

# Hack the Cookie

Author: Dorothy Spencer

Date: [02/12/2026]

Platform: HackerDNA

Difficulty: Very Easy Level

URL: <https://hackerdna.com/labs/hack-the-cookie>

## Objective:

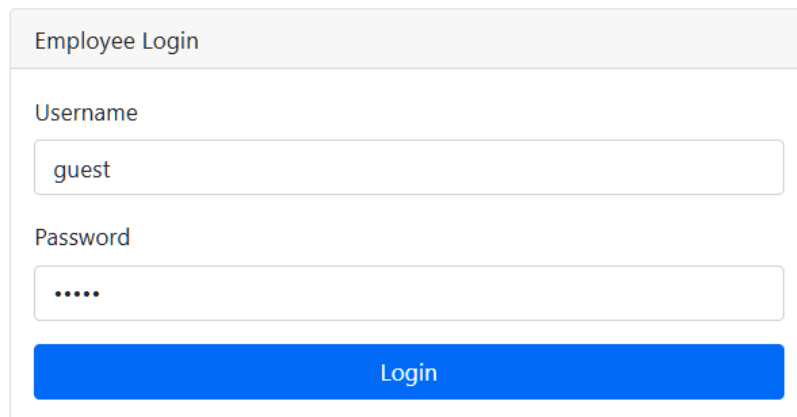
Manipulate the cookies to gain admin access to the site.

**Tool Needed:** [Base64](#)

Test Site being used in this scenario / documentation <https://hack-the-cookie.tiny.io> :

Objective: Try to obtain admin access to TechCorp

## TechCorp

A screenshot of a web form titled "Employee Login". It contains two input fields: "Username" with the text "guest" and "Password" with masked characters ".....". Below the fields is a blue "Login" button.

Employee Login

Username

guest

Password

.....

Login

## Click Login

**Open Developer Tools → Application → Cookies**

In your browser:

1. Press **F12**
2. Go to **Application** (Chrome) or **Storage** (Firefox)
3. Click **Cookies**
4. Select the site domain
  1. You will be looking for something with **user\_session**.  
If not, hit F5 to conduct a refresh of cookies and you should see the session now.

Application

Manifest

Service workers

Storage

Storage

- Local storage
- Session storage
- Extension storage
- IndexedDB
- Cookies
  - <https://hack-the-cookie.tiiny.io>
  - Private state tokens
  - Interest groups
- Bounce tracking mitigations
- Notifications
- Payment handler
- Periodic background sync
- Speculative loads
- Push messaging

| Name         | Value                                   | Dom...  | Path | Expir... | Size | Http... | Secure |
|--------------|---|---------|------|----------|------|---------|--------|
| PHPSESSID    | 8a60e92c9e01a40a17a63549ff39f4b7        | hack... | /    | Sessi... | 41   |         |        |
| user_session | eyJ1c2VyX2lkjoxL...CJ1c2VybmFtZSI6Im... | hack... | /    | 2026...  | 116  |         |        |

Cookie Value ☐ Show URL-decoded

eyJ1c2VyX2lkjoxL...CJ1c2VybmFtZSI6Imd1ZXN0liwicm9sZSI6Imd1ZXN0liwiZW1haWwiOiJndWVzdEB0ZWNoY29ycC5sb2NhbcCj9

Decode the cookie (Use [Base64 Encoder](#))

**BASE64** **Decode**

Decode and Encode **Encode**

Language: English Español Português Français Deutsch

Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

**Decode from Base64 format**

Simply enter your data then push the decode button.

eyJ1c2VyX2lkjoxL...CJ1c2VybmFtZSI6Imd1ZXN0liwicm9sZSI6Imd1ZXN0liwiZW1haWwiOiJndWVzdEB0ZWNoY29ycC5sb2NhbcCj9

Enter Cookie Value in this box

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

{ "user\_id": 1, "username": "guest", "role": "guest", "email": "guest@techcorp.local" }

Change "guest" to "admin"

This means you can **change the credentials** and the server will believe you.

Now **Encode** the new value:

The screenshot shows the 'BASE64 Decode and Encode' web application. At the top, there are tabs for 'Decode' and 'Encode', with 'Encode' selected and highlighted by a red box. Below the tabs, there's a language selector showing 'English' as the current language. A message states: 'Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to **encode** or decode your data.'

The main section is titled 'Encode to Base64 format' and includes the instruction: 'Simply enter your data then push the encode button.' Below this is a large text input area containing the JSON string: `{"user_id":1,"username":"guest","role":"admin","email":"guest@techcorp.local"}`.

Below the input area, there are several configuration options: a dropdown for 'Destination character set' set to 'UTF-8', a dropdown for 'Destination newline separator' set to 'LF (Unix)', and three unchecked checkboxes for 'Encode each line separately', 'Split lines into 76 character wide chunks', and 'Perform URL-safe encoding'. There is also a 'Live mode OFF' toggle and a red-bordered 'ENCODE' button. Below the button, the resulting Base64 encoded string is displayed: `eyJ1c2VyX2lkjoxLCJ1c2VybmFtZSI6Imd1ZXN0liwicm9sZSI6ImFkbWluliwiZW1haWwiOiJndWVzdEB0ZWNoY29ycC5sb2NhbCJ9`.

Paste the new value in your cookie session as seen in the next screen shot.

With the modified cookie in place now, we need to refresh the page (F5) to see if our elevated privilege to show as seen below.

After refreshing, the page should now display the admin access or link to log in.

This confirms that our cookie manipulation was successful and we've elevated our privileges from guest to admin.

The page will also show a flag that is needed to complete the course.

It should display below in RED.

The screenshot shows the 'TechCorp Internal Portal' interface on the left and a browser's developer tools on the right. In the portal, the 'Admin Panel' link is highlighted with a red arrow. Below it, a green box says 'Administrator access granted.' Underneath that, a red box labeled 'Sensitive Information' contains a red box with the text 'FLAG: 74'. A red arrow points from this flag to the 'user\_session' cookie in the browser's Application tab. The cookie's value is 'eyJ1c2VyX2lkjoiLC11c2VyYb...'. A red arrow points from this value to a text box in the portal. The text box contains the text 'FLAG: 74'. A red arrow points from this text box to the 'user\_session' cookie. The text box also contains the text 'FLAG: 74'. The text box also contains the text 'FLAG: 74'.

Quick Links

- Dashboard
- My Profile
- Documents
- Admin Panel

Administrator access granted.

Sensitive Information

FLAG: 74

Application

- Manifest
- Service workers
- Storage
  - Local storage
  - Session storage
  - Extension storage
  - IndexedDB
  - Cookies
    - https://hack-the-cookie.tiny.io
      - Private state tokens
      - Interest groups
      - Shared storage
      - Cache storage
      - Storage buckets
- Background services
  - Back/forward cache
  - Background fetch
  - Background sync
  - Bounce tracking mitigations
  - Notifications
  - Payment handler
  - Periodic background sync
  - Speculative loads
  - Push messaging
  - Reporting API
- Frames
  - top

| Name         | Value                        | D... | Pa... | Ex... | Size | Ht... | S |
|--------------|------------------------------|------|-------|-------|------|-------|---|
| PHPSESSID    | Ba60e92c9e01a40a17a6354...   | h... | /     | Se... | 41   |       |   |
| user_session | eyJ1c2VyX2lkjoiLC11c2VyYb... | h... | /     | 20... | 116  |       |   |

Paste the new cookie value here and click F5 to refresh page

Admin Rights now granted

No cookie selected  
Select a cookie to preview its value

Copy and paste this code in the required field indicated as in the below example.

The screenshot shows a challenge interface with a dark background. At the top, there are tabs for 'Flags Mode' and 'Learning Mode'. On the right, there are buttons for 'Official Solution' and 'Community Writeups'. The main area has a green box with the text 'OPEN THE TARGET AND FIND THE FLAGS'. Below this, there is a file icon and the text 'flag-user.txt'. A red arrow points from this text to a text input field. The input field contains the text 'XXXXXXXXXX\_XXXX\_XXXX\_XXXXXXXXXX'. To the right of the input field, there is a green button with a checkmark and the text 'Submit'. Above the 'Submit' button, there is a red arrow pointing to the text 'Then Click Submit'. To the right of the 'Submit' button, there is a green button with a plus sign and the text '+5 pts'. To the right of the '+5 pts' button, there is a yellow button with a gear icon and the text 'Upgrade Now'.

Flags Mode Learning Mode

Official Solution Community Writeups

OPEN THE TARGET AND FIND THE FLAGS

flag-user.txt

XXXXXXXXXX\_XXXX\_XXXX\_XXXXXXXXXX

Then Click Submit

Submit

+5 pts

Upgrade Now

It might be displayed prominently on the page or you might need to look around a bit to find it.