



AKS IT SERVICES

Website Security Audit Report: Fishery Survey of India

Report Prepared By

AKS Information Technology Services Pvt. Ltd.

www.aksitservices.co.in

Version 2.0

March 2025

Disclaimer

All rights reserved. All the information contained in this document is confidential and proprietary to AKS Information Technology Services Pvt. Ltd. No part of this document, or the document as a whole, may be copied, reproduced, disclosed, photographed, electronically transferred or used, for any reason whatsoever, other than for the purpose of operations/network security enhancement and internal Website review by Fishery survey of India. For any such activity to be undertaken by any party, explicit written consent will have to be obtained from AKS Information Technology Services Pvt. Ltd.

AKS Information Technology Services Pvt. Ltd. shall assume no liability for any changes or omissions or modifications in this document. AKS Information Technology Services Pvt Ltd. shall assume no liability of the Website code level changes that have been done post audit and certification. The hash value of the entire Website, generated on the day of issue of certificate, shall hold the final verification test in case of any query or clarification at later stage. All the recommendations are provided on 'as is' basis and are void of any warranty expressed or implied. AKS Information Technology Services Pvt. Ltd. shall not be liable for any damages financial or otherwise arising out of use/misuse of this report by any current employee of Fishery survey of India or any member of general public.

Document Reference

Item	Description
Document Title:	Website Security Audit Report v2.0(Final) of Fishery Survey of India
Department:	Application Security
Publish Date:	11 March 2025
Reference Document:	Website Security Audit Report v1.0(Initial) of _27-february-2025_FSI Portal

Author(s)			
Auditor			
Name	Designation	Start Date	End Date
Mr. Shashwat Bajpai	InfoSec Consultant	10 February 2025	10 March 2025
Prepared By			
Name	Designation	End Date of Preparation	
Mr. Shashwat Bajpai	InfoSec Consultant	11 March 2025	
Reviewed by			
Name	Designation	Date of Review	
Mr. Darshan Deswal	Asst. Manager - Application Security	11 March 2025	
Approved by			
Name	Designation	Date of Approval	
Mr. Rohit Singh Chauhan	Sr. Manager – Application Security	11 March 2025	

Document Distribution List			
Name	Organization	Designation	Email Id
Mr. Ashish Kumar	Fishery survey of India	--	programmer-1@fsi.gov.in

Table of Contents

1.	Executive Summary.....	5
1.1.	Summary of Findings.....	5
1.2.	Objective	6
1.3.	Scope	6
2.	Process Overview	7
2.1.	Methodology & Standard.....	7
2.2.	Standard.....	7
2.3.	Risk Rating Definition	8
2.4.	Tools Used	9
3.	Technical Summary	10
3.1.	Key Findings.....	10
4.	Recommendations	11
5.	Conclusion.....	12
	Appendix A: Site Structure / List of in-scope URLs.....	13
	Appendix B: Description on Tools	28

1. Executive Summary

As part of the Website Security Audit proposal, AKS IT's Security Consultants conducted the security audit of the Fishery Survey of India Website from 10 February 2025 to 10 March 2025. A grey box assessment was performed to identify the vulnerabilities defined by the CERT-In Guidelines, NIC Guidelines, OWASP standard and other best practices.

This is the final level of the Website security audit report and it is observed that all the previously reported vulnerabilities are mitigated.

1.1. Summary of Findings



Severity-Wise Status of Findings

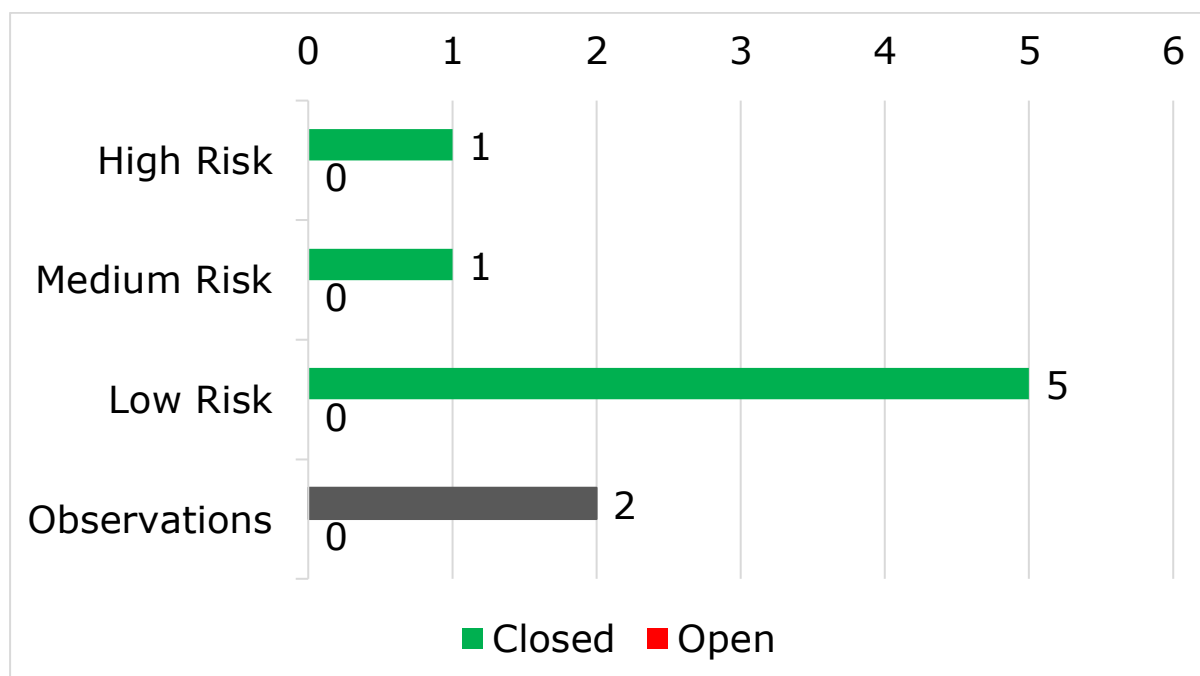


Figure 1: Severity Wise Status

1.2. Objective

The key objective of this Website Security Audit was to identify whether any vulnerabilities exist in the Website and to exploit those that can be seen and compromised by malicious users.

1.3. Scope

The scope of the assessment was to perform a Website security audit on the application hosted on the following URL:

- **<http://10.194.92.179/>**

Authentication mechanism was implemented on the following URL:

- **<http://10.194.92.179/Member/login>**

The following User Role was provided and was in the scope of audit.

- **Admin**

Refer [Appendix A](#) for the complete list of in-scope directories and URLs.

2. Process Overview

A Website Vulnerability Assessment is the process of identifying, quantifying and prioritizing the vulnerabilities in a Website for evaluating its security posture. The process involves an active analysis of the Website for any weaknesses, functional flaws and vulnerabilities. Any security issues that are identified are explained with an assessment of their impact and solutions for their mitigation.

2.1. Methodology & Standard

Security Consultants at AKS IT Services Pvt. Ltd. used the CERT-In Guidelines, NIC Guidelines, OWASP standard and other best practices for Website Security Testing Methodology for conducting the security audit of the in-scope Website.

The Website Audit Methodology is based on the 'grey-box' approach. The testing model consists of the following phases:

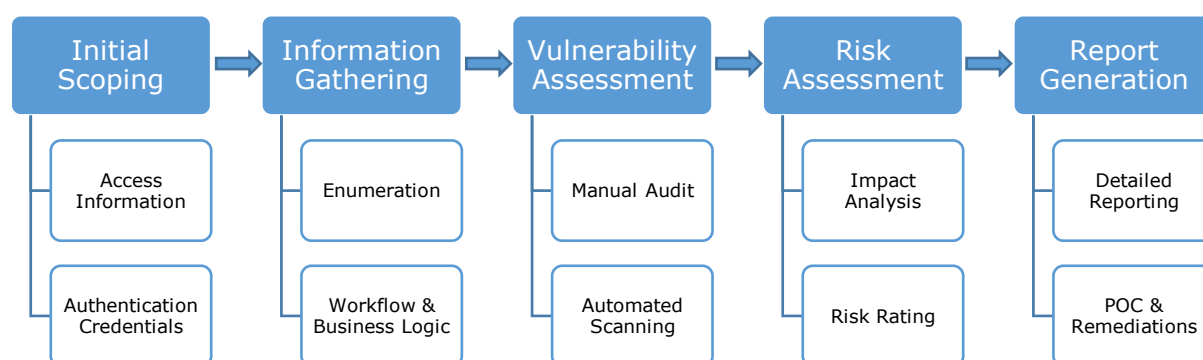


Figure 2: Methodology

2.2. Standard

The assessment aimed at identifying the vulnerabilities that are defined by following standards mentioned for conducting the final level security audit of the Fishery Survey of India Website.

- CERT-In Guidelines: <https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf>
- NIC Guidelines: https://meity.gov.in/writereaddata/files/checklist_development.pdf
- OWASP standard: [OWASP Web Security Testing Guide | OWASP Foundation](#)
- Best Practices.

2.3. Risk Rating Definition

The following definitions were used in determining the risk rating of the identified vulnerabilities:

High Risk

Impact

If the exploitation of the vulnerability can result in complete takeover of the system, alteration/destruction of the data, disclosure of sensitive information.

Exploitability

Exploitation for the vulnerability is easy and can be done using tools/scripts that are easily available or are open-source.

Medium Risk

Impact

The exploitation of the vulnerability can result in partial control of the system, partial destruction of the system/data, disclosure of semi-sensitive information.

Exploitability

Exploitation for the vulnerability is possible but may require expertise. Also, the required tools or scripts may not be readily available or are open-source.

Low Risk

Impact

The exploitation of the vulnerability can result in little or no impact on the system/data but may disclose less sensitive information that can be of interest.

Exploitability

Exploitation of the vulnerability itself may be complex and need to be chained with other vulnerabilities in order to have a major impact.

2.4. Tools Used

Security Consultants at AKS IT Services Pvt. Ltd. use a combination of following commercial and open-source tools for conducting the security audit of the in-scope Website:

Sr. No.	Name	Version	Type
1.	Burp Suite Professional	2025.1	Commercial
2.	Acunetix Vulnerability Scanner	24.5	Commercial
3.	GoBuster	3.6	Open Source
4.	SQLMAP	1.8	Open Source

Table 1: Tools Used

Refer [Appendix B](#) for a brief description on all the above-mentioned tools.

3. Technical Summary

During the final level Website security audit, the consultants of AKS IT Services Pvt. Ltd. revalidated the fixes implemented in order to mitigate the previously reported vulnerabilities in the in-scope Website. This section of the report covers the current status of vulnerabilities that were discovered and reported during the course of the security audit.

3.1. Key Findings

The following table lists the current status of all the vulnerabilities that were reported during the course of the security audit:

S. No.	Vulnerability	Severity	First Level	Interim Level	Final Level
1.	Cleartext submission of password	High	Open	Closed	Closed
2.	Parameter pollution	Medium	Open	Closed	Closed
3.	Lack of security headers	Low	Open	Closed	Closed
4.	Missing cookie attributes	Low	Open	Closed	Closed
5.	HTTP Trace method is enabled	Low	Open	Closed	Closed
6.	Vulnerable and Outdated Components	Low	Open	Closed	Closed
7.	Private IP Disclosure	Low	Open	Closed	Closed

Table 2: Status of Key Findings

S.no.	Observations	First Level	Interim Levels	Final Level
1.	Change password functionality	Open	Open	Functionality Removed
2.	Functionality not working	open	Open	Closed

Table 3: Status of Observations

4. Recommendations

The following points must be considered before and during the deployment of the application into the production environment:

- Any framework, library and/or server running with the older version must be upgraded with the latest version, security plug-ins and/or add-ons.
- The latest and stable TLS version deployment is suggested on the production server for further enhanced security.
- Proper implementation of HTTP Security Headers like Content Security Policy (CSP), X-XSS-Protection, X-Frame-Options, etc. is recommended on the production server.
- Implementation of HTTP Only and Same Site attributes on session cookies is recommended on the production server.
- Application server and framework must be configured to hide version details.
- Web Server and OS Level hardening need to be in place for the production server.
- Website should be behind a Web Application Firewall (WAF) for an added layer of protection against attempted attacks.

5. Conclusion

AKS IT Services Pvt. Ltd. completed the security audit of the Fishery Survey of India Website. This audit was based on the technologies, standards and known threats as of the date of this document. The certificate for safe for hosting with certain conditions appended below:

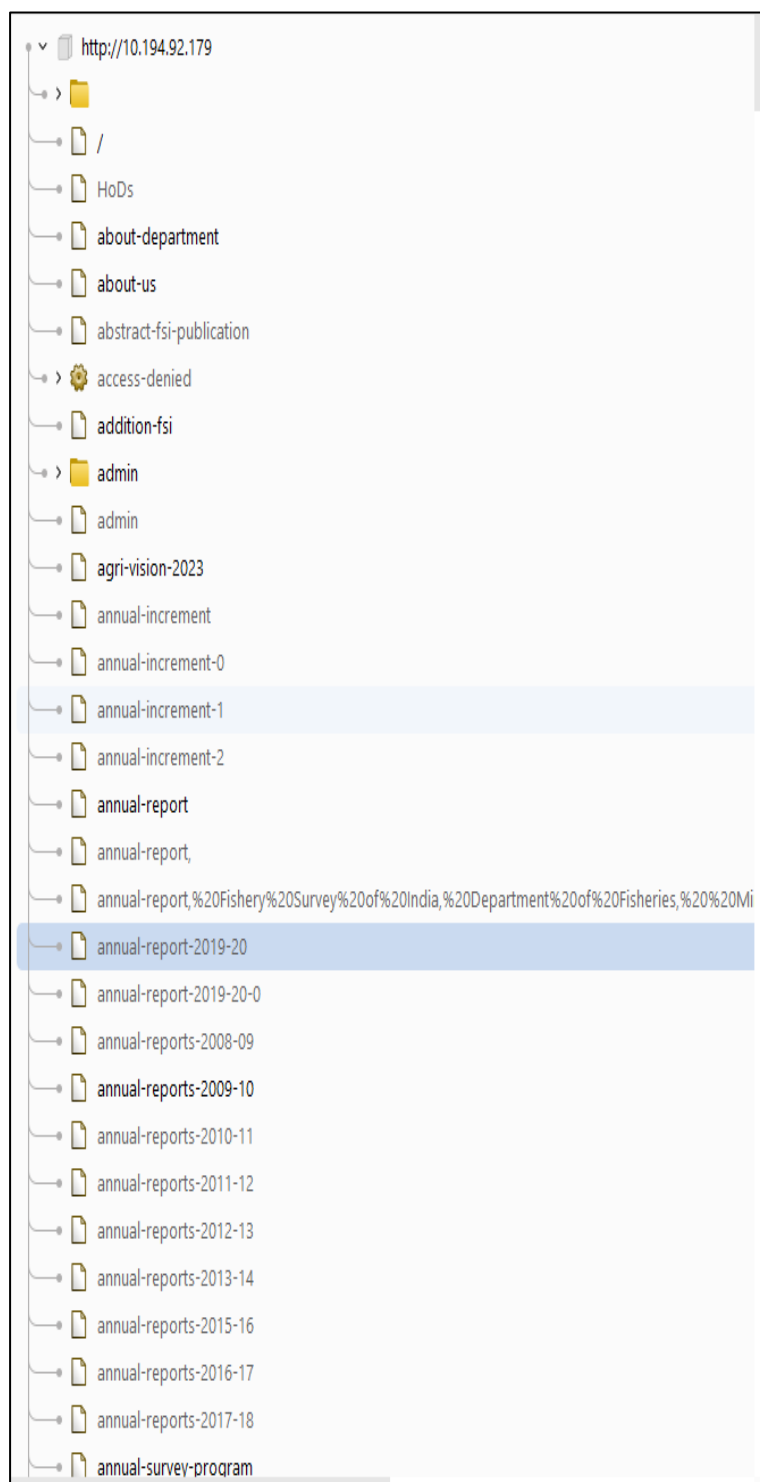
Recommendations for Hosting in Production Environment:

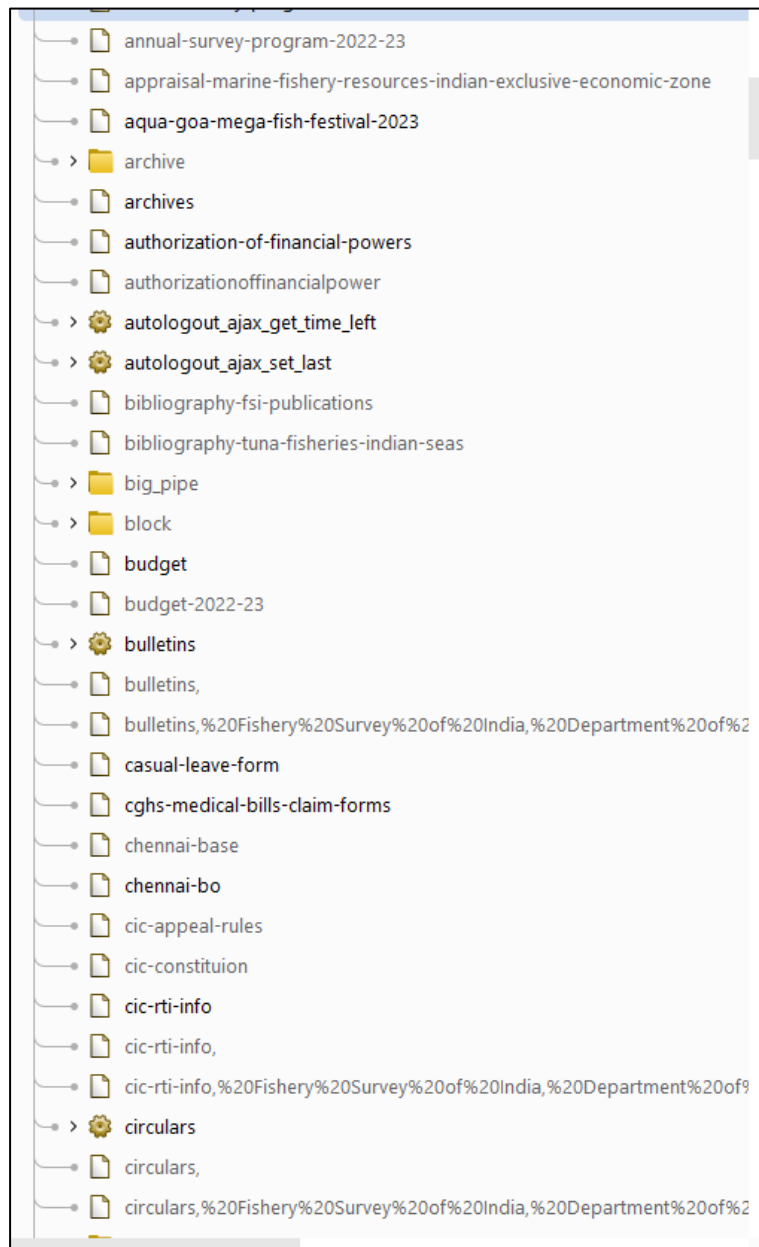
- Latest and stable TLS version should be used and disable weak SSL cipher suites.
- Web Server and OS Level hardening be done on the production server before deployment.
- Write permission should be granted only on the folder where the files are to be uploaded given in the following directory:
<https://fsi.gov.in/sites/default/files/>
<https://fsi.gov.in/themes/fsi/images/>
- Use the latest and stable version of all the software components in the application.
































Rohit Singh Chauhan
Sr. Manager – Application Security

Note: Regardless of the frequency of the Security Audits, no critical application can be considered 100% impervious to vulnerabilities & penetration. This is because of the discovery of new vulnerabilities and exploits. Therefore, it is necessary, as a good practice, to test and monitor information systems, application environment and platform versions used at least once in six months, along with keeping the Operating Systems and Applications patched and updated.

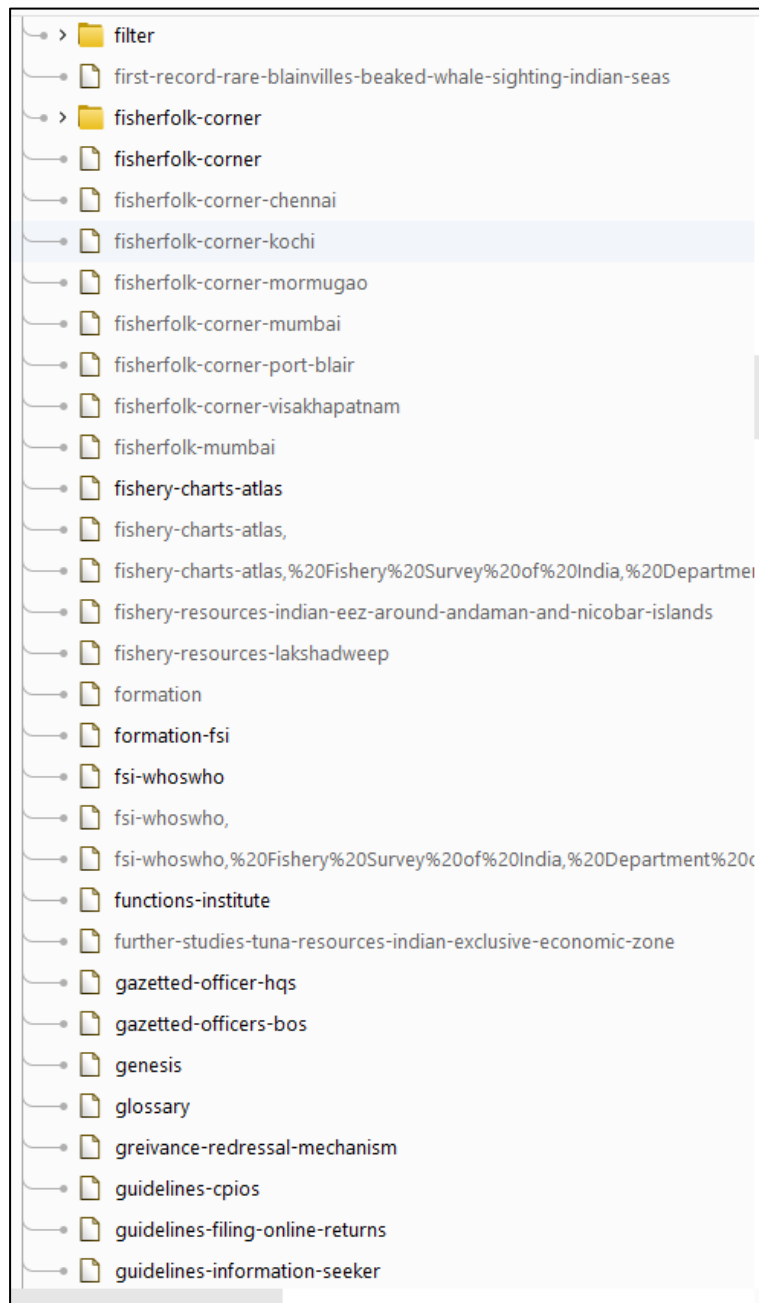
Appendix A: Site Structure / List of in-scope URLs

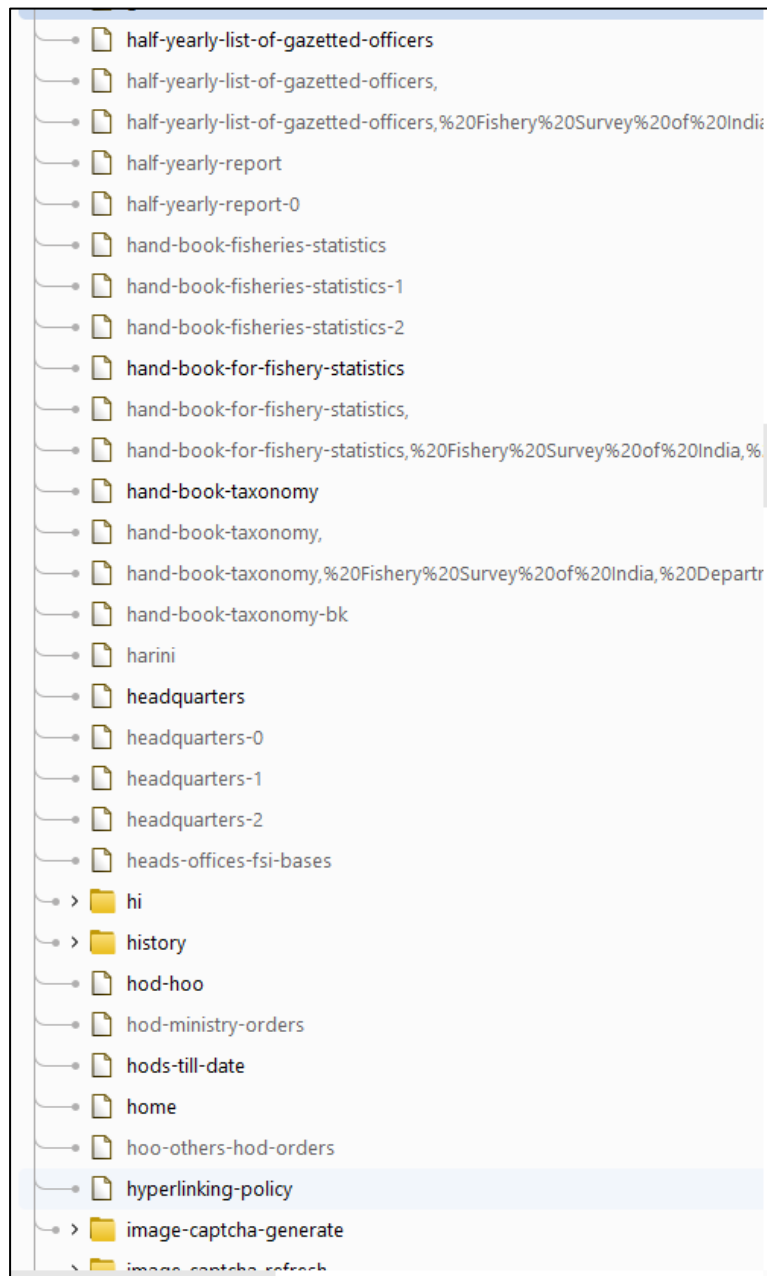


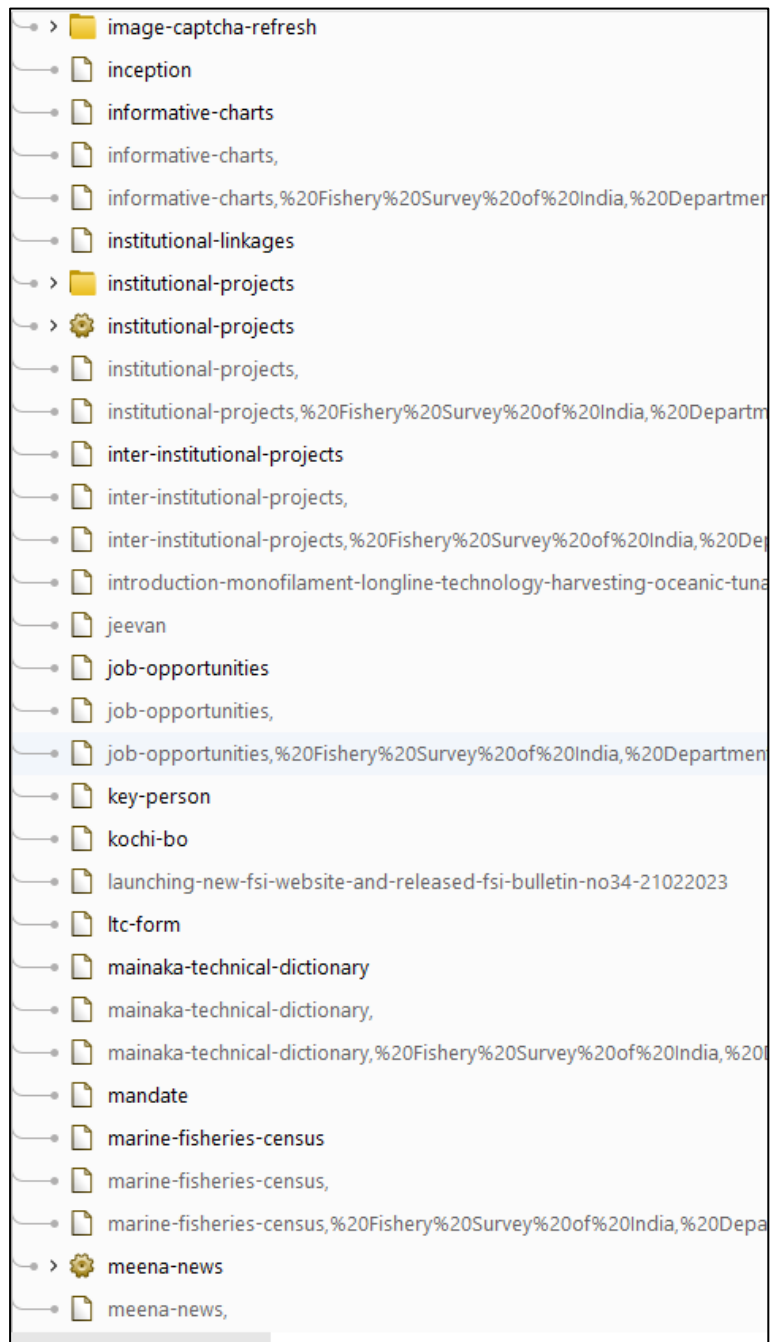


- >  **circulars-notices-orders**
-  circulars-port-blair
-  circulars-visakhapatnam
-  cochin-base
-  committee-chennai
-  committee-kochi
-  committee-mormugao
-  committee-mumbai
-  committee-port-blair
-  committee-visakhapatnam
- >  **committees**
-  comparative-study-demersal-fishery-resources-indian-waters-assessed-
-  compilations-oms
-  contact-us
-  content-archival-policy-cap
-  content-contribution-moderation-approval-policy-cmap
-  content-review-policy-crpf
- >  **contextual**
-  contingency-plan-event-defacement-natural-calamity
-  contributions-fishery-biology-indian-seas
-  copyright-policy
- >  **core**
-  cpios-first-apallate-authority
-  database
-  demersal-fisheries-resources-south-westcoast-india
-  demersal-fishery-resources-east-coast-india-update
-  demersal-fishery-resources-wadge-bank
-  demersal-fishery-resources-west-coast-india-update
-  demersal-resources-survey-continental-shelf
-  department-fisheries
-  depredation-longline-fishery-indian-waters

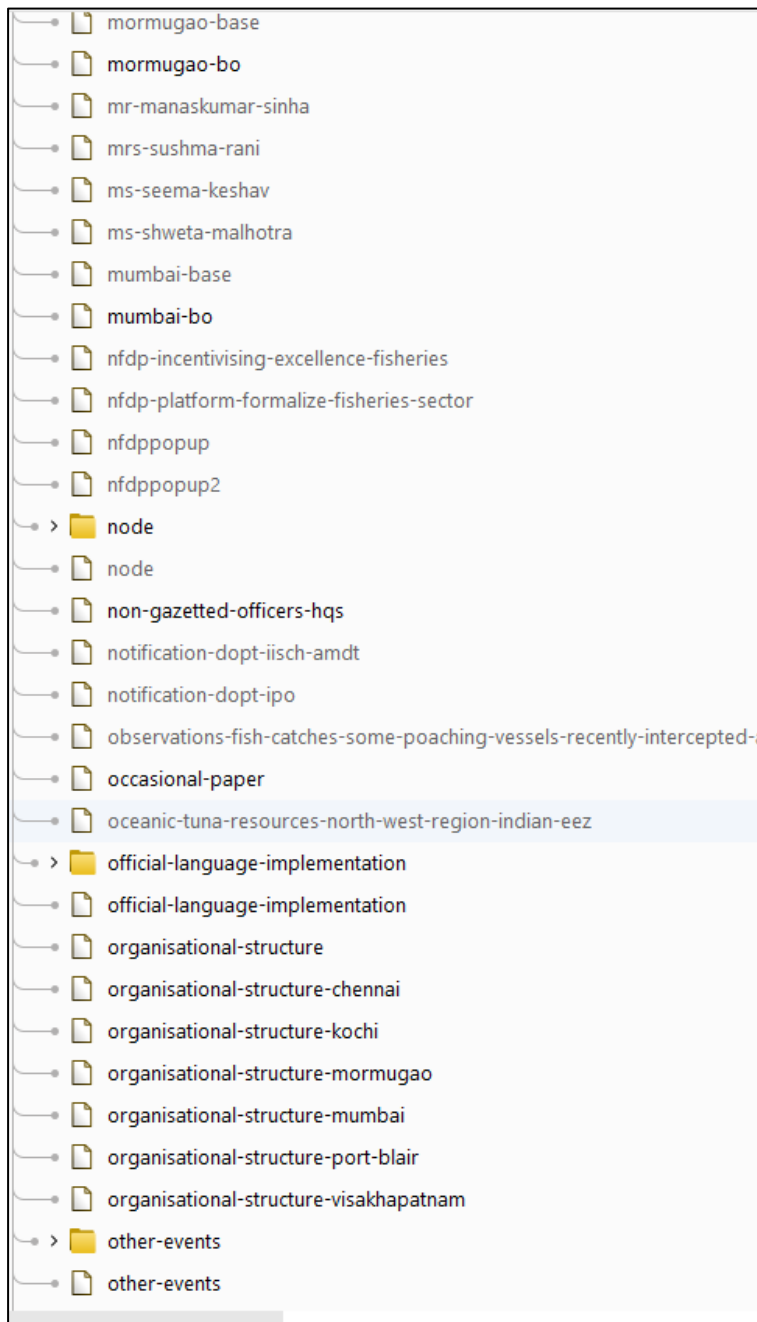
•	director
•	director-general-dgic
•	disclaimer
•	downloads
•	dr-annada-bhusan-kar
•	dr-ansuman-das
•	dr-h-d-pradeep
•	dr-jaya-chandra-dhas
•	dr-john-chembian
•	dr-raghab-p-dash
•	dr-sanjay-pandey
•	dr-sijo-p-varghese
•	dry-docking-repairs
•	duties-responsibilities
•	dy-director-general-engg
•	dy-director-general-fy
•	earned-medical-leave-forms
•	employees-against-whom-disciplinary-action
•	employees-against-whom-disciplinary-action,
•	employees-against-whom-disciplinary-action,%20Fishery%20Survey%20
•	> encrypt
•	> entity_reference_autocomplete
•	exploratory-squid-jigging-india-notes-biology-squid
•	extension-and-other-activities
•	faqs
•	> feedback
•	files-in-operation
•	files-in-operation,
•	files-in-operation,%20Fishery%20Survey%20of%20India,%20Department



































































































- meena-news,%20Fishery%20Survey%20of%20India,%20Department%20
- > member
- member
- mfv-blue-marlin
- mfv-lavanika
- mfv-matsya-darshini
- mfv-matsya-drushti
- mfv-matsya-nireekshani
- mfv-matsya-shikari
- mfv-matsya-varshini
- mfv-matsya-vrushti
- mfv-sagarika
- mfv-samudrika
- mfv-yellowfin
- ministry-department-who-s-who
- ministry-department-who-s-who,
- ministry-department-who-s-who,%20Fishery%20Survey%20of%20India,%20
- ministry-notifications
- minutes-of-meetings
- minutes-of-meetings,
- minutes-of-meetings,%20Fishery%20Survey%20of%20India,%20Departm
- > misc
- > modules
- mohini
- monthly-report-april-2023
- monthly-report-february-2023
- monthly-report-march-2023
- monthly-reports
- monthly-reports,
- monthly-reports,%20Fishery%20Survey%20of%20India,%20Department%
- mormugao-base



-  other-forms
-  page-not-found
-  paper-1-fishery-resources-indian-exclusive-economic-zone-special-refer
-  paper-1-observations-distribution-and-biology-indian-drift-fish-ariomm
-  paper-1-salient-observations-results-fishery-resources-survey-during-19
-  paper-1-some-observations-potential-fishery-resources-indian-exclusive
-  pf-advance-request-form
-  photo-gallery
- >  photo-gallery
-  photo-gallery,
-  photo-gallery,%20Fishery%20Survey%20of%20India,%20Department%20
-  pmmsy
-  port-blair-base
-  port-blair-bo
-  posn
-  present
-  privacy-policy
-  proceedings
-  proceedings,
-  proceedings,%20Fishery%20Survey%20of%20India,%20Department%20
-  procurement-details
-  procurement-details,
-  procurement-details,%20Fishery%20Survey%20of%20India,%20Departm
-  prof-sp-singh-baghel
- >  publications
-  publications
-  quarterly-report
-  quarterly-report-0
-  quarterly-report-march-2023
-  quarterly-reports
-  quarterly-reports-0

-  quarterly-reports
-  quarterly-return-on-deputation
-  quarterly-return-on-deputation,
-  quarterly-return-on-deputation,%20Fishery%20Survey%20of%20India,%20
- >  quickedit
-  rbe-2022-23
-  re-appropriation-funds-under-demand-43
-  recruitment
-  recruitment,
-  recruitment,%20Fishery%20Survey%20of%20India,%20Department%20o
- >  research-survey
-  research-survey
-  results-demersal-fisheries-resources-survey-along-east-coast-india-195
-  results-exploratory-fishing-conducted-during-1975-76
-  results-exploratory-fishing-conducted-during-1976-77
-  results-exploratory-fishing-conducted-during-1977-78
-  results-exploratory-fishing-conducted-during-1978-79
-  results-exploratory-survey-around-andaman-islands
-  revised-delegation-financial-powers-hodhoo-subordinate
-  rti-act-2005-english-hindi
- >  rti-disclosures
-  rti-disclosures
-  rti-disclosures,
-  rti-disclosures,%20Fishery%20Survey%20of%20India,%20Department%20o
-  rti-disclosures-headquarters
-  rti-disclosures-headquarters-0
-  rti-disclosures-headquarters-1
-  rti-fee-cost-rules
-  rti-fee-cost-rules-amendment
-  rti-fsi-info

-  rti-fsi-info,
-  rti-fsi-info,%20Fishery%20Survey%20of%20India,%20Department%20of%
-  rti-info-chennai
-  rti-info-kochi
- >  rti-info-transparency-audit
-  rti-notifications
-  rti-notifications,
-  rti-notifications,%20Fishery%20Survey%20of%20India,%20Department%20of%
-  rti-online-user-manual
-  rti-rules-2012
- >  run-cron
-  sathaanaantarana-0
- >  scientific-participation
-  scientific-participation
-  scientific-participation-visakhapatnam
-  scientist-participation-2022-23
-  scientist-participation-february-2023
-  scientist-participation-jan-2023
-  screen-reader-access
- >  search
-  section-officer-rti
-  security-policy
-  shb
-  shri-anil-verma
-  shri-ashish-kumar
-  shri-b-balanayak
-  shri-b-m-raut
-  shri-b-satheesh-kumar
-  shri-c-d-rao
-  shri-ch-bhaskar
-  shri-d-bhami-reddy

- shri-dharamvir-singh
- shri-e-ayooob
- shri-g-v-prasad
- shri-george-kurian
- shri-giriraj-singh
- shri-i-siddiqui
- shri-jacob-thomas
- shri-jacob-thomas-0
- shri-jai-krishna
- shri-kam-khan-suan
- shri-kumar-priyadarshi
- shri-m-subash
- shri-manoj-kumar-ot
- shri-mukesh
- shri-n-unnikrishnan
- shri-n-v-ramana-murthy
- shri-pankar-kumar
- shri-pratap-chandra-sarangi
- shri-raj-kumar-digvijay
- shri-rajendra-b-kokare
- shri-rajiv-ranjan-singh-alias-lalan-singh
- shri-s-kadam
- shri-s-kanthen
- shri-tiburtius
- shri-y-tharumar
- sitemap
- > sites
- smt-m-sreemathi
- smt-santosh-dalyan
- special-publications
- special-publications.

- special-publications,
- special-publications,%20Fishery%20Survey%20of%20India,%20Departm
- studies-fish-stock-assessment-indian-waters
- study-demersal-resources-wadge-bank-and-gulf-mannar
- sugundhi
- survey-fleet-1979-80
- survey-fleet-past
- survey-program-chennai
- survey-program-kochi
- survey-program-mormugao
- survey-program-mumbai
- survey-program-port-blair
- survey-program-visakhapatnam
- symposium-organized-ices-fao
- > taxonomy
- tender-chennai
- tender-chennai-0
- tenders
- terms-conditions
- test-operation
- > themes
- > token
- > toolbar
- totalpost
- training-programmes
- transparency-audit
- update.php
- vaarasaika-raipaorata-2010-11
- vaarasaika-raipaorata-2012-13
- vaarasaika-raipaorata-2013-14
- vaarasaika-raipaorata-2015-16

- vaarasaika-raiporata-2017-18
- > vessel-survey
- vessel-survey
- video-gallery
- > video-gallery
- video-gallery,
- video-gallery,%20Fishery%20Survey%20of%20India,%20Department%20
- visakhapatnam
- visakhapatnam-bo
- vishwa
- vision
- visit-b-sc-students-visakhapatnam-base-fsi-10012023
- visit-bfsc-students-vessel-mfv-matsya-varshini-06012023
- visitors
- visitors,
- visitors,%20Fishery%20Survey%20of%20India,%20Department%20of%20
- visitors-february-2023
- web-information-manger
- website-audit-certificates
- website-monitoring-plan
- whats-new
- > whoswho-zonal-offices
- workshop
- workshop-seminars-feb2023
- workshops-kochi-base-feb2023
- workshops-seminars-open-houses
- workshopseminarsymposium
- zonal-director-mormugao
- zonal-director-mumbai
- zonal-director-port-blair
- zonal-director-visakhapatnam

Appendix B: Description on Tools

Burp Suite Professional

Portswigger's Burp Suite Professional is an advanced set of tools for testing web security. Burp Suite offers the features for both manual and automated scans. Through Burp Suite, a user can intercept HTTP traffic, find hidden attack surface, assess strength of tokens, perform brute-forcing and fuzzing, construct CSRF exploits, modify HTTP messages, scan for common vulnerabilities including the OWASP Standard.

Acunetix Vulnerability Scanner

Acunetix is a web vulnerability scanner which is also a complete Website security testing solution that can be used both standalone and as part of complex environments. It offers built-in vulnerability assessment and vulnerability management, as well as many options for integration with market-leading software development tools.

GoBuster

GoBuster is a command line scanner that looks for existing or hidden web objects. It works by launching a dictionary attack against a web server and analyzing the response. GoBuster is used to brute-force URIs (directories and files) and DNS subdomains.

SQLMAP

SQLMAP is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.