

首先是反射 xss，在搜索框中我们输入 `<script>alert(/xss/)</script>` 会弹框



上源码，这里防护了 sql 注入，但是没有防护 xss

```
if (!isset($_GET['query']))
{
    http_redirect("/error.php?msg=Error, need to provide a query to search");
}

$pictures = Pictures::get_all_pictures_by_tag($_GET['query']);
?>
```

```

function get_all_pictures_by_tag($tag)
{
    $query = sprintf("SELECT *, UNIX_TIMESTAMP(created_on) as created_on_unix from pictures where tag like '%e'",
        mysql_real_escape_string($tag));
    $res = mysql_query($query);
    if ($res)
    {
        while ($row = mysql_fetch_assoc($res))
        {
            $to_ret[] = $row;
        }
        return $to_ret;
    }
    else
    {
        return False;
    }
}

```

接着再来个存储型 xss，留言板处

WackoPICKO.com

Home
Upload
Recent
Guestbook
Login

Guestbook

See what people are saying about us!

- by fds

Hi, I love your site!

- by adam

Name:

Comment:

<script>alert("XSS!");</script>

[Home](#) | [Admin](#) | [Contact](#) | [Terms of Service](#)

192.168.88.137:86 显示

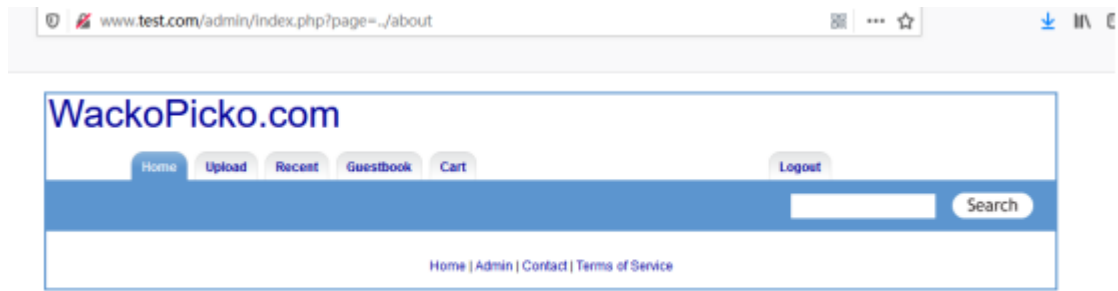
XSS!

<script>alert("XSS!");</script>

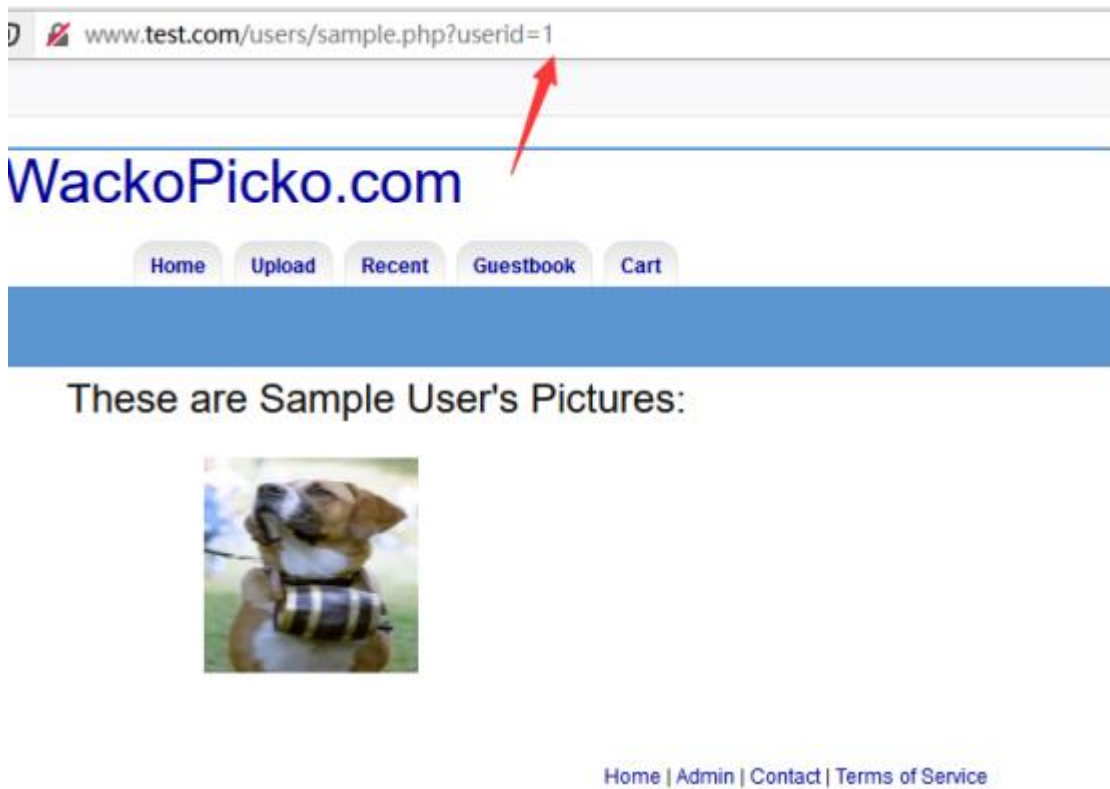
一直刷新就会一直弹框

后台存在弱口令，一个 admin，admin 账号和密码

后台有个包含漏洞





越权，修改 userid 可以看到其他用户的页面



购买照片时优惠券可以多次使用

Welcome to your cart admin

Pic name	Sample Pic	Price	Delete?
This grows outside my house		40 Tradebux	<input checked="" type="checkbox"/>
The house I share		20 Tradebux	<input checked="" type="checkbox"/>

Coupon Code	Coupon Amount
SUPERYOU21	10% Off
SUPERYOU21	10% Off
SUPERYOU21	10% Off
SUPERYOU21	10% Off
SUPERYOU21	10% Off
SUPERYOU21	10% Off
SUPERYOU21	10% Off

Enter Coupon Code:

[Continue to Confirmation](#)

[Home](#) | [Admin](#) | [Contact](#) | [Terms of Service](#)

SUPERYOU21 , 这样就可以使用零元购买到你想要的东西

当你登入用户的时候这边

Hello admin, you got 100 Tradebuxs to spend!

Cool stuff to do:

[Who's got a similar name to you?](#)

[Your Uploaded Pics](#)

[Your Purchased Pics](#)

Enter in our contest:

Answer the question for a chance to win 100 Tradebux!

What's your favorite color?

输入框又是一个 XSS，`<script>alert("XSS!");</script>`

Hello admin, you got 100 Tradebuxs to spend!

Cool stuff to do:

[Who's got a similar name to you?](#)

[Your Uploaded Pics](#)

[Your Purchased Pics](#)

Enter in our contest:

Answer the question for a chance to win 100 Tradebux!

What's your favorite color?

192.168.88.137:86 显示

XSS!

确定

192.168.88.137:86/submitname.php?value=<script>alert("XSS!");</script>

查看源代码

```
1 <?php
2 require_once("include/html_functions.php");
3 require_once("include/users.php");
4 session_start();
5 require_login();
6
7 if (!isset($_GET['val'])) {
8     http_redirect(Users::HOME_URL);
9 }
10
11
12
13 ?>
14
15 <?php our_header("home"); ?>
16
17 <div class="column prepend-1 span-24 first last">
18     <p>
19         Your favorite color is <?=$_GET['value']?> and you've been entered in our contest!
20     </p>
21 </div>
22
23 <?php our_footer(); ?>
```