Q 1/2: Is there a way for a hacker to access Daikibo's manufacturing status dashboard directly from the Internet?

1. Yes, they only need to steal the credentials of a Daikibo employee.
2. Yes, they can "brute-force" the authentication service and get in.
3. No, because Daikibo's employees follow perfect security guidelines and would never have allowed their credentials to get stolen.
4. **No, the attacker has no direct access to the status dashboard.**

You got it! In the original scope of the project we have listed that the dashboard will be living in Daikibo's Intranet. The only remote access to it would be through VPN tunnelling.

Q 2/2: Looking at the web\_requests.log - what is the user id with the most suspicious activity?

1. 5Eckr4DTaLLDaDMGqmMJ3g
2. **mdB7yD2dp1BFZPontHBQ1Z**
3. dBCm2JjBU815PB8zPDvKqv
4. rxExVoSitLbzzw1bTJwNuJ

Nailed it! It starts off with a regular login -> browsing of the dashboard. But then it turns into a regular, once-per-hour (see the timestamps) automated check of the statuses in all 4 factories with no page resources being loaded and with an obviously non-human punctuality.

**web\_requests.log**

2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T02:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T02:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T02:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T02:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T03:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T03:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T03:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T03:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T04:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T04:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T04:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T04:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T05:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T05:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T05:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T05:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T06:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T06:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T06:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T06:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T07:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T07:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T07:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T07:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T08:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T08:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T08:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T08:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T09:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T09:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T09:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T09:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T10:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T10:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T10:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T10:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T11:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T11:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T11:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T11:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T12:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T12:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T12:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T12:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T13:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T13:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T13:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T13:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T14:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T14:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T14:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T14:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T15:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T15:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T15:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T15:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T16:00:48.000Z GET "/api/factory/machine/status?factory=meiyo&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T16:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T16:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

2021-06-26T16:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=\*" {authorizedUserId: "mdB7yD2dp1BFZPontHBQ1Z"} 401 (UNAUTHORIZED)

**end**