

للغابات بكين بجامعة الدخول تسجيل نظام تحليل

على ونشرت بالعربية بالأصل مكتوبًا كان المقال هذا

الإنترنت. عبر الدخول تسجيل في للزراعة بكين جامعة يستخدمه الذي للنظام العكسية الهندسة عملية المقال هذا يتناول خلل من بالشبكة يتصل الذي المستخدم أفعال تقلد لكيتي ح ما برنامجي، بنظام الدخول تسجيل عملية تقلد هو الهدف وي. متصفح

الدخول. تسجيل عملية خلل إرسالها يتم التي الشبكة الطلبات مراقبة يمكننا، تطوير أدوات باستخدام CheckLogin.jsp على بناء إبداله يتم الذي index.jsp إلى طلب يليه، CheckLogin.jsp إلى هو الأول الطلب

أقرب. بشكل CheckLogin.jsp إلى ننظر دعونا

فحص خلل من action؟ هو ما ولكن والقيمة. المفتحات من أزواج عدة على ويحتوي طلب يستخدم أنه نرى المصدرة: مشاهدتها يمكننا التطوير، أدوات في

الصفحة: مصدر فحص يمكننا، action-الفعلي القيمة لإيجاد

الثنائي. السطر هي action قيمة

عبر كانت سواء الجامعي، الحرم في مكان أي من الدخول تسجيل نظام إلى الوصول يمكن؟ عنوان على نحصل كيف ولكن تلقائي؟ بشكل عليه الحصول يمكننا كيف ديناميكي. هو عنوان نوم. غرفة في باسلكي اتصال أو

الأولى؟ الصورة تذكر

من استخرجها يمكننا إليه. الوصول يمكن لا أي الدخول تسجيل النظام يعرف تلقائيًا. عنوان الويب الصفحة توفر الويب. الصفحة

يسمى مماثل ملحق يوجد وفيرفوكس بسرعة. الويب الصفحة كود من محددة أجزاء لإنشاء مفيدة أدوات يوفر

الصفحة. على عنوان على النقر يمكننا الميكروسكوب. أيقونة العنصر فحص أداة استخدمنا أننا من الرغم على النص. محتوا داخل تحديداً login_txt الفئة مع علامة داخل هو عنوان أن وتكشف بنيت التطوير أدوات سيعرض المطابق. الأول العنصر first() ويمثل، استعلام مع تتطابق التي العنصر select وظيفية يجد أن يمكن الدخول. تسجيل عملية تقلد الآن يمكننا والقيمة، المفتحات أزواج جميع مع

سنستخدم لأننا ذلك الطلب. post.abort() يوقف الطلب. جسم في والقيمة المفتحات أزواج يرسل من httpClient يتم لم إذا الإمكان. قدر الاتصال استخدام إعادة org.apache.http فئات تفضل لاحقة. طلبات في أخرى مرة استثناء. الاتصال نفس باستخدام آخر طلب إرسال يسبب أن يمكن الطلب، إنهاء

لاحقًا. ذلك سأشرح httpClient استخدام إعادة نريد لماذا

الممرور. وكلمة المستخدم اسم صرح من تحقق فقط للربط هذه بالشبكة. للربط كاف غيري checkLogin.jsp إلى إرسال الرد. الرمز رؤية يمكننا طباعة، بيان إضافة خلل من

التوصيل. في خطأ إلى و404 خاطئة، اعتماد بيانات إلى 303 يرمز نجاح، دخول تسجيل إلى 200 يرمز

طلب وهي index.jsp، هي تنفيذه التي التي الثانية الصفح

ممثل userid مبرر يتطلب الذي connect_action.jsp إلى طلب تقلد عليا الشبكة. بلوغ يمكننا لا ذلك، بعد
كيف الرقم. من 1 من أقل هو السابق الرقم لديه الذي للطلب userid أن لاحظت طالب. رقم مع يتوافق الذي userid=88888
القيمة؟ هذه على الحصول يمكننا

userid مع الشيء بنفس القيام يمكننا هل الوب. الصفحة من عنوان استخرجنا أننا تذكرت لاحظ، لحسن

الثاني يرجعه الذي الصفحة مصدر يحتوي connect.jsp على اللوجيك نفس ولكن المنقطة، الصفحة من الصورة هذه
إرساله. علينا يجب التي التالية للصفحة المطلوبين والقيمة المفتاح زوج على

المحتوى هو group(1)، userid=88888، مثل الكامل التتابع هو group(0) معياريًا. تعبيرًا على نعتد الحالة، هذه في
يتطابق التعبير كان إذا ما يحدد find() أكثر. أو واحدة مرة حدوث يعني + و رقم، أي تطابق \d. 88888، مثل الأقواس داخل
<frame مثل src كان إذا بأكمله. السلسلة مع يتطابق التعبير كان إذا ما يحدد matches() بين السلسلة من جزء أي مع
بأكمله. السلسلة مع يتطابق لا المعتاد التعبير لأن false سيجع matches() فإن، userid=88888&ip="،

الكود هو هذا:

```
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.util.ArrayList;
import java.util.LinkedList;
import java.util.List;
import java.util.regex.Matcher;
import java.util.regex.Pattern;

import org.apache.http.HttpEntity;
import org.apache.http.HttpResponse;
import org.apache.http.NameValuePair;
import org.apache.http.client.HttpClient;
import org.apache.http.client.entity.UrlEncodedFormEntity;
import org.apache.http.client.methods.HttpGet;
import org.apache.http.client.methods.HttpPost;
import org.apache.http.client.utils.URLEncodedUtils;
import org.apache.http.cookie.Cookie;
import org.apache.http.impl.client.AbstractHttpClient;
import org.apache.http.impl.client.DefaultHttpClient;
import org.apache.http.message.BasicNameValuePair;
import org.apache.http.protocol.HTTP;
import org.apache.http.util.EntityUtils;
import org.jsoup.Jsoup;
import org.jsoup.nodes.Document;
import org.jsoup.nodes.Element;
```

```

import org.jsoup.select.Elements;

public class Login{

    static void print(String format, Object... args) {
        System.out.println(String.format(format, args));
    }

    public static void main(String[] args) {
        HttpClient httpClient = new DefaultHttpClient();
        String ip;
        String userId;
        String username="130888888";
        String password = "88888888";

        ip=cssQueryFirstText("http://login.bjfu.edu.cn/index.jsp","span.login_txt");

        doPost(httpClient,"http://login.bjfu.edu.cn/checkLogin.jsp",
            "username",username,"password",password,
            "ip",ip,"action","checkLogin.jsp");
        String content=doGet(httpClient,"http://login.bjfu.edu.cn/user/index.jsp",
            "ip",ip,"action","connect");
        userId=userId(content);
        doGet(httpClient,"http://login.bjfu.edu.cn/user/network/connect_action.jsp",
            "userid",userId,"ip",ip,"type","2");
    }

    static String userId(String html){
        Document doc=Jsoup.parse(html);
        Element elem=doc.select("frame#main").first();
        String src=elem.attr("src");
        Pattern pattern=Pattern.compile("userid=(\\d+)");
        Matcher matcher=pattern.matcher(src);
        String ans="";
        if(matcher.find()){
            ans=matcher.group(1);
        }
        return ans;
    }
}

```

```

static String cssQueryFirstText(String url,String cssQuery) {
    String ip=null;
    try{
        Document doc=Jsoup.connect(url).get();
        Elements elems=doc.select(cssQuery);
        Element elem=elems.first();
        ip=elem.text();
    }catch(Exception e){
        e.printStackTrace();
    }
    return ip;
}

static String doGet(HttpClient httpClient, String url, String... pairs) {
    String entityContent=null;
    try {
        url = makeGetSrl(url, pairs);
        HttpGet get = new HttpGet(url);
        HttpResponse response = httpClient.execute(get);
        //print("%d", response.getStatusLine().getStatusCode());
        entityContent = entity(response);
        EntityUtils.consume(response.getEntity());
    } catch (IOException e) {
        e.printStackTrace();
    }
    return entityContent;
}

static void printEntity(HttpResponse rp){
    print("%s",entity(rp));
}

static String entity(HttpResponse response) {
    StringBuilder sb = new StringBuilder("");
    try {
        HttpEntity entity = response.getEntity();
        if (entity != null) {
            BufferedReader br = new BufferedReader(new InputStreamReader(
                entity.getContent()));
            String line = null;

```

```

        while ((line = br.readLine()) != null) {
            sb.append(line + "\n");
        }
    }
} catch (Exception e) {
    e.printStackTrace();
}
return sb.toString();
}

static String makeGetSrl(String url,String... pairs) {
    if(!url.endsWith("?")){
        url+="?";
    }
    List<NameValuePair>params=new LinkedList<NameValuePair>();
    int len=pairs.length;
    for(int i=0;i<len/2;i++){
        params.add(new BasicNameValuePair(pairs[2*i],pairs[2*i+1]));
    }
    String paramsStr=URLEncodedUtils.format(params,"utf-8");
    url+=paramsStr;
    return url;
}

static String doPost(HttpClient httpClient, String url, String... pairs) {
    String entityContent = null;
    try {
        HttpPost post = new HttpPost(url);
        List<NameValuePair> params = new ArrayList<NameValuePair>();
        for (int i = 0; i < pairs.length / 2; i++) {
            params.add(new BasicNameValuePair(pairs[2 * i], pairs[2 * i + 1]));
        }
        post.setEntity(new UrlEncodedFormEntity(params, HTTP.UTF_8));
        HttpResponse response = httpClient.execute(post);
        entityContent = entity(response);
        //print("%d", response.getStatusLine().getStatusCode());
        post.abort();
    } catch (Exception e) {
        e.printStackTrace();
    }
}

```

```

        return entityContent;
    }

    private static String getCookies(HttpClient client) {
        StringBuilder sb = new StringBuilder();
        List<Cookie> cookies = ((AbstractHttpClient)
            client).getCookieStore().getCookies();
        for(Cookie cookie: cookies)
            sb.append(cookie.getName() + "=" + cookie.getValue() + ";");
        return sb.toString();
    }
}

```

الجامعة. لشبكة صال ح ساب دون تشغله يمكنك لا قد أنه لاحظ. [] [] [] [] [] على الكامل الكود يوجد

إذا ما لتحديد الطعنات [] [] [] صفحات تستخدم تلقائيًا. الطعنات تخزن يوفر أنه هو HttpClient نفس استخدا إعادة سبب الوقت. في خطأ إلى يؤدي قد آخر متصفح إلى [] [] [] [] من رابط نسخ أن في السبب هو هذا الجلسة. نفس من الطلبات لأن باس تخداه! استمتع معياري. عبارات لتمارين الإنترنت على أدوات توجد جذا. مفيدة أدوات هي معياري وعبارات jsoup