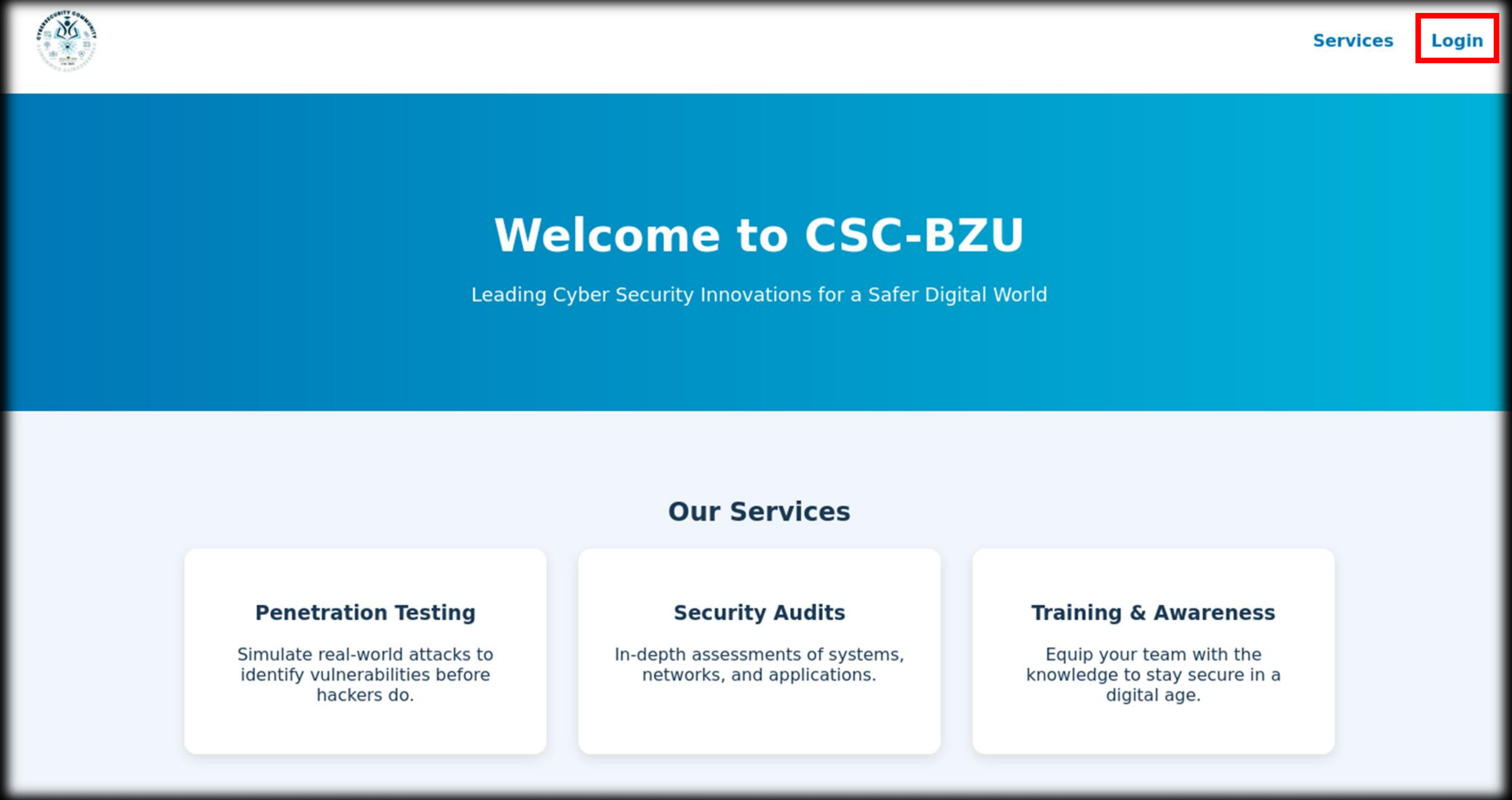
GUESSION CHALLENGE WALKTHROUGH

WRITTEN BY:
TALEEN SKAFI

BZU - CSC

Welcome to **Guession**, a web security challenge that dives into the risks of insecure session management and privilege escalation through predictable identifiers. In this scenario, you start with valid credentials for a low-privileged user named Jack. After logging in, you notice something unusual, the URL contains a sid parameter. Curious, you decode it and find a format like session_1001, hinting at a simple, sequential session ID system. With just a small change (switching it to session_1000) , you suddenly gain access to the admin account. No password guessing, no login bypass , just a well-timed observation and a predictable token. This challenge is a reminder of how critical it is to handle sessions securely, because even small implementation flaws can lead to full compromise.

When we open the challenge, we see a web page with some services and a login button. We click on the login button to discover the login portal.



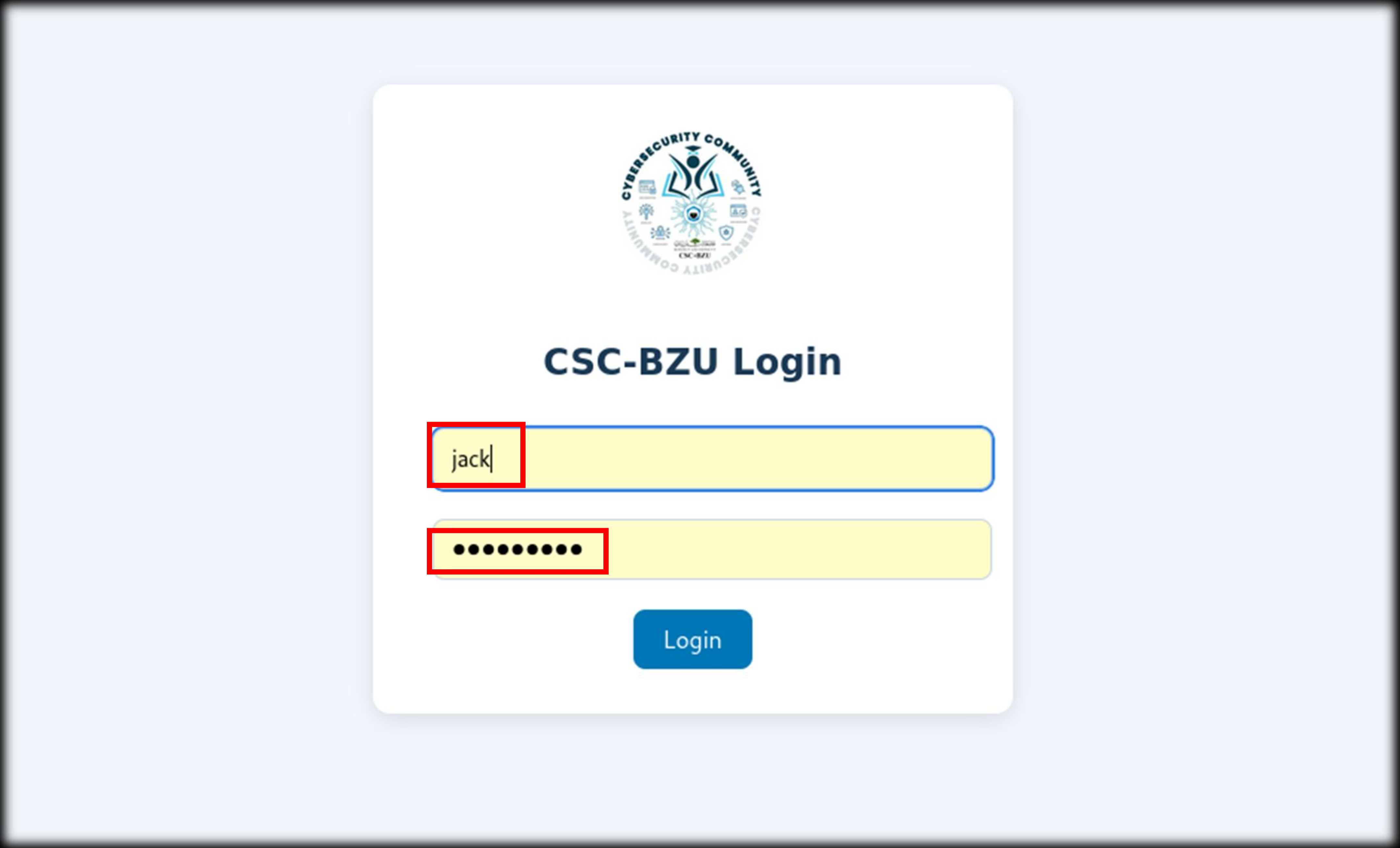
Welcome to CSC-BZU

Leading Cyber Security Innovations for a Safer Digital World

Our Services

Penetration Testing	Security Audits	Training & Awareness
Simulate real-world attacks to identify vulnerabilities before hackers do.	In-depth assessments of systems, networks, and applications.	Equip your team with the knowledge to stay secure in a digital age.

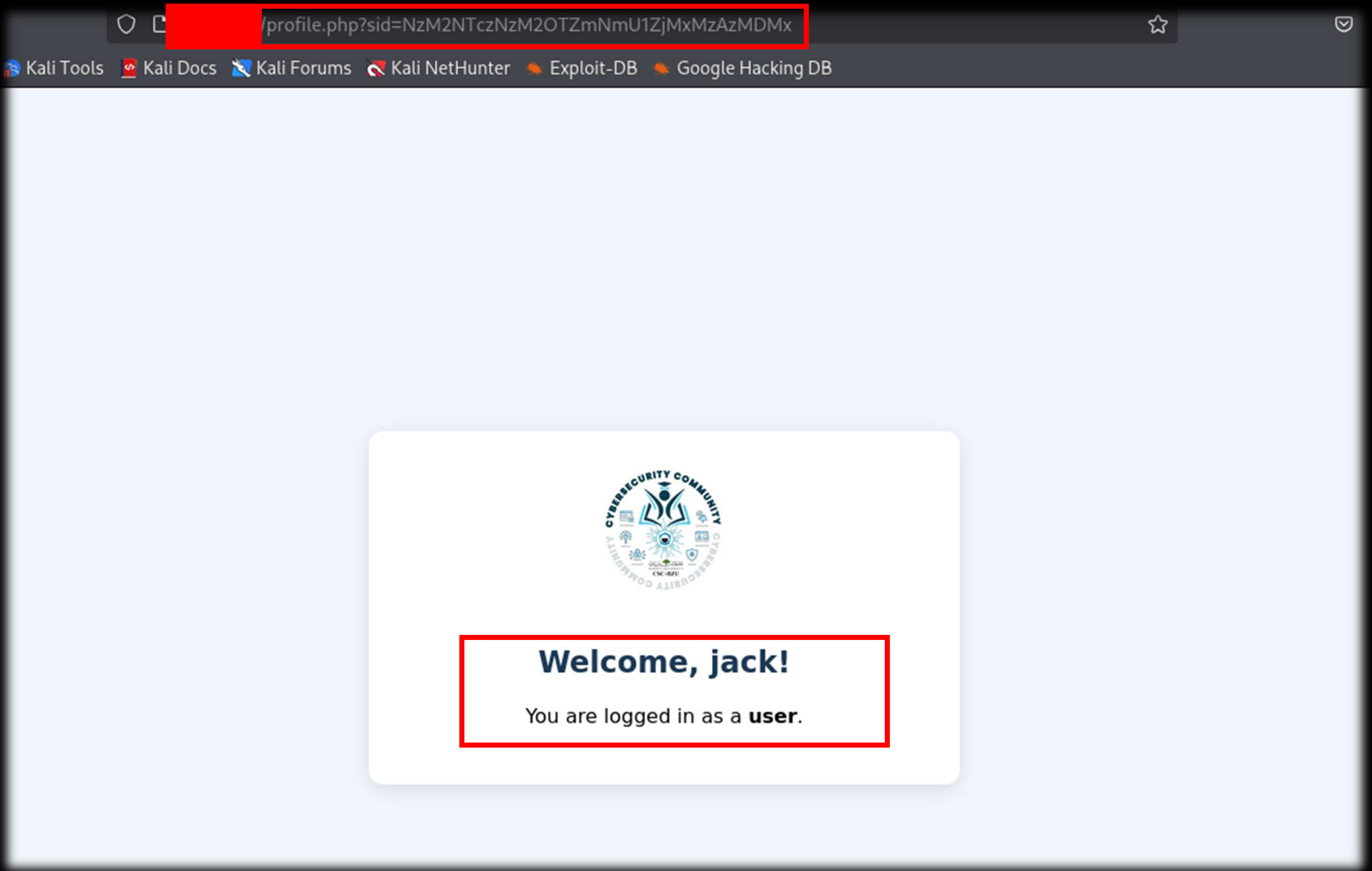
We’re now on the login portal, so let’s enter the provided credentials for **Jack** to sign in.


CSC-BZU Login

jack

••••••••••

Now that we're logged in as the user **Jack**, we notice a **sid** parameter in the URL. Let’s copy it and use **CyberChef** to decode it and see what it contains.

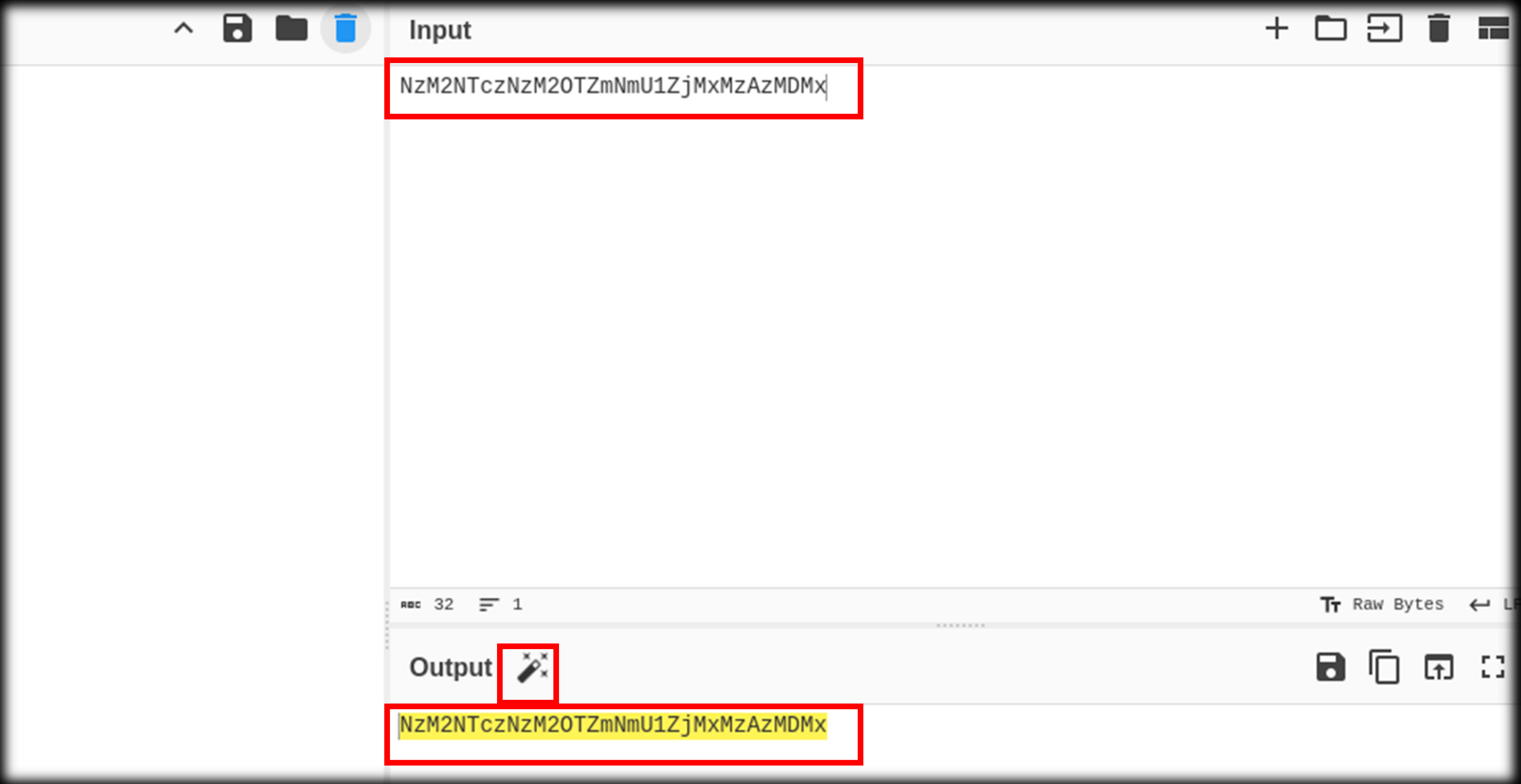


[redacted]/profile.php?sid=NzM2NTczNzM2OTZmNmU1ZjMxMzAzMDMx

Welcome, jack!

You are logged in as a **user**.

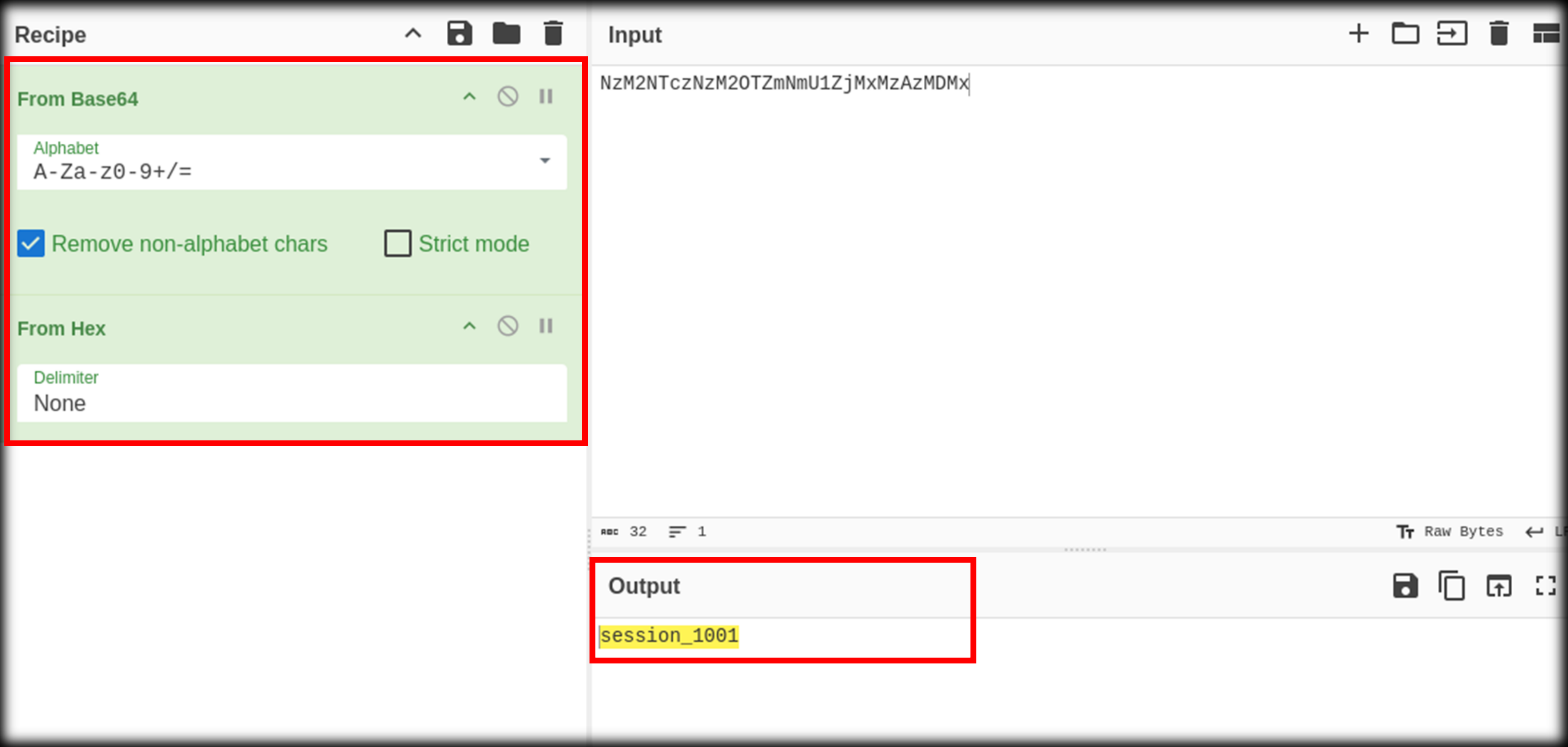
After pasting the value into **CyberChef** and clicking the Magic wand icon, we see that the data is first encoded in **Hex** and then in **Base64**.



```
NzM2NTczNzM2OTZmNmU1ZjMxMzAzMDMx
```

```
NzM2NTczNzM2OTZmNmU1ZjMxMzAzMDMx
```

Once the text decoded, it reveals the string: **session_1001**:



From Base64

Alphabet: A-Za-z0-9+/=

[✓ Remove non-alphabet chars] Strict mode

From Hex

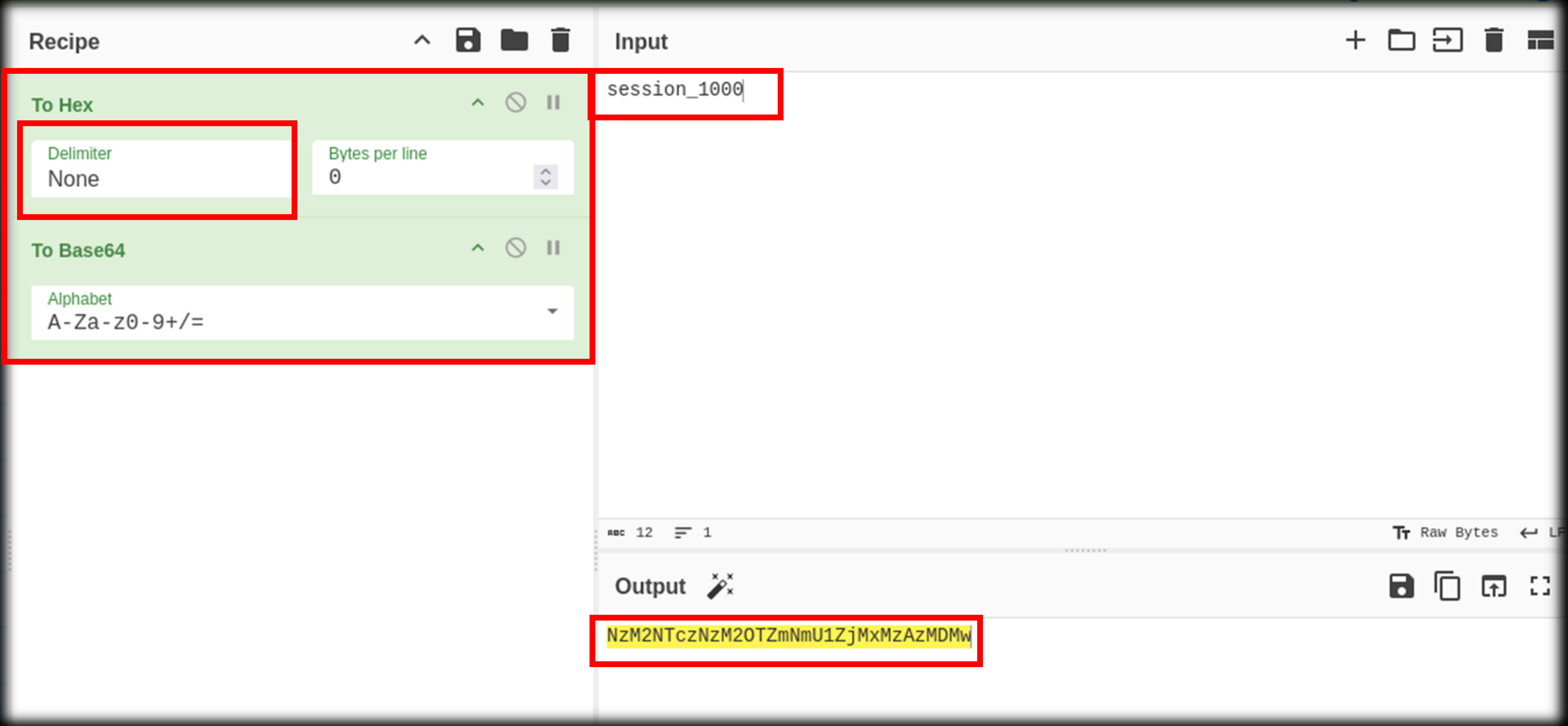
Delimiter: None

```
NzM2NTczNzM2OTZmNmU1ZjMxMzAzMDMx
```

abc 32 ≡ 1

```
session_1001
```

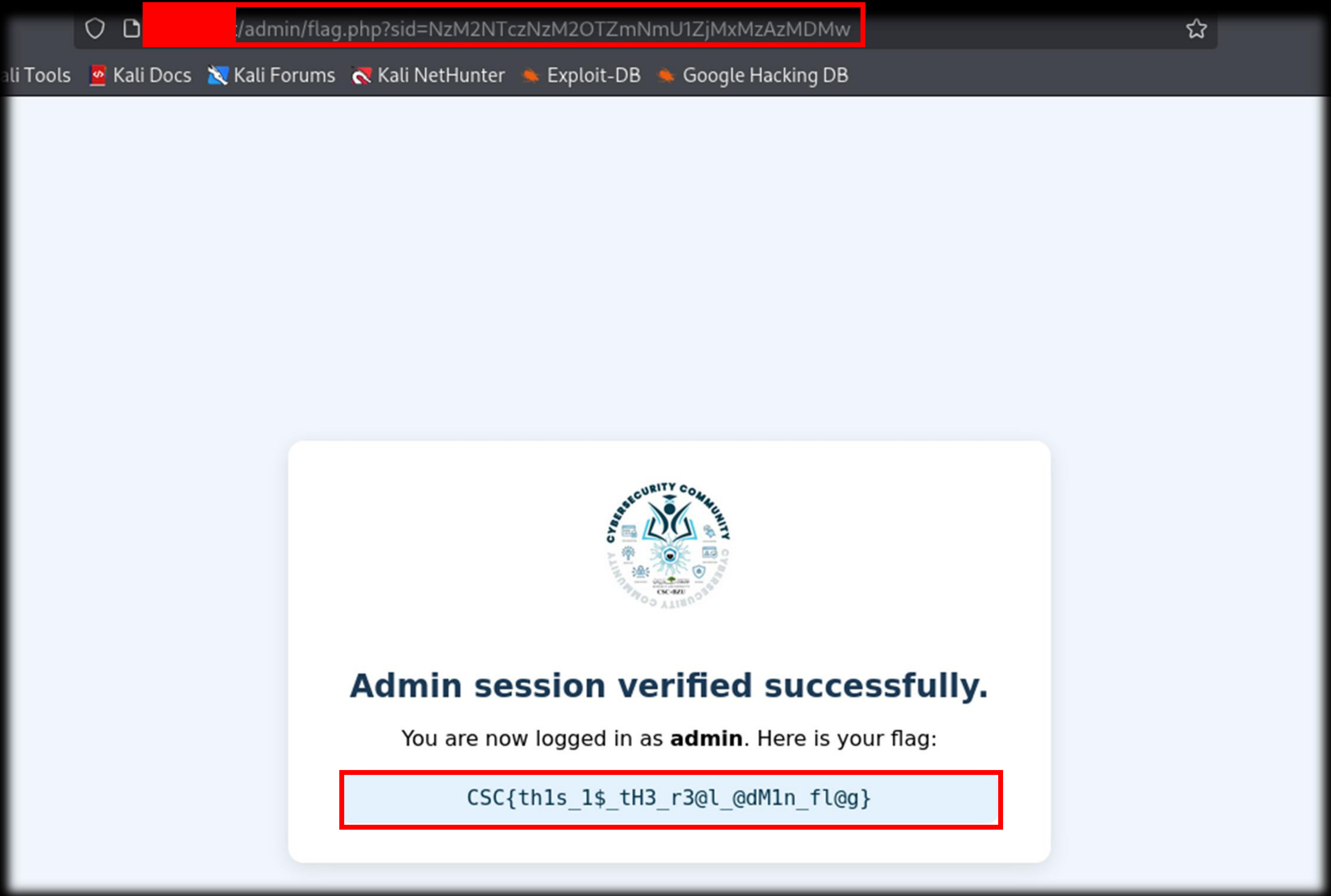
The value session_1001 suggests that the session IDs might be sequential. Let's try changing **1001** to **1000** in the decoded string, re-encode it, and see if it gives us access to another user's page.



```
session_1000
```

```
NzM2NTczNzM2OTZmNmU1ZjMxMzAzMDMw
```

After updating the sid in the URL with the re-encoded **session_1000** value, we refresh the page and it logs us in as the admin. Just like that, we've gained access to the admin panel and captured the flag.



[redacted]/admin/flag.php?sid=NzM2NTczNzM2OTZmNmU1ZjMxMzAzMDMw

Admin session verified successfully.

You are now logged in as **admin**. Here is your flag:

```
CSC{th1s_1$_tH3_r3@l_@dM1n_fl@g}
```