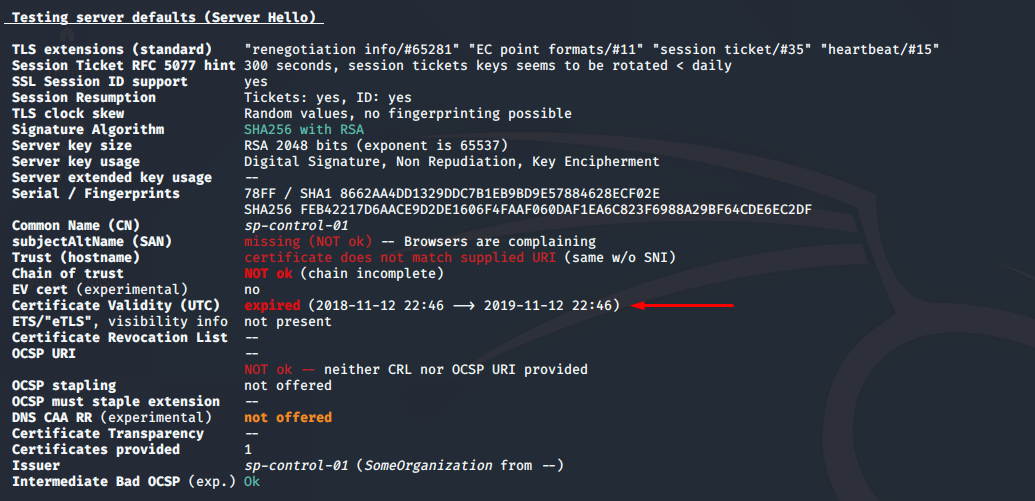
**Step-3:** If the output shows Expired SSL Certificate on Login Page Not Found consider as **IGNORE.**

1. **Expired SSL certificate without Login page:**

**Step-1:** Enter the domain name which is Not Having Login Page using command ./testssl.sh domain name and consider that domain name as Input



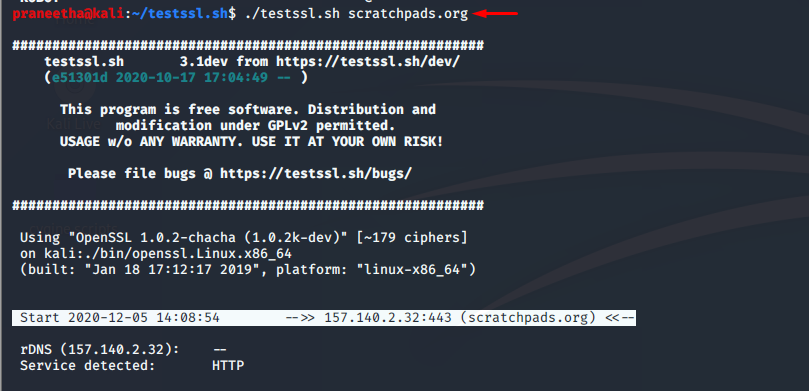
**Step-2:** If the Output shows Expired SSL certificate on without Login Page Consider alert as **MEDIUM** with alert severity score **5.3.**



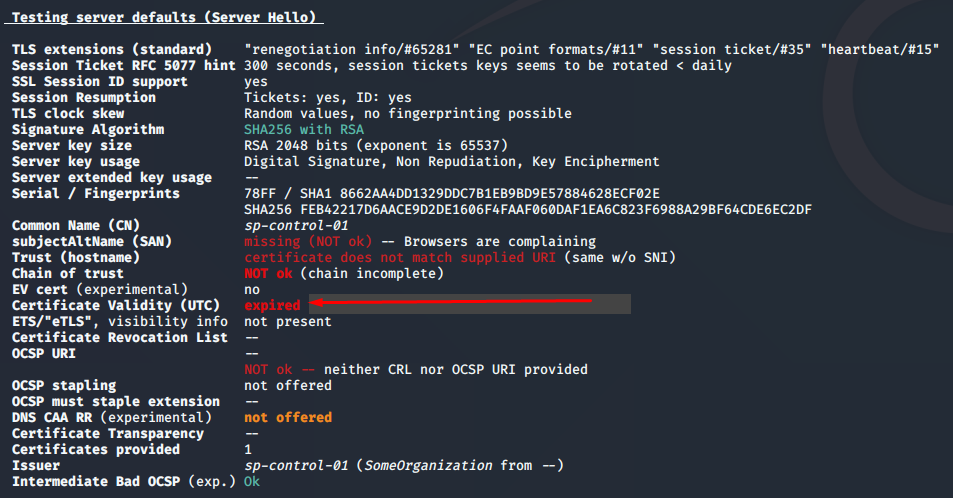
**Step-3:** If the output shows Expired SSL Certificate on Without Login Page Not Found consider as **IGNORE.**

1. **Lack Of SSL certificate on Login page:**

**Step-1:** Enter the Domain Name which is lack of ssl with a Login Page using command. /testssl.sh domain name consider this domain name as Input



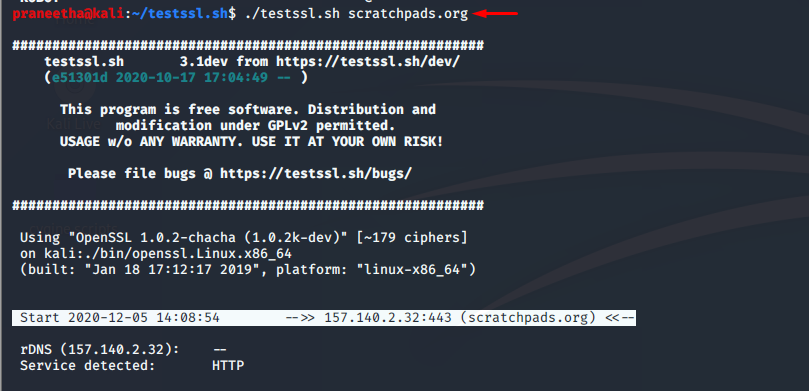
**Step-2:** If the output shows expired SSL certificate Consider alert as **CRITICAL** with alert severity score **9.8**



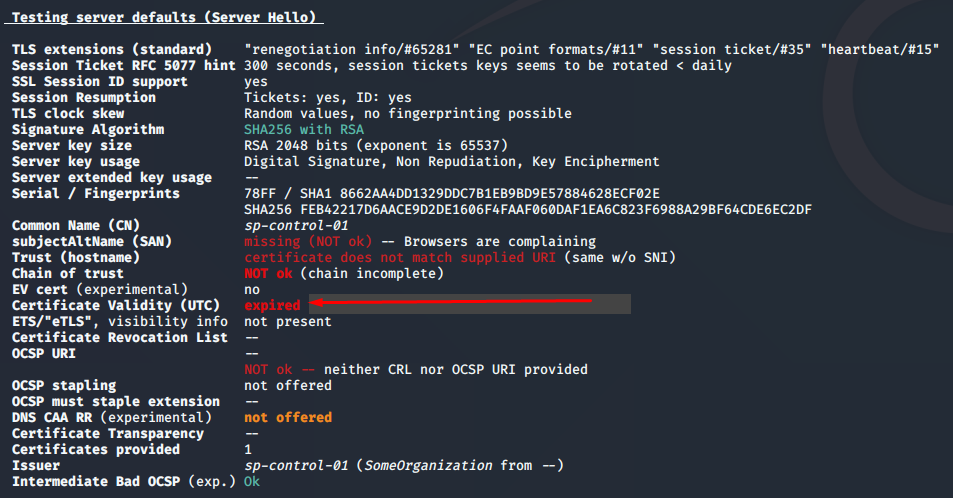
**Step-3:** Or Else Expired SSL Certificate on Login Page not found Consider as **IGNORE.**

1. **Lack of SSL Certificate without Login Page:**

**Step-1:** Enter the Domain Name which is lack of ssl without a Login Page using command. /testssl.sh domain name consider this domain name as Input



**Step-2:** If the output shows Lack of SSL certificate Without Login Page Found Consider alert as **MEDIUM** with alert severity score **5.3.**

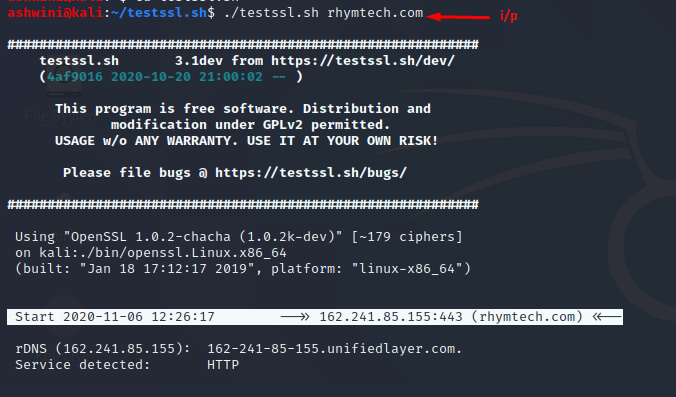


**Step-3:** Or Else Expired SSL Certificate on Without Login Page not found Consider as **IGNORE**

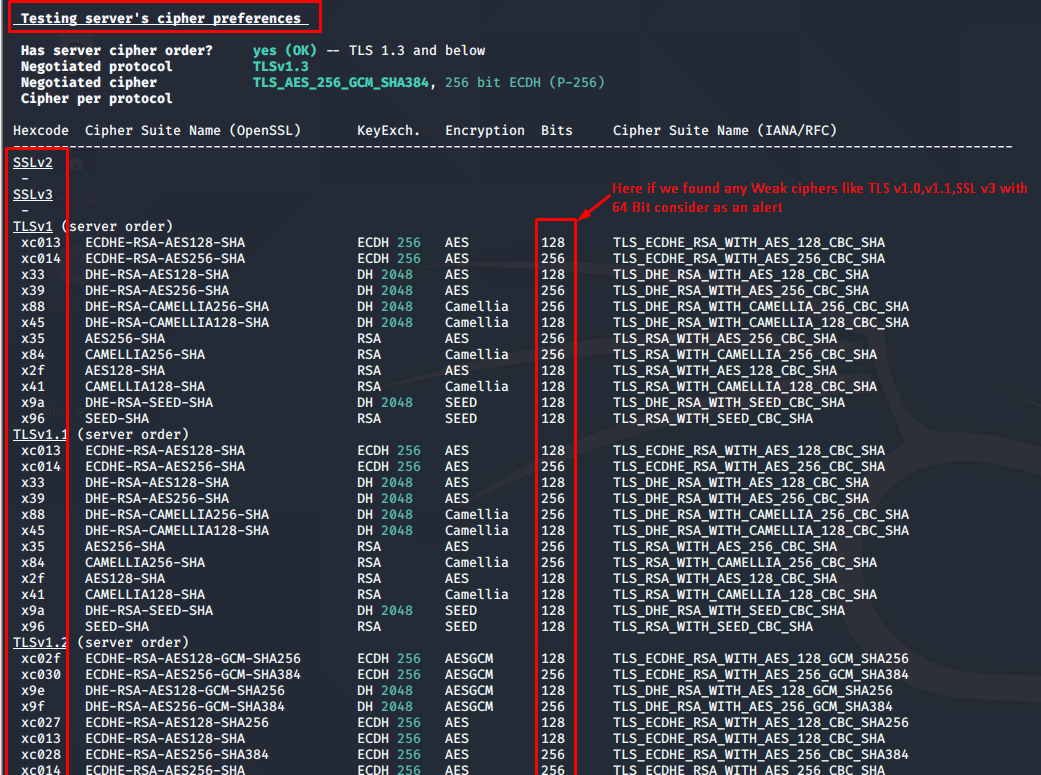
1. **Weak Ciphers**

Tool to check weak Ciphers **https://github.com/drwetter/testssl.sh.git**

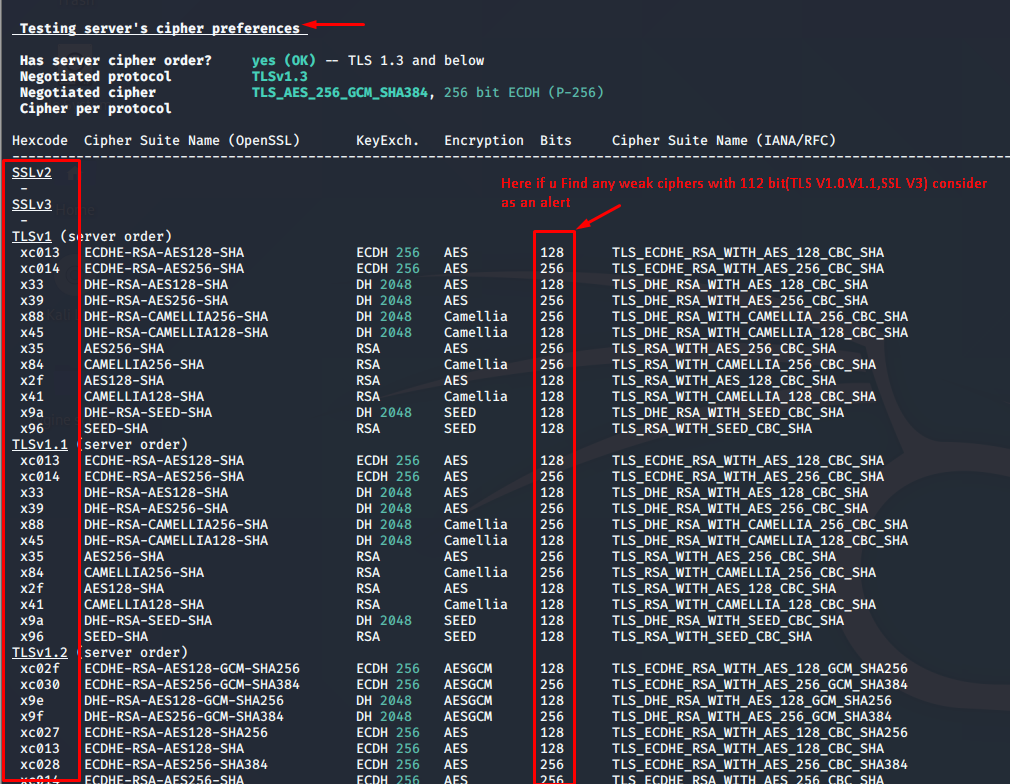
**Step-1:** Enter the domain name using command. /testssl.sh domain name consider this domain name as Input.



**Step-2:** If the Domain contains weak ciphers with 64 bit (TLS V1.0.V1.1, SSL V3) consider alert as **MEDIUM** with alert severity score **6.5**

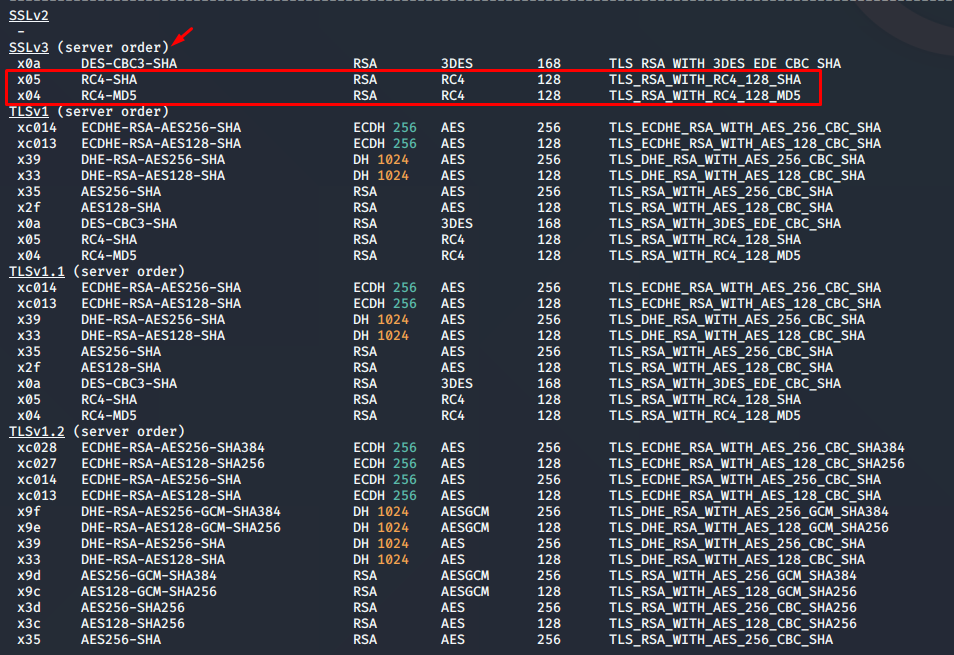


**Step-3:** If the Domain contains weak ciphers with 112 bit (SSL V3, T LS V1.0.V1.1,) consider alert as **MEDIUM** with alert severity score **4.3**



**Step-4:** If the Domain contains weak cipher with 128 bit (SSL V3, T LS V1.0.V1.1,) consider

Alert as **MEDIUM** with alert severity score **4.3**

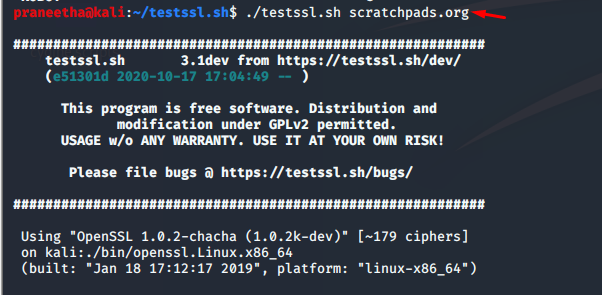


**Step-5:** Above Mentioned Weak Ciphers Not Found consider as **IGNORE**

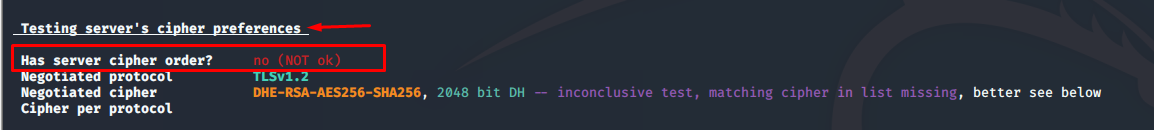
1. **Cipher Order:**

Tool to check Cipher Order testssl **https://github.com/drwetter/testssl.sh.git**

**Step-1:** Enter the Domain name using command ./testssl.sh domain name consider domain name as Input



**Step-2:** If the Output shows cipher order is not ok consider alert severity as **LOW** with alert score 2.

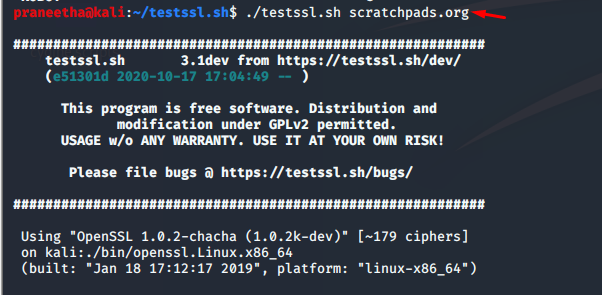


**Step-3:** Or else if the output shows cipher order is ok consider alert severity as **INFORMATIONAL** with alert score **0**

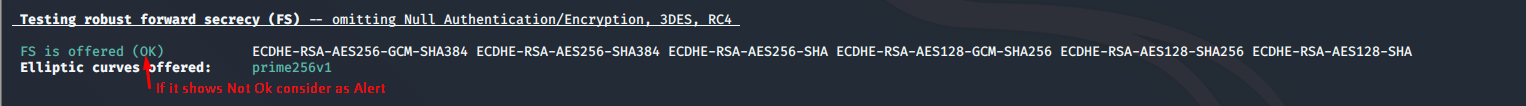
1. **Perfect Forward Secracy:**

Tool to check Perfect Forward Secracy testssl **https://github.com/drwetter/testssl.sh.git**

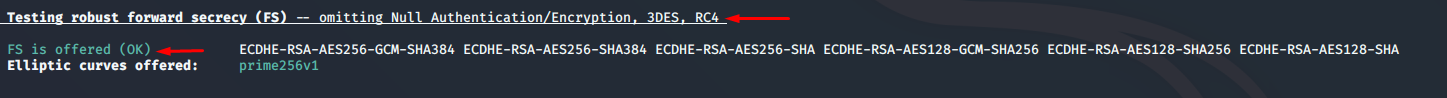
**Step-1:** Enter the Domain name using command ./testssl.sh domain name consider domain name as Input



**Step-2:** If the Output shows Perfect forward secracy Not Offered consider alert as **MEDIUM** with alert score **6.5**



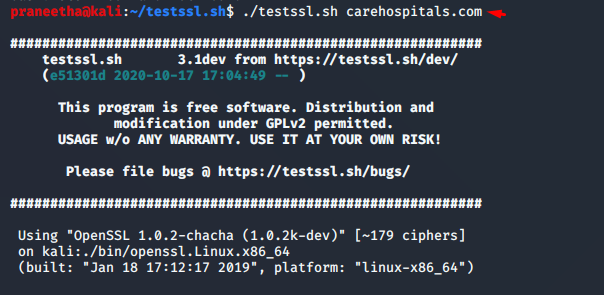
**Step-3:**Or else if the output shows Perfect forward secracy Offered OK consider alert as **INFORMATIONAL** with alert score **0**



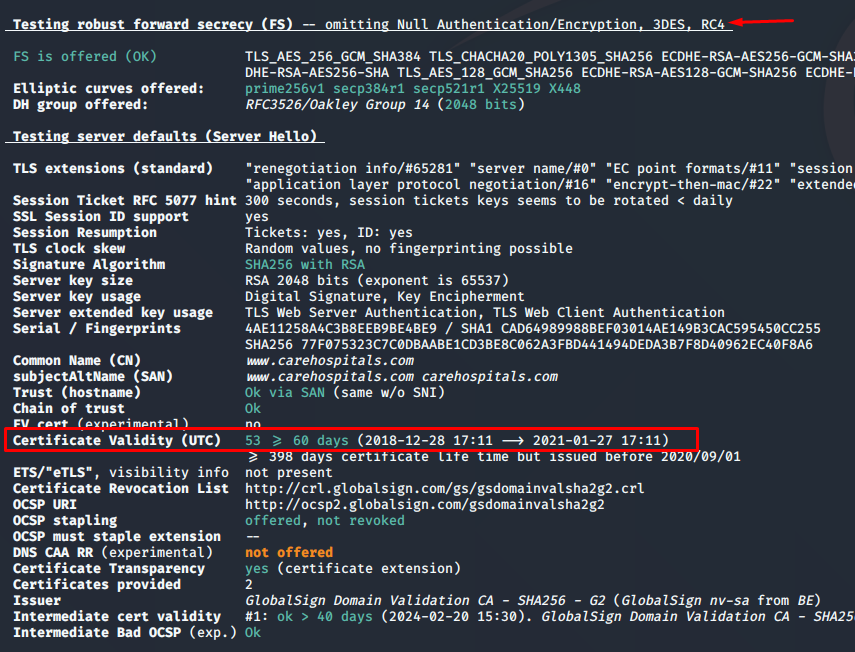
1. **SSL certificate expiration is longer than best practices**

Tool to check Perfect SSL certificate expiration is longer than best practices testssl **https://github.com/drwetter/testssl.sh.git**

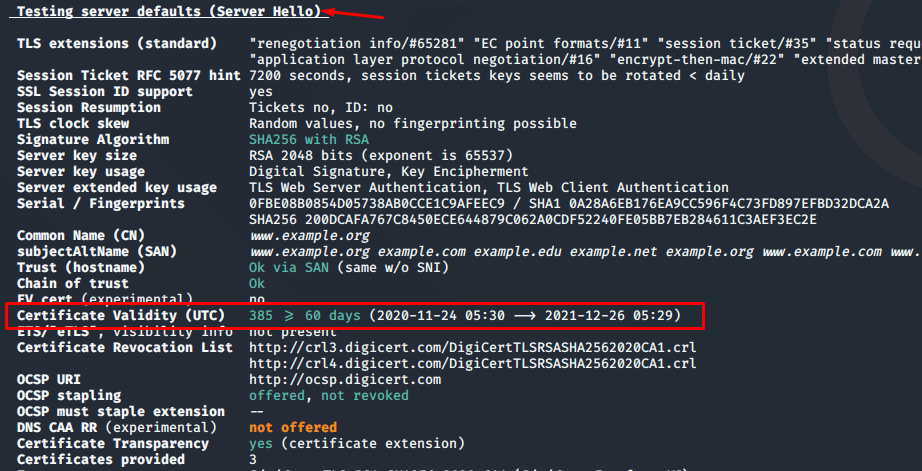
**Step-1:** Enter the Domain name using command ./testssl.sh domain name consider domain name as Input



**Step-2:** If the Output shows certificate validity(UTC) less than 60 days consider alert severity **LOW** with alert score **2**



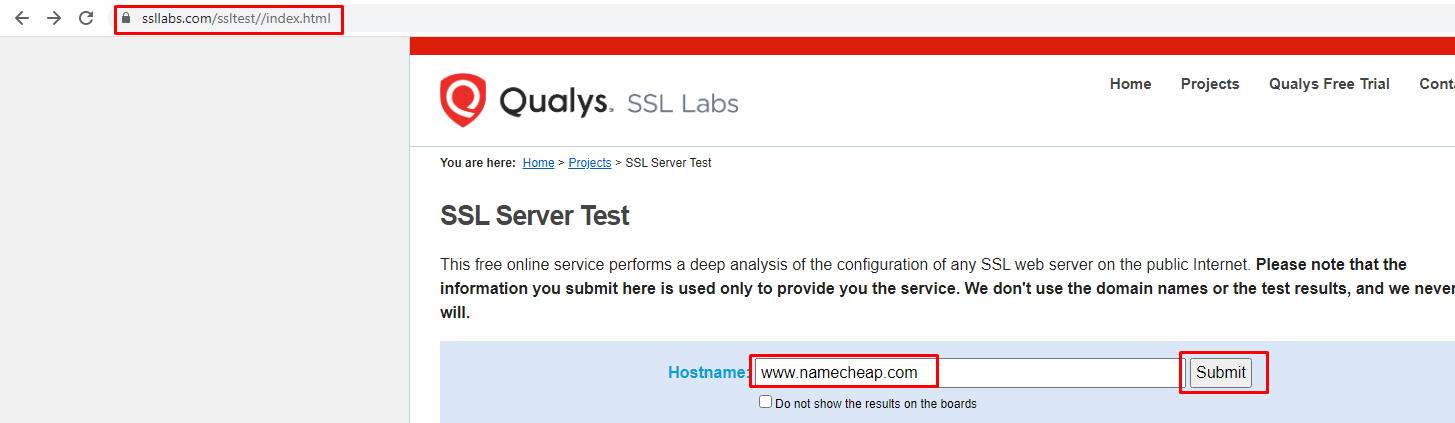
**Step-3:** If the Output shows certificate validity (UTC) greater than 60 days consider as **IGNORE**



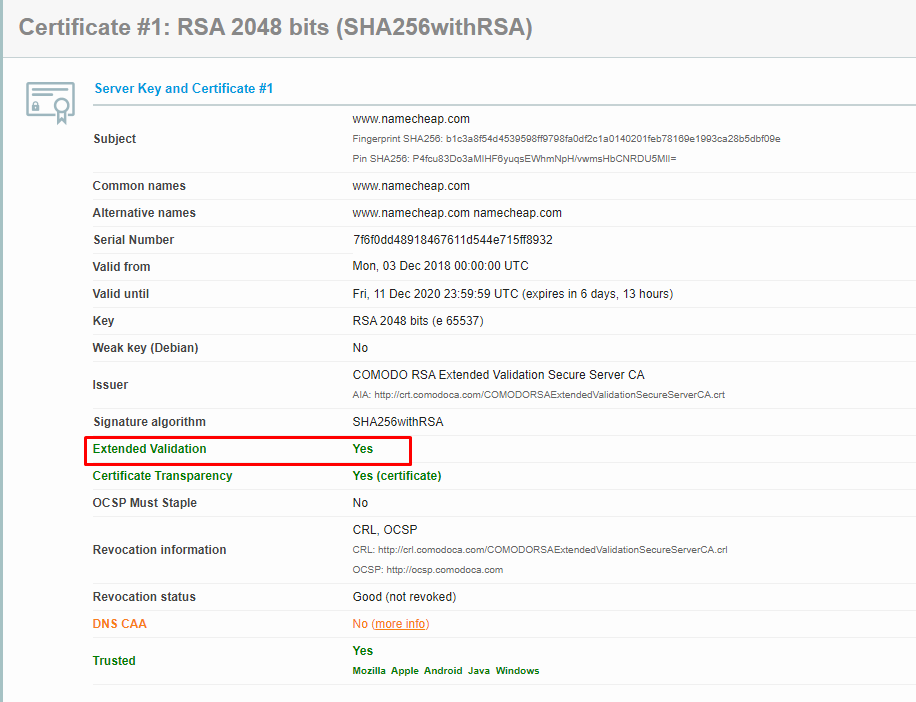
1. **Extended validation certificate detected**

URL to check extended validation certificate **https://www.ssllabs.com/ssltest//index.html**

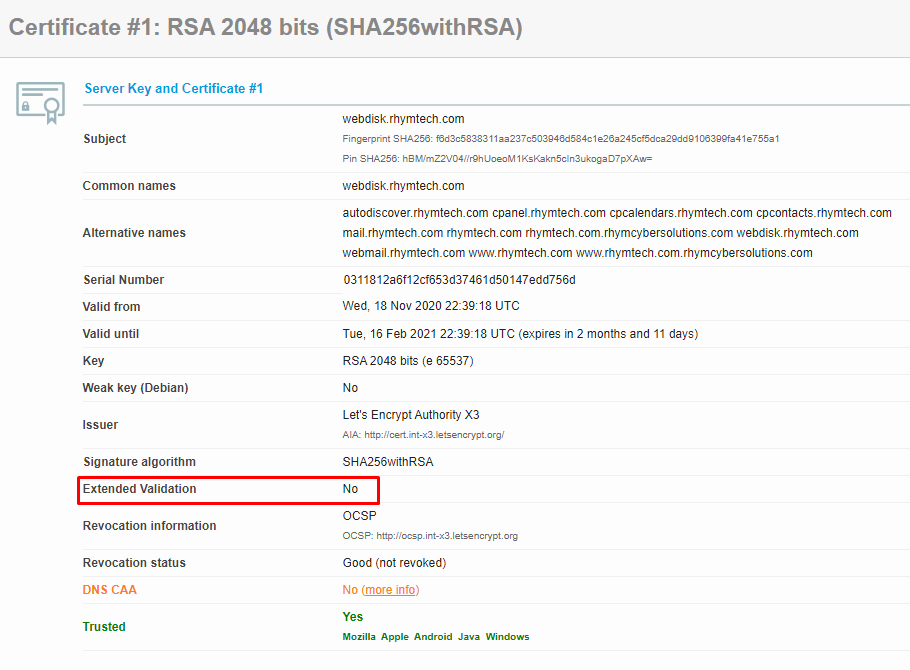
**Step-1:** Enter the domain name in the search field and click on submit and consider the domain name as input



**Step-2:** If the output shows Extended validation Yes consider alert severity as **INFORMATIONAL** with alert Score **0**



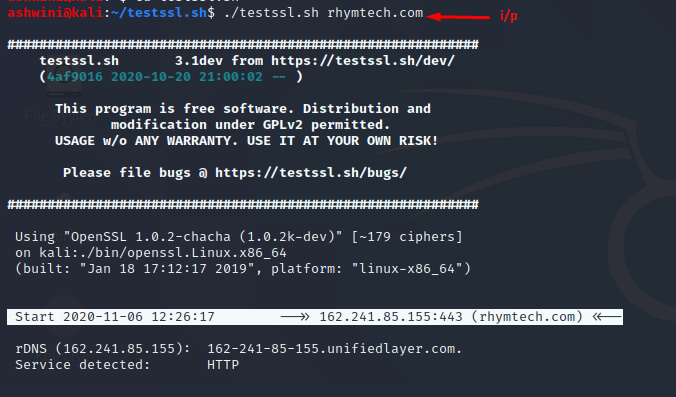
**Step-3:** If the output shows Extended validation No consider alert severity as **INFORMATIONAL** with alert Score **0**



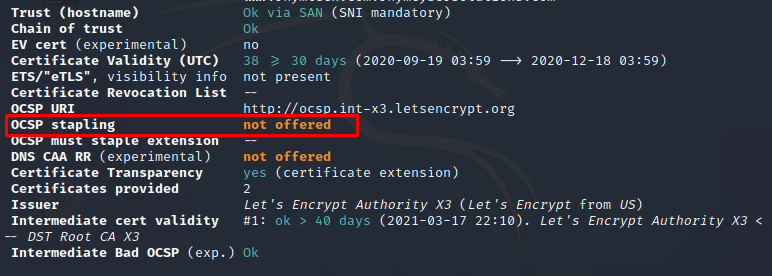
1. **TLS certificate status request(OCSP stapling) detected:**

Tool to check OCSP Stapling testssl https://github.com/drwetter/testssl.sh.git

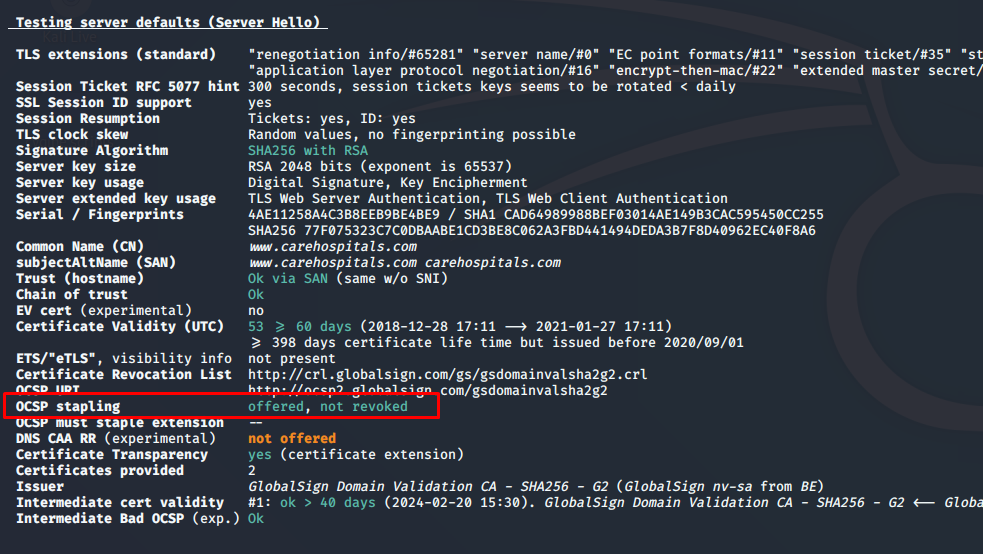
**Step-1:** Enter the Domain name using command ./testssl.sh domain name consider domain name as Input



**Step-2:** If the Output shows OCSP Stapling not offered consider alert as **MEDIUM** with alert score **5**



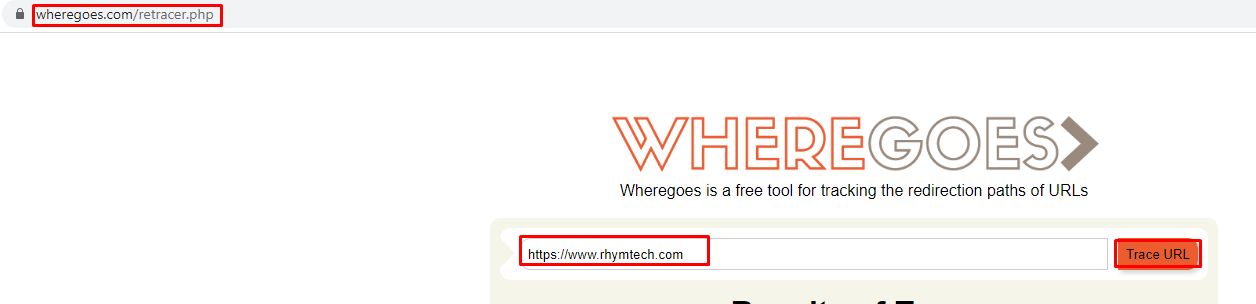
**Step-3** Or Else if the output shows OCSP Stapling offered consider alert as **INFORMATIONAL** with alert sore **0.**



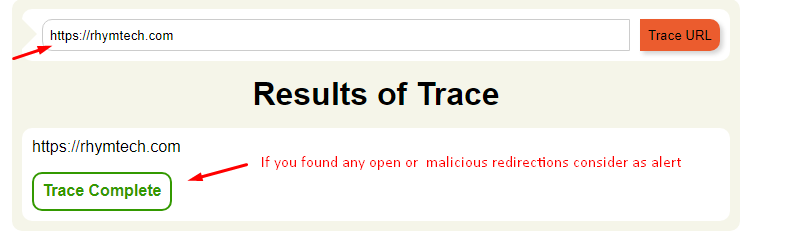
1. **Redirection:**

URL to check Redirections **https://wheregoes.com/retracer.php**

**Step-1:** Enter the URL in search field and click on Trace URL consider domain name as Input



**Step-2:** If the output shows any redirections like open redirections and Malicious Redirections consider alert as **MEDIUM** with alert score **6.1**



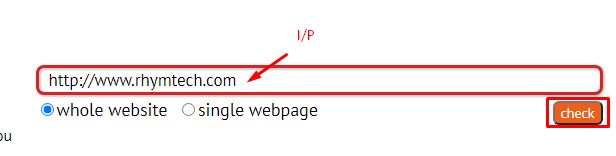
**Step-3:** If the output doesn’t show s any redirections consider as **IGNORE**

1. **Broken links:**

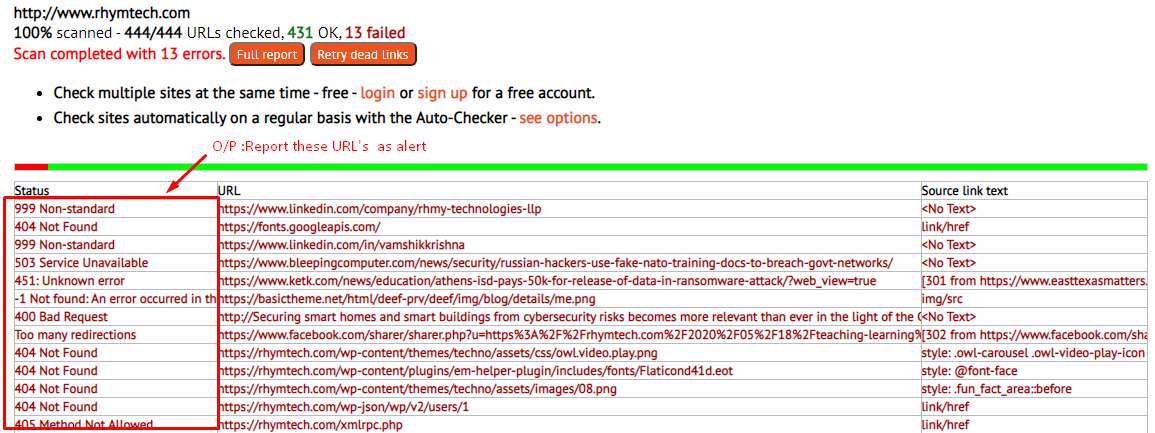
1. **Broken Link Inspection:**

URL to check Broken Link Inspection Deadlink checker **https://www.deadlinkchecker.com**

**Step-1**: Enter the domain name in search field and click on the check consider domain name as Input



**Step-2:** If the Output Shows Brokenlinks consider alert severity as **LOW** with alert score **2.**

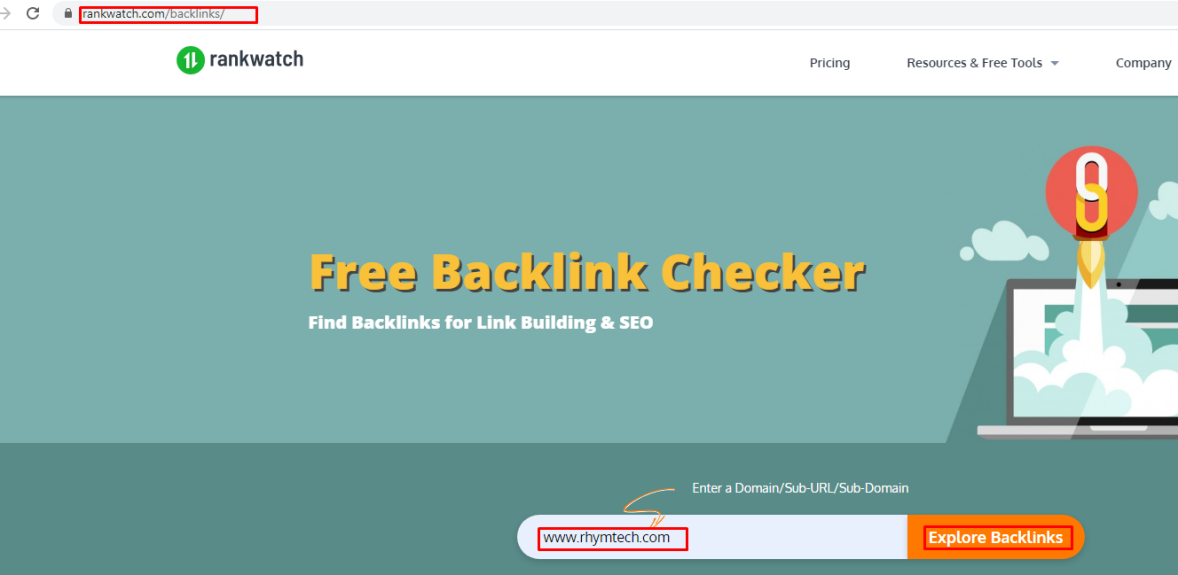


**Step-3:** If the Output doesn’t shows any broken links consider alert severity **INFORMATIONAL** With alert score **0**.

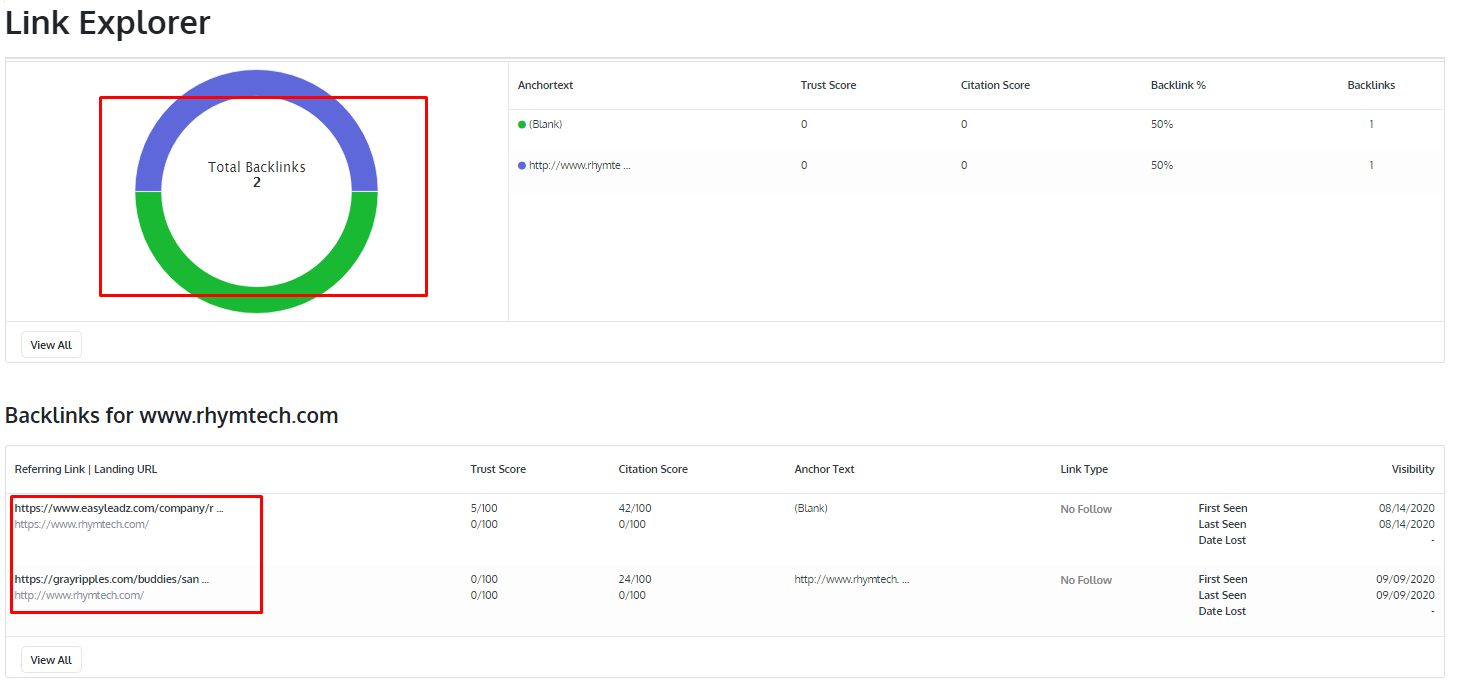
1. **Backlinks:**
2. **External Site Link:**

URL to check External Site Link Rankwatch https://www.rankwatch.com/backlinks/

**Step-1:** Enter the domain name in search field and click on the explore Backlinks consider domain name as Input



**Step-2:** If the Output shows Less Backlinks consider alert severity as **INFORMATIONAL** with alert Score **0**



**Step-3:** If the Output shows More Backlinks consider alert severity **INFORMATIONAL** with alert Score **0**

