New issue

Jump to bottom

There is an identity forgery vulnerability #1

Open thekingofsex opened this issue on Feb 17, 2021 · 1 comment

thekingofsex commented on Feb 17, 2021

No description provided.

thekingofsex commented on Feb 17, 2021 • edited Author

Student users can modify the cookie and forge the identity of the administrator after login
Look at the following code：
/Manager/index.aspx

```
public partial class Manager_index : System.Web.UI.Page
{
    protected void Page_Load(object sender, EventArgs e)
    {
        LearnSite.Common.CookieHelp.JudgeIsAdmin();
        if (!IsPostBack)
            Master.Page.Title = LearnSite.Common.CookieHelp.SetMainPageTitle() + "系统设置页面";
    }
    protected void Btnlogout_Click(object sender, EventArgs e)
    {
        if (Request.Cookies[LearnSite.Common.CookieHelp.mngCookieNname] != null)
        {
            LearnSite.Common.CookieHelp.ClearManagerCookies();
            LearnSite.Common.Others.ClearClientPageCache();
        }
        System.Threading.Thread.Sleep(300);
        Response.Redirect("~/Teacher/index.aspx", false);
    }
}
```

The administrator login page judges the user's identity through JudgIsAdmin() function.
Let's look at this function:
CookieHelp.cs

```
 public static void JudgeIsAdmin()
        {
            if (HttpContext.Current.Request.Cookies[mngCookieNname] == null)//没登录跳出
            {
                HttpContext.Current.Response.Redirect("~/Teacher/index.aspx", true);
            }
            else
            {
                string hs = HttpContext.Current.Request.Cookies[mngCookieNname]["Hs"].ToString();
                string hid = HttpContext.Current.Request.Cookies[mngCookieNname]["Hid"].ToString();
                if (hs != Common.WordProcess.GetMD5(hid.ToString()))
                {
                    ClearManagerCookies();//非法cookies，清除再跳转
                    Others.ClearClientPageCache();
                    System.Threading.Thread.Sleep(500);
                    HttpContext.Current.Response.Redirect("~/Teacher/index.aspx", true);
                }
            }
        }`
```

The identity of the administrator is verified by cookie.
Let's check how the administrator cookie is generated.

```
      public static string cfx = LearnSite.Common.XmlHelp.GetCookiesFix();
       public static string serverName = LearnSite.DBUtility.DbLinkEdit.serverNameFix();
       public static string tempcfx = cfx + serverName;
       public static string stuCookieNname = "S" + tempcfx;
       public static string teaCookieNname = "T" + tempcfx;
       public static string mngCookieNname = "M" + tempcfx;
```

So we only need to change the initials of the key of the student user's cookie to the initials of the administrator user, and then change the value of the cookie to the corresponding hid and hs of the administrator to complete the identity forgery

thekingofsex changed the title ~~there is~~ **There is an identity forgery vulnerability** on Feb 17, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant