BUUCTF刷题笔记 BuyFlag

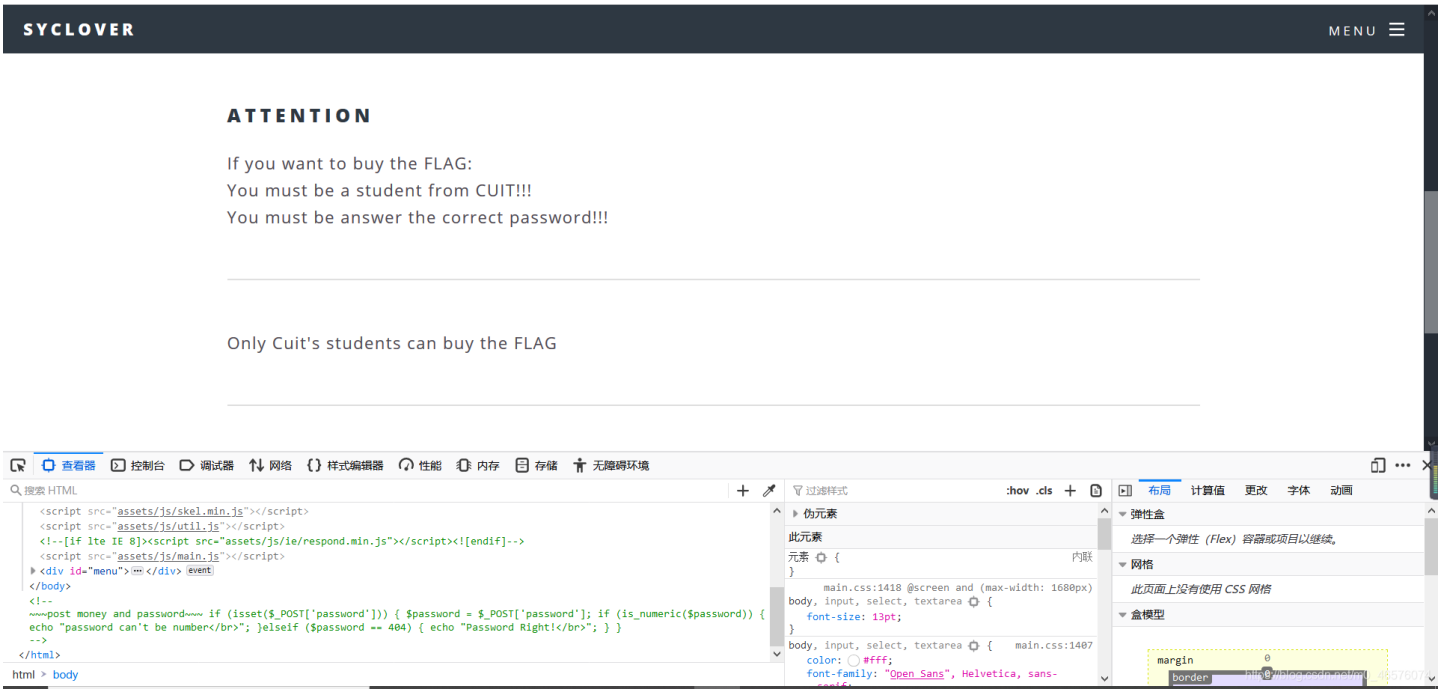
原创

m0_46576074 于 2020-05-12 08:51:30 发布 491 收藏 1

[极客大挑战 2019]BuyFlag

进入页面

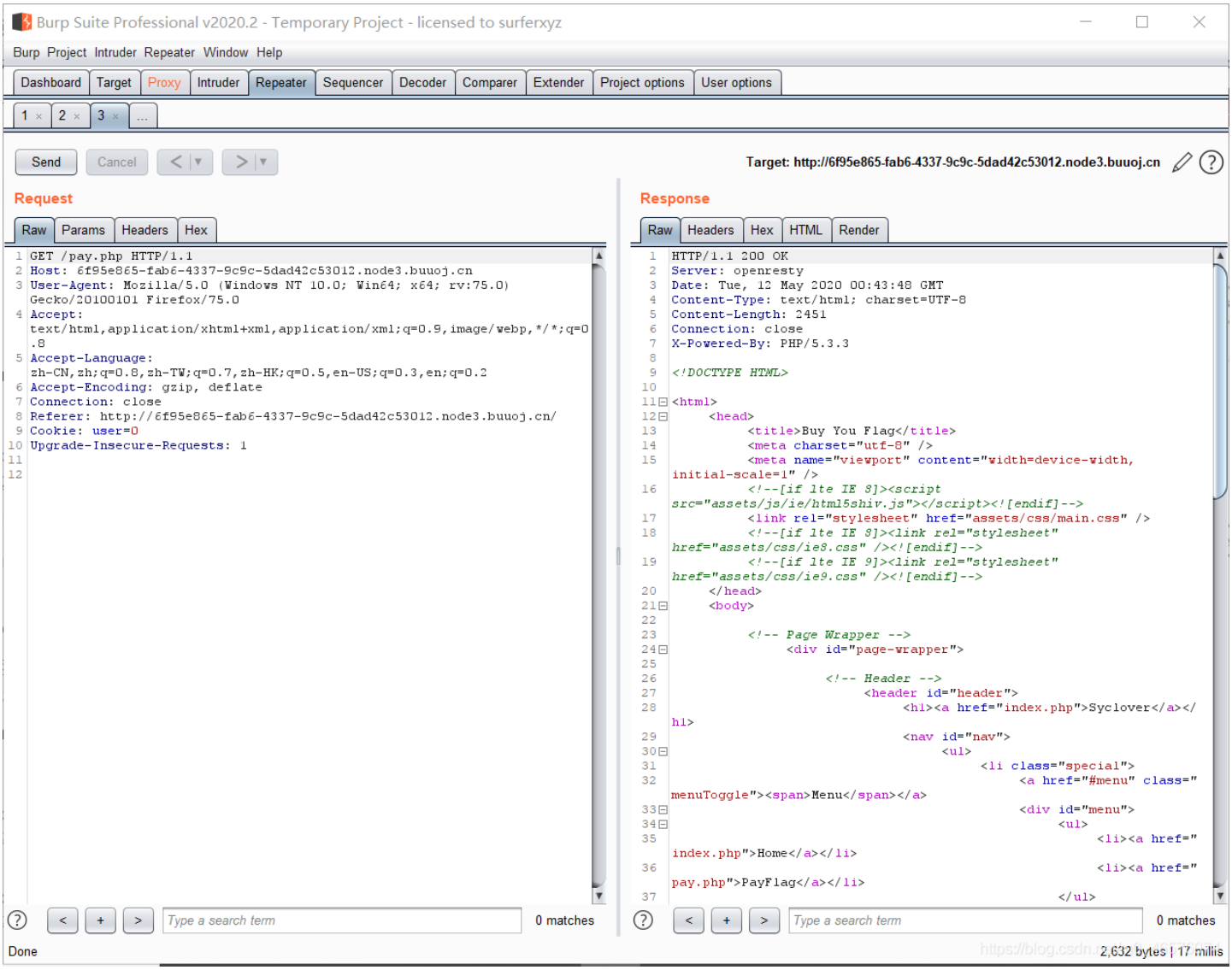
点击menu，进到payflag页面，查看源代码



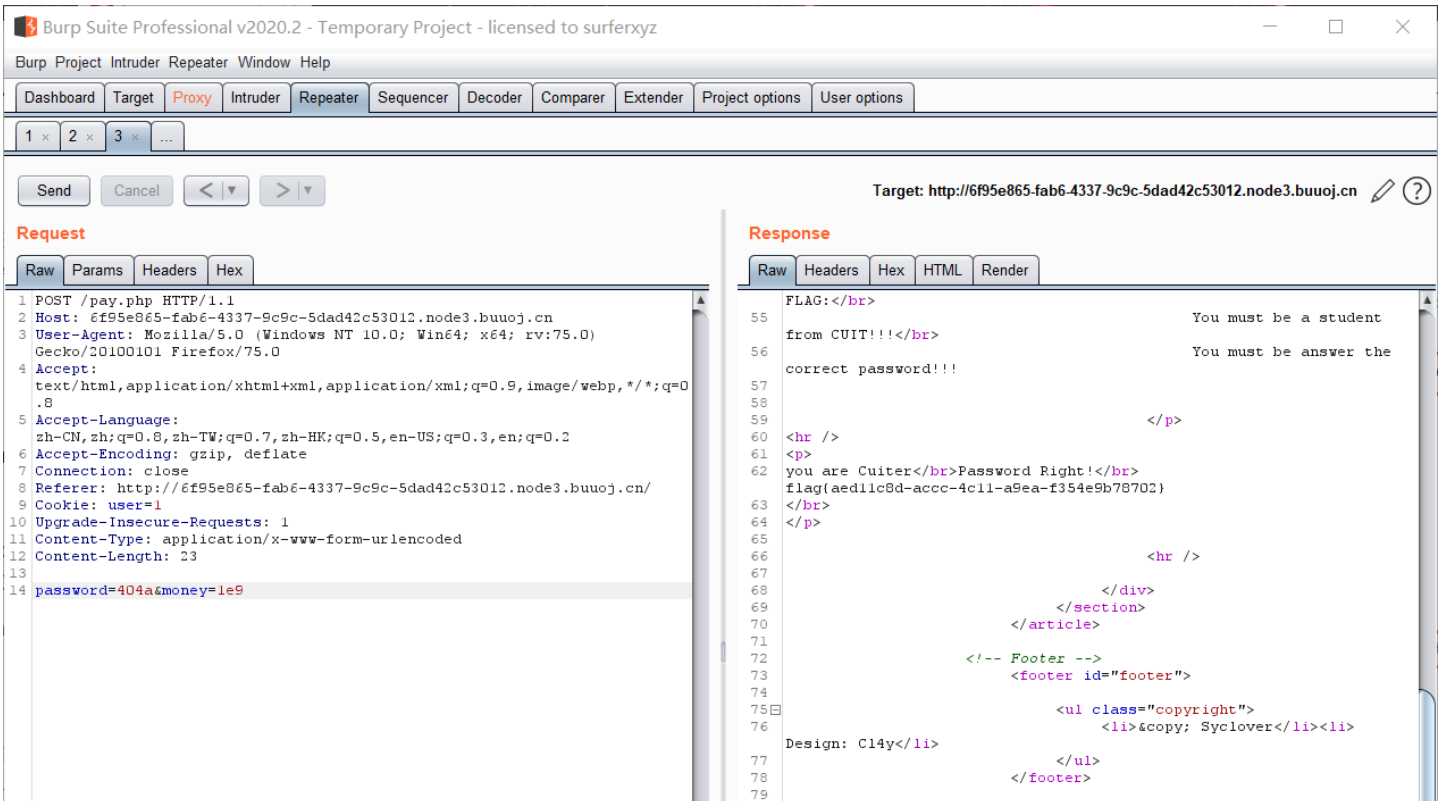
发现

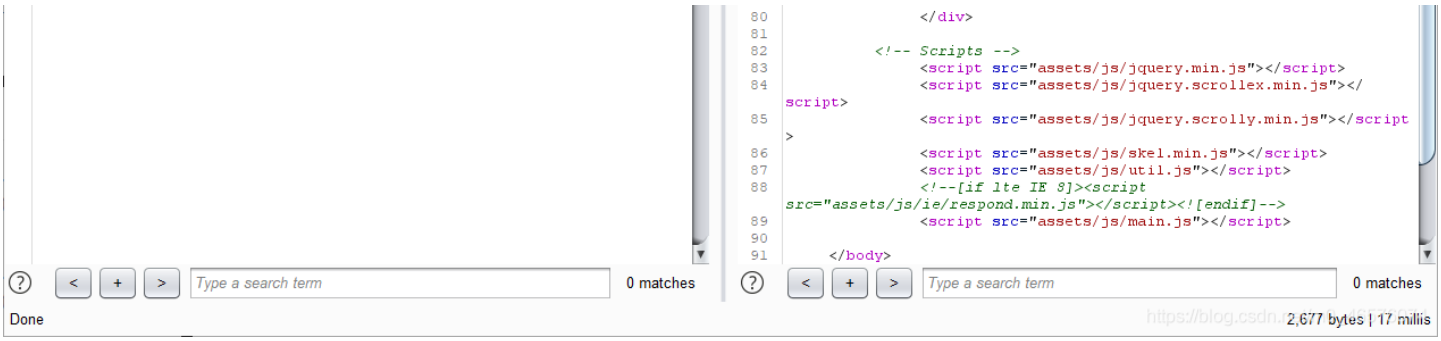
```
<!--
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
-->
```

使用burpsuite抓包



把user改成1，post参数password，money进去




80
81
82 <!-- Scripts -->
83 <script src="assets/js/jquery.min.js"></script>
84 <script src="assets/js/jquery.scrollex.min.js"></script>
85 <script src="assets/js/jquery.scrolly.min.js"></script>
86 <script src="assets/js/skel.min.js"></script>
87 <script src="assets/js/util.js"></script>
88 <!--[if lte IE 8]><script src="assets/js/ie/respond.min.js"></script><![endif]-->
89 <script src="assets/js/main.js"></script>
90
91 </body>
Type a search term
0 matches
Type a search term
0 matches
Done
2,677 bytes | 17 millis

得flag