



Saint Columban College
College of Computing Studies
Pagadian City



Cookies

Cookies 



Easy **Web Exploitation** **picoCTF 2021**

AUTHOR: MADSTACKS

Description

Who doesn't love cookies? Try to figure out the best one.
Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is:

NOT_RUNNING

Launch Instance

Hints

(None)

100,352 users solved

 63%
 Liked

 picoCTF{FLAG}

**Submit
Flag**

Author: The Analyst: Hyposelenia

Challenge: Cookies

Category: Web Exploitation

Date: 02/15/26



Saint Columban College
College of Computing Studies
Pagadian City



I. Objective

The objective of this challenge is to understand how browser cookies work, how they can be manipulated, and how improper handling of cookies in web applications can lead to security vulnerabilities that expose sensitive information such as hidden flags.

II. Background

Cookies are small pieces of data stored by websites in a user's browser. They are commonly used to remember user preferences, session information, or progress within a website. While cookies are helpful, they can become a security risk if a website **trusts user-controlled cookies without proper server-side validation**.

In web exploitation challenges, cookies are often used to demonstrate how attackers can modify client-side data to trigger unintended behavior in a web application. This challenge focuses on recognizing patterns in cookie values and exploiting weak logic tied to those values.

III. Tool Used

- **Web Browser (Google Chrome)** – Used to access the challenge website
- **Browser Developer Tools (Inspect)** – Used to view and modify cookies

IV. Methodology

1. Launched the challenge instance.

[NOT_RUNNING](#)

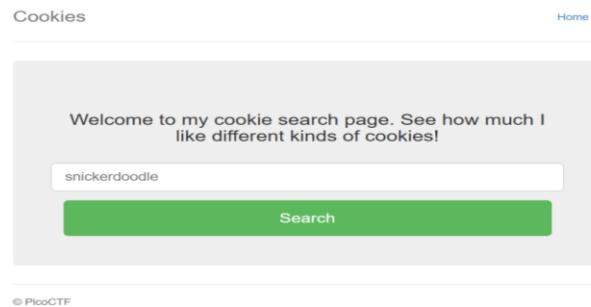
[Launch Instance](#)



Saint Columban College
College of Computing Studies
Pagadian City

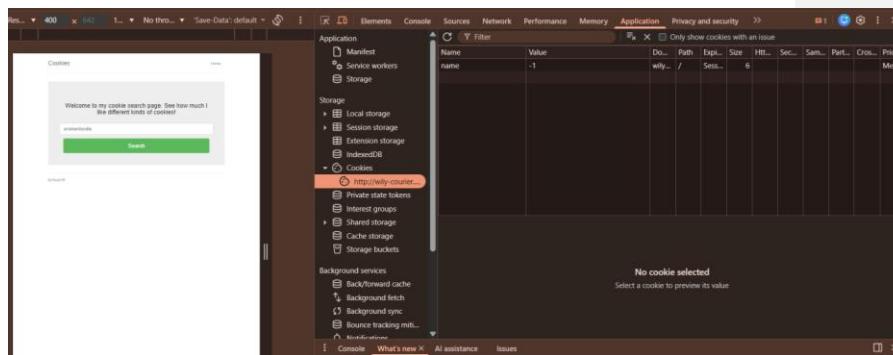


2. Copied the provided URL and accessed it using a web browser.
3. Explored the website and observed the search input field.



A screenshot of a web browser showing a search interface. The title bar says "Cookies". The main content area has a heading "Welcome to my cookie search page. See how much I like different kinds of cookies!" Below it is a search input field containing "snickerdoodle" and a green "Search" button. At the bottom left, it says "© PicoCTF".

4. Noticed that the challenge title referenced “Cookies,” suggesting the use of browser cookies.
5. Right-clicked the page and opened **Inspect (Developer Tools)**.
6. Navigated to the **Application** tab and selected **Cookies** for the website.



A screenshot of the browser's developer tools, specifically the Application tab under Cookies. It shows a list of cookies, including one named "name" with a value of "-1". The "Storage" section is also visible, showing local storage, session storage, and other items. A tooltip "https://willy-copper.com" points to the cookie entry. The status bar at the bottom indicates "No cookie selected".

7. Observed a cookie where the name value was initially set to -1, even before any input was provided.

Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Same...	Cross...	Prio...
name	-1	willy...	/	Sess...	6					Med...



Saint Columban College
College of Computing Studies
Pagadian City



8. Entered the word “**snickerdoodle**” into the search box and clicked the search button.
9. Noticed that the cookie value changed from -1 to 0.

Name	Value
name	0

10. Manually modified the cookie value from 0 to 1 and refreshed the page.

Name	Value
name	1

11. Observed that the displayed cookie name on the site changed.

Commented [Z.1]:

Name	Value
name	1

12. Continued incrementing the cookie value (2, 6, 7, and onward), refreshing the page each time.
- 13.



Saint Columban College College of Computing Studies Pagadian City



The screenshots show the browser's Application tab with the Storage panel open, specifically the Cookies section. The cookie 'name' is being modified across three different sessions.

- First Session:** Shows a cookie value of 2. The webpage content says "I love oatmeal raisin cookies!"
- Second Session:** Shows a cookie value of 6. The webpage content says "I love whoopie pie cookies!"
- Third Session:** Shows a cookie value of 7. The webpage content says "I love sugar cookies!"

14. Reached a cookie value of **18** and refreshed the page.

The screenshot shows the browser's Application tab with the Storage panel open, specifically the Cookies section. A cookie named 'name' has a value of 18. The webpage content is not visible in this specific screenshot, but the cookie value is clearly displayed in the developer tools.

15. Observed that instead of a cookie name, the **flag was displayed directly on the webpage**.



Saint Columban College
College of Computing Studies
Pagadian City



The screenshot shows a browser window with the title 'Cookies'. Inside the window, there is a message box with the word 'Flag:' followed by the flag value 'picoCTF{3v3ry1_l0v3s_c00k135_a4dadb49}'. Below the window, the browser's developer tools are visible, specifically the 'Storage' section under the 'Application' tab. A single cookie named 'name' is listed with the value '18'. The browser interface includes standard controls like zoom and refresh, and tabs for Elements, Console, Sources, Network, and Performance.

16. Retrieved and submitted the flag.

V. Result

picoCTF{3v3ry1_l0v3s_c00k135_a4dadb49}

This screenshot shows the same 'Cookies' challenge page from the previous step. The message box now displays the retrieved flag: 'Flag: picoCTF{3v3ry1_l0v3s_c00k135_a4dadb49}'. The footer of the page includes the copyright notice '© PicoCTF'.

VI. Explanation

Think of a cookie like a **sticky note** a website puts in your browser. The sticky note might say:

- “*You are on cookie number 0*”
- “*You are on cookie number 1*”
- “*You are on cookie number 2*”

The website reads this sticky note to decide what to show you.



Saint Columban College
College of Computing Studies
Pagadian City



In this challenge, the website **trusted the sticky note completely**. By changing the number on the note, we could tell the website to jump ahead—until it accidentally showed the secret flag.

Now you wondered, what did the cookie did in this challenge?

- *The cookie value acted like a **counter** or **index***
- *Each number corresponded to a different message or cookie name*
- *When the value reached **18**, the application revealed the flag*

This means the website relied entirely on **client-side cookie values** to control behavior.

Now, Cookies are stored in the browser, which means:

- Users can view them
- Users can modify them
- Attackers can exploit them

If a website uses cookies to control sensitive logic (such as access levels, secrets, or progression), attackers can manipulate those cookies to bypass restrictions.

I'll give you a real-life scenario:

Imagine logging into Facebook on a **public computer**:

- Facebook stores your session in a cookie
- If you forget to log out, the cookie remains
- Another person opens Inspect, reuses your session cookie
- They access your account **without knowing your email or password**

This is why cookies must be:

- Properly secured
- Expired correctly



Saint Columban College
College of Computing Studies
Pagadian City



- Validated on the server side

So, the purpose of the challenge?

This challenge teaches:

1. How cookies work
2. How cookies can be inspected and modified
3. Why trusting client-side data is dangerous
4. How attackers exploit weak cookie logic

This is a classic example of:

Insecure Client-Side State Management

VII. Conclusion

The Cookies challenge demonstrates how improper use of browser cookies can expose sensitive information. By manipulating a cookie value that controlled application behavior, the flag was revealed without exploiting any complex vulnerabilities. This highlights the importance of server-side validation, secure session handling, and cautious use of cookies in web applications. Understanding cookie-based vulnerabilities is essential for both secure web development and effective web exploitation.

— The Analyst: Hyposelenia