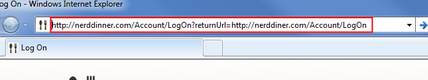
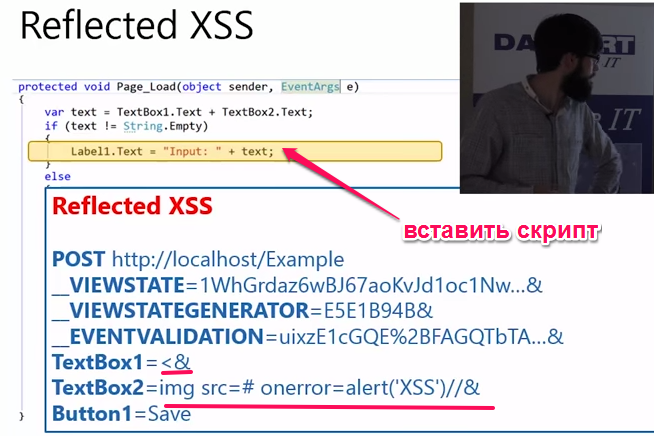
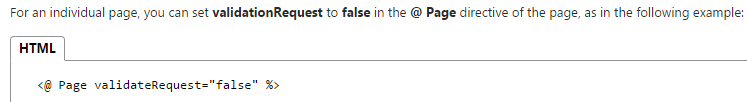
Чтобы не подменили адрес его нужно проверять Url.IsLocalUrl()

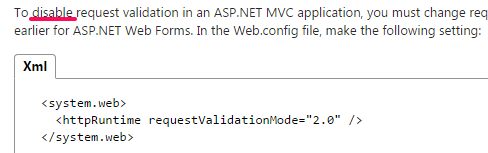


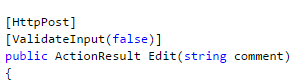




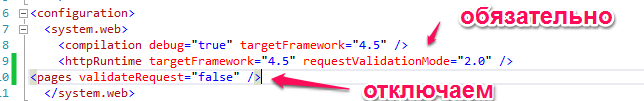
request validation

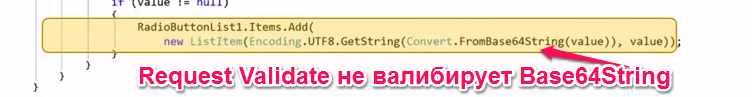


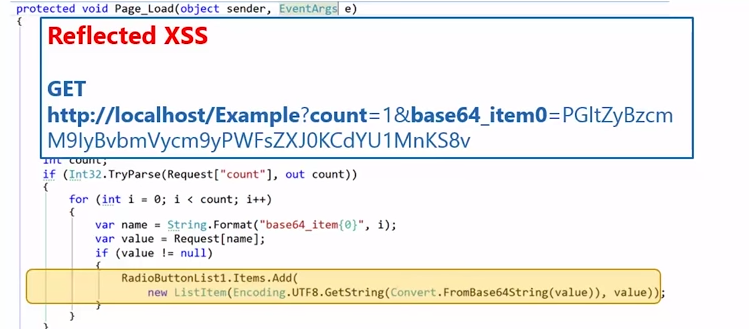




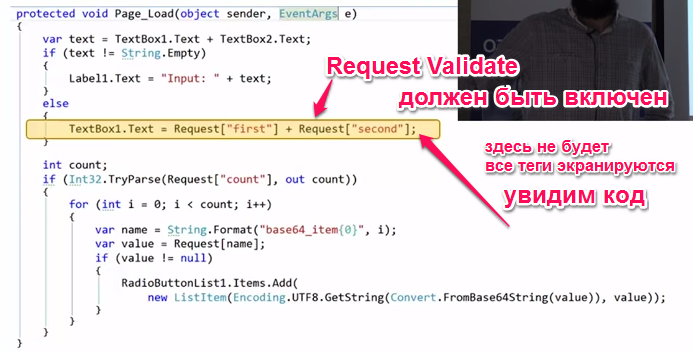


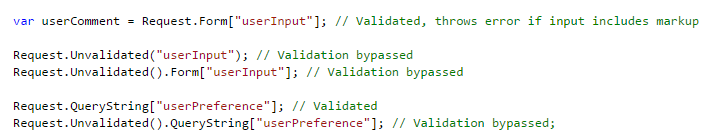


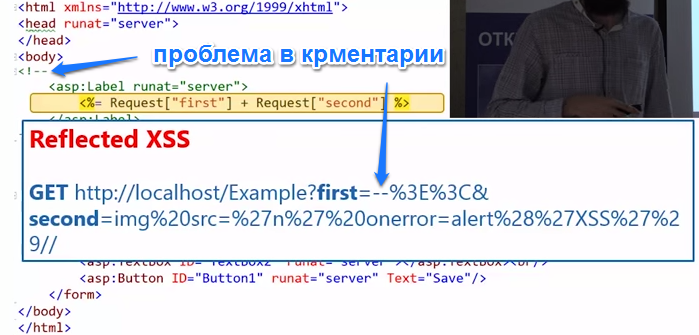




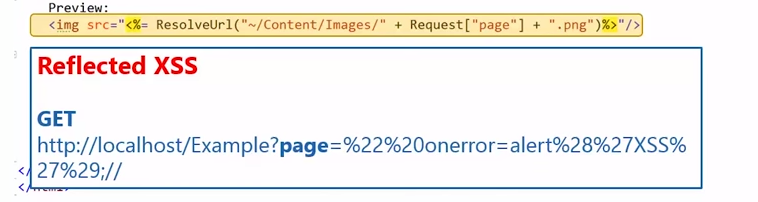
Некоторые теги Label поглощает script,alert и т.д. не дает вызвать js код



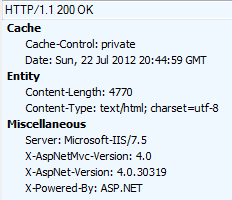




Уязвимость page=%22%20onerror=%28%27XXS%27%29;//



Скрытие информации

Многие не придают этому внимания, но я считаю, что данный пункт весьма важен. Выбирая когда-то замок для металлической двери я узнал, что многие замки вскрываются элементарно с помощью дрели, будь там три толстых ригеля (цилиндра, которые выезжают), но достаточно просверлить одно отверстие в нужном   
месте (так сказать нанести точечных удар по слабым местам) и замок открыт. Аналогично, если вы говорите, что у вас такой-то IIS, такая-то версия ASP.NET и т.д. Вы оказываете неоценимую помощь взломщику! Я люблю чистить логи Elmah с кружкой чая и смотреть как у меня на сайте пытаются найти php, mysql, с помощью чудных сервисов определить какая CMS используется и т.д.  
  
Вот, что сейчас возвращает мой сайт:  
  
  
  
Убираем X-Powered-By:

<system.webServer>

...

<httpProtocol>

<customHeaders>

<remove name="X-Powered-By" />

</customHeaders>

</httpProtocol>

...

</system.webServer>

Версию ASP.NET:

<system.web>

...

<httpRuntime enableVersionHeader="false" />

...

</system.web>

Версию MVC в Application\_Start:

MvcHandler.DisableMvcResponseHeader = true;

И самое сложное — это сервер, для чего мы сделаем HttpModule:

public class CustomServerHeaderModule : IHttpModule

{

public void Init(HttpApplication context)

{

context.PreSendRequestHeaders += OnPreSendRequestHeaders;

}

public void Dispose() { }

private void OnPreSendRequestHeaders(object sender, EventArgs e)

{

HttpContext.Current.Response.Headers.Set("Server", "Apache 2000 Server");

}

}

и добавим в конфиге:

<system.webServer>

...

<modules runAllManagedModulesForAllRequests="true">

...

<add name="CustomServerHeader" type="HackingMVC.HttpModules.CustomServerHeaderModule" />

</modules>

...

<system.webServer>

В итоге мы получили вот такой результат:  
  
