فایل راهنمای جلوگیری از حمله XSS در نرم افزار TZHavades (یزد)

نکات:

1. نباید تا جای ممکن ورودی های خام در نرم افزار نمایش داده شوند
2. تمامی ورودی ها برای اسکریپت های خطرناک باید چک شوند

بدین منظور در نرم افزار 2 تغییر کلی بوجود آمده است:

1. در فایل webconfig برای کنترل تمامی وودی ها از خطر XSS تگ validateRequest اضافه گردید:

[Old] <pages enableSessionState="true">

[New] <pages enableSessionState="true" validateRequest="true">

1. در صفحه oops.aspx که برای نمایش خطا طراحی شده و تمامی اطلاعات خطا را نمایش میدهد تغییر زیر بوجود آمده:

[Old] lblErrorMessage.Text = lMessage;

[New] lblErrorMessage.Text = Server.HtmlEncode(lMessage);