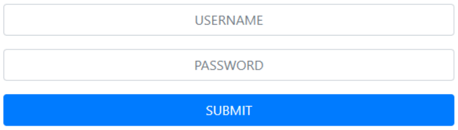
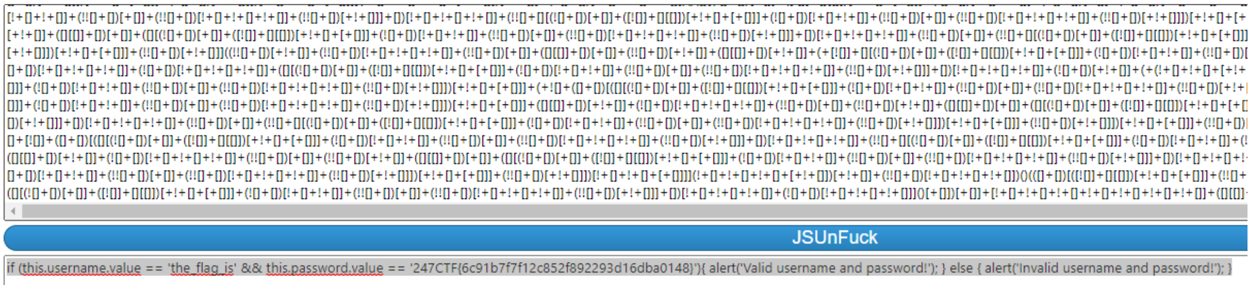
Trusted Client



לאחר כניסה לאתר אנחנו רואים דף התחברות, כאשר מנסים להזין פרטים אנחנו שמים לב שקופצת הודעה (alarm) אבל האתר לא שולח בקשה – לכן אפשר להניח שהבדיקה מתבצעת בצד הקליאנט.
לאחר כניסה לקוד האתר הבחנו במשהו לא מוכר:

```
<html>
<head>
  <title>Login Panel</title>
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.1.3/css/bootstrap.min.css" integrity="sha384-MCw98/SF
</head>
<body>
<div class="container h-100">
  <div class="row h-100 justify-content-center align-items-center">
    <div class="col-6">
      <form id="login">
          <div class="form-group">
            <input class="form-control text-center" id="username" name="username" placeholder="USERNAME" type="text" value="">
          </div>
          <div class="form-group">
            <input class="form-control text-center" id="password" name="password" placeholder="PASSWORD" type="password" value="">
          </div>
      <button type="submit" class="btn btn-primary btn-block">SUBMIT</button>
      </form>
    </div>
  </div>
</div>
<script>
window.onload=function() {
  document.getElementById('login').onsubmit=function() {
    [][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[
  return false;
  }
}
</script>
</body>
</html>
```

לאחר חיפושים בגוגל הבנו שמדובר בסוג של Obfuscation בשם JsFuck, חיפשנו אתר שמפענח ולאחר מכן מצאנו את https://codertab.com/jsunfuck שפלט לנו את הדגל:



```
if (this.username.value == 'the_flag_is' && this.password.value == '247CTF{6c91b7f7f12c852f892293d16dba0148}'){ alert('Valid username and password!'); } else { alert('Invalid username and password!'); }
```