Vulnerability analysis
The ghostcont application suffers from a numerical SQL injection vulnerability exploitable through the hidden input "ghostclass" of the results.php page. To test the presence of the vulnerability by means of Burp Repeater we can send the following HTTP bodies to the page results.php:
searchstring=the&ghostclass=2
and:
searchstring=the&ghostclass=1%2b1
We can observe that the results are the same (except for the image at the top of the page, which depends on the "ghostclass" input without a SQL query). This confirms us that the SQL expression "1+1" gets evaluated, therefore there is a numerical SQL injection vulnerability.