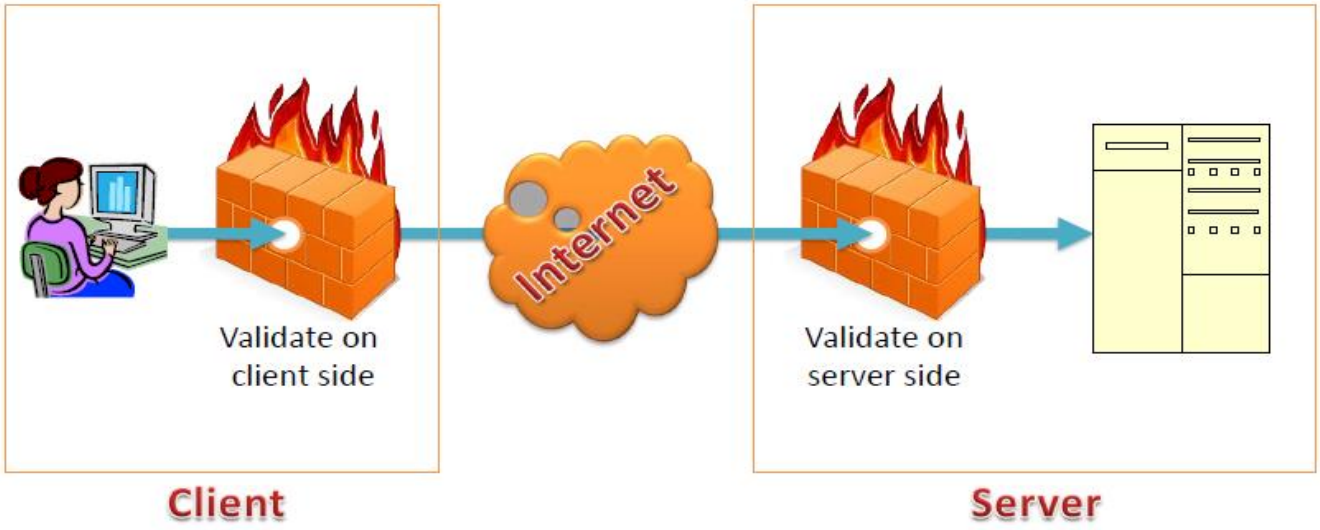
CHƯƠNG 8
VALIDATION

Giảng viên: Ths. Phạm Văn Tiệp

Validation ???

- Validation (kiểm lỗi) là một tính năng quan trọng trong ASP.NET MVC và được phát triển trong một thời gian dài
- Kiểm lỗi dữ liệu hạn chế được mã độc gửi đến server, dữ liệu sai do người dùng nhập
- Kiểm lỗi dữ liệu cần thực hiện ở 2 phía client và server



Validation – Trong ASP.NET MVC

- Với ASP.NET MVC chỉ cần viết một lần nhưng có thể kiểm lỗi cho cả 2 phía client và server
- Ở Model: thêm các data annotation để kiểm lỗi các thuộc tính
- Ở View:
  - Kiểm lỗi ở phía client: @Script.Render("~/bundles/jquery")

    Bổ sung vào form @Html.AntiForgeryToken() để tránh các request giả tạo
  - Hiển thị lỗi: @Html.ValidationMessageFor(Property) @Html.ValidationSummary()
- Ở Controller:
  - Kiểm lỗi ở phía server ModelState.IsValid(), ModelState.AddModelError()

Ví dụ

Model?
Controller?
View?

Lớp Model

```
public class EmployeeInfo
{
    [MinLength(5, ErrorMessage="Tên ít nhất 5 ký tự !")]
    public String FullName { get; set; }
    [Required(ErrorMessage="Không để trống !")]
    [Range(16, 65, ErrorMessage = "Tuổi phải từ 16 đến 65 !")]
    public int Age { get; set; }
}
```

Annotation	Thuộc tính	Mô tả
[MinLength]	FullName	Giới hạn số lượng ký tự tối thiểu là 5. Nếu không nhập vẫn hợp lệ vì không sử dụng Required
[Required]	Age	Không để trống
[Range]	Age	Giới hạn tuổi từ 16 đến 65

Controller

```
public class ValidatorController : Controller
{
    public ActionResult Index()
    {
        return View();
    }

    public ActionResult Validate(EmployeeInfo model)
    {
        if (ModelState.IsValid)
        {
            ModelState.AddModelError("", "Chúc mừng bạn đã nhập đúng !");
        }
        return View("Index");
    }
}
```

Kiểm lỗi phía server

Bổ sung thông báo lỗi model

View

```
@model Mvc5CodeDemo.Models.EmployeeInfo
<h2>Kiểm lỗi</h2>
@Html.ValidationSummary(true)
@using (Html.BeginForm("Validate", "Validator"))
{
    <div>Họ và tên</div>
    @Html.TextBoxFor(m => m.FullName)
    @Html.ValidationMessageFor(m => m.FullName)
    <div>Tuổi</div>
    @Html.TextBoxFor(m => m.Age)
    @Html.ValidationMessageFor(m => m.Age)
    <hr />
    <input type="submit" value="Kiểm lỗi" />
}

@section scripts{
    @Scripts.Render("~/bundles/jqueryval")
}
```

Thông báo lỗi chung không bao gồm lỗi đã thông báo cho từng thuộc tính

Thông báo lỗi cho từng thuộc tính

Thực hiện kiểm lỗi phía client

Thuộc tính kiểm lỗi

Annotation	Mô tả	Ví dụ
[Required]	Bắt buộc	[Required] `public String Name{get;set}`
[Range(Min, Max)]	Giới hạn số trong khoảng	[Range(16, 65)] `public String Age{get;set}`
[StringLength(Max)]	Giới hạn độ dài chuỗi	[StringLength (20, MinimumLength=5)] `public String Password{get;set}`
[EmailAddress]	Định dạng email	[EmailAddress] `public String Email{get;set}`
[CreditCard]	Định dạng số thẻ tín dụng	[CreditCard] `public String CardNumber{get;set}`
[Url]	Định dạng url	[Url] `public String Website{get;set}`
[Compare(Property)]	So sánh giá trị	[Compare("Password")] `public String ConfirmPassword{get;set}`
[RegularExpression(Regex)]	So khớp chuỗi	[RegularExpression("\d{9}")] `public String IdCard{get;set}`
[MinLength(Min)]	Giới hạn tối thiểu chuỗi, mảng	[MinLength(1)] `public String[] Hobbies{get;set}`
[MaxLength (Max)]	Giới hạn tối đa chuỗi, mảng	[MaxLength (255)] `public String Description{get;set}`

HTML 5 ELEMENT

- [DataType(DataType.Password, ErrorMessage = "")]

- DataType.CreditCard
- DataType.Currency
- DataType.Date
- DataType.DateTime
- DataType.Duration
- DataType.EmailAddress
- DataType.Html
- DataType.ImageUrl
- DataType.MultilineText
- DataType.Password
- DataType.PhoneNumber
- DataType.PostalCode
- DataType.Text
- DataType.Time
- DataType.Upload
- DataType.Url

Kiểm lỗi bằng tay

```
public ActionResult Validate(String FullName, int Age)
{
    if (String.IsNullOrEmpty(FullName))
    {
        ModelState.AddModelError("FullName", "Không để trống họ và tên");
    }
    else if (FullName.Length < 5)
    {
        ModelState.AddModelError("FullName", "Ít nhất 5 ký tự !");
    }

    if (Age < 16 && Age > 65)
    {
        ModelState.AddModelError("Age", "Tuổi phải từ 16 đến 65 !");
    }

    if (ModelState.Count == 0) // không có lỗi nào
    {
        ModelState.AddModelError("", "Chúc mừng bạn đã nhập đúng !");
    }
    return View("Index");
}
```

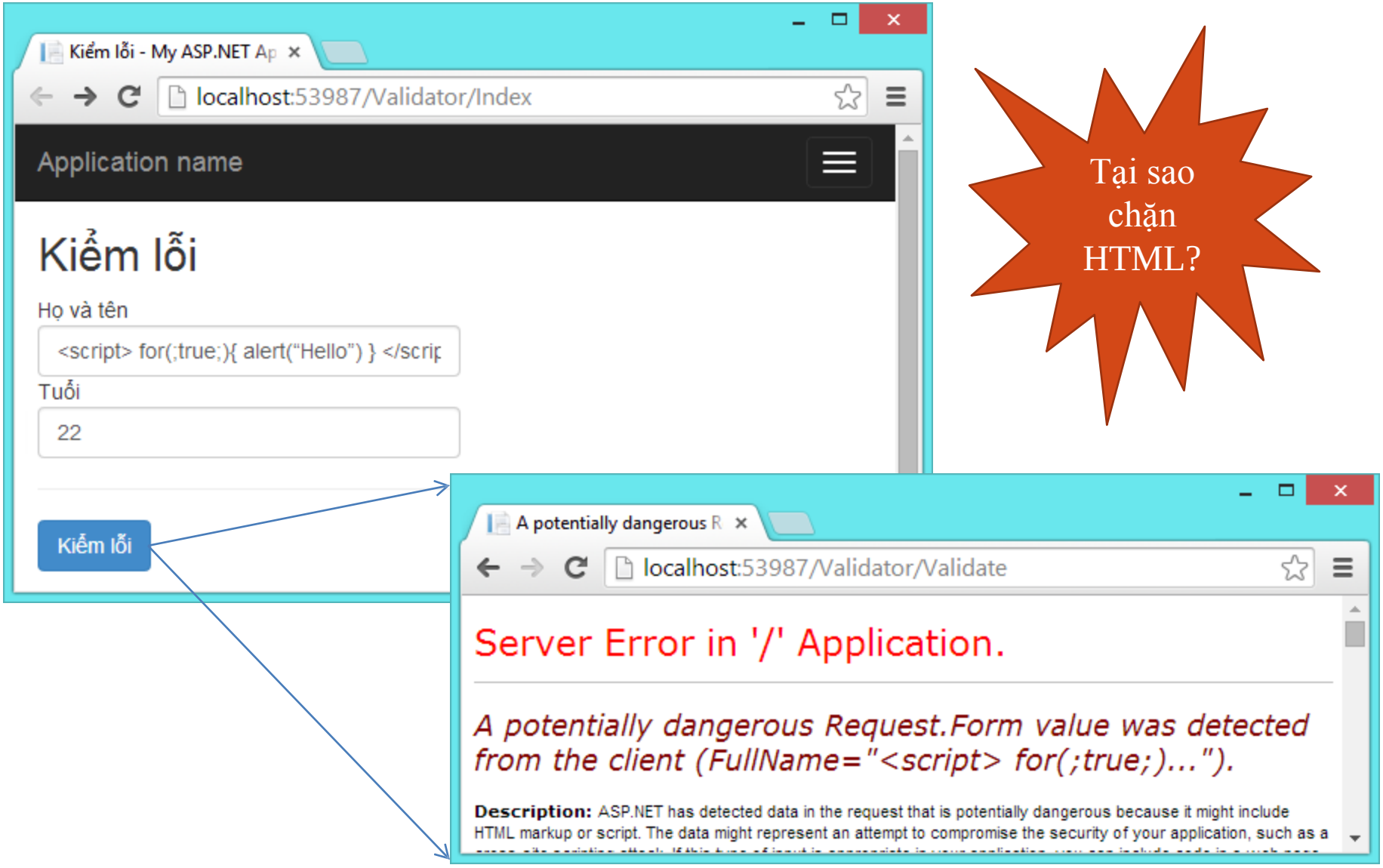
Thuộc tính kiểm lỗi tùy biến

```
public sealed class EvenNumberAttribute: ValidationAttribute
{
    public EvenNumberAttribute() : base("Vui lòng nhập số chẵn !") { }

    public override bool IsValid(object value)
    {
        if (value == null)
        {
            return true;
        }
        return Convert.ToInt64(value) % 2 == 0;
    }
}
```

```
[EvenNumber]
public String Age{get;set}
```

XSS


Kiểm lỗi - My ASP.NET Ap
localhost:53987/Validator/Index
Application name
Kiểm lỗi
Họ và tên
<script> for(;true;){ alert("Hello") } </scrip
Tuổi
22
Kiểm lỗi
Tại sao chặn HTML?
A potentially dangerous R
localhost:53987/Validator/Validate
Server Error in '/' Application.
A potentially dangerous Request.Form value was detected from the client (FullName="<script> for(;true;)...").
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

XSS


```
[ValidateInput(false)]
public ActionResult Validate(EmployeeInfo model)
{
    if (ModelState.IsValid)
    {
        ModelState.AddModelError("",
              "Chúc mừng bạn đã nhập đúng !");
    }
    return View("Index");
}
```

Chống yêu cầu giả với

- Bổ sung **@Html.AntiForgeryToken()** vào form để tránh các request giả mạo

```
@using (Html.BeginForm("Withdraw", "Bank")) {
    @Html.AntiForgeryToken()
    <fieldset>
        <legend>Fields</legend>
        <p>
            <label for="Amount">Amount:</label>
            @Html.TextBox("Amount")
        </p>
        <p>
            <input type="submit" value="Withdraw" />
        </p>
    </fieldset>
}
```

<img src="http://.../Bank/Withdraw?Amount=9999">
<link href="http://.../Bank/Withdraw?Amount=9999">