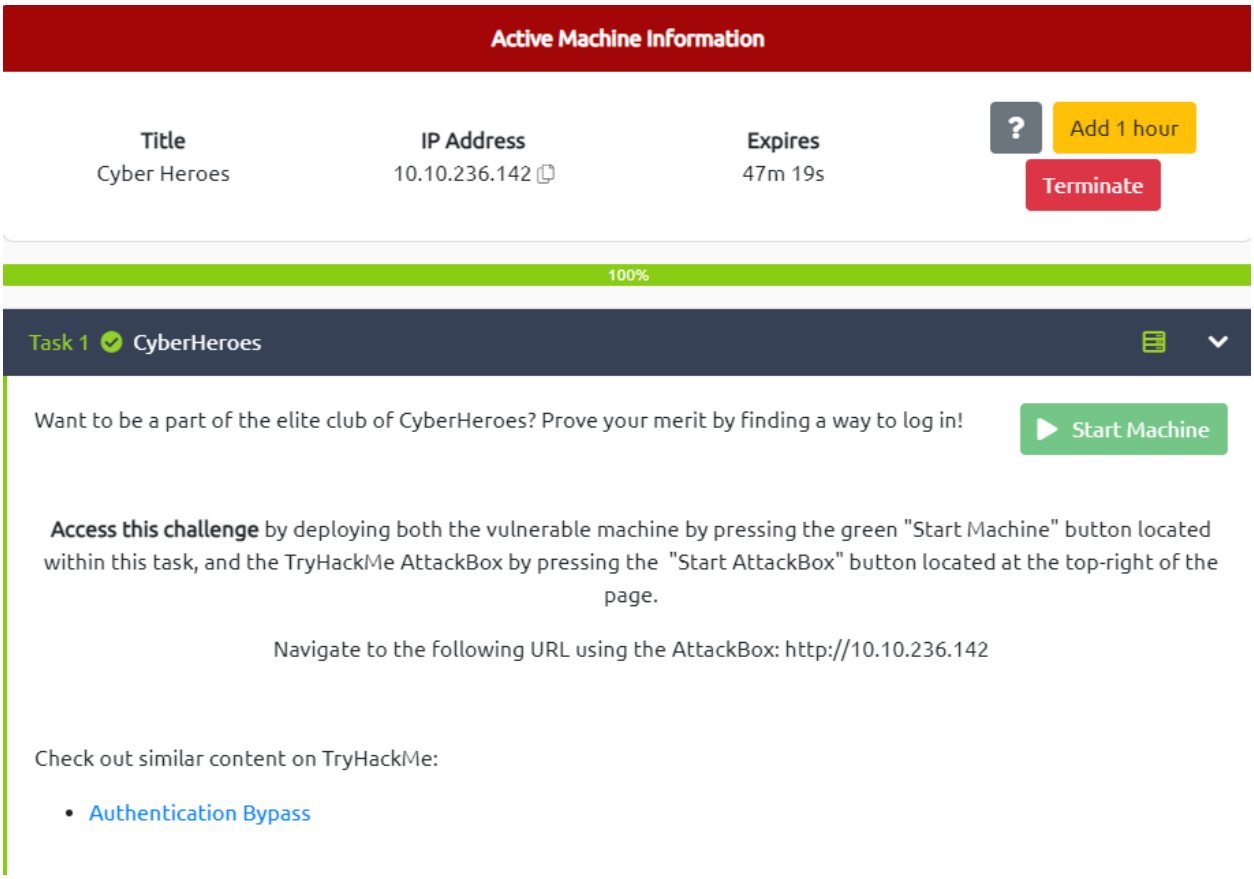
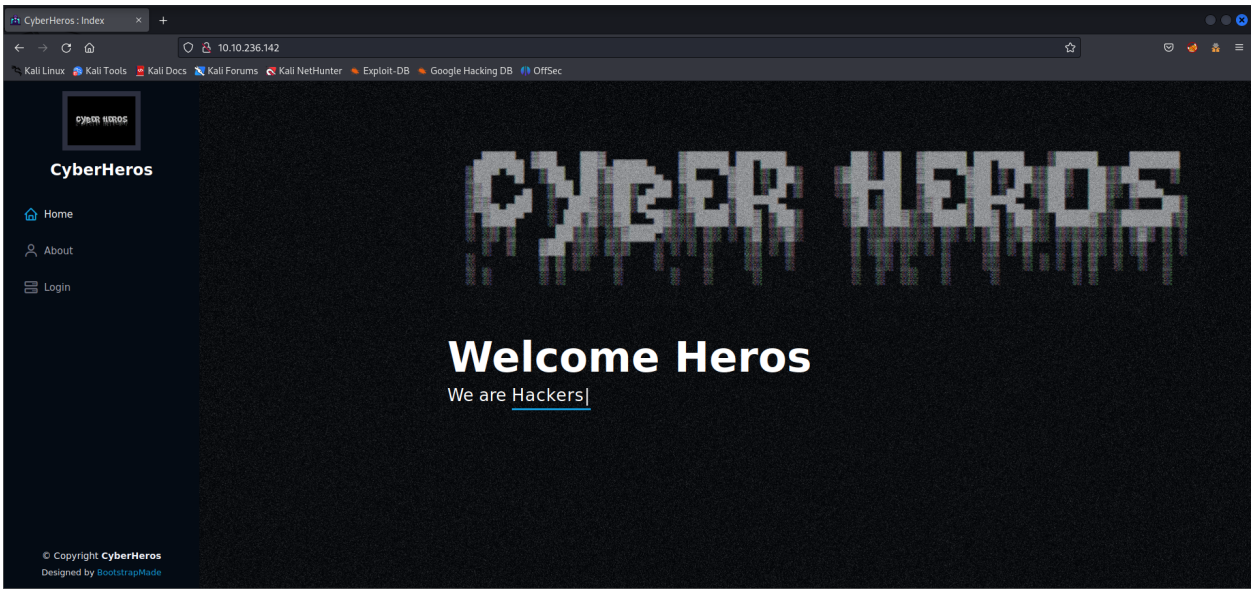
# Cyber Heroes (Really Really Easy!!)




---

As mentioned in the Task Description, we only need to use the web browser to complete this room

> ❗ Navigate to the following URL using the AttackBox: http://10.10.236.142




Let’s take a look at the source page

▼ Full Source Page

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

<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">

  <title>CyberHeros : Index</title>
  <meta content="" name="description">
  <meta content="" name="keywords">

  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">

  <!-- <link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400
i,600,600i,700,700i|Raleway:300,300i,400,400i,500,500i,600,600i,700,700i|Poppins:300,
300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet"> -->

  <link href="assets/vendor/aos/aos.css" rel="stylesheet">
  <link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
  <link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
  <link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
  <link href="assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
  <link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">

  <link href="assets/css/style.css" rel="stylesheet">

</head>
```

```
<body>
  <i class="bi bi-list mobile-nav-toggle d-xl-none"></i>
  <header id="header">
    <div class="d-flex flex-column">

      <div class="profile">
        <img src="assets/img/profile-img.png" alt="" class="img-fluid">
        <h1 class="text-light"><a href="index.html">CyberHeros</a></h1>
      </div>

      <nav id="navbar" class="nav-menu navbar">
        <ul>
          <li><a href="#hero" class="nav-link scrollto active"><i class="bx bx-home">
</i> <span>Home</span></a></li>
          <li><a href="#about" class="nav-link scrollto"><i class="bx bx-user"></i> <
span>About</span></a></li>
          <li><a href="login.html" class="nav-link scrollto"><i class="bx bx-server">
</i> <span>Login</span></a></li>
        </ul>
      </nav>
    </div>
  </header>

  <section id="hero" class="d-flex flex-column justify-content-center align-items-cen
ter">
    <div class="hero-container" data-aos="fade-in">
      <br><br><br><br><br><br><br>
      <h1>Welcome Heros</h1>
      <p>We are <span class="typed" data-typed-items="Hackers, Developers, Bug Hunter
s, Cyber Warriors, Cyber Gaurdians"></span></p>
    </div>
  </section>

  <main id="main">
    <section id="about" class="about facts">
      <div class="container">

        <div class="section-title">
          <h2>About Us</h2>
          <p>We are a group of young Hackers, Developers, Bug Hunters, Cyber Warrior
s, Cyber Gaurdians. We find vulnerabilities in the website legally and save them from
getting hacked, Join our forces, find the vuln on our login page and login to join u
s. :D</p>
          <br><h5>Heros are not born, They work hard and become one ! :D</h5>
        </div>

        <div class="section-title">
          <h2>Facts</h2>
          <p>Some Awesome Facts about our CyberHeros are team.</p>
        </div>

        <div class="row no-gutters">
```

```
          <div class="col-lg-3 col-md-6 d-md-flex align-items-md-stretch" data-aos="f
ade-up">
            <div class="count-box">
              <i class="bi bi-emoji-smile"></i>
              <span data-purecounter-start="0" data-purecounter-end="738" data-pureco
unter-duration="1" class="purecounter"></span>
              <p><strong>Internet Users</strong><br>Protected</p>
            </div>
          </div>

          <div class="col-lg-3 col-md-6 d-md-flex align-items-md-stretch" data-aos="f
ade-up" data-aos-delay="100">
            <div class="count-box">
              <i class="bi bi-journal-richtext"></i>
              <span data-purecounter-start="0" data-purecounter-end="521" data-pureco
unter-duration="1" class="purecounter"></span>
              <p><strong>Websites</strong></br>Protected</p>
            </div>
          </div>

          <div class="col-lg-3 col-md-6 d-md-flex align-items-md-stretch" data-aos="f
ade-up" data-aos-delay="200">
            <div class="count-box">
              <i class="bi bi-headset"></i>
              <span data-purecounter-start="0" data-purecounter-end="1453" data-purec
ounter-duration="1" class="purecounter"></span>
              <p><strong>Support</strong><br>Members Supported</p>
            </div>
          </div>

          <div class="col-lg-3 col-md-6 d-md-flex align-items-md-stretch" data-aos="f
ade-up" data-aos-delay="300">
            <div class="count-box">
              <i class="bi bi-people"></i>
              <span data-purecounter-start="0" data-purecounter-end="80" data-purecou
nter-duration="1" class="purecounter"></span>
              <p><strong>CyberHeros</strong><br>Our team members</p>
            </div>
          </div>


          <div class="section-title">
            <h2>Join Us</h2>
            <p>Are you a Hacker, Developer, Bug Hunter, if yes, join us by hacking th
e login page and become a CyberHero !</p>
          </div>

        </div>

      </div>
    </section>
```

```
  </main>

  <footer id="footer">
    <div class="container">
      <div class="copyright">
        &copy; Copyright <strong><span>CyberHeros</span></strong>
      </div>
      <div class="credits">
        <!-- All the links in the footer should remain intact. -->
        <!-- You can delete the links only if you purchased the pro version. -->
        <!-- Licensing information: https://bootstrapmade.com/license/ -->
        <!-- Purchase the pro version with working PHP/AJAX contact form: https://boo
tstrapmade.com/iportfolio-bootstrap-portfolio-websites-template/ -->
        Designed by <a href="https://bootstrapmade.com/">BootstrapMade</a>
      </div>
    </div>
  </footer>

  <a href="#" class="back-to-top d-flex align-items-center justify-content-center"><i
class="bi bi-arrow-up-short"></i></a>

  <script src="assets/vendor/purecounter/purecounter.js"></script>
  <script src="assets/vendor/aos/aos.js"></script>
  <script src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
  <script src="assets/vendor/glightbox/js/glightbox.min.js"></script>
  <script src="assets/vendor/isotope-layout/isotope.pkgd.min.js"></script>
  <script src="assets/vendor/swiper/swiper-bundle.min.js"></script>
  <script src="assets/vendor/typed.js/typed.min.js"></script>
  <script src="assets/vendor/waypoints/noframework.waypoints.js"></script>
  <script src="assets/vendor/php-email-form/validate.js"></script>

  <script src="assets/js/main.js"></script>

</body>

</html>
```

```
<li>
  <a href="login.html" class="nav-link scrollto">
    <i class="bx bx-server"></i>
    <span>Login</span>
  </a>
</li>
```

There is a `Login` button in the `nav` bar which route to the `login.html` page → Check it out!

▼ Full Login.html

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

<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">

  <title>CyberHeros : Login</title>
  <meta content="" name="description">
  <meta content="" name="keywords">

  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">

  <link href="assets/vendor/aos/aos.css" rel="stylesheet">
  <link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
  <link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
  <link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
  <link href="assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
  <link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">

  <link href="assets/css/style.css" rel="stylesheet">

  <style>
    .form {
      position: relative;
      z-index: 1;
      background: #ffffffa2;
      max-width: 650px;
      margin: 0 auto 40px;
      padding: 60px;
      box-shadow: 0 0 10px 0 rgba(0, 0, 0, 0.2), 0 5px 5px 0 rgba(0, 0, 0, 0.24);
    }
    .form input {
      font-family: "Roboto", sans-serif;
      outline: 0;
      background: #f2f2f2;
      width: 100%;
      border: 0;
      margin: 0 0 15px;
      padding: 15px;
      box-sizing: border-box;
      font-size: 14px;
    }
    .form button {
      font-family: "Roboto", sans-serif;
      text-transform: uppercase;
      outline: 0;
      background: #173b6c;
      width: 100%;
      border: 0;
      padding: 15px;
```

```
      color: #FFFFFF;
      font-size: 14px;
      -webkit-transition: all 0.3 ease;
      transition: all 0.3 ease;
      cursor: pointer;
    }
    .form button:hover,.form button:active,.form button:focus {
      background: #24436e;
    }
    .form .message {
      margin: 15px 0 0;
      color: #b3b3b3;
      font-size: 12px;
    }
    .form .message a {
      color: #173b6c;
      text-decoration: none;
    }
    .form .register-form {
      display: none;
    }

  </style>

</head>


<body>
  <i class="bi bi-list mobile-nav-toggle d-xl-none"></i>
  <header id="header">
    <div class="d-flex flex-column">

      <div class="profile">
        <img src="assets/img/profile-img.png" alt="" class="img-fluid">
        <h1 class="text-light"><a href="index.html">CyberHeros</a></h1>
      </div>

      <nav id="navbar" class="nav-menu navbar">
        <ul>
          <li><a href="index.html" class="nav-link scrollto active"><i class="bx bx-h
ome"></i> <span>Home</span></a></li>
        </ul>
      </nav>
    </div>
  </header>


  <main id="main">

    <section id="hero" class="d-flex flex-column justify-content-center align-items-c
enter">
      <div class="hero-container">
        <br><br><br><br>
        <div class="">
```

```
          <div class="form">
          <h4 id="flag"></h4>
            <form id="todel"class="">
              <div class="section-title">
                <h2>Login</h2>
                <h4>Show your hacking skills and login to became a CyberHero ! :D</h4
>
              </div>
              <input type="text" id="uname" placeholder="username"/>
              <input type="password" id="pass" placeholder="password"/>
            </form>
            <button id="rm" onclick="authenticate()">login</button>
          </div>
        </div>
      </div>
    </section>

  </main>

  <script>
    function authenticate() {
      a = document.getElementById('uname')
      b = document.getElementById('pass')
      const RevereString = str => [...str].reverse().join('');
      if (a.value=="h3ck3rBoi" & b.value==RevereString("54321@terceSrepuS")) {
        var xhttp = new XMLHttpRequest();
        xhttp.onreadystatechange = function() {
          if (this.readyState == 4 && this.status == 200) {
            document.getElementById("flag").innerHTML = this.responseText ;
            document.getElementById("todel").innerHTML = "";
            document.getElementById("rm").remove() ;
          }
        };
        xhttp.open("GET", "RandomLo0o0o0o0o0o0o0o0o0o0gpath12345_Flag_"+a.value+"_"+
b.value+".txt", true);
        xhttp.send();
      }
      else {
        alert("Incorrect Password, try again.. you got this hacker !")
      }
    }
  </script>

  <footer id="footer">
    <div class="container">
      <div class="copyright">
        &copy; Copyright <strong><span>CyberHeros</span></strong>
      </div>
      <div class="credits">
        <!-- All the links in the footer should remain intact. -->
        <!-- You can delete the links only if you purchased the pro version. -->
        <!-- Licensing information: https://bootstrapmade.com/license/ -->
        <!-- Purchase the pro version with working PHP/AJAX contact form: https://boo
tstrapmade.com/iportfolio-bootstrap-portfolio-websites-template/ -->
```

```
        Designed by <a href="https://bootstrapmade.com/">BootstrapMade</a>
      </div>
    </div>
  </footer>

  <a href="#" class="back-to-top d-flex align-items-center justify-content-center"><i
class="bi bi-arrow-up-short"></i></a>

  <script src="assets/vendor/purecounter/purecounter.js"></script>
  <script src="assets/vendor/aos/aos.js"></script>
  <script src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
  <script src="assets/vendor/glightbox/js/glightbox.min.js"></script>
  <script src="assets/vendor/isotope-layout/isotope.pkgd.min.js"></script>
  <script src="assets/vendor/swiper/swiper-bundle.min.js"></script>
  <script src="assets/vendor/typed.js/typed.min.js"></script>
  <script src="assets/vendor/waypoints/noframework.waypoints.js"></script>
  <script src="assets/vendor/php-email-form/validate.js"></script>

  <script src="assets/js/main.js"></script>

</body>

</html>
```

From line **123** → **144** we will find the script of the authenticate process

```
<script>
    function authenticate() {
      a = document.getElementById('uname')
      b = document.getElementById('pass')
      const RevereString = str => [...str].reverse().join('');
      if (a.value=="h3ck3rBoi" & b.value==RevereString("54321@terceSrepuS")) {
        var xhttp = new XMLHttpRequest();
        xhttp.onreadystatechange = function() {
          if (this.readyState == 4 && this.status == 200) {
            document.getElementById("flag").innerHTML = this.responseText ;
            document.getElementById("todel").innerHTML = "";
            document.getElementById("rm").remove() ;
          }
        };
        xhttp.open("GET", "RandomLo0o0o0o0o0o0o0o0o0o0gpath12345_Flag_"+a.value+"_"+b.valu
e+".txt", true);
        xhttp.send();
      }
      else {
        alert("Incorrect Password, try again.. you got this hacker !")
      }
    }
</script>
```

Focus on these line:

```
const RevereString = str => [...str].reverse().join('');
if (a.value=="h3ck3rBoi" & b.value==RevereString("54321@terceSrepuS"));
```

The above script could written like this for easily understand:

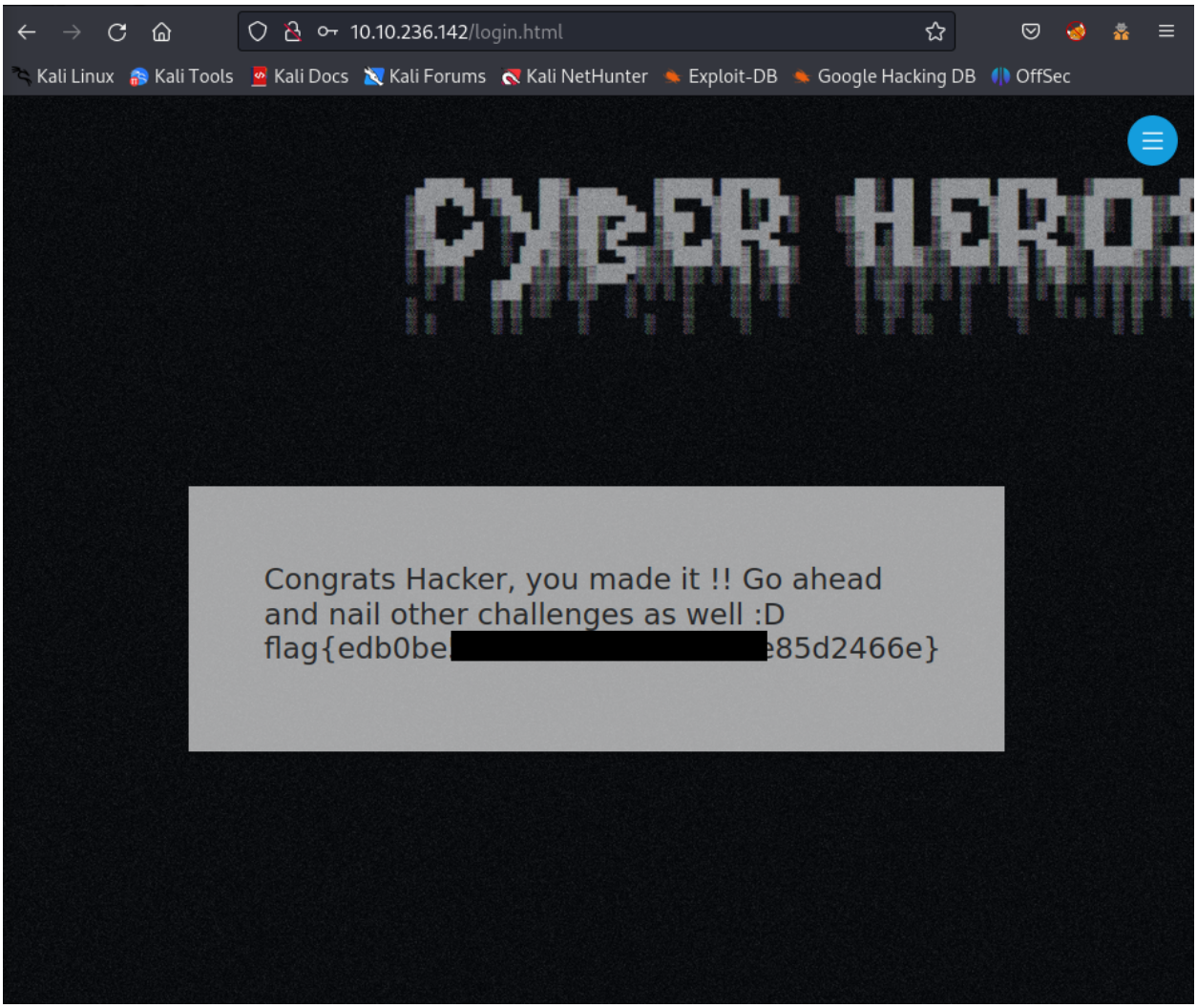
```
function RevereString(str) {
  return str.split('').reverse().join('');
}
```

As we can see, the `RevereString` function simply reverses the `string` which is parsed in.

We run the code above and will get the output of the user's password


Or you can manually reverse it by your own by reading the string from **right → left** 😂 How easy it is!

Use the above credential to login the page (h3ck3rBoi:SuperSecret@12345)


10.10.236.142/login.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Congrats Hacker, you made it !! Go ahead and nail other challenges as well :D
flag{edb0be[redacted]e85d2466e}