VB XSS

BY UNCLE RAT

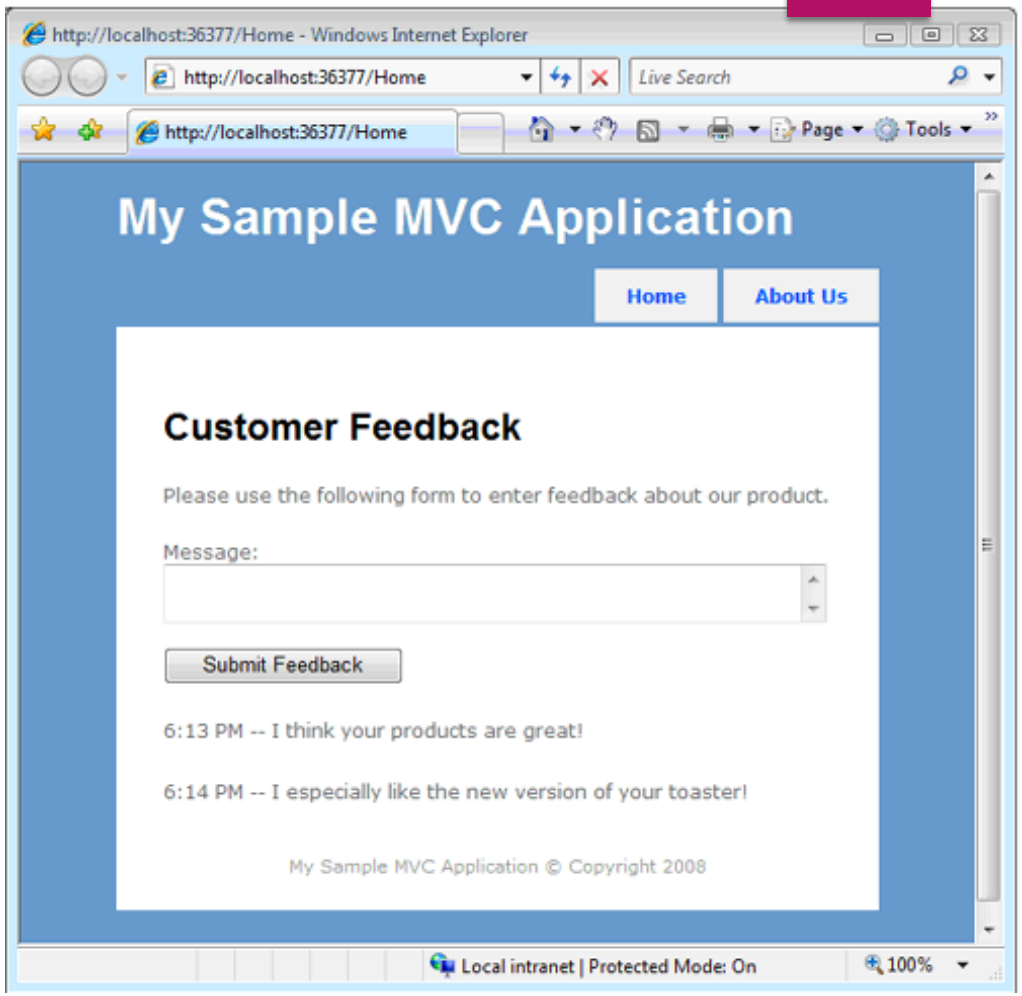
Agenda

- What is it
- Attack strategy
- Defences
- Furher resources

What is it

What is it

- Very similar to Javascript XSS
- Unsanitized input leads to XSS
- Let's look at an example >>>>



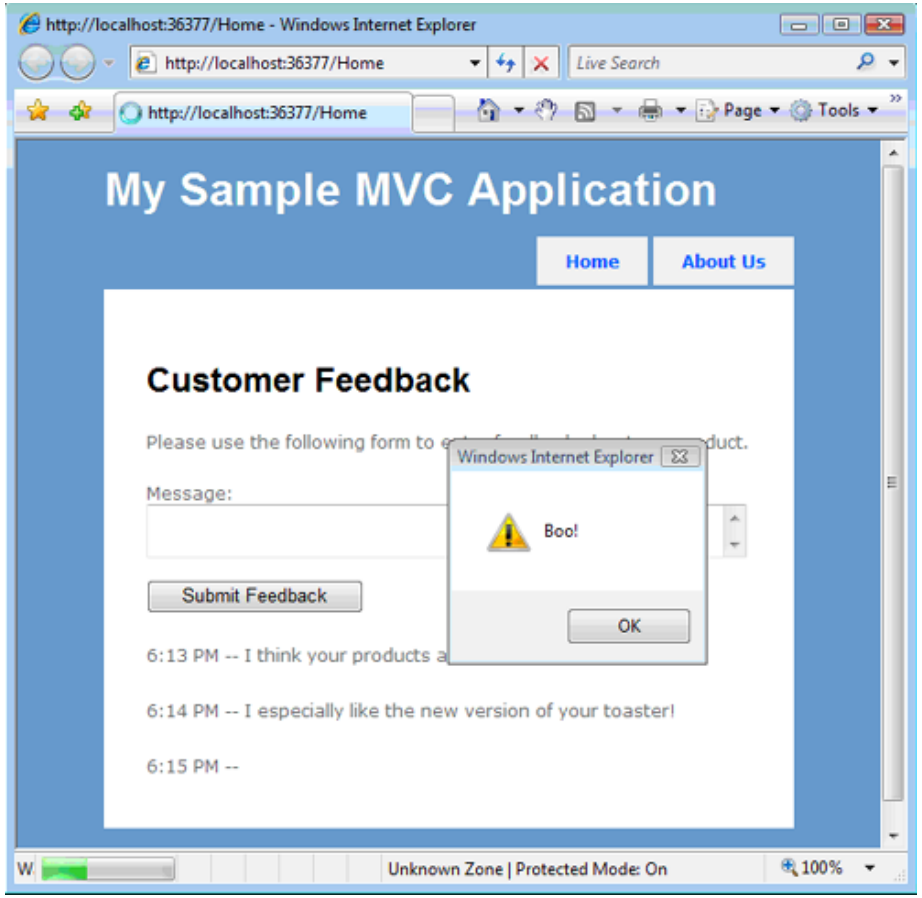
What is it

…

- <% For Each feedback As CustomerFeedback.Feedback In ViewData.Model% >
  -
    - <%=feedback.EntryDate.ToShortTimeString()%> --
      - <%=feedback.Message%>
  -
- <% Next %>

- </asp:Content>

What is it



HTML Copy

```
<script>alert("Boo!")</script>
```

Attack strategy

Attack strategy

- Similar to stored XSS
  - <img src=x>
  - If it renders a broken image, investigate further

Defences

Defences

- HTML encoding the view
  - <%=Html.Encode(feedback.Message)%>
- HTML encoding the controller
  - newFeedback.Message = Server.HtmlEncode(message)