70-486 Q&As

Developing ASP.NET MVC Web Applications

Pass Microsoft 70-486 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/70-486.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

DRAG DROP

You are building an ASP.NET MVC web application.

The application will be viewed by users on their mobile phones.

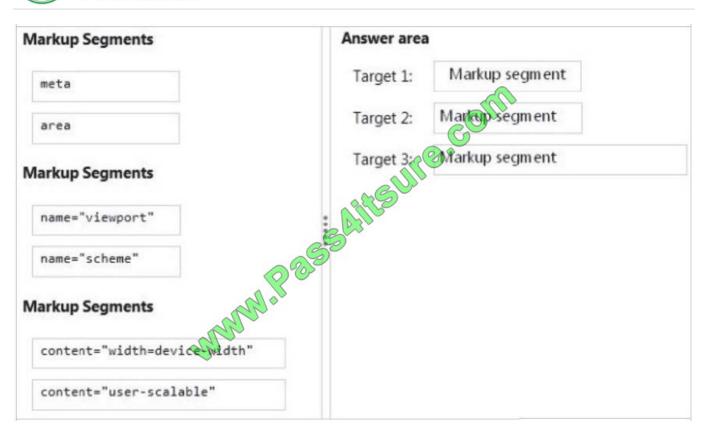You need to ensure that the page fits within the horizontal width of the device screens.
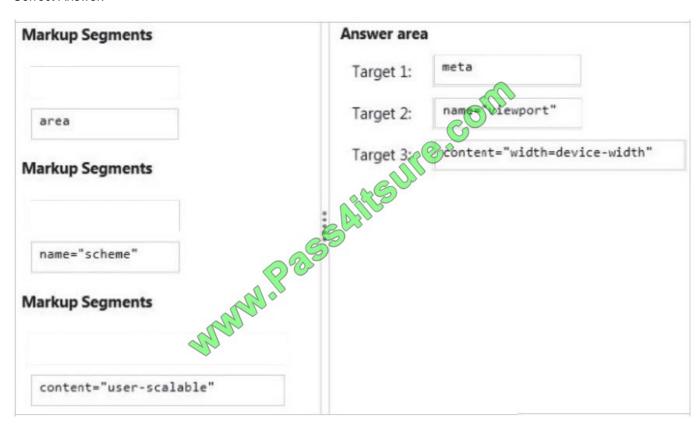
You have the following markup:

```
<!DOCTYPE html>
<html>
<head>
    <title>@ViewBag.Title</title>
    <Target 1 Target 2 Target 3>
    <link href="@Url.Content("~/Content/Site.css")"
        rel="stylesheet" type="text/css" />
    <script src="@Url.Content("~/Scripts/jquery-1.6.2.min.js")"
        type="text/javascript"></script>
</head>
<body>
```

Which markup segments should you include in Target 1, Target 2 and Target 3 to complete the markup? (To answer, drag the appropriate markup segments to the correct targets. Each line of code may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)

Select and Place:

Markup Segments

meta

area

Markup Segments

name="viewport"

name="scheme"

Markup Segments

content="width=device-width"

content="user-scalable"

Answer area

Target 1:   Markup segment

Target 2:   Markup segment

Target 3:   Markup segment

Correct Answer:

Markup Segments

area

Markup Segments

name="scheme"

Markup Segments

content="user-scalable"

Answer area

Target 1:   meta

Target 2:   name="viewport"

Target 3:   content="width=device-width"

The viewport tag in the ASP.NET MVC 4 layout file (/Views/Shared/_Layout.cshtml) sets the viewport to the device width. The following line shows the viewport tag in the ASP.NET MVC 4 layout file.

References: https://www.codeproject.com/Articles/472005/Techniques-for-Mobile-friendly-ASP-NET-MVC-web

QUESTION 2

HOTSPOT

You develop an ASP.NET MVC application. The application includes a feature that allows users to reset their passwords. The feature is enabled by a ForgotPassword controller method and a corresponding Razor view.
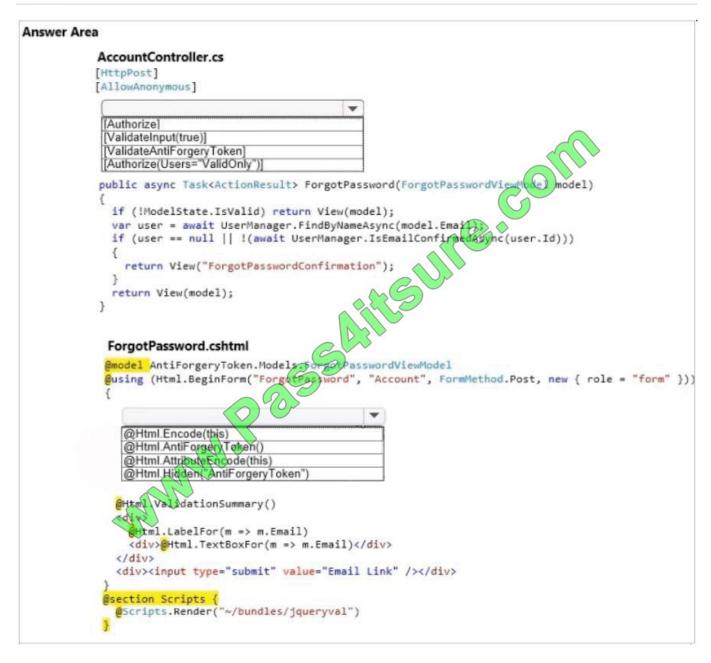
You need to prevent Cross-Site Request Forgery (CSRF) attacks.

How should you complete the relevant code? To answer, select the appropriate code segment from each list in the answer area.
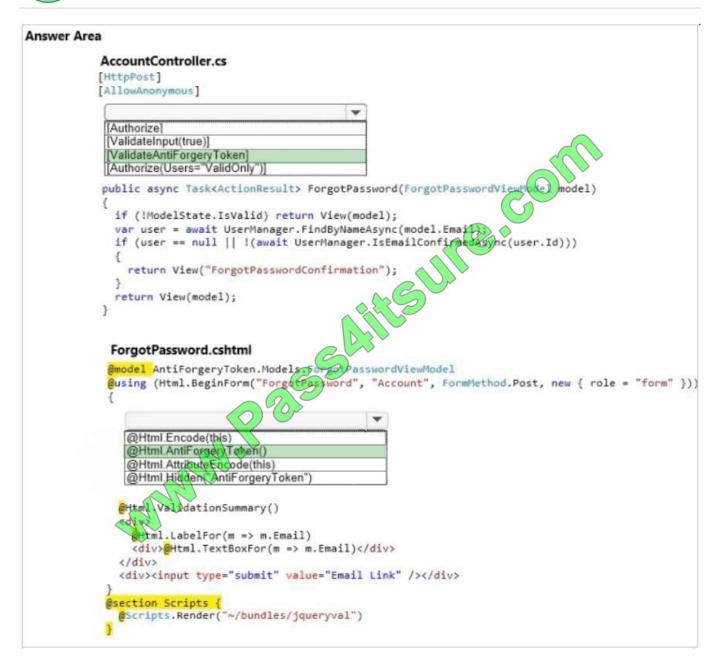
Hot Area:

Hot Area:

Answer Area

AccountController.cs
```
[HttpPost]
[AllowAnonymous]
```
```
┌─────────────────────────────────────┐ ▼
│                                      │
├─────────────────────────────────────┤
│ [Authorize]                          │
│ [ValidateInput(true)]                │
│ [ValidateAntiForgeryToken]           │
│ [Authorize(Users="ValidOnly")]       │
└─────────────────────────────────────┘
```
```
public async Task<ActionResult> ForgotPassword(ForgotPasswordViewModel model)
{
  if (!ModelState.IsValid) return View(model);
  var user = await UserManager.FindByNameAsync(model.Email);
  if (user == null || !(await UserManager.IsEmailConfirmedAsync(user.Id)))
  {
    return View("ForgotPasswordConfirmation");
  }
  return View(model);
}
```

ForgotPassword.cshtml
```
@model AntiForgeryToken.Models.ForgotPasswordViewModel
@using (Html.BeginForm("ForgotPassword", "Account", FormMethod.Post, new { role = "form" }))
{
```
```
    ┌─────────────────────────────────────┐ ▼
    │                                      │
    ├─────────────────────────────────────┤
    │ @Html.Encode(this)                   │
    │ @Html.AntiForgeryToken()             │
    │ @Html.AttributeEncode(this)          │
    │ @Html.Hidden("AntiForgeryToken")     │
    └─────────────────────────────────────┘
```
```
    @Html.ValidationSummary()
    <div>
      @Html.LabelFor(m => m.Email)
      <div>@Html.TextBoxFor(m => m.Email)</div>
    </div>
    <div><input type="submit" value="Email Link" /></div>
}
@section Scripts {
  @Scripts.Render("~/bundles/jqueryval")
}
```

Correct Answer:

Answer Area

AccountController.cs

```
[HttpPost]
[AllowAnonymous]
```

▼
[Authorize]
[ValidateInput(true)]
[ValidateAntiForgeryToken]
[Authorize(Users="ValidOnly")]

```
public async Task<ActionResult> ForgotPassword(ForgotPasswordViewModel model)
{
    if (!ModelState.IsValid) return View(model);
    var user = await UserManager.FindByNameAsync(model.Email);
    if (user == null || !(await UserManager.IsEmailConfirmedAsync(user.Id)))
    {
        return View("ForgotPasswordConfirmation");
    }
    return View(model);
}
```

ForgotPassword.cshtml

```
@model AntiForgeryToken.Models.ForgotPasswordViewModel
@using (Html.BeginForm("ForgotPassword", "Account", FormMethod.Post, new { role = "form" }))
{
```

▼
@Html.Encode(this)
@Html.AntiForgeryToken()
@Html.AttributeEncode(this)
@Html.Hidden("AntiForgeryToken")

```
    @Html.ValidationSummary()
    <div>
        @Html.LabelFor(m => m.Email)
        <div>@Html.TextBoxFor(m => m.Email)</div>
    </div>
    <div><input type="submit" value="Email Link" /></div>
}
@section Scripts {
    @Scripts.Render("~/bundles/jqueryval")
}
```

*

 At the top of the action that we created to handle the posted form, the one with the [HttpPost] attribute added, we\'ll add another attribute named

[ValidateAntiForgeryToken]. This makes the start of our action now look like the following:

[HttpPost]

[ValidateAntiForgeryToken]

public ActionResult ChangeEmail(ChangeEmailModel model)

{

string username = WebSecurity.CurrentUserName;

rest of function omitted

*

we must add the unique token to the form to change the user\\'s email when we display it. Update the form in the ChangeEmail.aspx view under /Account/

ChangeForm:

t.NewEmail) %>

QUESTION 3

The GetDealPrice method must be called by using Ajax.

You need to get the price of a product by using the GetDealPrice method of the ProductController.

Which code segment should you use? (Each correct answer presents a complete solution. Choose all that apply.)

A.
```
$.ajax({
    type: "POST",
    dataType: "json",
    contentType: "application/json",
    url: "Product/GetDealPrice",
    data: "{'productId': '" + productId + "'}",
     success: function (data) {
       $(".price").html(data.d);
     }
});
```

B.
```
$.load({
    dataType: "json",
    contentType: "application/json",
    url: "Product/GetDealPrice/" + productId,
     success: function (data) {
       $(".price").html(data.d);
     }
});
```

C.
```
$.ajax({
    type: "GET",
    dataType: "json",
    contentType: "application/json",
    url: "Product/GetDealPrice/" + productId,
     success: function (data) {
       $(".price").html(data.d);
     }
});
```

D.
```
$.getJSON("Product/GetDealPrice/" + productId
    function (data) {
       $(".price").html(data.d);
     }
);
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: CD

QUESTION 4

You manage an application that has a custom API. Your company purchases another company. Employees from the purchased company use their own Microsoft Azure Active Directory (Azure AD).

You need to reconfigure the application to ensure that all users can access the application by using the API.

You have the following requirements:

Implement authentication for Azure API management.

Configure the API gateway for proper authorization.

Integrate metrics into one dashboard.

Apply additional restrictions to all roles.

What should you implement? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Requirement	Capability
Provide authentication for API management.	Azure virtual networks Groups Ipsec VPN
Configure the gateway.	Transforms Operations Policies
Integrate metrics into one dashboard.	Application Insights Azure Monitor Log analytics Stream Analytics
Add restrictions for all users.	Active Diretory Domain Services(AD DS) Azure Key Vault Role-Based Access Control(RBAC)

Correct Answer:

Box 1: Groups

Add an external Azure AD group

After you enable access for users in an Azure AD instance, you can add Azure AD groups in API Management. Then, you can more easily manage the association of the developers in the group with the desired products.

To configure an external Azure AD group, you must first configure the Azure AD instance on the Identities tab by following the procedure in the previous section.

You add external Azure AD groups from the Groups tab of your API Management instance.

Box 2: Policies

Policies are applied inside the gateway which sits between the API consumer and the managed API. The gateway receives all requests and usually forwards them unaltered to the underlying API. However a policy can apply changes to both

the inbound request and outbound response.

Box 3: Application Insights

Application Insights is an extensible Application Performance Management (APM) service for web developers on multiple platforms. Use it to monitor your live web application.

Box 4: Role-Based Access Control (RBAC)

Apply additional restrictions to all roles.

Azure API Management relies on Azure Role-Based Access Control (RBAC) to enable fine-grained access management for API Management services and entities (for example, APIs and policies).

References:

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-aad

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-policies

https://docs.microsoft.com/en-us/azure/api-management/api-management-role-based-access-control

---

QUESTION 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution,

while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are developing a collaborative text editor. Multiple users may simultaneously edit the same document from within the application.

You need to ensure that users can see edits from all users as soon as they are made.

Solution: Implement the application by using ASP.NET MVC. Implement the document editor as a SignalR hub that brokers changes across client browser instances.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

https://www.dotnetcurry.com/aspnet-mvc/780/real-time-collaboration-aspnet-mvc-signalr

[70-486 PDF Dumps](#)   [70-486 Practice Test](#)   [70-486 Study Guide](#)