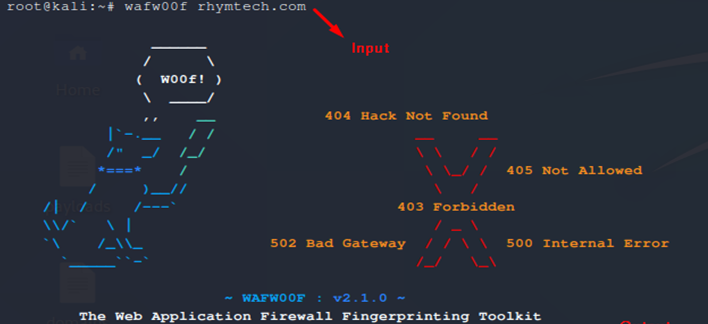
**APPLICATION SECURITY**

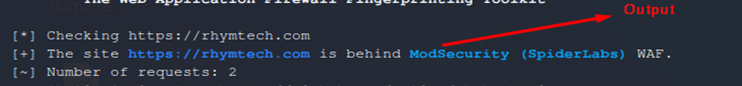
1. **Web application Firewall detection:**

Tool to check web application Firewall **Wafw00f** default Kali Linux Tool

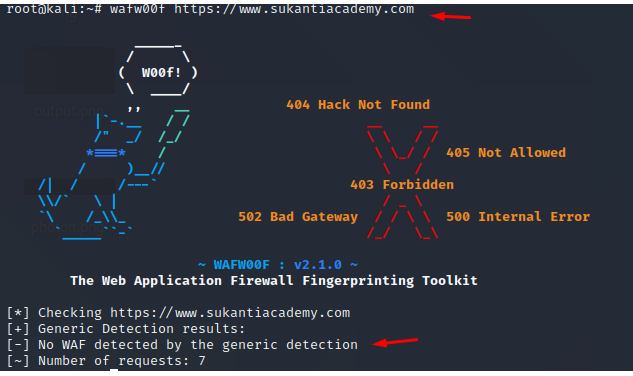
**Step-1:** Enter the domain name using command wafw00f consider domain name as Input



**Step-2:** If the output shows the site is behind the firewall Consider alert severity **MEDIUM** and with alert score **6**



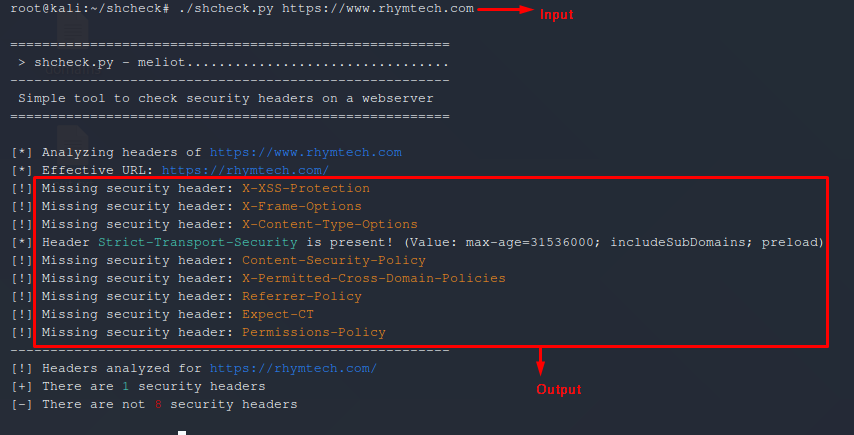
**Step-3:** If the output shows No WAF detected alert severity **INFORMATIONAL** and with alert score **0**



1. **Missing security headers:**

Tool to check missing security headers shcheck **https://github.com/meliot/shcheck.git**

**Step-1:** Enter the domain name by using the ./shcheck.py domain name and consider domain name as input



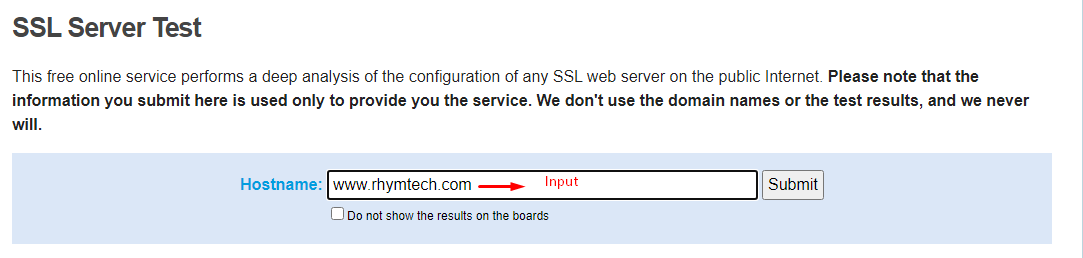
**Step-2:** If headers are not found:

* If HTTP Strict Transport Security Header is missing consider alert severity as **MEDIUM** and with alert score **5.3**
* If HTTP Strict Transport Security Header is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**
* If X-Frame-Options Header is missing consider alert severity as **MEDIUM** and with alert score **6.5**
* If X-Frame-Options Header is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**
* If X-Content-Type-Options Header is missing Consider alert severity as **MEDIUM** and with alert score **6.1**
* If X-Content-Type-Options Header is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**
* If Content-Security-Policy Header is missing Consider alert severity as **MEDIUM** and with alert score **6.5**
* If Content-Security-Policy Header is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**
* If Referrer-Policy Header is missing Consider alert severity as **MEDIUM** and with alert score **6.1**
* If X-Permitted-Cross-Domain-Policies Header is missing Consider alert severity as **LOW** and with alert score **3**
* If X-Permitted-Cross-Domain-Policies is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**
* If Feature-Policy Header is missing Consider alert severity as **LOW** and with alert score **3**
* If Feature-Policy Header is enabled Consider alert severity as **INFORMATIONAL** and with alert score **0**
* If Expect-CT Header is missing Consider alert severity as **LOW** and with alert score **3**
* If Expect-CT Header is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**
* If X-XSS-ProtectionHeader is missing Consider alert severity as **MEDIUM** and with alert score **6.1**
* If X-XSS-ProtectionHeader is enabled consider alert severity as **INFORMATIONAL** and with alert score **0**

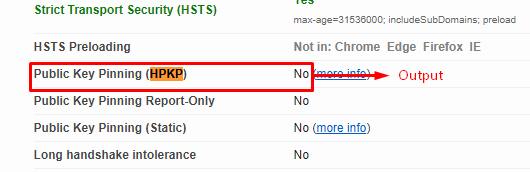
**Public Key Pinning Extension for HTTP (HPKP)**

Tool to check HPKP: **https://www.ssllabs.com/ssltest//index.html**

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

****

**Step-2:** If the output shows Public Key Pinning Extension for HTTP (HPKP) is missing Consider alert severity as **MEDIUM** and with alert score **4.3**

****

**Step-3:** If the output shows Public Key Pinning Extension for HTTP (HPKP) is Yes Consider alert severity as **INFORMATIONAL** with alert score **0**

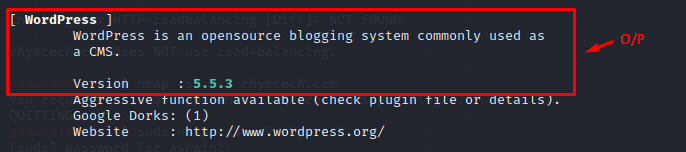
1. **CMS Security:**
2. **CMS version detection:**

Tool to check CMS Version whatweb **https://github.com/urbanadventurer/WhatWeb.git**

**Step-1:** Enter the domain name using command. /whatweb –v rhymtech.com consider domain name as input



**Step-2:** If the output shows CMS wordpress versionConsider alert severity as **INFORMATIONAL** and with alert score **0**



**Step-3:** If CMS version not found **IGNORE**

1. **CMS vulnerabilities:**

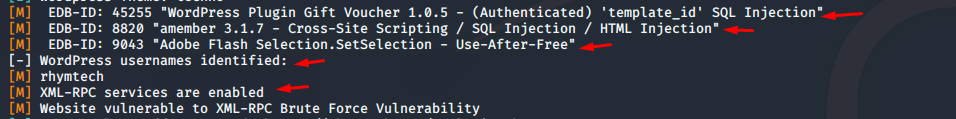
Tool to check CMS Vulnerabilities **https://github.com/Dionach/CMSmap**

**Step-1:** Enter the domain name using command ./cmsmap.py domain name consider domain name as input



**Step-2:** Consider the Wordpress Vulnerabilities

If the output shows wordpress vulnerabilities like xmlrpc wordpress username etc., consider alert as **MEDIUM** with alert score **6.1.**



If the output doesn’t show any wordpress vulnerabilities consider as **IGNORE.**

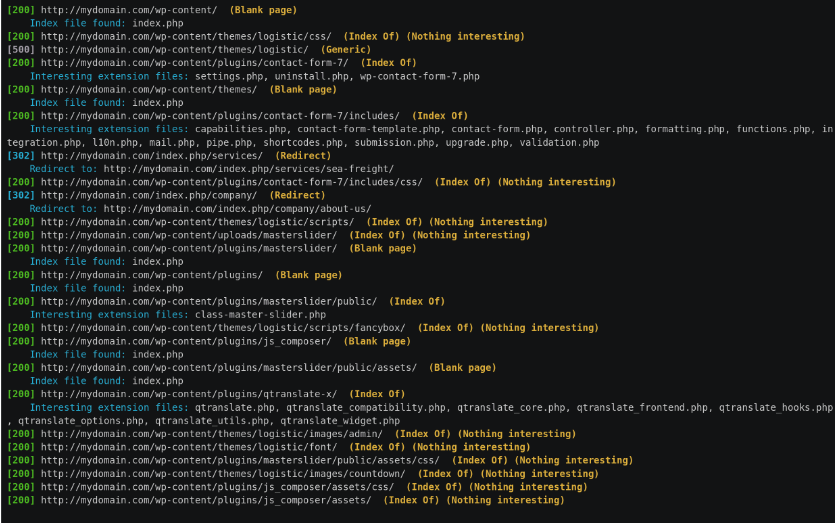
1. **Directory listing**
2. **Directory Listing:**

Tool to check directory listingdirhunt **https://github.com/Nekmo/dirhunt**

**Step-1:** Enter the domain name using the command dirhunt domain nameconsider domain name as Input



**Step-2:** The Output will give some url open each url and find for the directories if directories found consideralert severity as **MEDIUM** and with alert score **5**

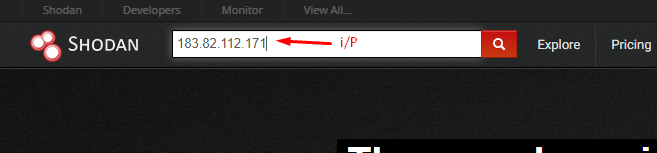


**Step-3:** If the output shows No directory after opening each URL Consider as **IGNORE.**

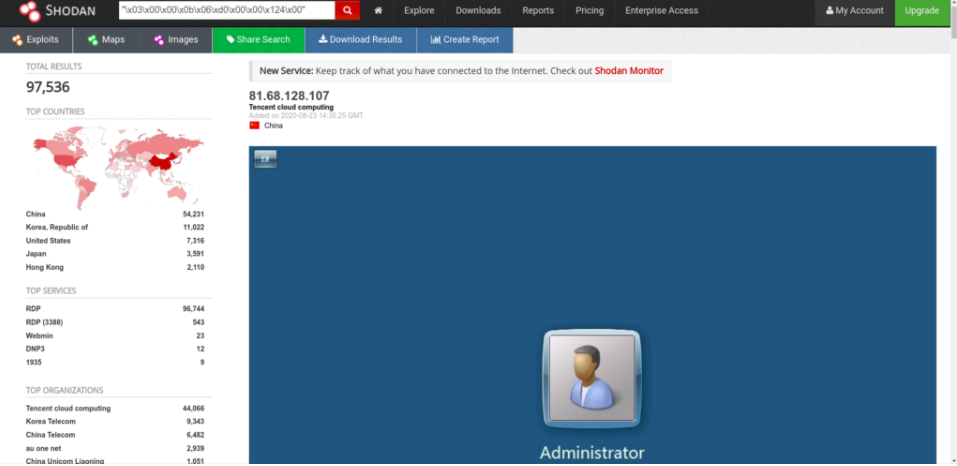
1. **Information Disclosure**
2. **User enumeration**

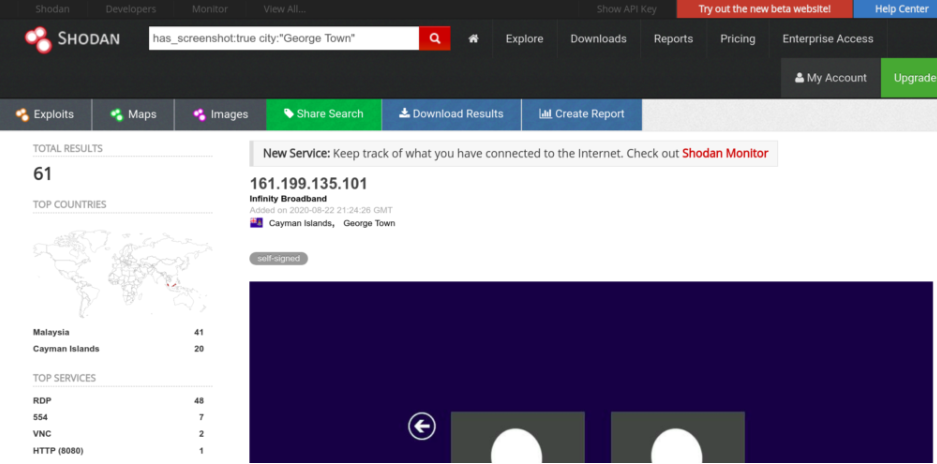
URL to check User enumeration Shodan **https://www.shodan.io**

**Step-1:** Enter the domain name in search field and consider this domain name as Input.



**Step-2:** If user Details Found Consider alert as **INFORMATIONAL** with alert score **0**





**Step-3:** If the output does not show any user details consider as **IGNORE**

1. **Sensitive commercial or business data**

**Manual Check**

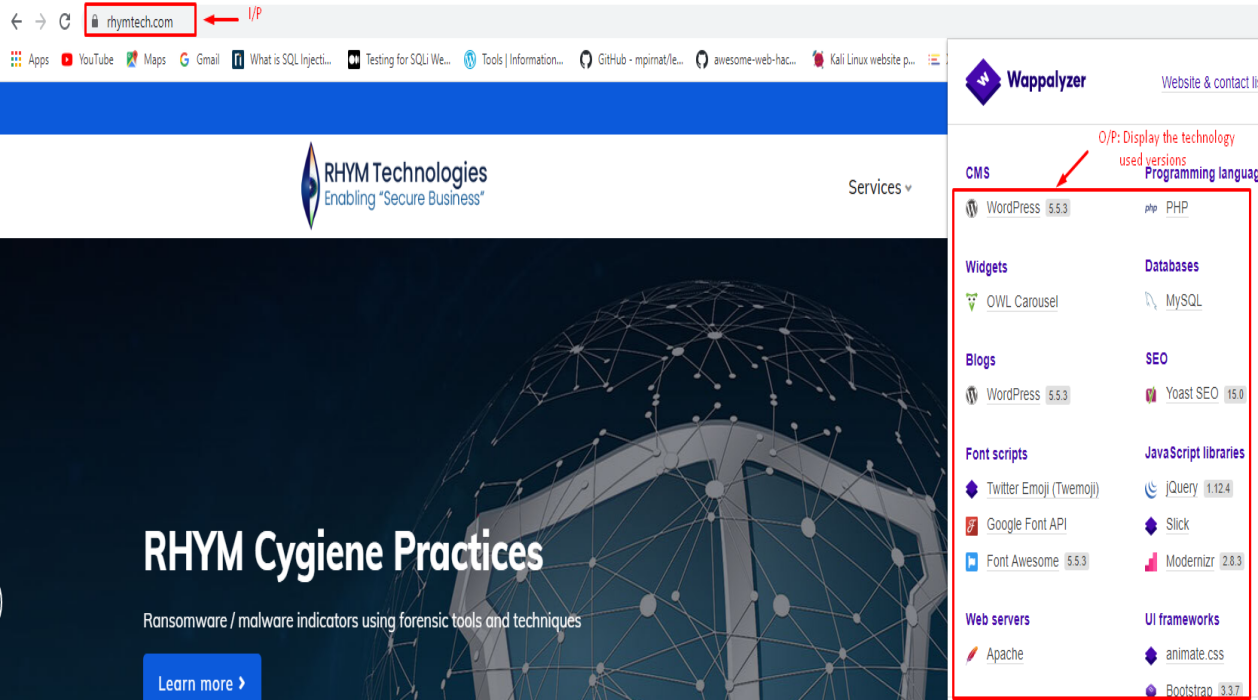
1. **Web application technical details**

URL to check web application details **Wappalyzer chrome Extension**

**Step-1:** Enter the Domain name and consider domain name as Input

**Step-2:** click on the Wappalyzer chrome extension there we can see the web application details

**Step-3:** If web application technical details are found Consider alert severity as **INFORMATIONAL** and with alert score **0**



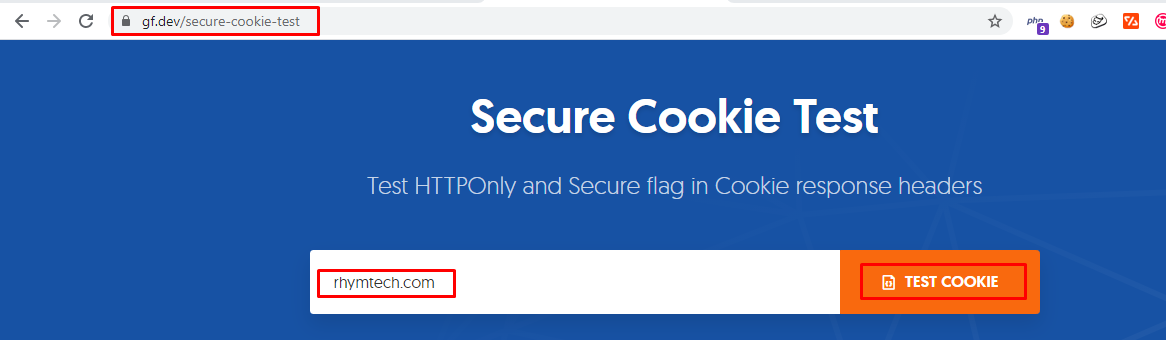
**Step-4:** If web application technical details are not found consider as **IGNORE**

1. **Insecure cookies**

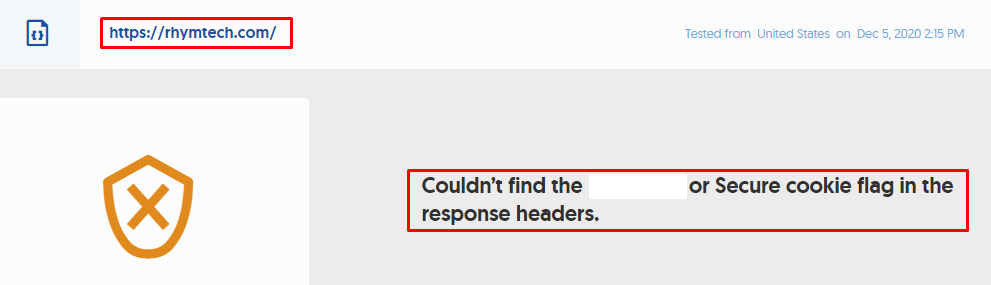
**a. Cookie missing secure attribute**

URL to check cookie missing secure attribute gf.dev/secure-cookie-test

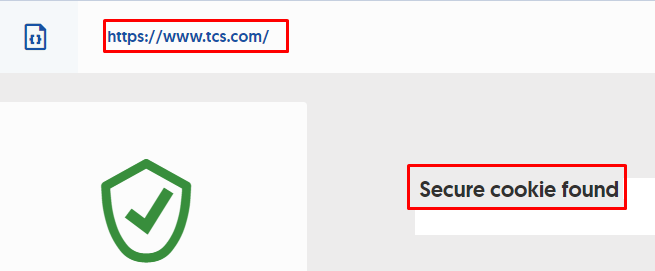
**Step-1:** Enter the domain name in search field and click on the Test Cookie and consider the domain name as Input



**Step-2:** If the Output shows could not find secure cookie flag response header consider alert as **MEDIUM** with alert score **5**

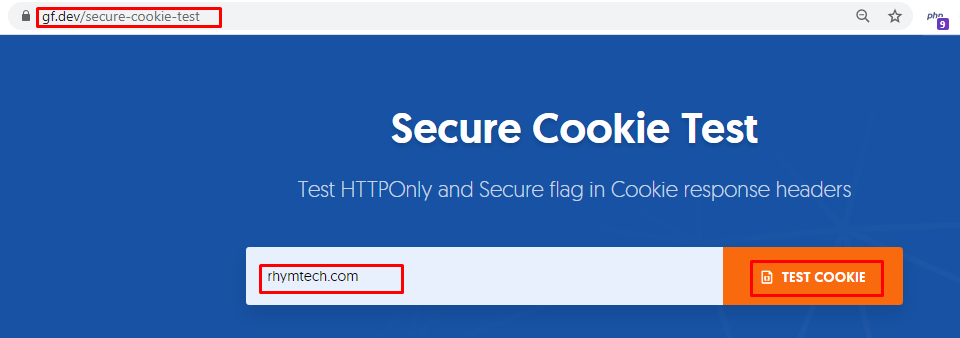


**Step-3:** If the Output shows secure cookie found consider as **IGNORE**

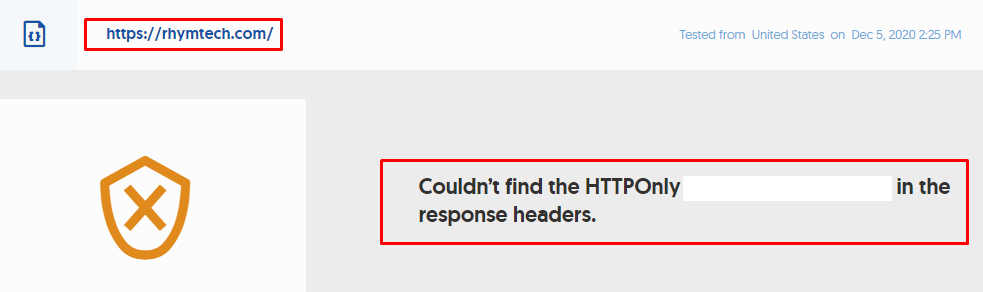


1. **Session cookie missing 'HTTP ONLY' attribute**

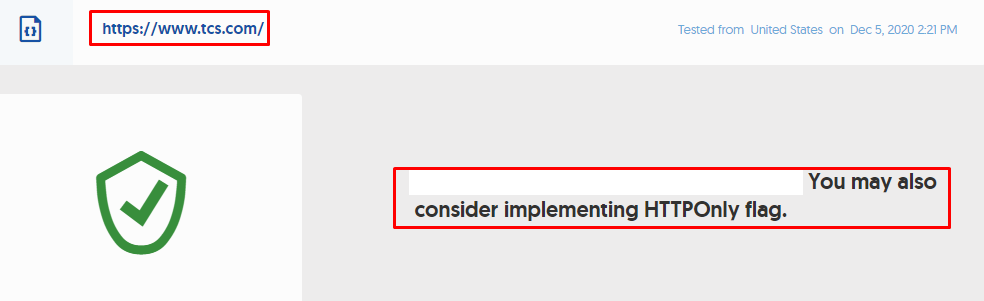
**Step-1:** Enter the domain name in search field and click on the Test Cookie and consider the domain name as Input



**Step-2:** If the Output shows could not find HTTPOnly response header consider alert as **MEDIUM** with alert score **6.1**



**Step-3:** If the Output shows HTTPOnly found consider as **IGNORE**



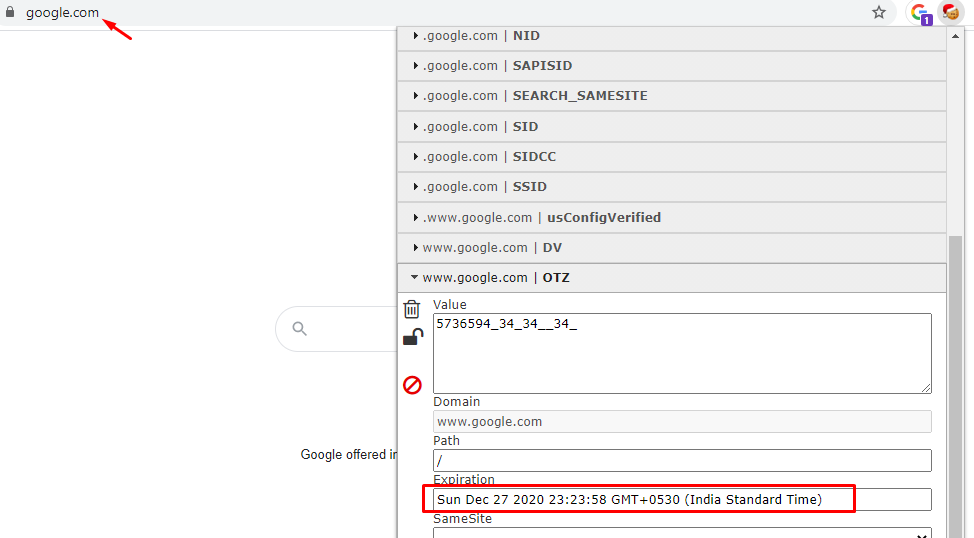
1. **Cookie expiry details:**

Tool to check cookie expiry details **edit this cookie (chrome Extension)**

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

**Step-2:** Click on this Edit cookie Chrome Extension if the output shows that Application is setting cookie expiration to future date or cookie the cookie is going to be never expiry consider as alert severity **MEDIUM**  with alert score **5**

**Here we are showing Google page as demo example for better understanding**



**Step-3:** Every time if cookie is getting expired consider as **IGNORE**