

## Bixi:

### Logging:

The app did not encrypt the username and password in JSON.

PII: username, password

RequestResponseConnectionTimingComment

authorization: Bearer  
4yNqPwqHKTgPnsIj3j8XLqFd+SXwhDCAHfrp4ZF6BQJzWjBZKd7gFsnJX99vp/uGuUK5MS7uZq0FRfrLG1D263DehNs+XPvVcoyqTc5XgR+q7rx6xeeMA=  
  
x-  
session: eyJhIjoIwZUzU2MmY1Yzc5NDIzMiIsImgiOnRydWUsIm50IiwWQ5ODk1My00NTRjLTQzZWYtOTYwNS0xNDEzMzYWRkN2EifQ==  
=  
accept-language: en\_US  
user-device: Google Android SDK built for arm64  
x-carrier: Android  
x-carrier-b64: QW5kcm9pZA==  
user-agent: com.eightd.biximobile:android:10:2025.33.3.1757612536  
x-locale-language: en  
x-locale-region: US  
x-device-density: 440  
x-design-id: X  
x-location: 0.0,0.0  
x-timestamp-ms: 1764119724934  
x-timestamp-source: ntp; age=488679  
x-polaris-api-key: TVRWQVBjX21vYmIsZTo4Q0p0b2pGS3Qke0RYIVdX  
x-polaris-authorization: empty  
x-polaris-mtvl-  
telemetry: app\_version:2025.33.3.1757612536,is\_location\_services\_enabled:true,is\_push\_notifications\_enabled:true  
is\_bike\_lanes\_layer\_enabled:true,is\_bike\_angels\_layer\_enabled:false  
x-polaris-ba-api-key: AwNEBWVGK215B403eUfYMLYr0LLJvXa1PHCLioN7qdZRBxqjQAYvcaEX5NjbpICz  
x-preferred-units: metric  
content-type: application/json;messageType=pb.ap1.endpoints.v1.lbs\_bff.ReadPolarisLogin2FARequest; charset=utf-8  
content-length: 85  
accept-encoding: gzip

JSONCopyEditReplaceView: auto

```
{
  "device_id": "320f562f5c794232",
  "password": "1234567",
  "username": "ays12345@gmail.com"
}
```

After the login request made, A separate request later was sent to Sentry. (3rd-party error and crash analytics service).

The app sends:exception logs, stack traces, view hierarchy,device model, OS version, timestamps, event IDs

RequestResponseConnectionTimingComment

POST https://o4507234886615040.ingest.us.sentry.io/api/4507297273479168/envelope/ HTTP/1.1  
User-Agent: sentry.java.android/8.11.0  
X-Sentry-Auth: Sentry  
sentry\_version=7,sentry\_client=sentry.java.android/8.11.0,sentry\_key=ce01246084b5366547c14f0d186fd650  
Content-Encoding: gzip  
Content-Type: application/x-sentry-envelope  
Accept: application/json  
Connection: close  
Host: o4507234886615040.ingest.us.sentry.io  
Accept-Encoding: gzip  
Content-Length: 3433

Raw [decoded gzip]CopyEditReplaceView: auto

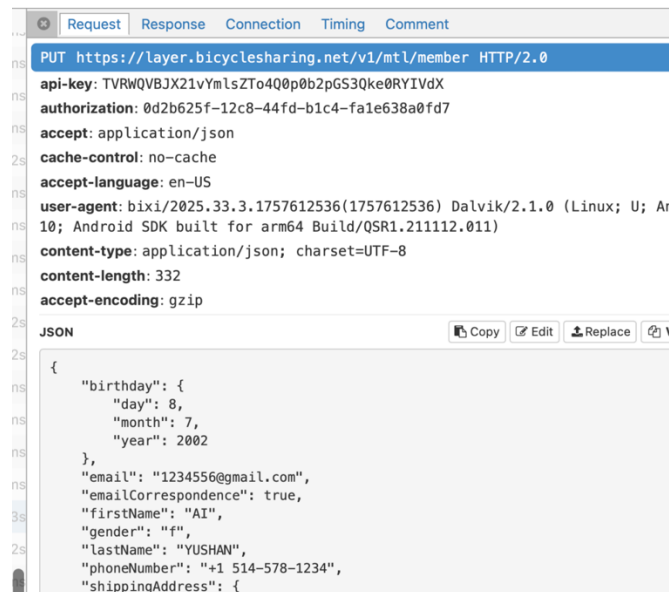
```
{
  "event_id": "df42d9f78e7a4e5c8f29f61e73620e5",
  "sdk": {
    "name": "sentry.java.android",
    "version": "8.11.0",
    "packages": [
      {
        "name": "sentry.java.android",
        "version": "8.11.0"
      }
    ]
  },
  "content_type": "application/json",
  "type": "event",
  "length": 17418,
  "timestamp": "2025-11-26T01:37:35.566Z",
  "exception": {
    "values": [
      {
        "type": "RecaptchaException",
        "value": "Site key invalid"
      }
    ]
  },
  "content_type": "application/json",
  "type": "session",
  "length": 260,
  "sid": "e6df3be176bc4749af4782f5dc02f172",
  "did": "c12477dd899a4b5a91760a53b13ca80b",
  "started": "2025-11-26T01:30:03.212Z",
  "content_type": "application/json",
  "filename": "view-hierarchy.json",
  "type": "attachment",
  "attachment_type": "event.view_hierarchy",
  "rendering_system": "android.view.system",
  "windows": [
    {
      "type": "com.android.internal.policy.DecorView",
      "width": 1080.0,
      "height": 2340.0
    }
  ]
}
```

More third parties:

- Google Firebase(send App version & configuration version)
- Google Recaptcha (payload is Binary protobuf — encrypted)
- Mapbox (send App version, Location permission level (“always allowed”), Whether location is enabled, Device info)
- Sentry

Edit profile:

PII exposure in the response payload: email, names, phone, tax region, billing, subscriptions...



The screenshot shows a web browser's developer tools with the 'Response' tab selected. It displays an HTTP PUT request to `https://layer.bicyclesharing.net/v1/mtl/member` with a status of 200. The request headers include `api-key`, `authorization`, `accept`, `cache-control`, `accept-language`, `user-agent`, `content-type`, `content-length`, and `accept-encoding`. The response is a JSON object containing personal information:

```
{
  "birthday": {
    "day": 8,
    "month": 7,
    "year": 2002
  },
  "email": "1234556@gmail.com",
  "emailCorrespondence": true,
  "firstName": "AI",
  "gender": "f",
  "lastName": "YUSHAN",
  "phoneNumber": "+1 514-578-1234",
  "shippingAddress": {
```

When opening ride history:

All the info in the response payload is not encrypted, include PII:

- number of previous rides
- Which stations I used
- Precise GPS coordinates of start and end
- Times, durations, distances, and costs
- Which specific bikes I rode

## Communato:

### Logging:

The app did not encrypt the username and password in JSON.

PII: username, password

The screenshot displays a network traffic analysis tool interface. On the left, a list of requests is shown with columns for Path, Method, Status, Size, and Time. The selected request is a POST to `https://foidentityprovider.reservauto.net/Login?Ret...` with a status of 302 and a size of 240b. The right pane shows the details of this request, including headers, cookies, and the response body. The response body is URL-encoded and contains a JSON payload with fields for `__RequestVerificationToken`, `ResetPassword`, `Username`, and `Password`. The `Username` and `Password` fields are visible in the response, indicating that the data is not encrypted.

Path	Method	Status	Size	Time
https://play.googleapis.com/log/batch	POST	200	2.0kb	89ms
https://oauthaccountmanager.googleapis.com/v1/s...	POST	200	709b	75ms
https://fcmtoken.googleapis.com/register	POST	200	478b	211ms
https://play.googleapis.com/log/batch	POST	200	2.0kb	63ms
https://oauthaccountmanager.googleapis.com/v1/s...	POST	200	708b	105ms
https://fcmtoken.googleapis.com/register	POST	200	478b	147ms
https://play.googleapis.com/log/batch	POST	200	2.0kb	64ms
https://play.googleapis.com/log/batch	POST	200	1.4kb	57ms
https://foidentityprovider.reservauto.net/cdn-cg/c...	POST	200	15.5kb	55ms
https://challenges.cloudflare.com/cdn-cg/challeng...	POST	200	159.3kb	132ms
https://attester.gateway.icloud.com/token-request?	POST	200	515b	66ms
https://challenges.cloudflare.com/cdn-cg/challeng...	POST	200	58.3kb	140ms
https://firebaseanalytics-pa.googleapis.com/v1/firel...	POST	200	664b	2s
https://challenges.cloudflare.com/cdn-cg/challeng...	POST	200	44.3kb	275ms
https://foidentityprovider.reservauto.net/cdn-cg/c...	POST	200	8.7kb	134ms
https://foidentityprovider.reservauto.net/Login?Ret...	POST	200	7.2kb	111ms
https://app-analytics-services.com/a	POST	204	1.3kb	55ms
https://foidentityprovider.reservauto.net/Login?Ret...	POST	302	209b	173ms
https://app-analytics-services.com/a	POST	204	543b	52ms
https://foidentityprovider.reservauto.net/Login?Pas...	POST	302	240b	207ms
https://foidentityprovider.reservauto.net/Login?Cus...	POST	302	225b	93ms

Request Details:

- Priority: u=0, i
- Accept-Encoding: gzip, deflate, br
- Accept-Language: zh-CN, zh-Hans;q=0.9
- Sec-Fetch-Mode: navigate
- Origin: null
- User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18\_7 like Mac OS X; communato; 2.10.1+2025100910) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
- Content-Length: 240
- Cookie: cf\_clearance=TDyC1XD\_ug4fpGAd2oCKUarBnE8SvqZew22xELVbLY-1764121633-1.2.1.1-njn807PPK3qZw\_mTVaetNSwVetxnjjeVwcy574dMA97FcZXRKSezkVHLIwJtYosq7gCbhA.wAKS\_MuNLVrMZAIP5JkaBqK3kfPaokzZ6LS89L19Yf9myL4V1bPwF.vRDHQL8sdn4AF09FcrPigeo dN43dIZwLB.NbBTUFEE4RRs\_hGwhZcyTDJ4TSkarZ7RRPgrr1WBuAKEB2xP4K2GfH8fj1HN9V8ghmUJrapuNxC8
- Cookie: .AspNetCore.AntiForgery.IZ-CHXtpVo=CTDJBANUsObZV6p8tE15rFdm1a7LElq1LFgh18GZ43oK6IzvepgJ1wrzP1e-KnotwFonBw1ZqeuoJFS3nPh4Xfqb4yPT56N51Gn2zZadFL9gusYcPzUmR3Y11UpYK2KhYppjPyNzn0SREVtQULDppe8
- Cookie: T1PM1s=67.7991688076778
- Cookie: x-ms-routing-name=sel
- Cookie: X-APP-ID=elNYcrxXTEK5TGpLCSxgV
- Cookie: X-APP-PACKAGE=com.communato.reservauto
- Cookie: X-APP-PLATFORM=iOS
- Cookie: X-APP-VERSION=2.10.1+2025100910
- Cookie: X-DEVICE-MODEL=iPhone14,5
- Sec-Fetch-Dest: document
- URL-encoded

Response Body (URL-encoded):

```
__RequestVerificationToken: cfdJBANUsObZV6p8tE15rFdm1a7LElq1LFgh18GZ43oK6IzvepgJ1wrzP1e-ResetPassword: 'false'Username: '645723'Password: '645723'
```

### Apps/Domains Contacted:

- Google Analytics (sent device model, OS version, app version, session ID)
- Google Notifications (polling suggests background/ language sync)

When opening profile: the data is not encrypted in the response payload:

PII exposure: email, names, phone, home address, emergency contacts....