Web Application Security Audit Report

Website of High Commission of India, Accra, Ghana

No. 9 Ridge Road, Roman Ridge
PO Box CT-5708, Cantonments
Accra, Ghana, PIN - 00233

Developed by

Jadon Webtech Pvt. Ltd.

Contents

Table 1: Evaluation Summary

Application Details	Name: **Website of High Commission of India, Accra, Ghana** Version & Build: Not available Release Date: Not available
Customer Name and Address	High Commission of India, Accra, Ghana No. 9 Ridge Road, Roman Ridge PO Box CT-5708, Cantonments Accra, Ghana, PIN - 00233
Developed by	Jadon Webtech Pvt. Ltd.
Production URL	https://www.hciaccra.gov.in
Test / Temporary URL	https://www.hciaccra.gov.in
Infrastructure Details	Operating System : Linux Web Server : Apache Server-side Script : PHP Database : MySQL
User Roles	Not Available
Hash of Final Build	Not Available
Audited on	9th March 2018 to 21st March 2018 (Period of Assessment) 20th April 2022 to 21st April 2022 (Closure Verification)
Audit Location	STQC IT Services, Kolkata
Evaluation Method	Different software testing techniques (both manually and using tools) has been used to unearth application security vulnerabilities, weaknesses in the following broad application aspects. a) Data and Input Validation b) Authentication c) Authorization and Access Control d) Session Management e) Error Handling f) Use of Cryptography / Data Protection g) Others (Reference Operating Procedure of the laboratory: OP09)
Evaluated By	Amrita Som, SO “SB”
Report Prepared By	Arpita Datta, Scientist ‘E’
Report Reviewed By	Tapas Bandopadhaya , Scientist ‘F’ Head, e-Security
Report Sent on	21st April 2022
Other Remarks	The report presents the findings of the audit during the audit period only. This assessment result presents the state of security of the web application as it appears through its web interface and does not include the assessment result of application code review, hosting infrastructure and associated security processes

1.0 Introduction

STQC IT Services, Kolkata has carried out security evaluation of the application as detailed in the Table-1. The vulnerabilities/weaknesses observed during the testing along with the recommendations to plug the vulnerabilities are given below. The observations indicate the status of the application during the evaluation period (Ref. Table-1) only.

2.0 Summary Observations

The audit was conducted on the official Website of High Commission of India, Accra, Ghana, hosted in the developer's domain, by using automated tools followed by manual verification of discovered security vulnerabilities.

The application has been audited, following Open Web Application Security Project (OWASP) Application Security Verification Standard 4.0 [ASVS v4.0], to discover Security vulnerabilities / weaknesses. The assessment focused to discover the listed security vulnerabilities as per the OWASP Top 10 - 2017 list. Discovery of typical security issues of an web application, related to, improper input validation, insecure direct object reference, unvalidated directs and forwards, Cross-Site Scripting(XSS),Cross-Site Request Forgery(CSRF), Broken Authentication and Session Management (e.g. weak passwords, weak session management), various injection flaws (like SQL injection, command injection etc.), security mis-configurations, sensitive data exposure, missing or improper access control etc. and also related to well-known platform and components, are attempted in this exercise.

The initial assessment observations have been shared as assessment report (as referred below). On receipt of the confirmation of the closure of the reported issues, the assessment team will verify and make final comment in this assessment report.

Ref.-1: Assessment report : Report No. ES/EMBI/171806/OR/C1/022921
: Report No. ES/EMBI/171806/OR/C2/050353

Disclaimer: *This report is valid for the web application code in its present state only. Reassessment is recommended for any change in the application code.*

3.0 Security Issues as per OWASP ASVS

SN	Test/Parameter	Observation	Remarks
3.1 Data & Input Validation			
3.1.1	Input Validation	Vulnerabilities have been observed during assessment.	Not complied.
3.1.2	Sanitization and sandboxing	Vulnerabilities have been observed during assessment	Not complied.
3.1.3	Output encoding and Injection Prevention	No vulnerable issues has been found during audit.	Complied.
3.1.4	Deserialization Prevention	Such option is not available in the application	Not Applicable.
3.1.5	File Upload	Such option is not available in the application	Not Applicable.
3.1.6	File execution	Such option is not available in the application	Not Applicable.
3.1.7	File Storage	Such option is not available in the application	Not Applicable.
3.1.8	File Download	No vulnerable issues has been found during audit.	Complied.
3.2 Authentication			
3.2.1	Password Security	Such option is not available in the application	Not Applicable.
3.2.2	General Authenticator	Such option is not available in the application	Not Applicable.
3.2.3	Authenticator Lifecycle	Such option is not available in the application	Not Applicable.
3.2.4	Credential Recovery	Such option is not available in the application	Not Applicable.
3.2.5	Out of Band Verifier	Such option is not available in the application	Not Applicable.
3.2.6	Single or Multi Factor One Time Verifier	Such option is not available in the application	Not Applicable.
3.3 Authorization & Access Control			
3.3.1	General Access Control Design	Such option is not available in the application	Not Applicable.
3.3.2	Operation Level Access Control	Such option is not available in the application	Not Applicable.
3.3.3	Other Access Control Considerations	Such option is not available in the application	Not Applicable.
3.4 Session Management			
3.4.1	Fundamental Session Management	Such option is not available in the application	Not Applicable.
3.4.2	Session Binding	Such option is not available in the application	Not Applicable.
3.4.3	Session Logout and Timeout	Such option is not available in the application	Not Applicable.
3.4.4	Cookie-based Session Management	Vulnerabilities have been observed during assessment.	Not complied.
3.4.5	Defences against Session Management Exploits	Such option is not available in the application	Not Applicable.
3.5 Error Handling			
3.5.1	Log Content Requirements	Such option is not available in the application	Not Apaplicable.
3.5.2	Error Handling	No vulnerable issues has been found during audit.	Complied.
3.6 Use of Cryptography / Data Protection			
3.6.1	Algorithm	Such option is not available in the application.	Not applicable.
3.6.2	Client-side Data Protection	Such option is not available in the application.	Not applicable.

3.6.3	Sensitive Private Data	Such option is not available in the application.	Not applicable.
3.6.4	Communications Security	No vulnerable issues has been found during audit.	Complied.
3.6.5	Deployed Application Integrity Controls	Such option is not available in the application.	Not applicable.
3.7 Configuration Management			
3.7.1	Dependency	No vulnerable issues has been found during audit.	Complied.
3.7.2	Unintended Security Disclosure	No vulnerable issues has been found during audit.	Complied.
3.7.3	HTTP Security Headers	Vulnerabilities have been observed during assessment.	Not complied.
3.7.4	Validate HTTP Request Header	No vulnerable issues has been found during audit.	Complied.
3.8 Others			
3.8.1	Business Logic Security	Such option is not within scope of web application security audit.	Not applicable.
3.8.2	SSRF Protection	No vulnerable issues has been found during audit.	Complied.

4.0: Details of Audit Observations

Sl. No	Web Application Vulnerabilities	Observation	Remarks / Recommendations
0.0	**Functional Issue**		
0.1	Link to Non-existent Domain	Case 1: Additional form for Business Visa/ Conference Visa can be downloaded from the following pages (Fig. 0.1.1) and forms are linked to .com domain. If Download is clicked, the linked pages are not found in the target server (Fig. 0.1.2): https://www.hciaccra.gov.in/page/visaform/ https://www.hciaccra.gov.in/page/other-consular-services/ (Fig. 0.1.3) Case 2: The links to http://indiainbusiness.nic.in and http://www.ieeve.in/, as referred in the following pages are non-existent: https://www.hciaccra.gov.in/news_detail/?newsid=368 https://www.hciaccra.gov.in/page/in-india	Functional issue should be resolved.
1.0	**Data & Input Validation**		
1.1	Missing Input Validation: Trade Enquiry	If the Trade Enquiry – India form is filled up with incorrect data type like non-numeric inputs are given as **Year Established**, **TIN / PAN No.**, **Postal Code**, **Fax** etc. (Fig. 1.1.1), form gets saved successfully on submission (Fig. 1.1.2). If all input fields are filled up with URL-encoded JavaScript (Fig. 1.1.3), form is also submitted successfully (Fig 1.1.4): https://www.hciaccra.gov.in/trade_register/?q=India	All user inputs and data in all forms must be validated to be of proper data type and within range and should also be validated in the server-side.
1.2	Missing Input Validation: Feedback	In the feedback form, if URL-encoded JavaScript is given as **Address**, **Feedback / Detail** fields (Fig. 1.2.1), form gets successfully submitted (Fig. 1.2.2): https://www.hciaccra.gov.in/feedback/?q=type	All user inputs and data in all forms must be validated to be of proper data type and within range and should also be validated in the server-side.
1.3	Missing Validation of Query Parameter	Total number of tenders are divided among multiple pages and no. of records to be displayed per page is passed as query parameter pagesize (Fig. 1.3.1). If datatype of the query parameter pagesize is manipulated to array by appending square brackets, Internal Server Error occurs (Fig. 1.3.2): https://www.hciaccra.gov.in/tenders.php?page=2&year=&month=&pagesize=30 https://www.hciaccra.gov.in/event.php?page=2&year=&month=&page size=30 (Fig. 1.3.3)	All user inputs and data in all forms must be validated to be of proper data type and within range and should also be validated in the server-side.
2.0	**Session Management**		
2.1	Missing Attributes of Session Cookie	Session cookie PHPSESSID is set with SET-COOKIE directive when the website is opened in the web client (Fig. 2.1.1).	Cookie-based session tokens should have

Sl. No	Web Application Vulnerabilities	Observation	Remarks / Recommendations
		Cookie-based session tokens do not have 'Secure' and 'HttpOnly' attributes set. Session tokens also do not utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks. https://www.hciaccra.gov.in/	the 'Secure' attribute and 'HttpOnly' attribute set.
3.0	**Configuration Management**		
3.1	Missing Security Header	Referrer Policy Response header, which increases exposure to various cross-site injection attacks, is missing and "Referrer-Policy" may be set to "no-referrer" or "same-origin" (Fig. 3.1.1). The Referer request header contains the address of the previous web page from which a link to the currently requested page was followed. The Referer header allows servers to identify where people are visiting them from and may use that data for analytics, logging, or optimized caching. **Strict-transport-security** header is missing. **HTTP Strict Transport Security (HSTS)** is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion: Strict-Transport-Security: max-age=31536000; includeSubDomains https://www.hciaccra.gov.in/	Security headers may be configured properly.
3.2	Unsafe Third-party Link	The webpages inside the application are linked to various external websites, some of which are listed below, using anchor tags (<a>) along with the attributes 'href' and target="_blank. Link tags of this kind (i.e. with target="_blank" attribute) expose parts of the window object of the original page to the linked page via window.opener object and this can be exploited for phishing attacks if the linked page is malicious (Fig. 3.2.1): https://mea.gov.in https://www.india.gov.in/ http://www.iccrindia.net/ https://www.itecgoi.in/index.php https://rtionline.gov.in/ http://ayush.gov.in/ http://indiainbusiness.nic.in/ https://presidentofindia.nic.in/ https://www.pmindia.gov.in/en/ https://parliamentofindia.nic.in/ http://www.pbdindia.gov.in/en https://www.hciaccra.gov.in/	The attribute rel ="noopener noreferrer" may be added to each link element with target="_blank.

Appendix

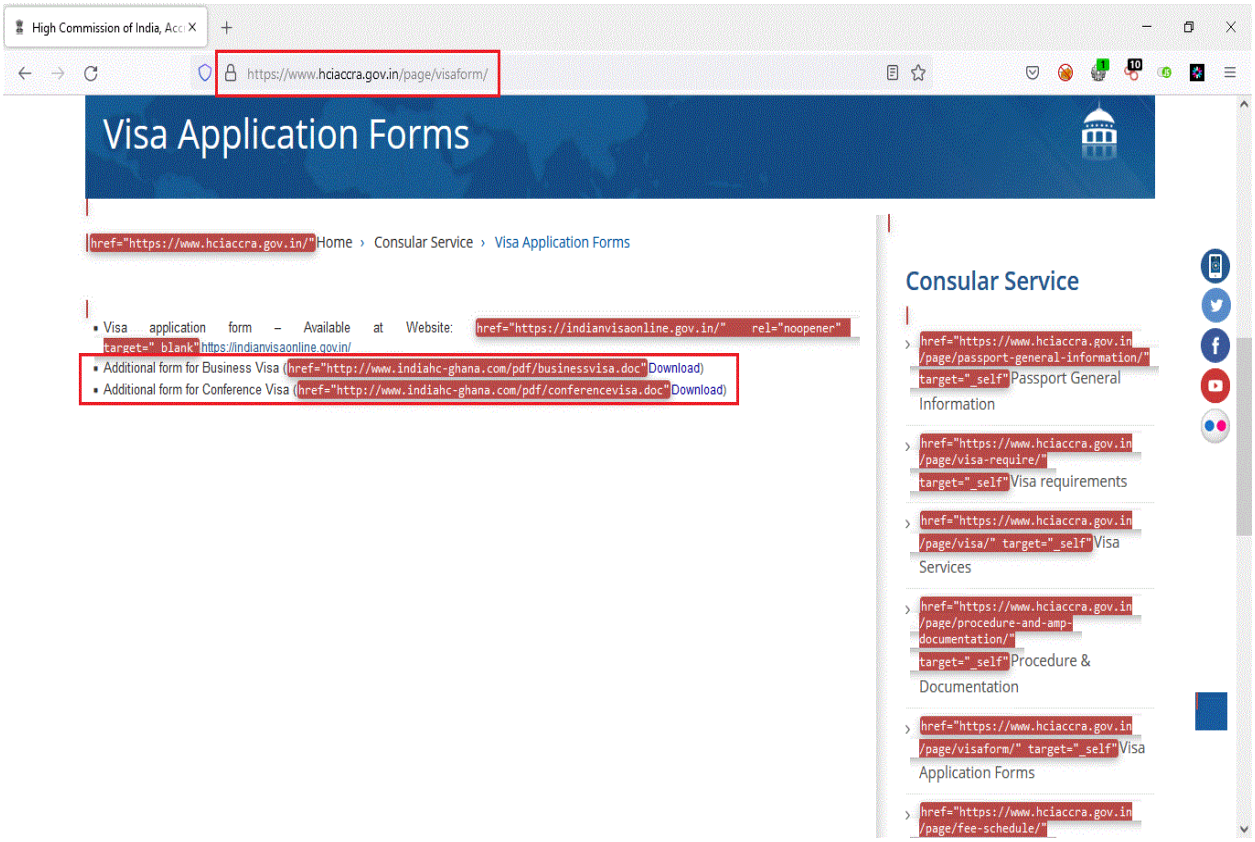

Fig. 0.1.1: Download links in Visa Application Forms page

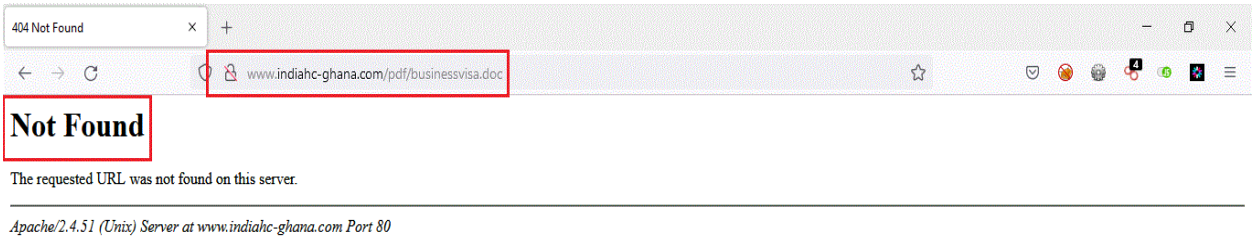

Fig. 0.1.2: Pages are linked to .com domain and are not found

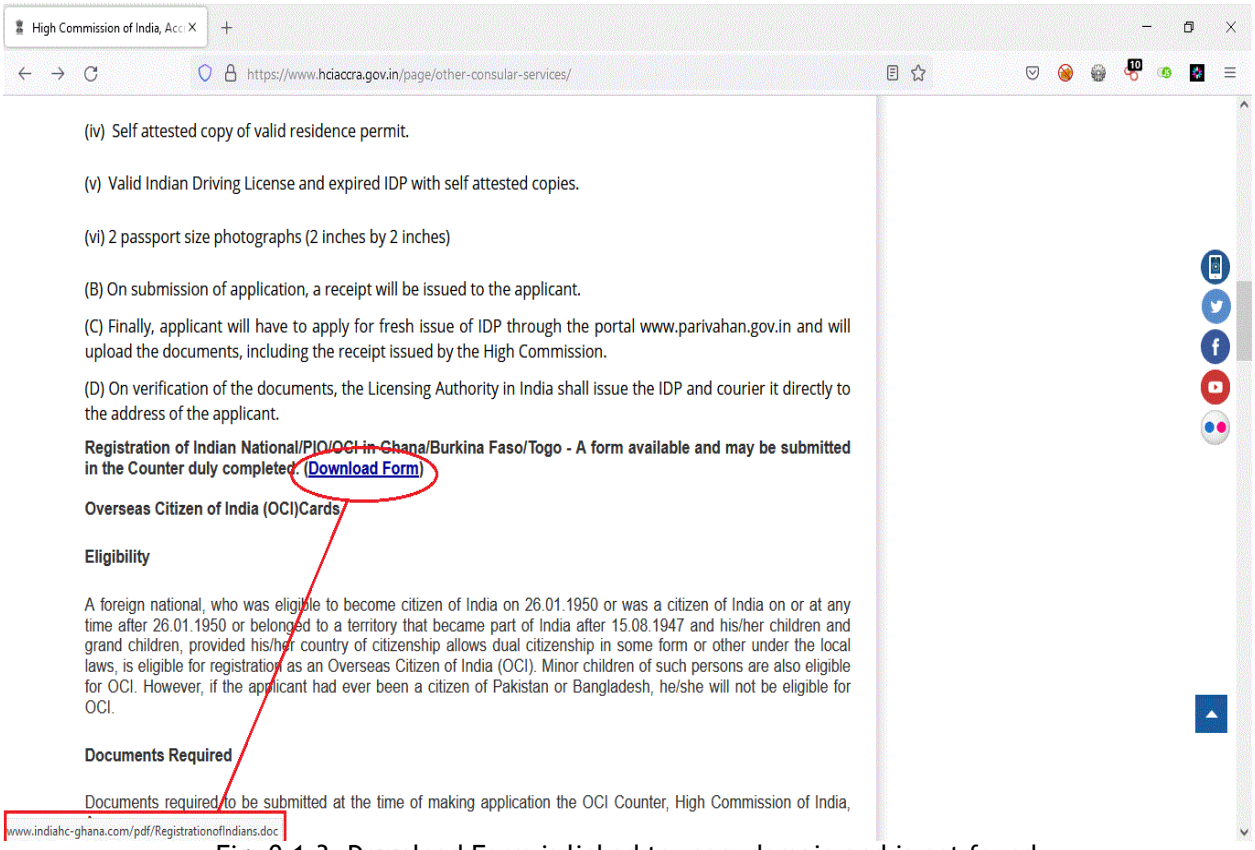

Fig. 0.1.3: Download Form is linked to .com domain and is not found

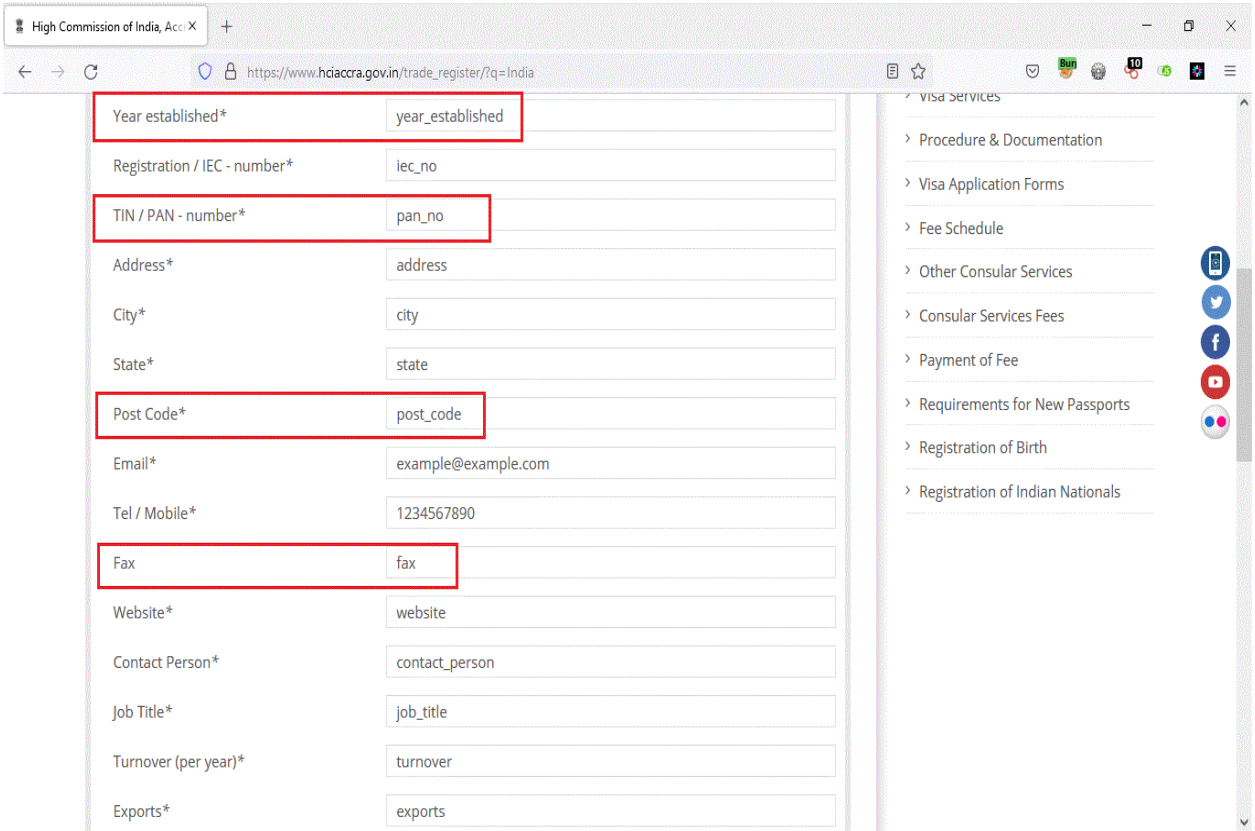

Fig. 1.1.1: Trade Registration form has been filled up with incorrect data

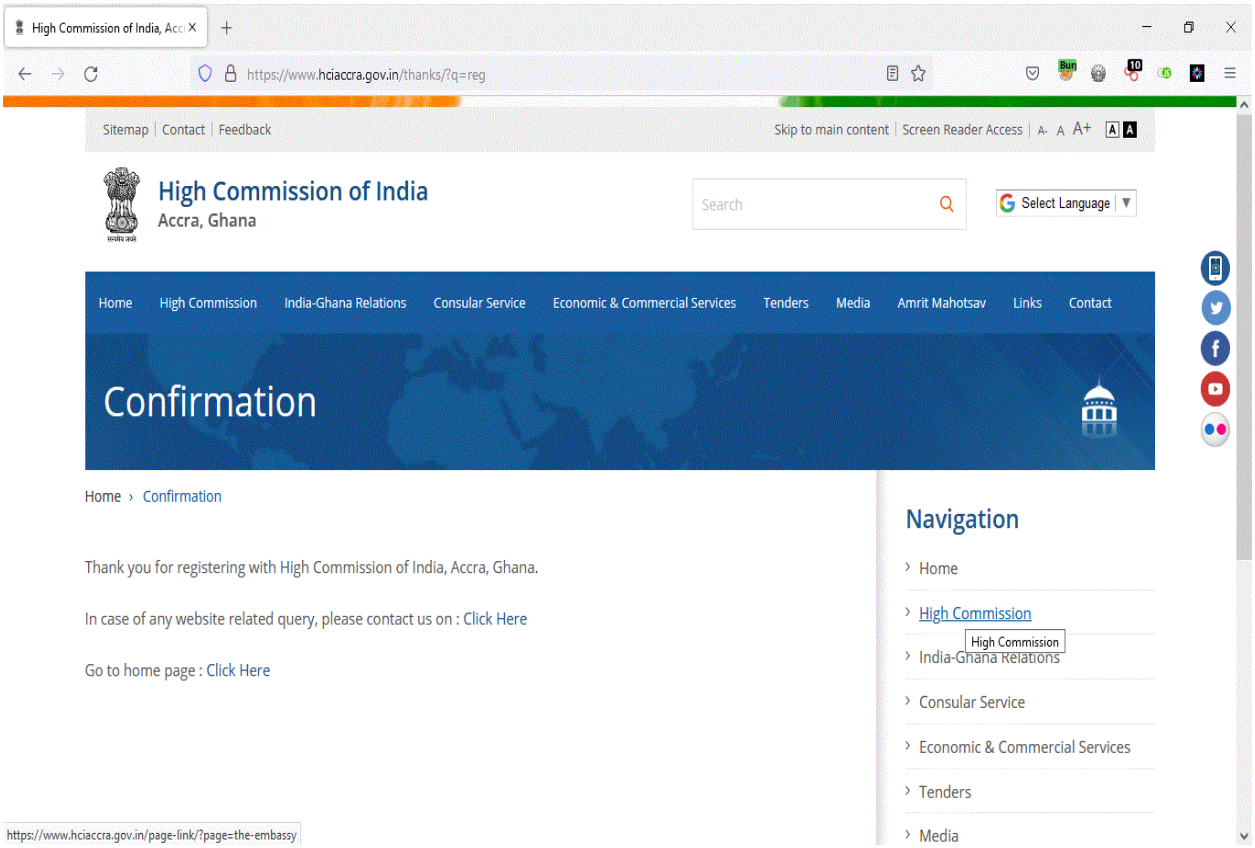

Fig. 1.1.2: Form is submitted successfully

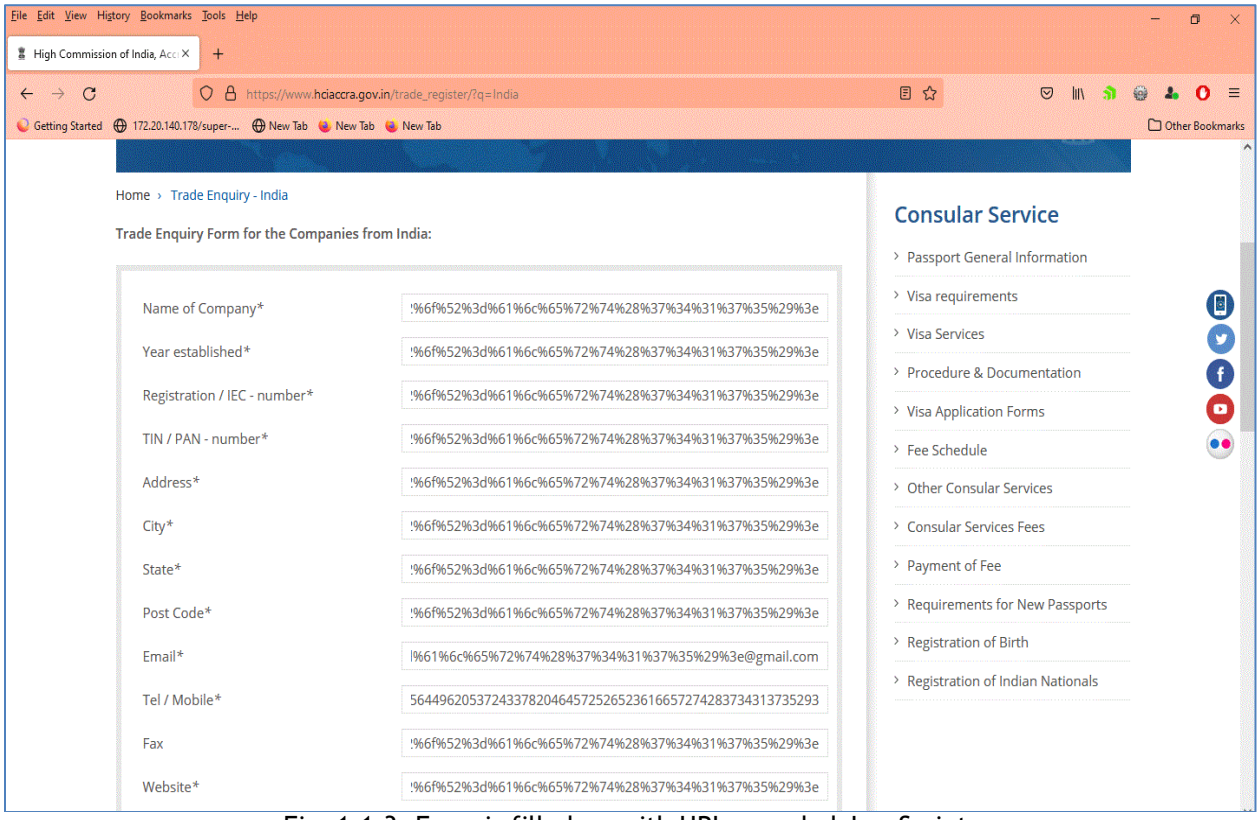

Fig. 1.1.3: Form is filled up with URL-encoded JavaScript

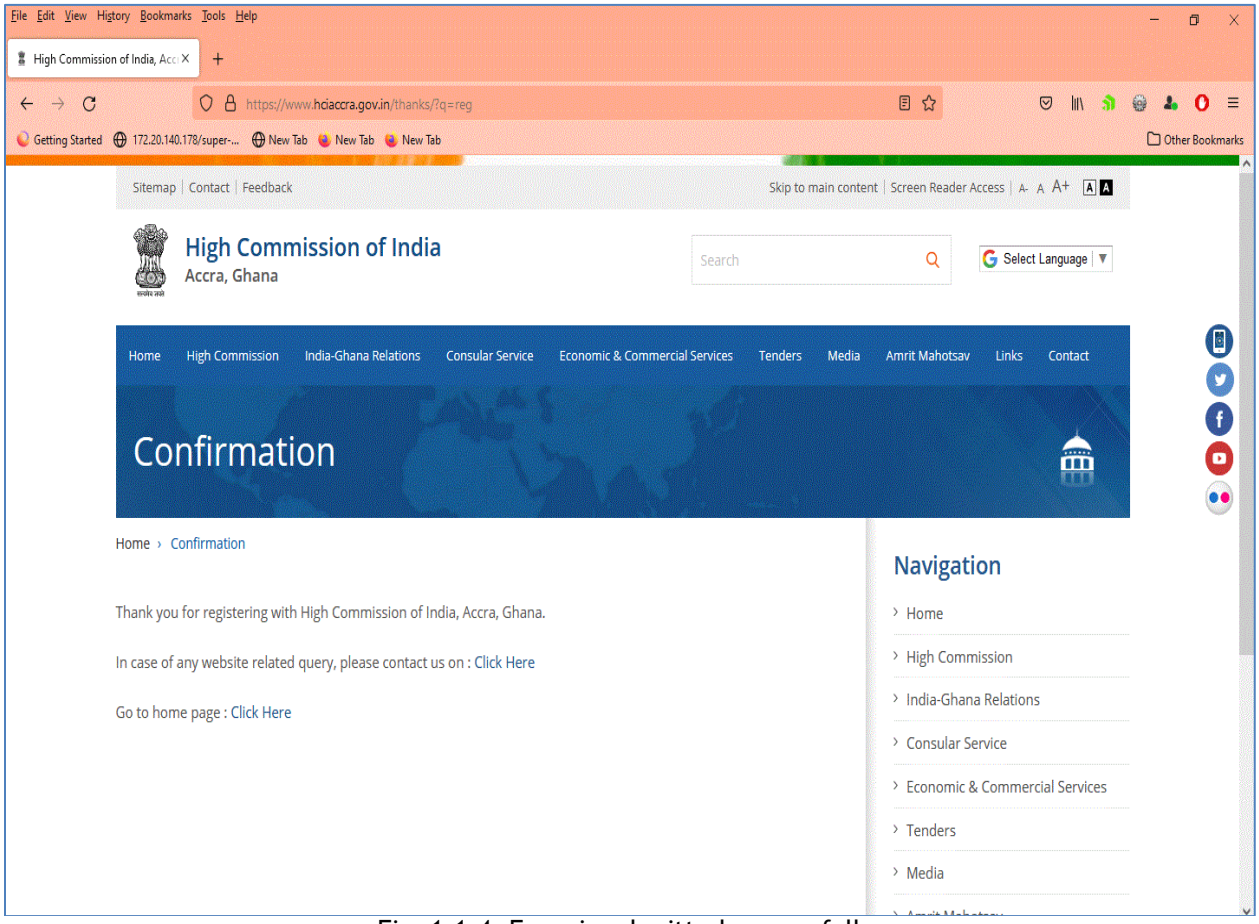

Fig. 1.1.4: Form is submitted successfully

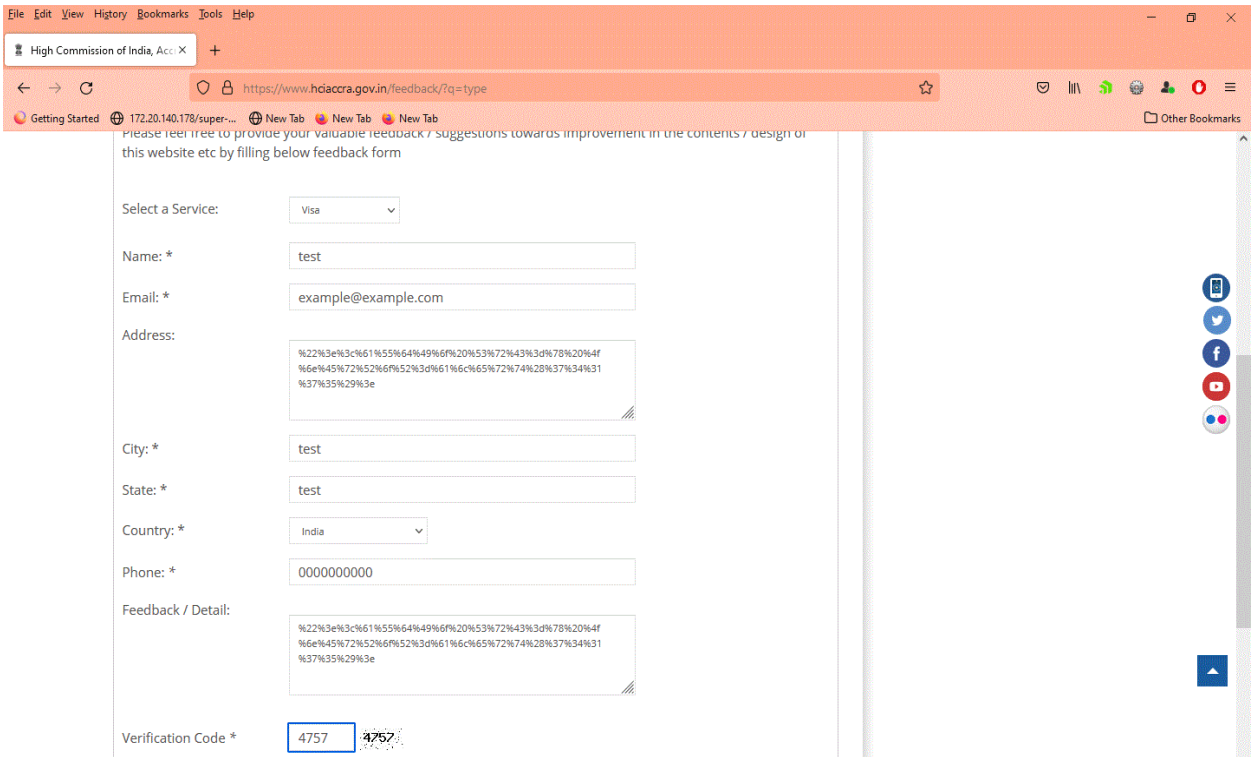

Fig. 1.2.1: Address and Feedback are filled up with URL-encoded JavaScript

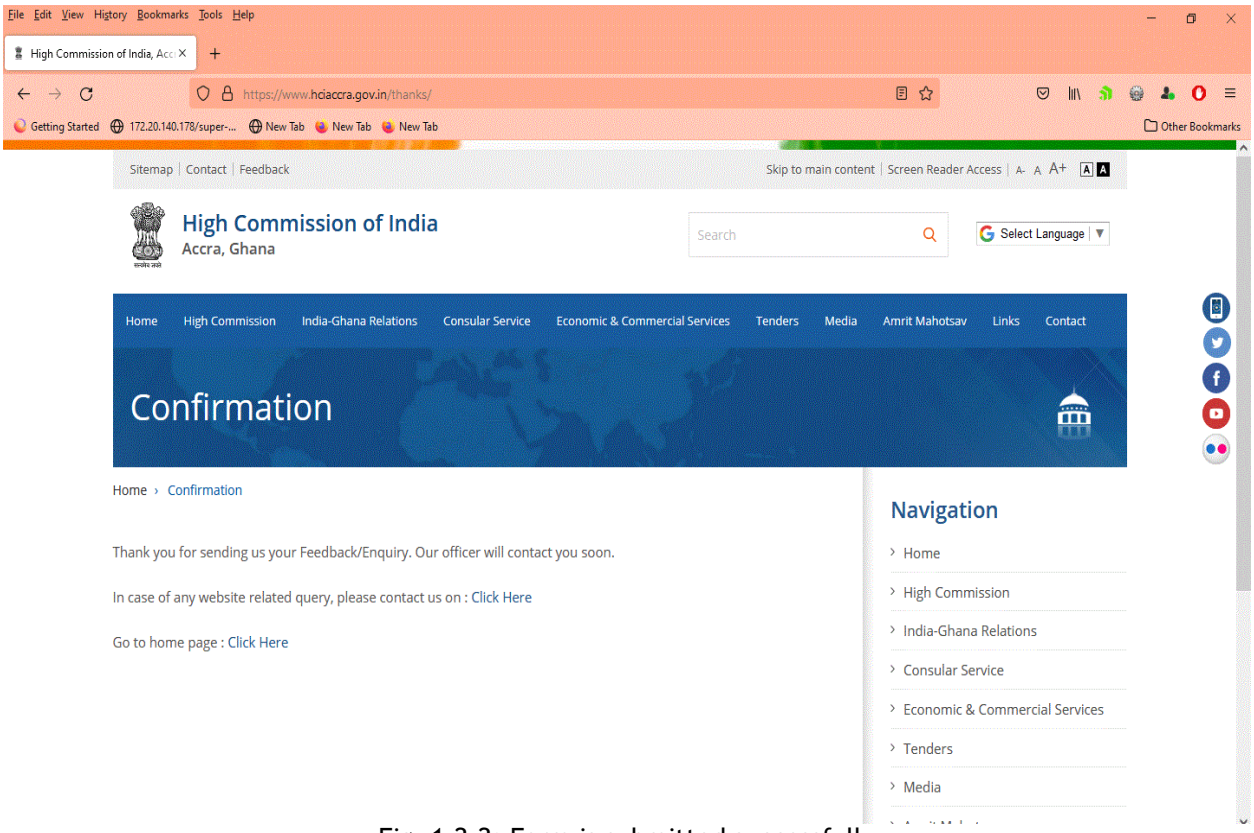

Fig. 1.2.2: Form is submitted successfully

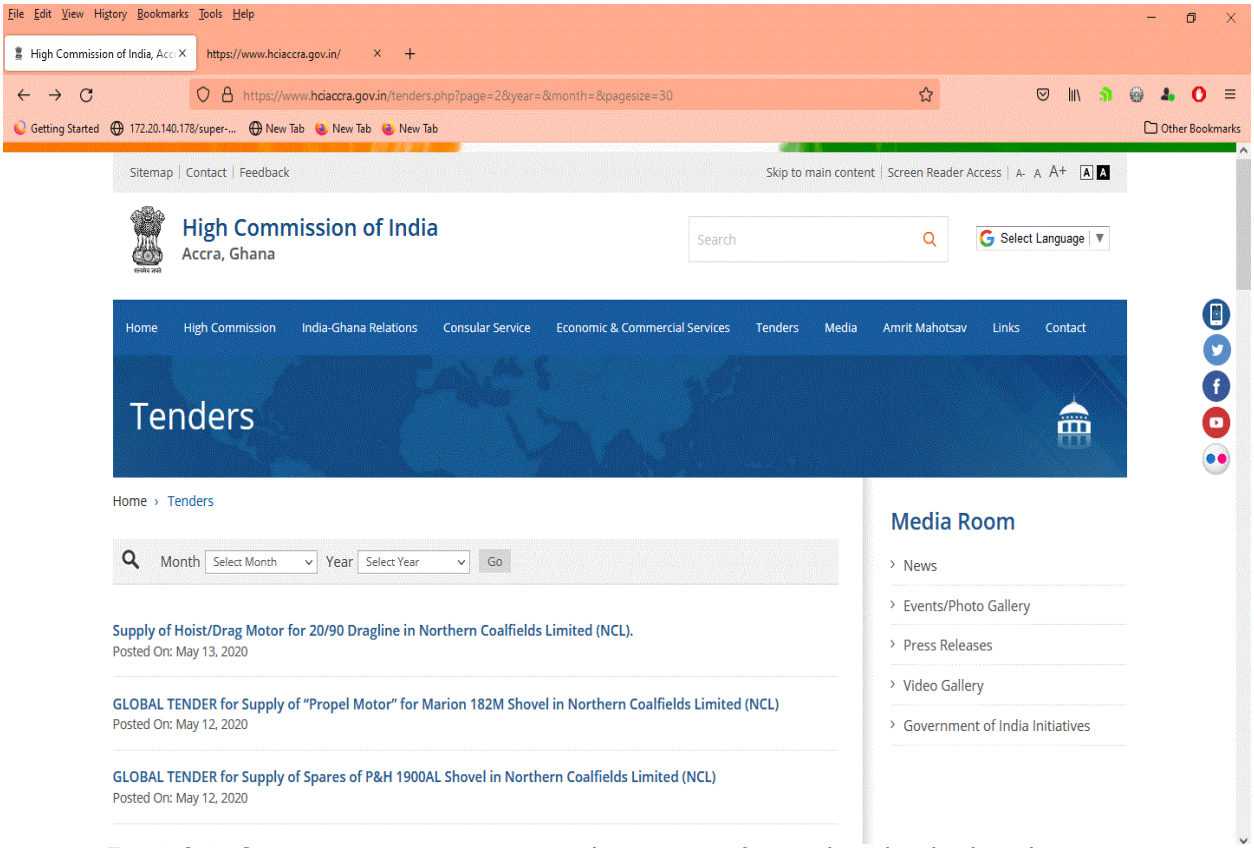

Fig. 1.3.1: Query parameter pagesize indicates no. of records to be displayed per page

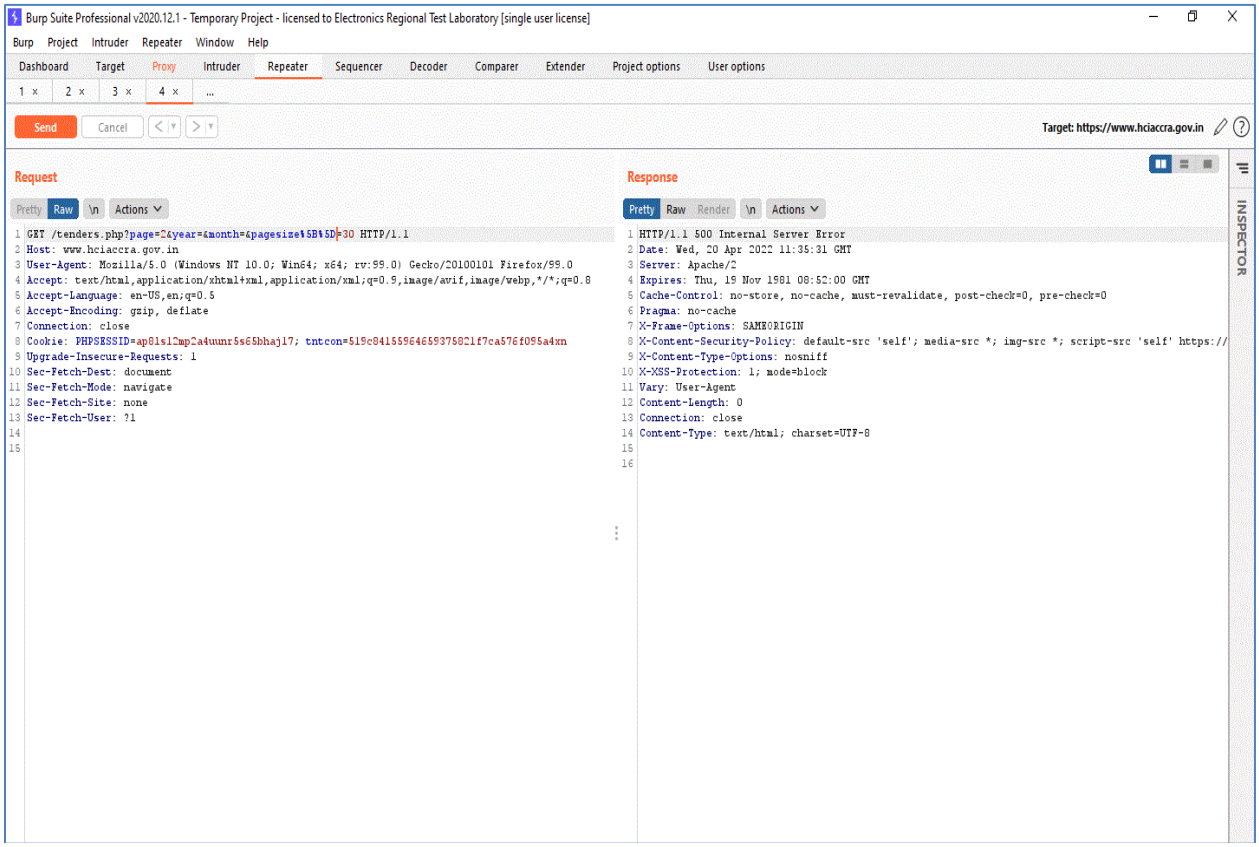

Fig. 1.3.2: Missing data type validation

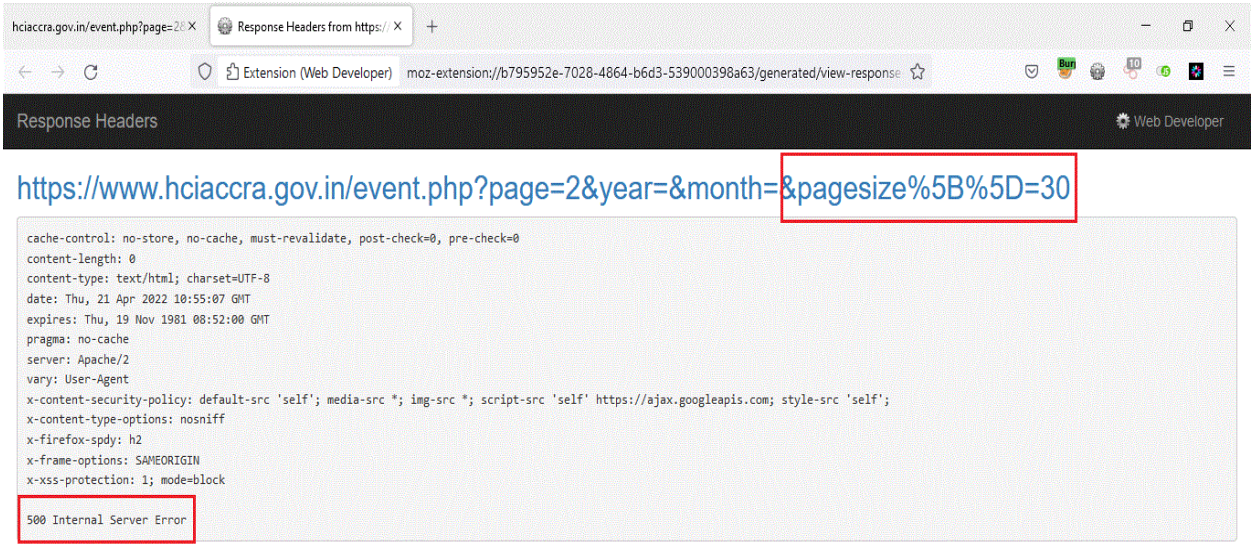

Fig. 1.3.3: Internal server error occurs due to missing data type validation

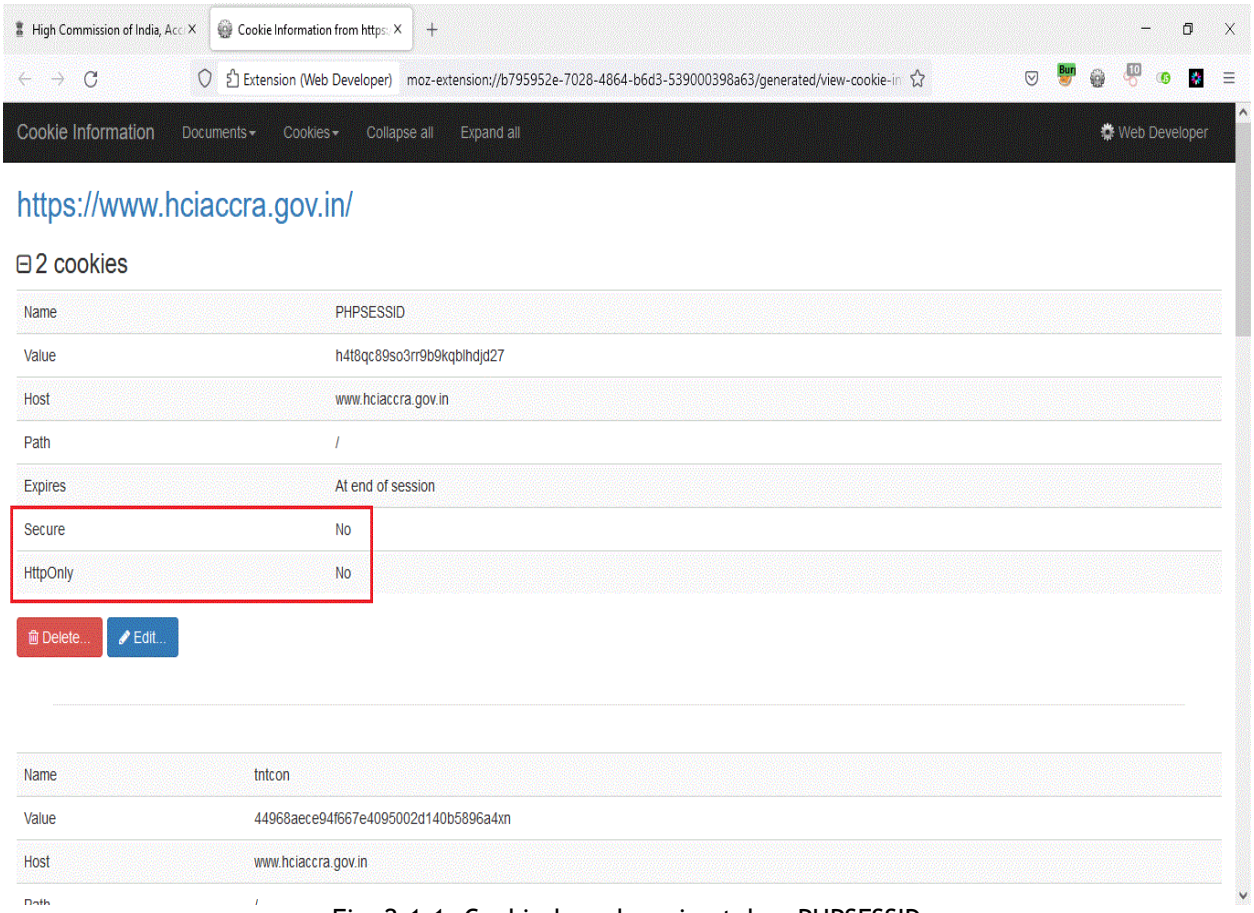

Fig. 2.1.1: Cookie-based session token PHPSESSID

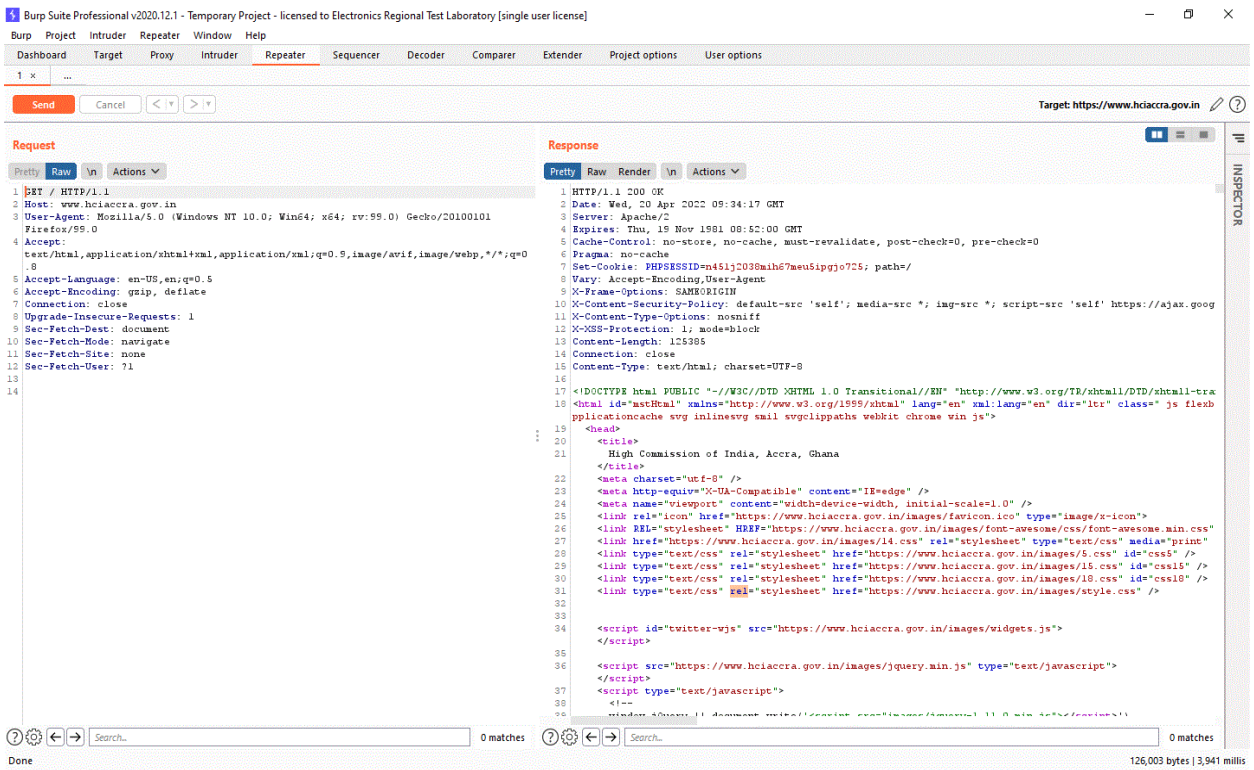

Fig. 3.1.1: HTTP response headers

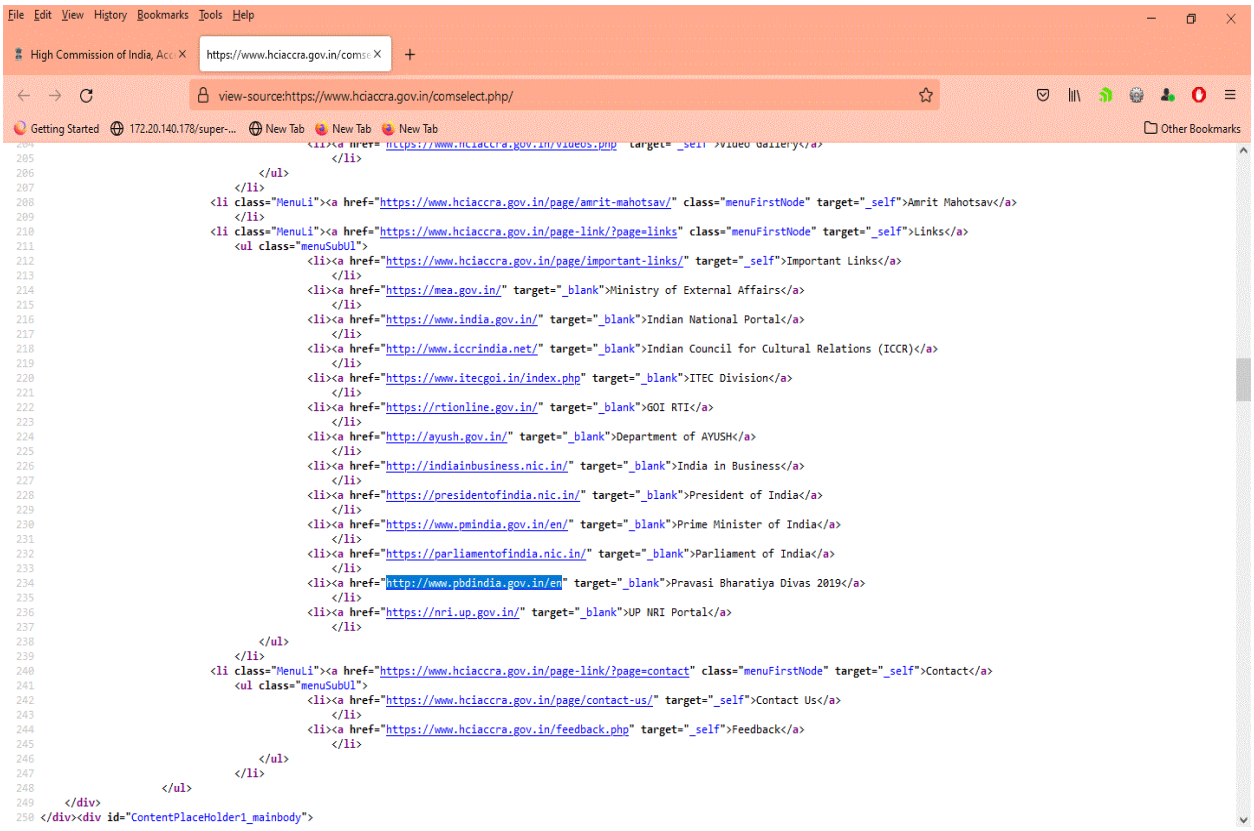

Fig. 3.2.1: Third-party links