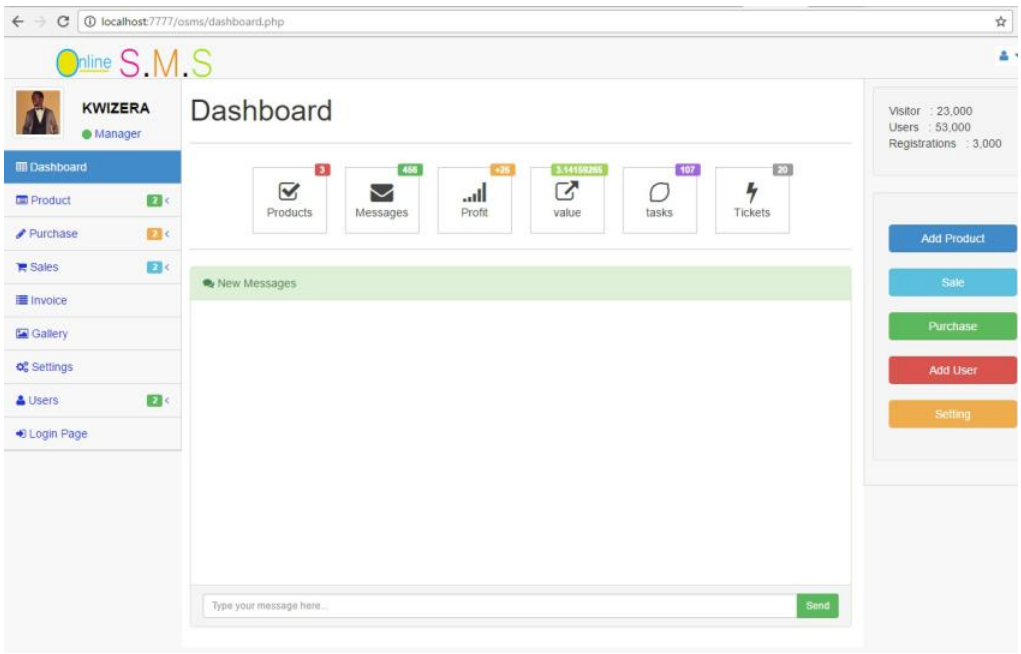
nu11secur1ty Update README.MD ... on Sep 20, 2021 History

..	
docs	last year
PoC-CVE-nu11-14.py	last year
README.MD	last year
chromedriver.exe	last year
osms.zip	last year
templeate_report.txt	last year

README.MD

CVE-2021-36624



Vulnerable PHP code and logic: `ExLogin.php`

```
<?php
// Start the session
session_start();


include '../config/config.php';
include '../config/config1.php';
include '../config/connect.php';

 $UName = ($_POST["Username"]);
 $PW = ($_POST["Password"]);
 $PassWord=0;
 $UserName=0;
$quer= mysqli_query($conn,"SELECT * FROM user where username='$UName' AND passwourd='$PW'");
while($ss = mysqli_fetch_array($quer))
        {
        $UserName=$ss['username'];
        $PassWord=$ss['passwourd'];
        $userid=$ss['userid'];
        $name=$ss['name'];
        $profilepicture=$ss['profilepicture'];
        $IDBranch=$ss['IDBranch'];
        $role=$ss['role'];
        }

if($PassWord!=$PW || $UserName!=$UName ){
echo "<script>alert('Incorrect UserName or Password')</script>";
echo "<script>location.href='../index.php'</script>";
```

```
}
else
{
$_SESSION["Id"]=$userid;
$_SESSION["name"]=$name;
$_SESSION["profilepicture"]=$profilepicture;
$_SESSION["IDBranch"]=$IDBranch;
$_SESSION["role"]=$role;

?>

<!--<script>
var person = prompt("Please enter your name", "Harry Potter");
if (person != null) {
    document.getElementById("demo").innerHTML =
    "Hello " + person + "! How are you today?";
}
</script>-->
<script>location.href='../dashboard.php'</script>"; -->

<?php } ?>
```

Description:

Sourcecodester Phone Shop Sales Managements System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

Reproduce:

href

Proof:

href

BR nu11secur1ty