Hacking ASP.Net: Tips and Tricks

James Jardine
james@secureideas.com
(866) 404-7837
@JardineSoftware

©2013 Secure Ideas LLC | http://www.secureideas.com
James Jardine

- Principal Security Consultant at Secure Ideas
- .Net Developer Since the Beta Release
- SANS Instructor and Author
  - Dev544: Secure Coding in .Net
- Open Source Projects
  - EventValMod - http://sourceforge.net/projects/eventvalmod
- Podcaster
  - Professionally Evil Perspective
  - Down the Rabbit Hole
- Blogs

©2013 Secure Ideas LLC | www.secureideas.com
Topics

- ASP.Net
- RequestValidation
- ViewState
- EventValidation
- GET/POST & Postback
- Conclusion
ASP.Net

Versions

• 1.1
• 2.0
• 3.0
• 3.5
• 4.0
• 4.5 *

Editions

• WebForms
• MVC
• Web Pages
• Web API
• WCF
Testing ASP.Net

• Similar to other technologies
  – GETs/POSTs, etc
  – AJAX
  – Cookies, Hidden Fields, Forms
  – Session State, Authentication

• Differentiators
  – Request Validation
  – View State
  – Event Validation
  – Other Built In Controls
Request Validation

- Attempt to block XSS Attacks
- In 2.0+ only works for **HTML** Context
  - `<[char]`, `!`, `?`, `/>`, `&`#
- Prior to 2.0 most likely disabled

---

Server Error in '/' Application.

A potentially dangerous Request.Form value was detected from the client (ctl00$MainContent$txtUserName="j<s").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkId=212874.
Request Validation Bypass

- Not Really!
- If database stores data as varchar (not nvarchar)
- Use unicode-wide `%uFF1C` `<`
- RequestValidation doesn't detect this but...

- Database will convert it to the `<` character

Of course output encoding does block this as well
Request Validation Bypass 2

- Addition of % Character (<%tagname>)
- Reported to work in IE (I was unsuccessful)
- Reported by Zamir Paltiel (http://www.securityfocus.com/archive/1/524043)

- An older bypass was to use a null character like `<%00tagname>`
- Browser specific and doesn't really work anywhere

Of course output encoding does block this as well
Request Validation Config

- Set in the Web.Config File
  
  `<system.web>
  <pages validateRequest="true" />
  </system.web>`

- Set at the Page Level
  
  `<%@ ValidateRequest="true" %>`
Yes, It’s Interesting

ViewState v2.0 compatible [MAC is not enabled]
ViewState

- Base64 Encoded By Default
  - Can be encrypted

- Vulnerabilities
  - Parameter Tampering, XSS, Info Leakage

©2013 Secure Ideas LLC | www.secureideas.com
ViewState Manipulation

ViewState - Protected

Server Error in '/' Application.

Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

Source Error:

[No relevant source lines]

Source File: c:Users\obyeknu\AppData\Local\Temp\Temporary ASP.NET Files\root\06eacefd\4967d7bApp_web_ypSjxqvk.4.cs  Line: 0

Stack Trace:

ViewStateException: Invalid viewstate.
    Client IP: 127.0.0.1
    Port: -
    User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
    ViewState: V69pcyPScHytr81c3qgcS8owMzVzyV81a8XO2hR8ozZ95yYNINQ2ZUn5jo9Rbcsu
    Referer: http://localhost:16442/ControlPanelSection3.aspx
    Path: /ControlPanelSection3.aspx

[HttpException (0x80004005): Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.]

[HttpException (0x80004005): Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.]

[HttpException (0x80004005): Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.]

©2013 Secure Ideas LLC | www.secureideas.com
The Problem

This is **wrong** common advice!!

Solution 1

Refer to the following thread for a discussion about this issue:

http://forums.asp.net/t/955145.aspx[^]

You can fix this by setting the `EnableViewStateMAC` property to false. Refer to more information about `EnableViewStateMAC` in the link given below:


ViewStateMac

- Provides Tamper Protection for:
  - ViewState
  - EventValidation

Web.Config

```xml
<pages enableViewStateMac="true"/>
```

Page Level

```csharp
<%@ Page Language="C#" EnableViewStateMac="true"...
```

©2013 Secure Ideas LLC | www.secureideas.com
Event Validation

- Protects Drop Down Lists
- Protects against forged post backs
- Protected by ViewStateMac
- Creates an array of numeric hashes
- Not User Specific
  - Doesn't Protect against CSRF

```
<input type="hidden" name="__EVENTVALIDATION" value="/wEWBALsL0qAu3wv7QBAqnOkfQNAoznisYG"/>
```
Event Validation - EventValMod

- Modifies the Event Validation field
- Stand Alone App / Written in .Net
- http://sourceforge.net/projects/eventvalmod
Event Validation - VEHICLE

ViewState Hidden Event Enumerator
- Formerly known as ria-scip

Works with ZAP

Features
- Event Execution of Disabled/Invisible Controls
- Server Control Property Injection
- Edit the ViewState Field
- Error-Based Control Name Enum
- ViewState/EventValidation Reconstruction

https://github.com/hacktics/vehicle
EventValidation Config

- Set in the Web.Config File
  ```xml
  <system.web>
    <pages enableEventValidation="true" />
  </system.web>
  ```

- Set at the Page Level
  ```jsp
  %@ EnableEventValidation="true" %
  ```
Bad, Bad, Bad!!

ViewState v2.0 compatible [MAC is not enabled]
ViewStateUserKey

- Protects against Cross Site Request Forgery
  - Provides a user "salt" to ViewStateMac
- Not enabled by default
- Only works for requests with ViewState
  - http://www.testsite.mm/deleteuser.aspx?id=5 (doesn't work)

- Recommendation:
  ```csharp
  protected void Page_Init(object sender, EventArgs e)
  {
      Page ViewStateUserKey = Session.SessionId;
  }
  ```
Postback

- Webforms are based around "Postbacks"
- Caused by Events (ex. button_click)
- Triggered by ___ViewState or ___EventTarget

```javascript
if (!Page.IsPostBack){
    // Authorization/Populate Data
    lblCopy.Text = "copy 2013";
    if(!User.IsInRole("Admin"))
        Response.Redirect("Unauthorized.aspx");
}
else{
    // Execute Events
}
```
Postback Attacks

- **Authorization Bypass**
  ```javascript
  if(!User.IsInRole("Admin"))
  Response.Redirect("Unauthorized.aspx");
  ```
  
  Recommendation:
  - Check Authorization on Every Request

- **XSS (ViewState Tampering)**
  ```javascript
  lblCopy.Text = "copy 2013";
  ```

  Recommendation:
  - Enable ViewStateMac
  - Set text on every request
GET/POST Exchange

Server Control GETs and POSTs are interchangeable:
- TextBox
- ListBox
- ViewState/EventValidation
- Etc.

Based on Request Type

Can Call POST requests with GET
- Good for CSRF

Can Trigger Postback with GET request
GET/POST Fix

- **WebForms**
  
  ```
  if(Request.RequestType == "POST")
  ```

- **MVC**
  
  ```
  [HttpPost]
  void DoSomething()
  ```
Authentication Cookie

- HTTPOnly (Hard Coded)
- Secure Flag may not be set
  - Sometimes there is an error if behind a Load Balancer that strips SSL
  - Should Recommend Manually setting this value
- Self-Contained – Not tracked on server
  - Timeout is key. Lives until the timeout expires on the cookie
  - FormsAuthentication.Logout only removes cookie from the browser (doesn’t kill it)
Misc. Files

- Trace.axd
- Elmah.axd

- Use URL Authorization in the Web.config

- Web.config (crown jewels) – GOOD LUCK!!
  - IIS is set up to not serve this file
Conclusion

• ASP.Net has good security features
  – You have to understand them

• ViewStateMac is IMPORTANT!
  – EventValidation
  – ViewState
  – ViewStateUserKey

• Developers are not up to speed on these things
  – Share this info with developers
Hacking ASP.Net: Tips and Tricks

James Jardine

james@secureideas.com
(866) 404-7837
@JardineSoftware