Vulnerability Report

Reported by: Gopi Kumar

Email: gjmgopi21@gmail.com

Organization: DROP Organization

Position: Cyber Security

Date: 27/01/2026

Vulnerability : Security Misconfiguration

Sensitive Data Exposure

Severity Risk : High

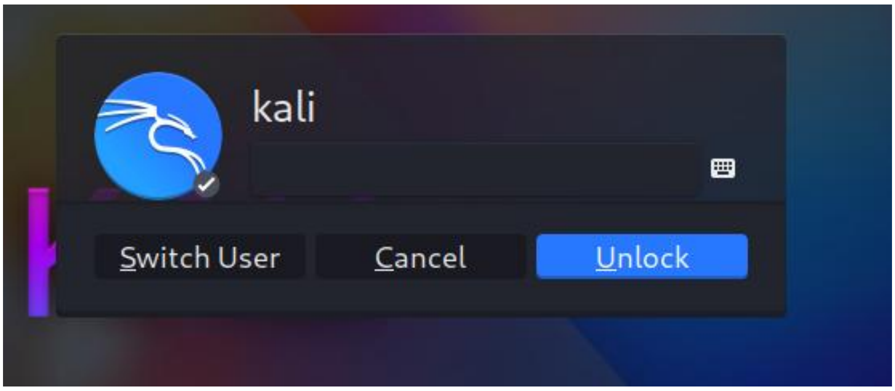
Description

During testing of the college website, it was observed that **improper server configuration** allowed **public access to sensitive directories and files**. Some internal files, including uploaded documents and configuration-related data, were accessible without authentication.

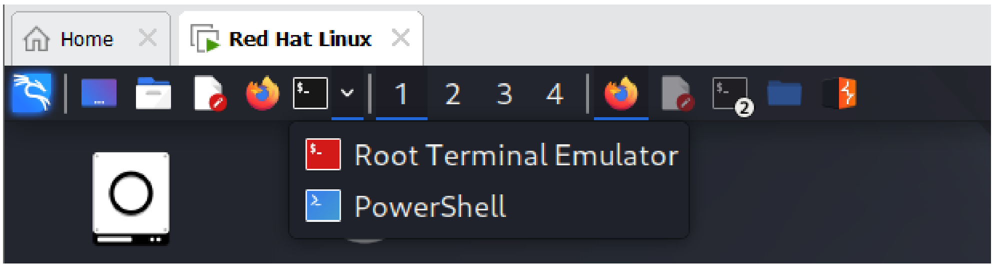
Proof Of Concept : (POC)

First, we started the **Kali Linux machine** and opened the **root terminal** to perform the security testing. After that, we accessed the target college website using a web browser to analyze its configuration.

Kali Linux machine



root terminal

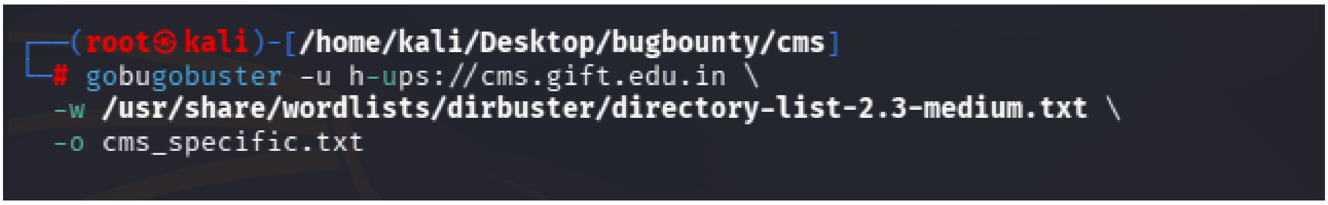


After that, we used the **Gobuster** tool to perform **directory enumeration** on the target college website in order to identify hidden and publicly accessible directories.

Command :

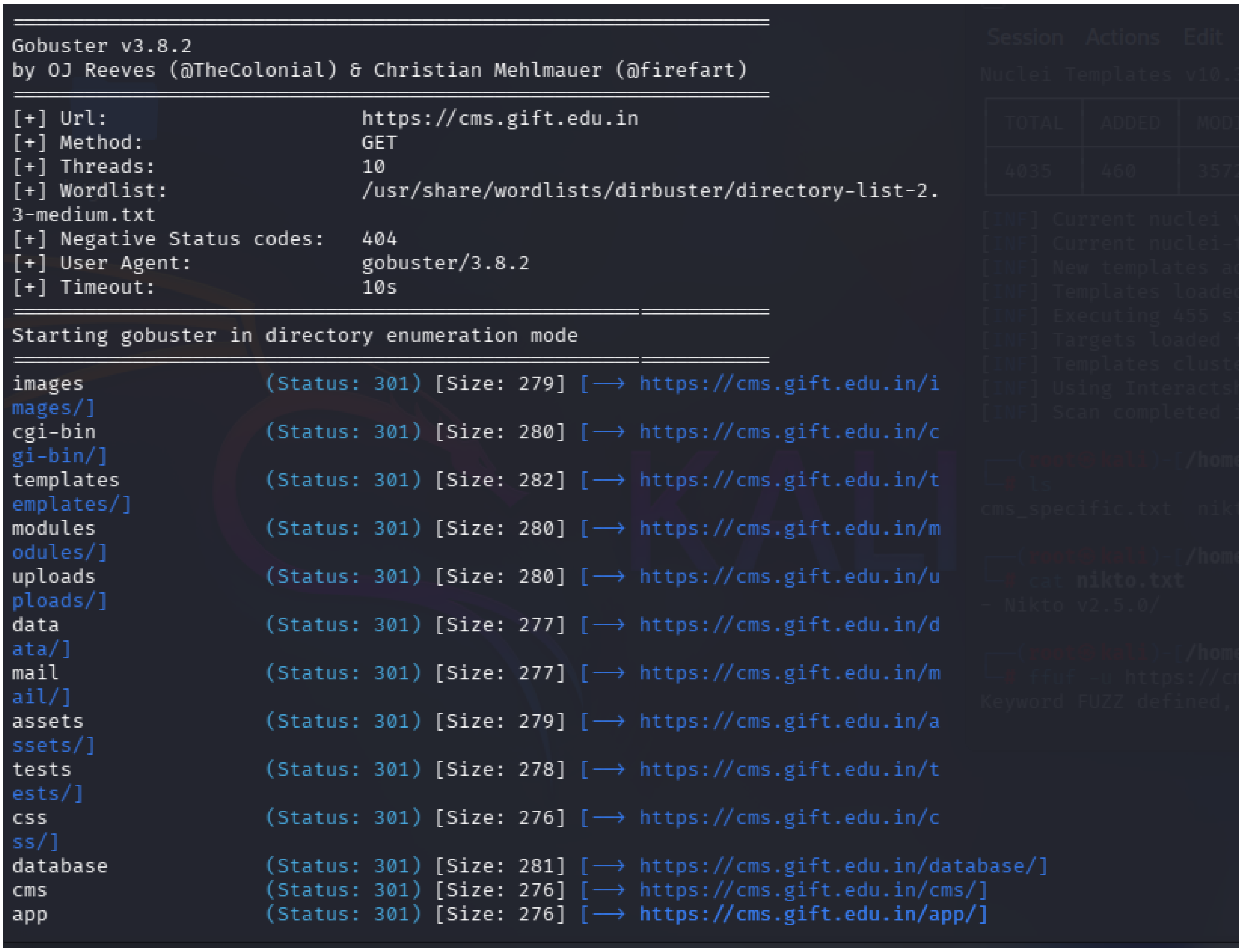
gobuster -u h-ups://cms.gift.edu.in \ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt \

 -o cms_specific.txt



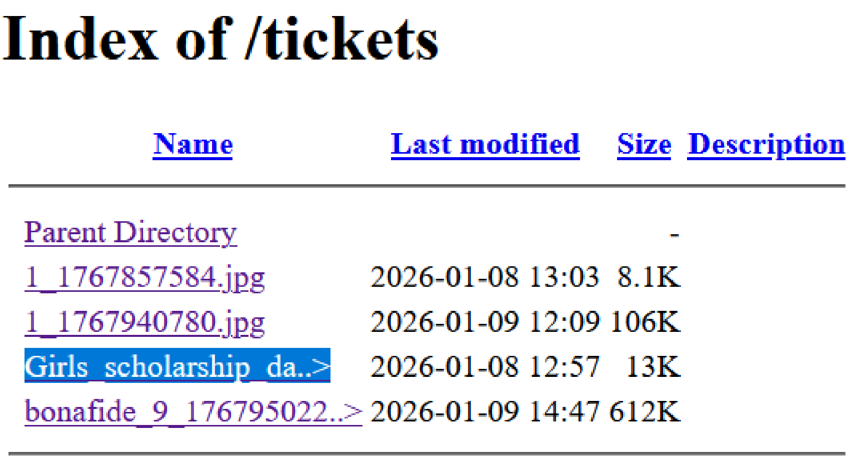
```
┌──(root㉿kali)-[/home/kali/Desktop/bugbounty/cms]
└─# gobugobuster -u h-ups://cms.gift.edu.in \
  -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt \
  -o cms_specific.txt
```

After running the directory enumeration using **Gobuster**, we were able to **identify several valid paths** on the target website. These paths were accessible directly through the browser **without any authentication or authorization**.



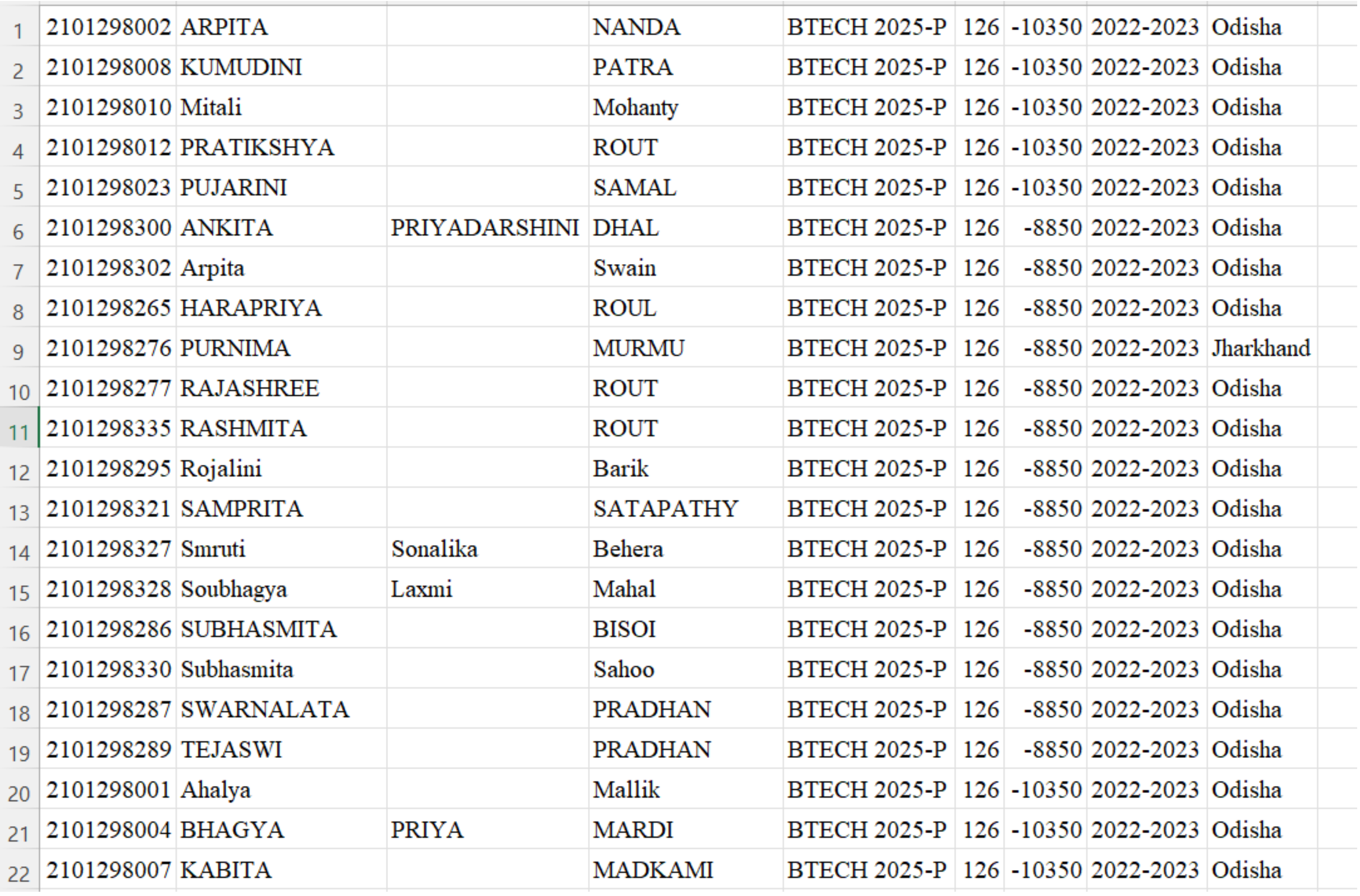
```
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://cms.gift.edu.in
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
images               (Status: 301) [Size: 279] [--> https://cms.gift.edu.in/i
mages/]
cgi-bin              (Status: 301) [Size: 280] [--> https://cms.gift.edu.in/c
gi-bin/]
templates            (Status: 301) [Size: 282] [--> https://cms.gift.edu.in/t
emplates/]
modules              (Status: 301) [Size: 280] [--> https://cms.gift.edu.in/m
odules/]
uploads              (Status: 301) [Size: 280] [--> https://cms.gift.edu.in/u
ploads/]
data                 (Status: 301) [Size: 277] [--> https://cms.gift.edu.in/d
ata/]
mail                 (Status: 301) [Size: 277] [--> https://cms.gift.edu.in/m
ail/]
assets               (Status: 301) [Size: 279] [--> https://cms.gift.edu.in/a
ssets/]
tests                (Status: 301) [Size: 278] [--> https://cms.gift.edu.in/t
ests/]
css                  (Status: 301) [Size: 276] [--> https://cms.gift.edu.in/c
ss/]
database             (Status: 301) [Size: 281] [--> https://cms.gift.edu.in/database/]
cms                  (Status: 301) [Size: 276] [--> https://cms.gift.edu.in/cms/]
app                  (Status: 301) [Size: 276] [--> https://cms.gift.edu.in/app/]
```

After identifying multiple valid paths using Gobuster, we accessed each discovered path directly in the web browser. While browsing these paths, we observed that some pages displayed sensitive data without requiring any authentication or authorization.



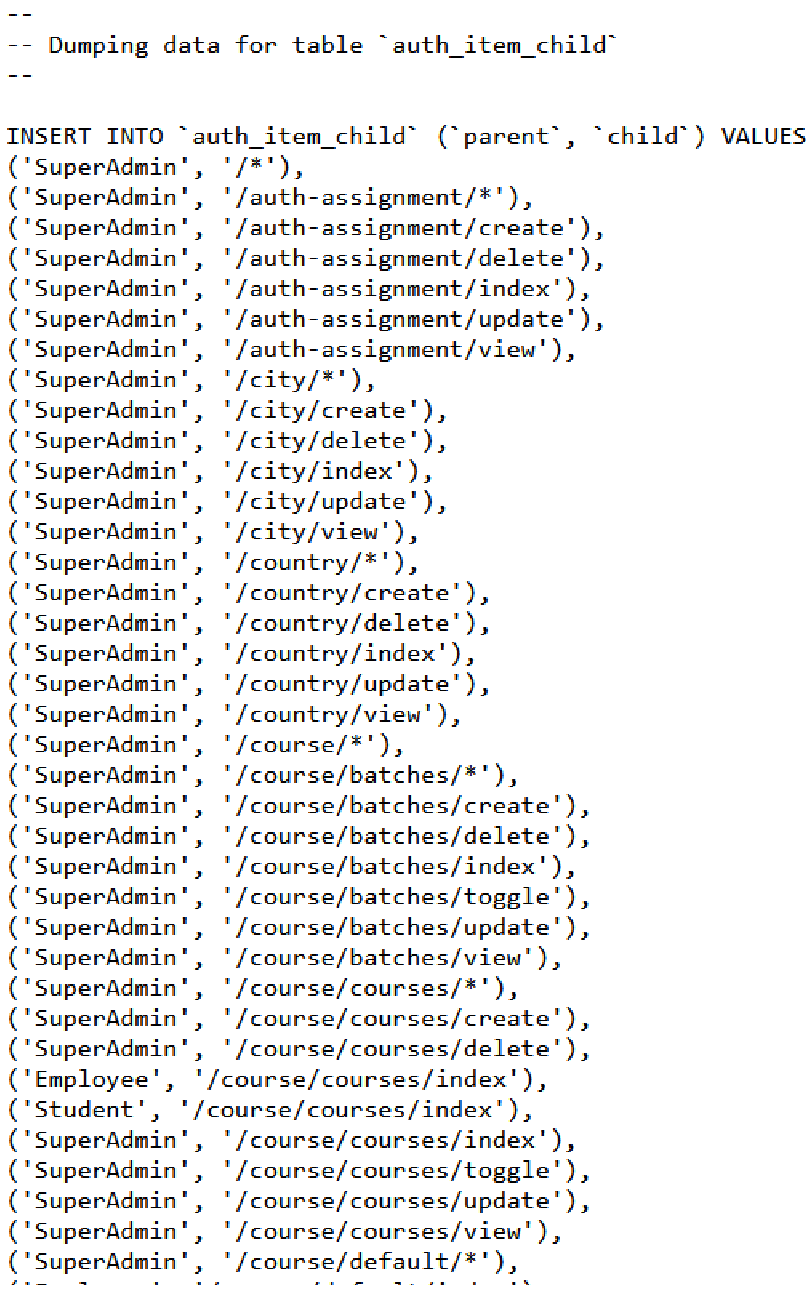
Index of /tickets

```
        Name                Last modified    Size  Description
-------------------------------------------------------------------
Parent Directory                                -
1_1767857584.jpg          2026-01-08 13:03  8.1K
1_1767940780.jpg          2026-01-09 12:09 106K
Girls_scholarship_da..>   2026-01-08 12:57   13K
bonafide_9_176795022..>   2026-01-09 14:47 612K
-------------------------------------------------------------------
```



1	2101298002	ARPITA		NANDA	BTECH 2025-P	126	-10350	2022-2023	Odisha
2	2101298008	KUMUDINI		PATRA	BTECH 2025-P	126	-10350	2022-2023	Odisha
3	2101298010	Mitali		Mohanty	BTECH 2025-P	126	-10350	2022-2023	Odisha
4	2101298012	PRATIKSHYA		ROUT	BTECH 2025-P	126	-10350	2022-2023	Odisha
5	2101298023	PUJARINI		SAMAL	BTECH 2025-P	126	-10350	2022-2023	Odisha
6	2101298300	ANKITA	PRIYADARSHINI	DHAL	BTECH 2025-P	126	-8850	2022-2023	Odisha
7	2101298302	Arpita		Swain	BTECH 2025-P	126	-8850	2022-2023	Odisha
8	2101298265	HARAPRIYA		ROUL	BTECH 2025-P	126	-8850	2022-2023	Odisha
9	2101298276	PURNIMA		MURMU	BTECH 2025-P	126	-8850	2022-2023	Jharkhand
10	2101298277	RAJASHREE		ROUT	BTECH 2025-P	126	-8850	2022-2023	Odisha
11	2101298335	RASHMITA		ROUT	BTECH 2025-P	126	-8850	2022-2023	Odisha
12	2101298295	Rojalini		Barik	BTECH 2025-P	126	-8850	2022-2023	Odisha
13	2101298321	SAMPRITA		SATAPATHY	BTECH 2025-P	126	-8850	2022-2023	Odisha
14	2101298327	Smruti	Sonalika	Behera	BTECH 2025-P	126	-8850	2022-2023	Odisha
15	2101298328	Soubhagya	Laxmi	Mahal	BTECH 2025-P	126	-8850	2022-2023	Odisha
16	2101298286	SUBHASMITA		BISOI	BTECH 2025-P	126	-8850	2022-2023	Odisha
17	2101298330	Subhasmita		Sahoo	BTECH 2025-P	126	-8850	2022-2023	Odisha
18	2101298287	SWARNALATA		PRADHAN	BTECH 2025-P	126	-8850	2022-2023	Odisha
19	2101298289	TEJASWI		PRADHAN	BTECH 2025-P	126	-8850	2022-2023	Odisha
20	2101298001	Ahalya		Mallik	BTECH 2025-P	126	-10350	2022-2023	Odisha
21	2101298004	BHAGYA	PRIYA	MARDI	BTECH 2025-P	126	-10350	2022-2023	Odisha
22	2101298007	KABITA		MADKAMI	BTECH 2025-P	126	-10350	2022-2023	Odisha

While browsing the discovered paths, SQL structure files were found, exposing database-related information without authentication.



```
--
-- Dumping data for table `auth_item_child`
--

INSERT INTO `auth_item_child` (`parent`, `child`) VALUES
('SuperAdmin', '/*'),
('SuperAdmin', '/auth-assignment/*'),
('SuperAdmin', '/auth-assignment/create'),
('SuperAdmin', '/auth-assignment/delete'),
('SuperAdmin', '/auth-assignment/index'),
('SuperAdmin', '/auth-assignment/update'),
('SuperAdmin', '/auth-assignment/view'),
('SuperAdmin', '/city/*'),
('SuperAdmin', '/city/create'),
('SuperAdmin', '/city/delete'),
('SuperAdmin', '/city/index'),
('SuperAdmin', '/city/update'),
('SuperAdmin', '/city/view'),
('SuperAdmin', '/country/*'),
('SuperAdmin', '/country/create'),
('SuperAdmin', '/country/delete'),
('SuperAdmin', '/country/index'),
('SuperAdmin', '/country/update'),
('SuperAdmin', '/country/view'),
('SuperAdmin', '/course/*'),
('SuperAdmin', '/course/batches/*'),
('SuperAdmin', '/course/batches/create'),
('SuperAdmin', '/course/batches/delete'),
('SuperAdmin', '/course/batches/index'),
('SuperAdmin', '/course/batches/toggle'),
('SuperAdmin', '/course/batches/update'),
('SuperAdmin', '/course/batches/view'),
('SuperAdmin', '/course/courses/*'),
('SuperAdmin', '/course/courses/create'),
('SuperAdmin', '/course/courses/delete'),
('Employee', '/course/courses/index'),
('Student', '/course/courses/index'),
('SuperAdmin', '/course/courses/index'),
('SuperAdmin', '/course/courses/toggle'),
('SuperAdmin', '/course/courses/update'),
('SuperAdmin', '/course/courses/view'),
('SuperAdmin', '/course/default/*'),
('Employee', '/course/default/index'),
```

Impact :

- Help attackers understand the **database structure and application logic**
- Lead to further attacks such as **IDOR, privilege escalation, or data manipulation**
- Put **student and institutional data** at risk
- Affect the **confidentiality and integrity** of the system

Thank You