

# राईकवाCTF

CHALLENGE NAME : [US TRIP-1]

DEV : [KANISHK KUMAR & SAMARTH GHANTE]

CATEGORY : [WEB EXPLOITATION]

LEVEL : [MEDIUM]



2024

### Challenge Description:

IIT kharakpur is organizing a US Industrial Visit. The cost of the registration is \$1000. But as always there is an opportunity for intelligent minds. Find the hidden login and Get the flag to get yourself a free US trip ticket

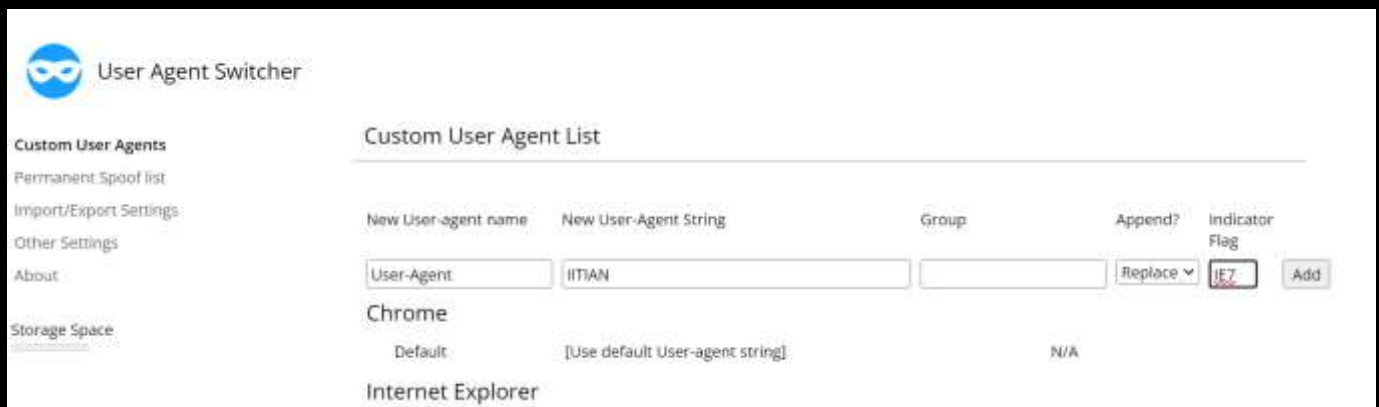
### Solution:

- 1) From the question description we get to know that we have to find a hidden login page and bypass the login to get the flag. So we start by clicking the hyperlink on the homepage.
- 2) By clicking on the link we are redirected to a page that says "YOU ARE NOT AN IITIAN GO BACK". Here by inspecting the page, we can see that there's a hint in the alt tag of the image, which says "Change User Agent to IITIAN".



- 3) So we have to change the user-agent name (The name that appears while visiting the site) to "IITIAN". We can use multiple ways to do this like using a browser extension, using burp suite, or other tools like Insomnia.
- 4) Here, I will be solving using the Google extension. Firstly we will download the extension and add it to Chrome. Then we will create a custom user agent by going to the settings and setting the New User-String to IITIAN





The image shows the 'User Agent Switcher' web application. On the left, there are navigation links: 'Custom User Agents', 'Permanent Spoof list', 'Import/Export Settings', 'Other Settings', 'About', and 'Storage Space'. The main area is titled 'Custom User Agent List' and contains a table with columns: 'New User-agent name', 'New User-Agent String', 'Group', 'Append?', and 'Indicator Flag'. The first row is for 'User-Agent' with the string 'IITIAN', an empty group, 'Replace' as the append action, and 'IE7' as the indicator flag. Below this, there are sections for 'Chrome' (Default, [Use default User-agent string]) and 'Internet Explorer' (N/A).

5) Now by changing the user agent string to 'IITIAN' we can access the login page. Here we have to bypass the login using SQL injection.

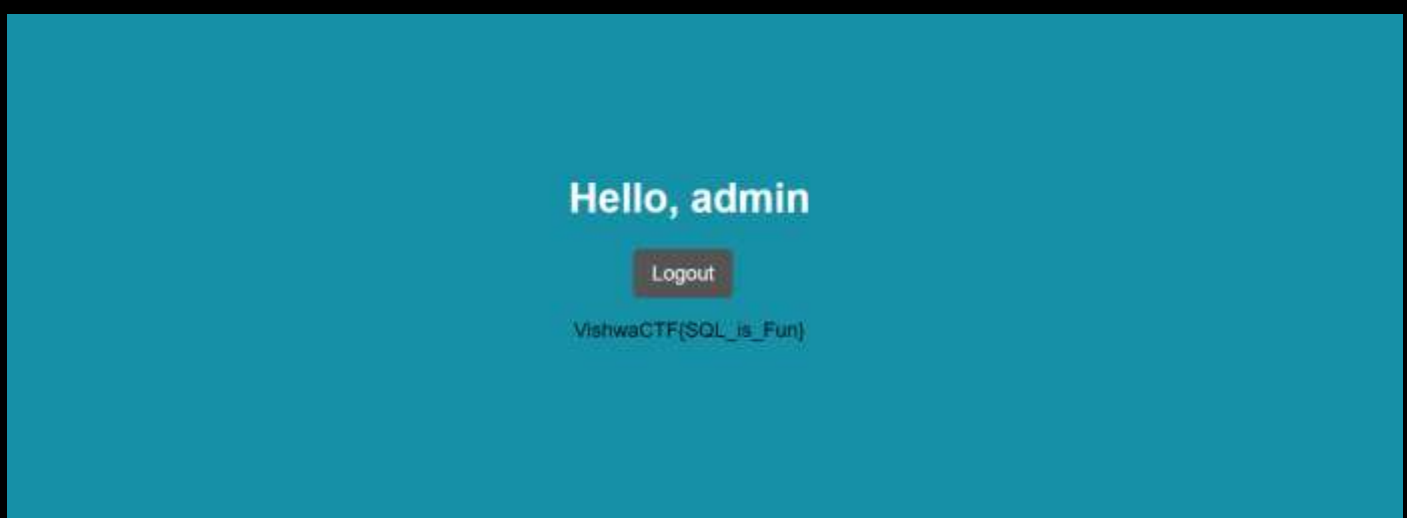
6) By trying injecting multiple queries we can see that SQL injection is not working on username. Hence we will try to Inject the password with SQL queries.

7) Let's try injecting [' or '1'='1] for username "admin". Boommm!!!! , It works !!!!!!! . Congratulations you have bypassed the login.



The image shows a login form on the IIT Kharakpur website. The header says 'Welcome to IIT Kharakpur, US trip form' and 'Login to get your registration ID'. The form is titled 'LOGIN' and has two input fields: 'User Name' (containing 'admin') and 'User Name:' (containing a masked password '\*\*\*\*\*'). There is a 'Login' button at the bottom right of the form.

' or '1'='1



The image shows a teal background with the text 'Hello, admin' in white. Below it is a 'Logout' button. At the bottom, the text 'VishwaCTF{SQL\_is\_Fun}' is displayed.

8) We got the flag, The flag is : VishwaCTF{SQL\_is\_Fun}