Pratikkhalane Follow

Sep 21, 2021 · 2 min read · Listen

Save

CVE-2021–36560

Authentication Bypass of The Admin Panel.

🧑‍💻 Discovered by **Pratik Khalane**

📄 **Vulnerable version: 1.0**

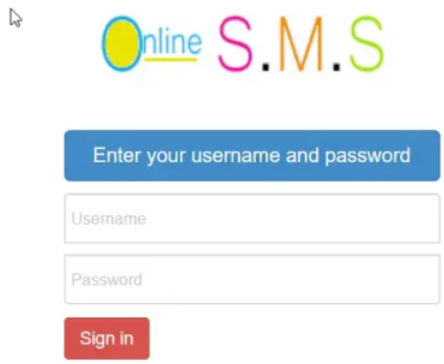
🔗 **Vendor Homepage:** https://www.sourcecodester.com/

Bug Description:

An attacker can easily bypass the login page to get into the dashboard of the admin panel.

Steps to Reproduce:

1. Go to the admin panel of the online SMS login page.



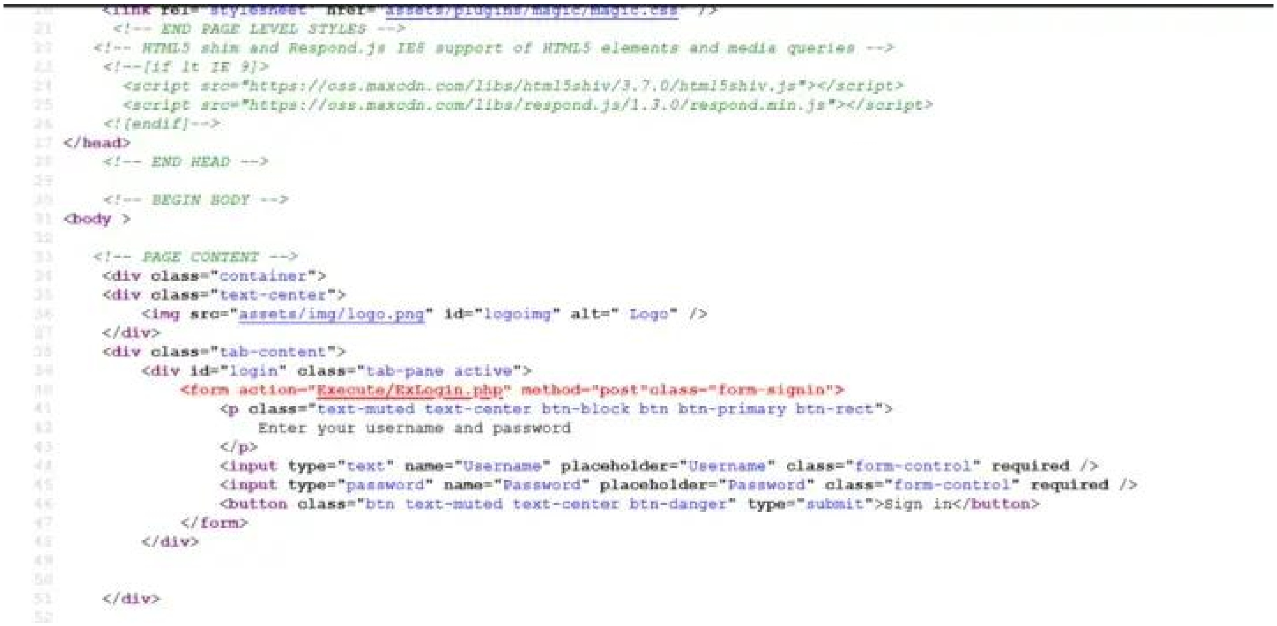
LOGIN PAGE

2. Now there are 2 ways by which you can bypass the page

i) Using Tools: Over here we can brute force the directory by using the dirbuster wordlist. By this, you can discover that there is a **dashboard.php** page that can lead to the admin panel very easily.

ii)Without using the tools:

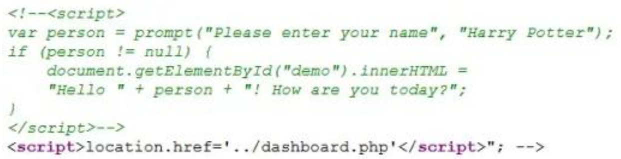
Step1: Press Ctrl + U for looking at the website source code.



```
      <link rel="stylesheet" href="assets/plugins/magic/magic.css" />
       <!-- END PAGE LEVEL STYLES -->
     <!-- HTML5 shim and Respond.js IE8 support of HTML5 elements and media queries -->
      <!--[if lt IE 9]>
        <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
        <script src="https://oss.maxcdn.com/libs/respond.js/1.3.0/respond.min.js"></script>
      <![endif]-->
</head>
      <!-- END HEAD -->

      <!-- BEGIN BODY -->
<body >

     <!-- PAGE CONTENT -->
      <div class="container">
      <div class="text-center">
          <img src="assets/img/logo.png" id="logoimg" alt=" Logo" />
      </div>
      <div class="tab-content">
          <div id="login" class="tab-pane active">
              <form action="Execute/ExLogin.php" method="post"class="form-signin">
                  <p class="text-muted text-center btn-block btn btn-primary btn-rect">
                      Enter your username and password
                  </p>
                  <input type="text" name="Username" placeholder="Username" class="form-control" required />
                  <input type="password" name="Password" placeholder="Password" class="form-control" required />
                  <button class="btn text-muted text-center btn-danger" type="submit">Sign in</button>
              </form>
          </div>


      </div>
```

Source_code

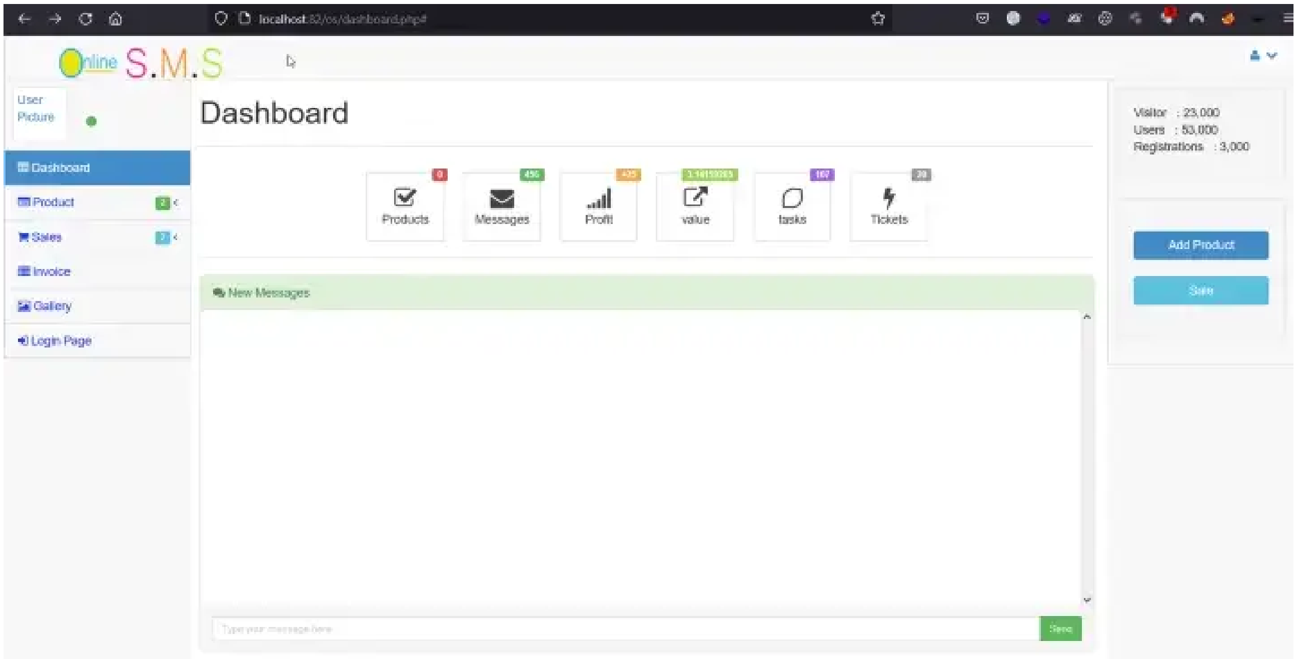
Step 2: Now as you can see that the form action is leading us to go for the Exlogin.php page.



```
<!--<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>"; -->
```

ExLogin.php

Step 3: As you can see that we got the location which we can attempt to visit and bypass the admin panel.



Dashboard

Bugbounting Bug Bounty Webapplicationpentest Pentesting Cve