

# Security Reconnaissance Report

## Target: soundcloud.org

Scan ID: 053169e5-88a5-4ba6-9653-e0744a038375

Date: 2025-04-23 02:28:58

Status: complete

## Executive Summary

Risk Score	Critical	High	Medium	Low	Total
High	0	10	2	1	13

## Domain Dns

### Domain Information

Domain	soundcloud.org
IP Address	34.120.95.14
Location	
Hosting	

### WHOIS Information

Registrar	Gandi SAS
Created	2007-05-15T17:21:04
Updated	2025-03-21T16:26:02
Expires	2026-05-15T17:21:04

## DNS Records

### A Records

34.120.95.14

### NS Records

ns-cloud-b4.googledomains.com.  
ns-cloud-b1.googledomains.com.  
ns-cloud-b2.googledomains.com.  
ns-cloud-b3.googledomains.com.

### TXT Records

"google-site-verification=HtQPPx-a8-y5eUHlXwKqpy1384jU17JNRIq6C\_Kl2iQ"

### SOA Records

ns-cloud-b1.googledomains.com. cloud-dns-hostmaster.google.com. 84 21600 3600 259200 300

## SSL/TLS Information

Issuer	Let's Encrypt
Subject	*.soundcloud.org
Valid Until	Jun 3 08:13:26 2025 GMT
Grade	A

## Tech Stack

### Server Information

Web Server	ESF
CMS	
Database	
Operating System	

### Frameworks

Vue.js

## Ports Network

### Open Ports

Port	Service
80	http
443	https

## Files Directories

### Sensitive Files

File	Sensitivity Level
------	-------------------

.git/HEAD	high
.env	high
.htaccess	low
robots.txt	low
sitemap.xml	low
config.php	high
wp-config.php	high
configuration.php	low
config.js	low
database.yml	high
settings.py	low
web.config	low
phpinfo.php	medium
info.php	medium
test.php	medium
server-status	low
server-info	low
crossdomain.xml	low
clientaccesspolicy.xml	low
composer.json	low
package.json	low
Dockerfile	low
docker-compose.yml	low
Jenkinsfile	low

## Discovered Directories

- admin
- administrator
- backup
- backups
- config
- dashboard
- db
- debug
- default
- dev
- files
- home
- images

- img
- install
- log
- login
- logs
- old
- panel
- private
- root
- secure
- security
- setup
- site
- staging
- temp
- test
- tmp
- upload
- uploads
- user
- users
- web
- wp-admin
- wp-content

## Api Endpoints

### API Configuration

Authentication	Unknown
CORS	Unknown
Swagger/OpenAPI	Not found
GraphQL	Not found

## Js Analysis

## Cloud Security

### Cloud Resources

S3 Buckets	2
Azure Blobs	0
Google Storage	2

Firebase Apps	0
CloudFront	0
Publicly Exposed	No

# Vulnerabilities

## Security Overview

Risk Score	High
Vulnerabilities	12
CVEs	0

## Vulnerabilities

Name	Severity	Description	Remediation
Open Redirect	Medium	Application allows open redirects	Validate redirects against a whitelist
CSRF Vulnerability	Medium	Application contains forms without CSRF tokens	Implement CSRF tokens for all state-changing operations
Information Disclosure	High	Application exposes sensitive information through profiles	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through folders	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through test pages	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through server status	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through server logs	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through error messages	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through configuration files	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through logs	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through error messages	Remove or restrict access to files containing sensitive information
Information Disclosure	High	Application exposes sensitive information through logs	Remove or restrict access to files containing sensitive information

# Email Credentials

## Email Addresses

- info@soundcloud.org
- contact@soundcloud.org
- admin@soundcloud.org
- support@soundcloud.org
- sales@soundcloud.org
- help@soundcloud.org

- webmaster@soundcloud.org
- security@soundcloud.org

## Exposed Data Types

Data Type	Count
Email Addresses	8
Passwords	0
Phone Numbers	0
Names	0
Addresses	0

## Recommendations

- Address all critical and high severity vulnerabilities immediately
- Implement CSRF tokens for all state-changing operations
- Remove or restrict access to sensitive files exposed on the web server
- Implement API authentication mechanisms
- Implement a Web Application Firewall (WAF) for additional protection
- Perform regular security assessments and penetration testing
- Set up security monitoring and logging
- Develop and maintain a security incident response plan
- Keep all software components and libraries up to date
- Apply the principle of least privilege across all systems