

Cookie Hacking

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

The image shows a screenshot of a web browser displaying a login page for 'TechCorp'. The page has a light gray header bar with the text 'Employee Login'. Below this, there are two input fields: 'Username' and 'Password'. The 'Username' field contains the value 'guest'. The 'Password' field contains the value '.....'. At the bottom of the form is a large blue rectangular button with the word 'Login' written in white. The entire form is contained within a white rectangular box with rounded corners.

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.

Screenshot of the Chrome DevTools Application tab showing cookies for the domain `https://hack-the-cookie.tiiny.io`. A red box highlights the cookie name `user_session`, and a red arrow points from the cookie value in the table to the URL in the sidebar.

Name	Value	Dom...	Path	Expir...	Size	Http...	Secure
PHPSESSID	8a60e92c9e01a40a17a63549ff39f4b7	hack...	/	Sessi...	41		
user_session	eyJ1c2VyX2lkjoxLCJ1c2VybmcFtZSI6Imd1ZXN0Iiwicm9sZSI6Imd1ZXN0IiwizW1haWwiOjJndWVzdEB0ZWNoY29ycC5sb2NhbcJ9	hack...	/	2026...	116		

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

Screenshot of the **BASE64** Decode and Encode tool. The **Decode** button is highlighted with a red box and a red arrow points to the input field where the cookie value is pasted.

Decode from Base64 format
 Simply enter your data then push the decode button.

eyJ1c2VyX2lkjoxLCJ1c2VybmcFtZSI6Imd1ZXN0Iiwicm9sZSI6Imd1ZXN0IiwizW1haWwiOjJndWVzdEB0ZWNoY29ycC5sb2NhbcJ9
 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.

Source character set: UTF-8
 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 a green-themed web application for Base64 encoding. At the top, there are two buttons: 'Decode' and 'Encode', with 'Encode' being highlighted by a red box. Below the buttons, a message says: '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.' To the right, language options are listed: English, Español, Português. The main section is titled 'Encode to Base64 format' and contains a text input area with the JSON string: {"user_id":1,"username":"guest","role":"admin","email":"guest@techcorp.local"}. Below the input area, a note says: 'To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.' There are several configuration options: 'UTF-8' (selected) and 'LF (Unix)' for character set and newline separator respectively; checkboxes for 'Encode each line separately', 'Split lines into 76 character wide chunks', and 'Perform URL-safe encoding'; and a 'Live mode OFF' button with a note about real-time encoding support. The 'ENCODE' button at the bottom is also highlighted with a red box. The resulting encoded output is shown in a text area below: eyJ1c2VyX2lkIjoxLCJ1c2VybmcFtZSI6Imd1ZXN0Iiwicm9sZSI6ImFkbWluliwiZW1haWwiOiJndVVzdEB0ZWNoY29ycC5sb2NhCJ9.

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 a browser window with the following elements:

- TechCorp Internal Portal** (Title bar)
- guest@techcorp.local Logout** (User info)
- Quick Links** (Dashboard, My Profile, Documents, Admin Panel)
- Admin Panel** (highlighted with a red arrow)
- Administrator access granted.** (Message in a green box)
- Sensitive Information** (Section)
- FLAG:** **74** (Flag value highlighted with a red box and arrow)
- Application Tab (Developer Tools)**
 - Cookies** section:
 - https://hack-the-cookie.tiny.io
 - Private state tokens
 - Interest groups
 - Shared storage
 - Cache storage
 - Storage buckets
 - Background services** section:
 - Back/forward cache
 - Background fetch
 - Background sync
 - Bounce tracking mitigations
 - Notifications
 - Payment handler
 - Periodic background sync
 - Speculative loads
 - Push messaging
 - Reporting API
 - Frames** section:
 - top
- Console Tab (Developer Tools)**

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 the following elements:

- Flags Mode** (Mode button)
- Learning Mode** (Mode button)
- Official Solution** (Link)
- Community Writeups** (Link)
- OPEN THE TARGET AND FIND THE FLAGS** (Instruction)
- flag-user.txt** (Flag name)
- Submit** (Submit button)
- +5 pts** (Points)
- Then Click Submit** (Text)
- Upgrade Now** (Link)

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