Sri Lanka Institute of Information Technology

Web Security – IE2062

Topic: Bug Bounty Report 2

Y2S2.WE.CS

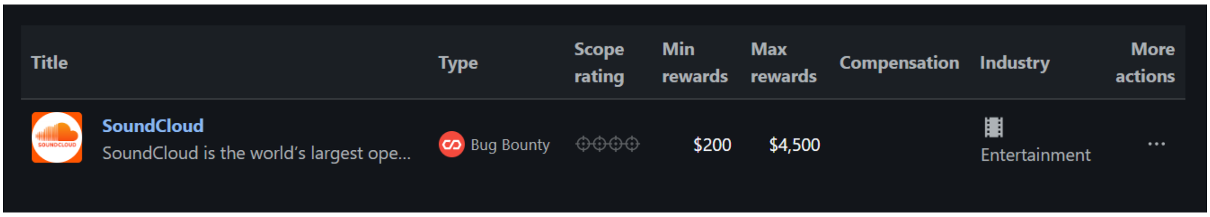
Name: S.D.W.Gunaratne

(IT23241978)

Table of Content

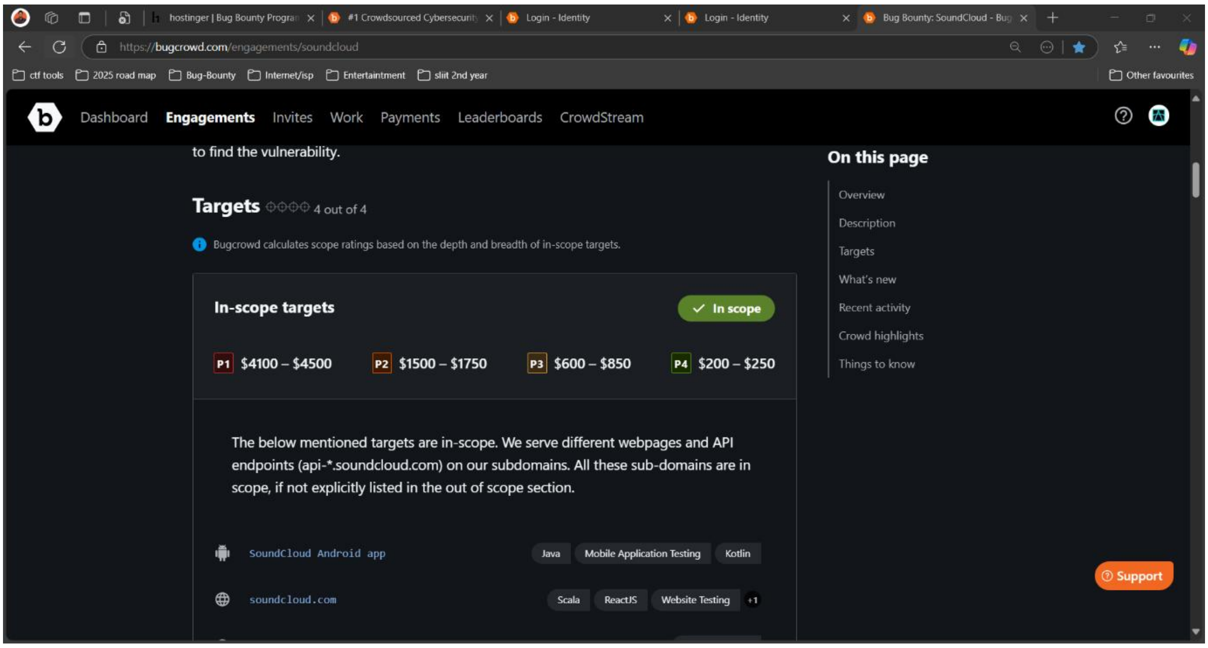
How I started?

1. Once I search from Bug crowd, I saw the SoundCloud bug bounty program.



Title	Type	Scope rating	Min rewards	Max rewards	Compensation	Industry	More actions
SoundCloud SoundCloud is the world's largest ope...	Bug Bounty	○○○○	$200	$4,500		Entertainment	⋯

2. Then, I discovered full main domain allowed for scope, so that I choose https://soundcloud.com .



to find the vulnerability.

Targets ○○○○ 4 out of 4

Bugcrowd calculates scope ratings based on the depth and breadth of in-scope targets.

In-scope targets ✓ In scope

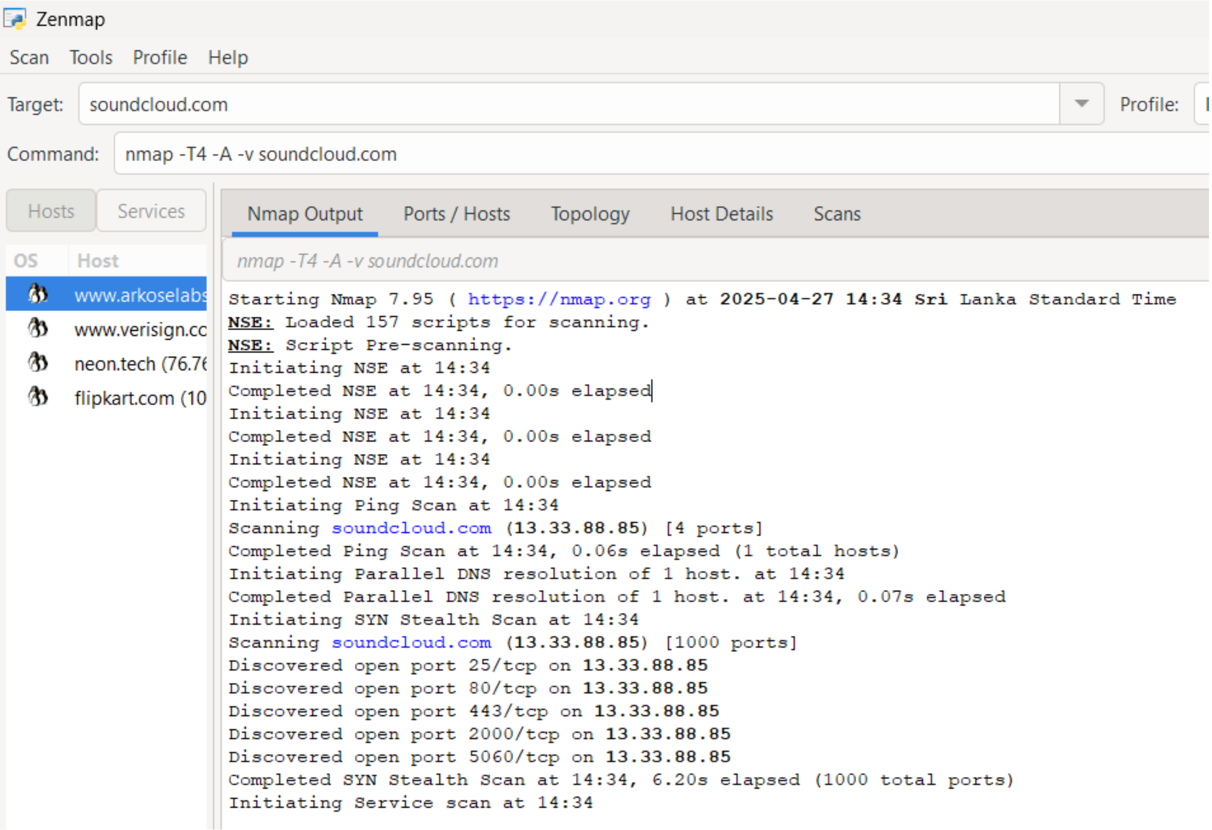
P1 $4100 – $4500 P2 $1500 – $1750 P3 $600 – $850 P4 $200 – $250

The below mentioned targets are in-scope. We serve different webpages and API endpoints (api-*.soundcloud.com) on our subdomains. All these sub-domains are in scope, if not explicitly listed in the out of scope section.

SoundCloud Android app	Java, Mobile Application Testing, Kotlin
soundcloud.com	Scala, ReactJS, Website Testing, +1

3. I use several methods/tools to do penetration testing.

4. First, I used Nmap. It helps me to find what are the open ports, Identify the web technologies such as webservers.



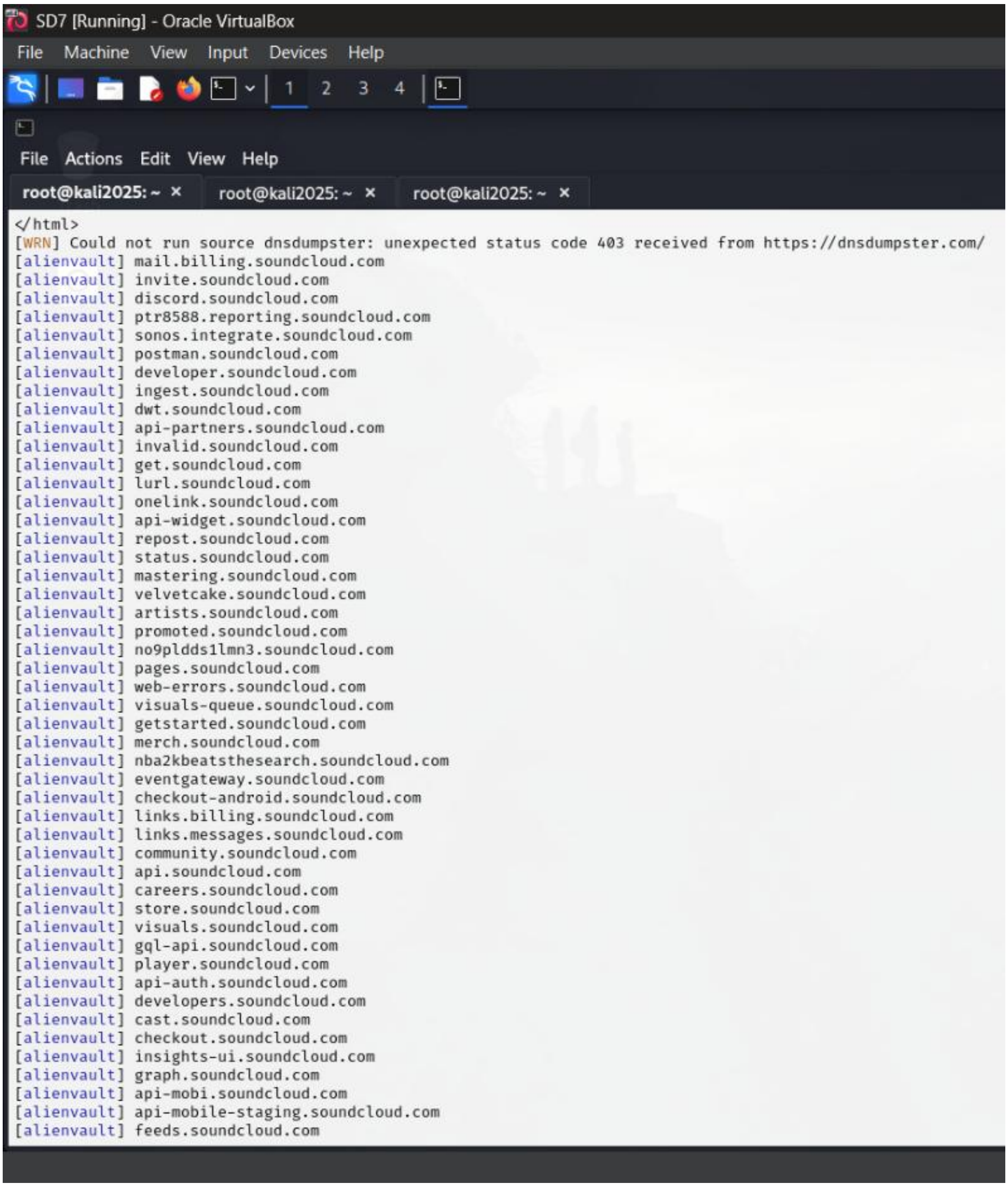
Target: soundcloud.com

Profile:

Command: nmap -T4 -A -v soundcloud.com

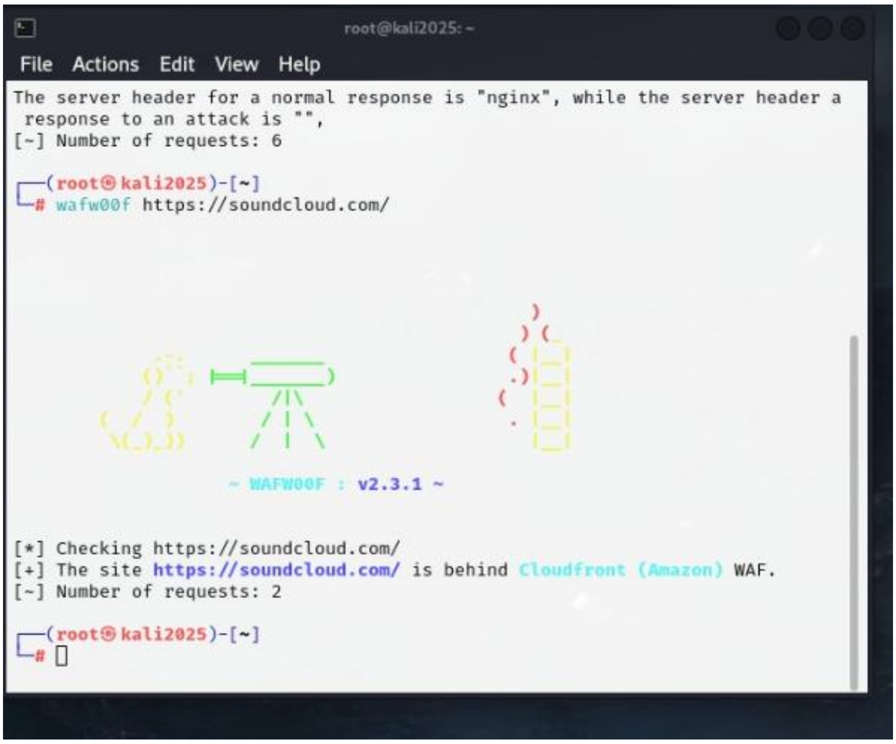
```
nmap -T4 -A -v soundcloud.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 14:34 Sri Lanka Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating Ping Scan at 14:34
Scanning soundcloud.com (13.33.88.85) [4 ports]
Completed Ping Scan at 14:34, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:34
Completed Parallel DNS resolution of 1 host. at 14:34, 0.07s elapsed
Initiating SYN Stealth Scan at 14:34
Scanning soundcloud.com (13.33.88.85) [1000 ports]
Discovered open port 25/tcp on 13.33.88.85
Discovered open port 80/tcp on 13.33.88.85
Discovered open port 443/tcp on 13.33.88.85
Discovered open port 2000/tcp on 13.33.88.85
Discovered open port 5060/tcp on 13.33.88.85
Completed SYN Stealth Scan at 14:34, 6.20s elapsed (1000 total ports)
Initiating Service scan at 14:34
```

5. Secondly, I used Subfider tool to find hidden or forgotten web asserts. Because hidden web assert can have poor security, unpatched vulnerabilities.


SD7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
root@kali2025: ~
root@kali2025: ~
root@kali2025: ~

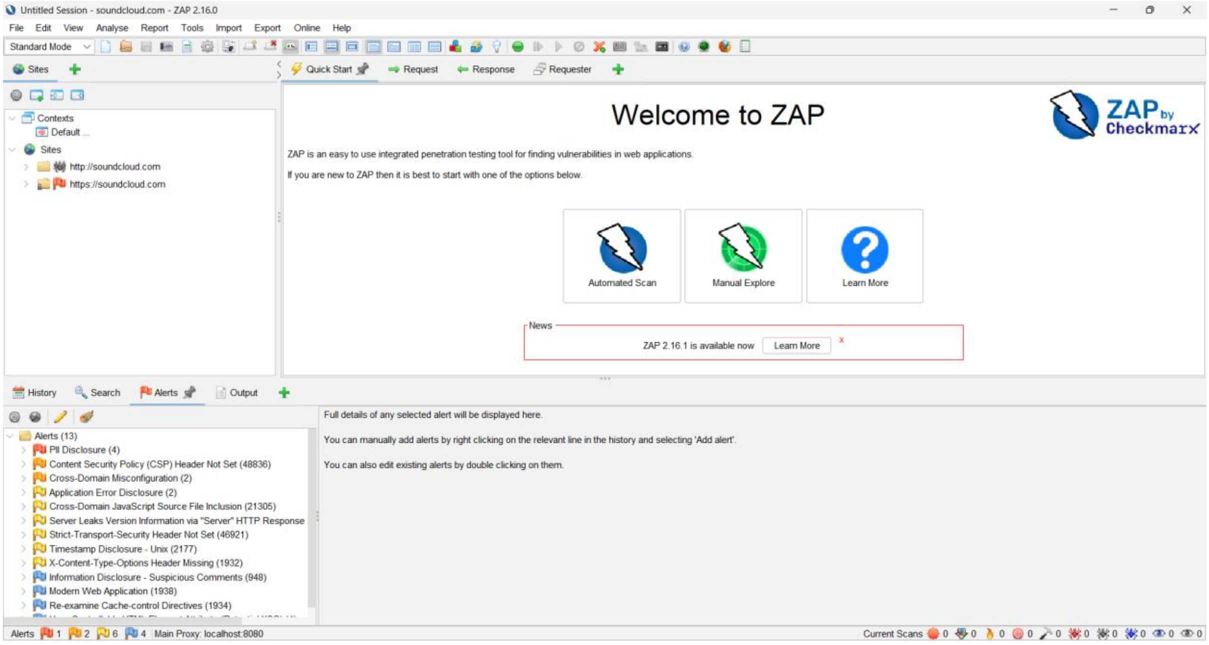
```
</html>
[WRN] Could not run source dnsdumpster: unexpected status code 403 received from https://dnsdumpster.com/
[alienvault] mail.billing.soundcloud.com
[alienvault] invite.soundcloud.com
[alienvault] discord.soundcloud.com
[alienvault] ptr8588.reporting.soundcloud.com
[alienvault] sonos.integrate.soundcloud.com
[alienvault] postman.soundcloud.com
[alienvault] developer.soundcloud.com
[alienvault] ingest.soundcloud.com
[alienvault] dwt.soundcloud.com
[alienvault] api-partners.soundcloud.com
[alienvault] invalid.soundcloud.com
[alienvault] get.soundcloud.com
[alienvault] lurl.soundcloud.com
[alienvault] onelink.soundcloud.com
[alienvault] api-widget.soundcloud.com
[alienvault] repost.soundcloud.com
[alienvault] status.soundcloud.com
[alienvault] mastering.soundcloud.com
[alienvault] velvetcake.soundcloud.com
[alienvault] artists.soundcloud.com
[alienvault] promoted.soundcloud.com
[alienvault] no9pldds1lmn3.soundcloud.com
[alienvault] pages.soundcloud.com
[alienvault] web-errors.soundcloud.com
[alienvault] visuals-queue.soundcloud.com
[alienvault] getstarted.soundcloud.com
[alienvault] merch.soundcloud.com
[alienvault] nba2kbeatsthesearch.soundcloud.com
[alienvault] eventgateway.soundcloud.com
[alienvault] checkout-android.soundcloud.com
[alienvault] links.billing.soundcloud.com
[alienvault] links.messages.soundcloud.com
[alienvault] community.soundcloud.com
[alienvault] api.soundcloud.com
[alienvault] careers.soundcloud.com
[alienvault] store.soundcloud.com
[alienvault] visuals.soundcloud.com
[alienvault] gql-api.soundcloud.com
[alienvault] player.soundcloud.com
[alienvault] api-auth.soundcloud.com
[alienvault] developers.soundcloud.com
[alienvault] cast.soundcloud.com
[alienvault] checkout.soundcloud.com
[alienvault] insights-ui.soundcloud.com
[alienvault] graph.soundcloud.com
[alienvault] api-mobi.soundcloud.com
[alienvault] api-mobile-staging.soundcloud.com
[alienvault] feeds.soundcloud.com
```

6. Thirdly, I used Wafwoof tool to find website is protected by a WAF (web application firewall). Because if WAF is active, so pen tester do their test without blocked, and they can do their testing with bypass WAF.



```
The server header for a normal response is "nginx", while the server header a
 response to an attack is "",
[~] Number of requests: 6

┌──(root㉿kali2025)-[~]
└─# wafw00f https://soundcloud.com/

                ~ WAFW00F : v2.3.1 ~

[*] Checking https://soundcloud.com/
[+] The site https://soundcloud.com/ is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

┌──(root㉿kali2025)-[~]
└─# 
```

7.Finaly, I use OWASP zap to automatically find the vulnerabilities.



Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.16.1 is available now

```
Alerts (13)
  PII Disclosure (4)
  Content Security Policy (CSP) Header Not Set (48836)
  Cross-Domain Misconfiguration (2)
  Application Error Disclosure (2)
  Cross-Domain JavaScript Source File Inclusion (21305)
  Server Leaks Version Information via "Server" HTTP Response
  Strict-Transport-Security Header Not Set (46921)
  Timestamp Disclosure - Unix (2177)
  X-Content-Type-Options Header Missing (1932)
  Information Disclosure - Suspicious Comments (948)
  Modern Web Application (1938)
  Re-examine Cache-control Directives (1934)
```

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

```
Alerts 1 2 6 4  Main Proxy: localhost:8080
```

With getting these tool’s support, I found below details about vulnerability.

2) Introduction

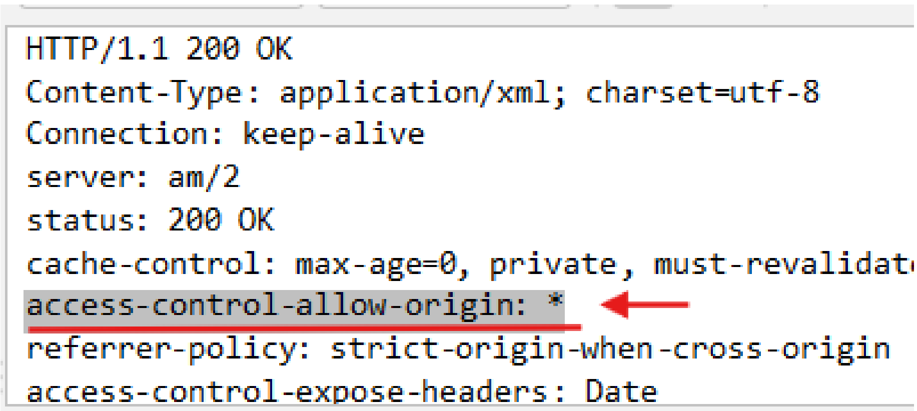
1.1 Domain	**https://soundcloud.com**
1.2 Severity	• Medium

3) Vulnerability

3.1 Vulnerability title	Cross-Domain Misconfiguration CWE-264 OWASP_2021_A01
3.2 Vulnerability description	**Alert description:** Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server. **Extra information:** The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third-party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address whitelisting. *Basic idea: a website's settings are messed up, letting other websites see data they shouldn't, even if the data was supposed to be somewhat protected.*
3.3 Affected components	Component: Web server/API Header: Access-Control-Allow-Origin: *

Issue Type: Cross-Origin Resource Sharing (CORS) Misconfiguration

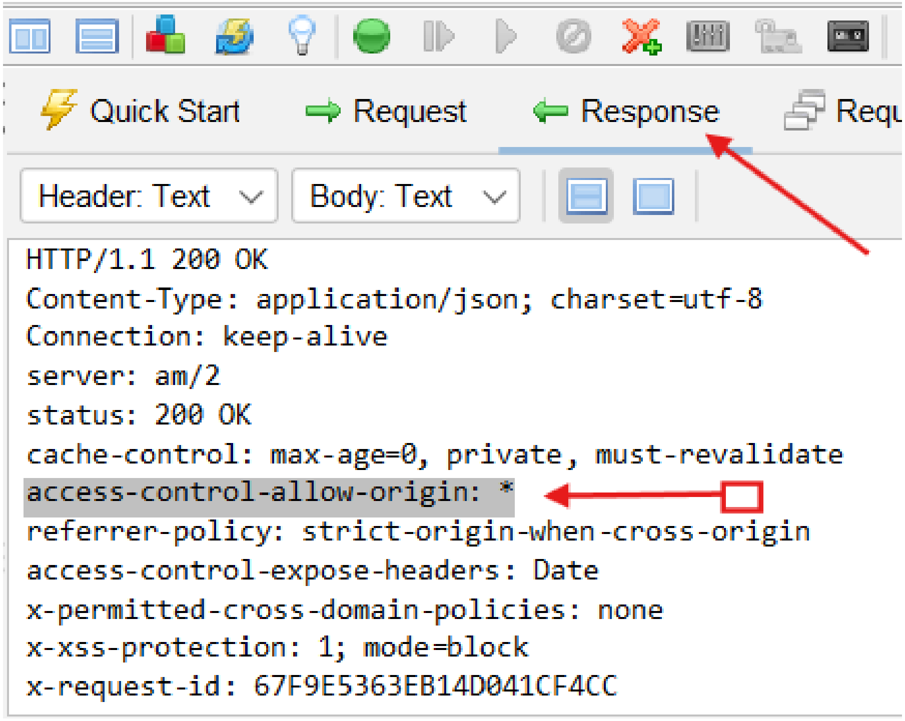
Location: Response headers from unauthenticated API endpoints



```
HTTP/1.1 200 OK
Content-Type: application/xml; charset=utf-8
Connection: keep-alive
server: am/2
status: 200 OK
cache-control: max-age=0, private, must-revalidat
access-control-allow-origin: *
referrer-policy: strict-origin-when-cross-origin
access-control-expose-headers: Date
```

(Picture shows, http response header with CORS misconfigurations)

3.4 Impact assessment



```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: keep-alive
server: am/2
status: 200 OK
cache-control: max-age=0, private, must-revalidate
access-control-allow-origin: *
referrer-policy: strict-origin-when-cross-origin
access-control-expose-headers: Date
x-permitted-cross-domain-policies: none
x-xss-protection: 1; mode=block
x-request-id: 67F9E5363EB14D041CF4CC
```

Above picture represent, server responds.

This allows any domain to make cross-origin read requests to unauthenticated API endpoints. While most browsers restrict cross-origin reads on authenticated endpoints, this misconfiguration:

	• Allows attackers to fetch public data from another origin • May expose data meant for internal or trusted usage only • Weakens the Same-Origin Policy (SOP) enforcement • Can be combined with other vulnerabilities for advanced attacks

3.5 Steps to reproduce	• Visit the site: https://soundcloud.com
	• Open the developer tools in browser
	• Go Network
	• Find the header
	• Confirm: “ Access-Control-Allow-Origin: * “
	• **Go to console and run this:**
	`fetch("https://soundcloud.com")`
	`  .then(res => res.text())`
	`  .then(data => console.log(data));`
	• If data can see, that means API is accessible cross-origin.

3.6 Proof of concept	**As a result, API data from the target domain is shown on another domain, proving the misconfiguration.**
3.7 Proposed mitigation or fix	Ensure that sensitive data is not available in an unauthenticated manner (using IP address whitelisting, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.