مرکز تخصصی

آپا

دانشگاه صنعتی اصفهان

(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

گزارش سامانه

https://esale.samt.ac.ir

تاریخ

شهریور ماه ۱۴۰۳

www.nsec.ir

۱-۱ مقدمه

این ارزیابی با شرایط ذیل انجام شده است:

نسخه مورد بررسی	
وب سرویس مورد استفاده	
نوع ارزیابی	

۱-۲ ارزیابی سرویس

طبق ارزیابی های انجام شده، موارد زیر در این سامانه مشاهده شد.

APA-IUT CERT

نام آسیب‌پذیری: Exposed JavaScript Files

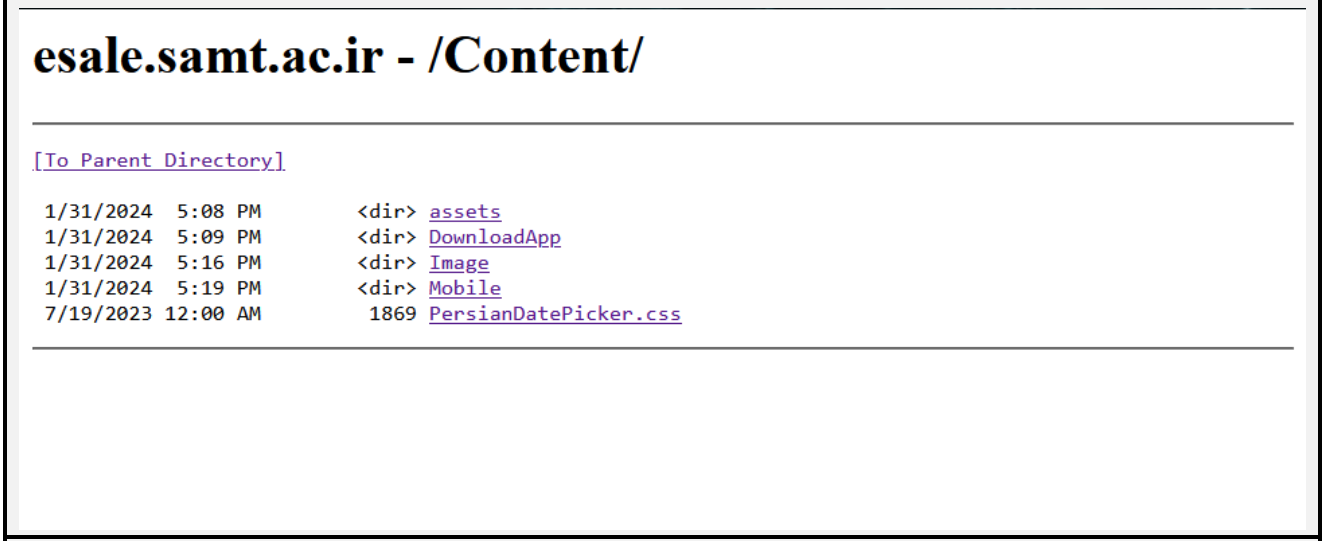
آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/Content/

سطح خطر:

توضیح مختصر:

آسیب‌پذیری Exposed JavaScript Files به حالتی اشاره دارد که فایل‌های JavaScript یک وب‌سایت بدون هیچ محدودیت امنیتی در دسترس عموم قرار دارند . و در این وبسایت نیز همین مشکل را داشتیم که همه ی فایل ها در اختیار همه قرار داشت.



esale.samt.ac.ir - /Content/

[To Parent Directory]

```
1/31/2024  5:08 PM        <dir> assets
1/31/2024  5:09 PM        <dir> DownloadApp
1/31/2024  5:16 PM        <dir> Image
1/31/2024  5:19 PM        <dir> Mobile
7/19/2023 12:00 AM         1869 PersianDatePicker.css
```

راه حل:

برای کاهش خطرات ناشی از Exposed JavaScript Files، می‌توانید اقدامات زیر را انجام دهید:

۱. بررسی و پاکسازی کدهای حساس :اطمینان حاصل کنید که هیچ اطلاعات حساس، مانند کلیدهایAPI ، توکن‌ها، یا اطلاعات پیکربندی در فایل‌های JavaScript قرار ندارد.

۲. Minifyو Obfuscate کدها :با فشرده‌سازی و مبهم‌سازی کدهایJavaScript ، خواندن و تحلیل آنها برای مهاجمان دشوارتر می‌شود.

۳. کنترل دسترسی مناسب :دسترسی به مسیرهای حساس را محدود کنید و تنها به فایل‌هایی که باید عمومی باشند اجازه نمایش دهید.

٤. CORS (Cross-Origin Resource Sharing)را تنظیم کنید :اطمینان حاصل کنید که فایل‌های جاوا اسکریپت تنها برای دامنه‌های مجاز قابل دسترسی هستند.

٥. استفاده از ابزارهای امنیتی :با استفاده از اسکنرهای امنیتی وب‌سایت، می‌توانید آسیب‌پذیری‌ها را شناسایی و اصلاح کنید.

اجرای این اقدامات به محافظت از فایل‌های جاوا اسکریپت و کاهش خطرات مرتبط با افشای آنها کمک می‌کند.

نام آسیب‌پذیری: net 4.0.30319 exploit.

آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/fa
-

سطح خطر: Medium 4.3

Vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N)

توضیح مختصر:

CVE-2015-6099

آسیب‌پذیری XSS در ASP.NET موجود در Microsoft .NET Framework 4 تا ٤,٦ به مهاجمان اجازه می‌دهد کدهای مخرب را از طریق ورودی‌های دستکاری‌شده به صفحات وب تزریق کنند، که می‌تواند منجر به سرقت اطلاعات یا اجرای عملیات غیرمجاز شود. برای رفع این مشکل، به‌روزرسانی‌های امنیتی را اعمال کنید و ورودی‌ها را اعتبارسنجی و پاکسازی کنید.

Server Error in '/' Application.

The resource cannot be found.

Description: HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly.

Requested URL: /fa

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4465.0

راه حل:

برای رفع آسیب‌پذیری XSS درASP.NET ، از آخرین به‌روزرسانی‌های امنیتی مایکروسافت استفاده کنید، ورودی‌های کاربر را به‌طور کامل اعتبارسنجی و پاکسازی کنید، و از کتابخانه‌های امنیتی مانند **AntiXSS Library**برای جلوگیری از تزریق کدهای مخرب استفاده کنید.

نام آسیب‌پذیری: net 4.0.30319 exploit.

آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/fa
-

سطح خطر: High 9.3

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C)

توضیح مختصر:

CVE-2015-2504

آسیب‌پذیری در Microsoft .NET Framework نسخه‌های ۲٫۰ SP2 تا ٤٫٦ به دلیل شمارش نادرست اشیا قبل از کپی آرایه رخ می‌دهد و به مهاجمان اجازه می‌دهد تا (۱) کد دلخواه را از طریق یک برنامه دستکاری‌شده XAML (XBAP) اجرا کنند یا (۲) محدودیت‌های امنیتی دسترسی به کد را دور بزنند. این مشکل به عنوان .NET Elevation of Privilege Vulnerability شناخته می‌شود.

Server Error in '/' Application.

The resource cannot be found.

Description: HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly.

Requested URL: /fa

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4465.0

راه حل:

به‌روزرسانی .NET Framework: آخرین به‌روزرسانی‌های امنیتی و پچ‌های منتشر شده توسط مایکروسافت را نصب کنید تا آسیب‌پذیری‌های موجود برطرف شوند.

نام آسیب‌پذیری: .net 4.0.30319 exploit

آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/fa
-

سطح خطر: High 8.5

Vector: (AV:N/AC:M/Au:S/C:C/I:C/A:C)

توضیح مختصر:

CVE-2011-3416

آسیب‌پذیری "ASP.Net Forms Authentication Bypass Vulnerability" در ASP.NET موجود در Microsoft .NET Framework نسخه‌های ١,١ SP1، ٢,٠ SP2، ٣,٥ SP1، ٣,٥,١ و ٤,٠ به کاربران از راه دور که قبلاً احراز هویت شده‌اند، امکان می‌دهد به حساب‌های کاربری دلخواه دسترسی پیدا کنند از طریق نام کاربری دستکاری‌شده.

Server Error in '/' Application.

The resource cannot be found.

Description: HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly.

Requested URL: /fa

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4465.0

راه حل:

١. به‌روزرسانی: آخرین به‌روزرسانی‌های امنیتی و پچ‌های مربوط به .NET Framework را نصب کنید.
٢. کنترل دسترسی: تنظیمات امنیتی Forms Authentication را بررسی و به‌روز کنید تا از نفوذ به حساب‌های کاربری جلوگیری کنید.
٣. بازبینی و تست: کدهای احراز هویت و دسترسی را بررسی و تست کنید تا آسیب‌پذیری‌ها شناسایی و برطرف شوند.

نام آسیب‌پذیری: Remote code execution in Windows HTTP Protocol Stack

آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/Content/

سطح خطر: Critical 9.8

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

توضیح مختصر:

CVE-2022-21907

این آسیب‌پذیری به یک حمله‌کننده از راه دور اجازه می‌دهد تا کد دلخواه را بر روی سیستم هدف اجرا کند. مشکل ناشی از یک خطای مرزی در ویژگی HTTP Trailer Support در HTTP Protocol Stack (http.sys) است. با ارسال یک درخواست HTTP به‌طور خاص دستکاری‌شده به وب‌سرور، مهاجم می‌تواند یک بافر اورفلاو را فعال کند و کد دلخواه خود را بر روی سیستم اجرا نماید.

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server : Microsoft-IIS/10.0
X-Aspnetmvc-Version : 5.2
X-Aspnet-Version : 4.0.30319
X-Powered-By : ASP.NET
Date : Wed, 11 Sep 2024 05:57:15 GMT
Content-Length: 360513
```

راه حل:

به‌روزرسانی: آخرین به‌روزرسانی‌ها و پچ‌های امنیتی مربوط به HTTP.sys و سیستم‌عامل خود را نصب کنید.

غیرفعال کردن ویژگی‌های غیرضروری: اگر HTTP Trailer Support برای نیازهای شما ضروری نیست، آن را غیرفعال کنید.

پیکربندی صحیح: تنظیمات امنیتی وب‌سرور را بررسی و اطمینان حاصل کنید که به‌درستی پیکربندی شده است.

نام آسیب‌پذیری: Bootstrap v3.3.7

آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/Content/assets/js/bootstrap.js
-

سطح خطر: Medium 6.1

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

توضیح مختصر:

CVE-2022-26624

آسیب‌پذیری Cross-Site Scripting (XSS) در نسخه‌های Bootstrap v3.1.11 و v3.3.7 از طریق پارامتر Title در فایل /vendor/views/add_product.php شناسایی شده است. این آسیب‌پذیری به مهاجمان این امکان را می‌دهد که کدهای جاوااسکریپت مخرب را از طریق این پارامتر به وب‌سایت تزریق کنند.

```
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
```

راه حل:

به‌روزرسانی: از آخرین نسخه‌های Bootstrap استفاده کنید، زیرا نسخه‌های جدیدتر ممکن است آسیب‌پذیری‌های امنیتی را برطرف کرده باشند.

نام آسیب‌پذیری: jquery.js

آدرس آسیب‌پذیر:

- https://esale.samt.ac.ir/Content/assets/js/jquery.js
-

سطح خطر: Medium 6.1

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

توضیح مختصر:

CVE-2019-11358

آسیب‌پذیری در jQuery نسخه‌های قبل از ۳,٤,۰، که در Drupal ، Backdrop CMS و سایر محصولات استفاده می‌شود، ناشی از نحوه نادرست پردازش jQuery.extend(true, {}, ...) به دلیل آلودگی Object.prototype است. اگر منبع شیء ناشناخته‌ای دارای خاصیت __proto__ قابل شمارش باشد، می‌تواند Object.prototype بومی را گسترش دهد.

```
/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */
!function (a, b) { "use strict"; "object" == typeof module && "object" == typeof m
function (a) { if (!a.document) throw new Error("jQuery requires a window with a d
```

راه حل:

به‌روزرسانی: به نسخه ۳,٤,۰ یا بالاتر از jQuery ارتقا دهید که این آسیب‌پذیری را برطرف کرده است..

نام آسیب‌پذیری: ftp bruteforce

آدرس آسیب‌پذیر:

- 5.34.203.10

سطح خطر: : High 8.1

vector CVSS:3.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

توضیح مختصر:

پورت ۲۱ باز است که باعث می شود بروت فورس بخورد

```
┌──(root㉿kali)-[~]
└─# ftp 5.34.203.10
Connected to 5.34.203.10.
220-FileZilla Server 1.5.1
220 Please visit https://filezilla-project.org/
Name (5.34.203.10:root): admin
331 Please, specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
ftp> get
(remote-file)
usage: get remote-file [local-file]
ftp>
ftp> sSsSsS
```

راه حل:

بستن پورت های اضافی که به کار نمی اید.

نام آسیب‌پذیری: smb bruteforce

آدرس آسیب‌پذیر:

- 5.34.203.10

سطح خطر: High 8.1

vector CVSS:3.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

توضیح مختصر:

پورت 445 باز است که باعث می شود بروت فورس بخورد

[smb-signing-not-required] [javascript] [medium] esale.samt.ac.ir:445

در صورت عدم الزام به امضای SMB، یک مهاجم می‌تواند به طور بالقوه ترافیک SMB را رهگیری و تغییر دهد بدون اینکه شناسایی شود. این آسیب‌پذیری معمولاً توسط ابزارهای امنیتی پرچم‌گذاری می‌شود، زیرا می‌تواند برای انجام انواع مختلفی از حملات مورد سوءاستفاده قرار گیرد، از جمله حملات "مرد میانی" (Man-in-the-Middle).

```
┌──(root㉿kali)-[~]
└─# smbclient //esale.samt.ac.ir/share -U username

Password for [WORKGROUP\username]:
```

راه حل:

امضای SMB به عنوان یک ویژگی امنیتی عمل می‌کند که ارتباطات بین مشتریان و سرورهای SMB را احراز هویت می‌کند. هنگامی که این ویژگی فعال باشد، یک امضای رمزنگاری‌شده به بسته‌های SMB اضافه می‌شود که صحت و تمامیت داده‌های منتقل شده را تضمین می‌کند.

نام آسیب‌پذیری: login bruteforce

آدرس آسیب‌پذیر:

- https://adminesale.samt.ac.ir/Pages/Login/login.aspx

سطح خطر: High 8.1

vector CVSS:3.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

توضیح مختصر:

کپچا صفحه ادمین به درستی کار نمی کند و می توان با یک کپچا چندین ریکوئست زد.

Request

Pretty Raw Hex

```
POST /BLL/BLLLogin.aspx/cplogin HTTP/2
Host: adminesale.samt.ac.ir
Cookie: ASP.NET_SessionId=kccy5rl5subfy5i4wdttqhms
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 105
Origin: https://adminesale.samt.ac.ir
Referer: https://adminesale.samt.ac.ir/Pages/Login/login.aspx
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  'Pusername':'repino7017@barakal.com',
  'Ppassword':'uTH19rT3yt7k',
  'Premember':'false',
  'Pcaptcha':'ohehj9'
}
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Cache-Control: private, max-age=0
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 11 Sep 2024 08:19:35 GMT
Content-Length: 7

{
  "d":0
}
```

راه حل:

استفاده صحیح از کپچا یا استفاده از پلاگین های امن تر.

نقص های طراحی سایت

هدرهای سایت:

https://esale.samt.ac.ir/

در بخش های مختلف سایت ، از هدرهای مهمی صرف نظر شده از جمله:

x-frame-options

x-content-type-options

Robots.txt:

در تمامی ساب دامین ها ، برای یوزر ،فایل robots.txt باز است.
توصیه میشود که خوانش این فایل برای یوزر های عادی بسته باشد.

```
User-agent: *
Allow: /
Disallow: /class/
Disallow: /data/
Disallow: /inc/
Disallow: /incc/
Disallow: /images/
Disallow: /lib/
Disallow: /request/
Disallow: /tmp/
Sitemap: https://epub.samt.ac.ir/sitemap.xml
```

اطلاعات طراح سایت:

https://esale.samt.ac.ir/Content/Mobile/.idea/dictionaries/Vahid.xml

اطلاعات فردی در سایت آمده است ، که کار را برای پیدا کردن یوزرنیم و پسورد آسان تر میکند.

```
-<component name="ProjectDictionaryState">
  -<dictionary name="Vahid">
    -<words>
        <w>searchbar</w>
        <w>swiper</w>
        <w>webfont</w>
      </words>
    </dictionary>
  </component>
```

Public and private key

https://esale.samt.ac.ir/elements/Xml/privatekey.xml
https://esale.samt.ac.ir/elements/Xml/publickey.xml

در فایل هایی که یوزر به آن دسترسی دارد ، فایل کلیدی در آن وجود دارد که و احتمالا مربوط به سرور می باشد.

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
−<RSAKeyValue>
  −<Modulus>
    0vJ4xntToN9+wfRzfTFzMMB6dg/s3KrF71Zykf67ODefff7+34nlcA430Pis5KZD5s0NrXtpsam0esYcxr9G2D3N8sSthAYtzDQXLe+ktRypiOQ0VjOyT4D1T2PgB3WidZzpJzWPI6flfs1BkX/lkeaBKPO9aAriIKoiXiLl3zE=
  </Modulus>
  <Exponent>AQAB</Exponent>
  −<P>
    2eZtKSvU7Q+qWHajoQ/Sed4JElCArevzBLGMAd7tdvRtiLAaso9lnYP4a2IrwoLbEOYWQXdqLeewBAjuYEwSYQ==
  </P>
  −<Q>
    99TR3SamoyaCmXnVtMu9ovSbNerjpNCxHTcR+Q5m+Qut4c5ZrSx1Fmz/OuLjHidOqGoY3sncBvBnDrtmHFOe0Q==
  </Q>
  −<DP>
    pBPcHQVxZzTFm6lyW0Rzw+qKwCy4SL6EFwOunnYEL++sTyH0aIKMDMkkFZAtzWEFnjrzhUZrQLfWlaM4BHEj4Q==
  </DP>
  −<DQ>
    MG4nYMc30zQoW2OiroUOFvUkC6JOQBwEMIhde8UjvFFa9oCDp8LDUtGUAubpqS/XQDQTjh32YGjESu22I5z3sQ==
  </DQ>
  −<InverseQ>
    QnMwZvRxUxUtQgxtNz//uN2YeUrLb9YQe4s0A5PJnjYC+MomAFtmptzf86+v970Sxe5EjWmQ2d4fD+sU3q4S2g==
  </InverseQ>
  −<D>
    BS2BsKiCCdy2gyr9gzUJpWiSEPAM4bE45Mony4TXwlZeLjTqO2EqfizBKrpR3xZkLAf8NhYFhwB5/zn55ph3FAgI0PvjBuMDYhe49L2iGewEMa4Q5xn9GbjeakPf0ixZGvLqGsvkEOI5DjCzKb8fW1IBpd4uqbNz4V6jZqP7zME=
  </D>
</RSAKeyValue>
```


This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
−<RSAKeyValue>
  −<Modulus>
    0vJ4xntToN9+wfRzfTFzMMB6dg/s3KrF71Zykf67ODefff7+34nlcA430Pis5KZD5s0NrXtpsam0esYcxr9G2D3N8sSthAYtzDQXLe+ktRypiOQ0VjOyT4D1T2PgB3WidZzpJzWPI6flfs1BkX/lkeaBKPO9aAriIKoiXiLl3zE=
  </Modulus>
  <Exponent>AQAB</Exponent>
</RSAKeyValue>
```


ارور های ۵۰۰ :

در سایت ارور ها هندل نشده است و با هر اروری ، دیتا هایی از بک اند به کلاینت ارسال میشود.

A potentially dangerous Request.QueryString value was detected from the client (cat="<script>alert</scrip...").

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.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.QueryString value was detected from the client (cat="<script>alert</scrip...").

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was detected from the client (cat="<script>alert</scrip...").]
   System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11778640
   System.Web.HttpValueCollection.EnsureKeyValidated(String key) +11775613
   System.Web.HttpValueCollection.Get(String name) +24
   Mars.UI.Controllers.ProductController.GetSearchResult(Int32 PageNumber, String SearchKey, Int32 recordCount) in E:\projects\Mars-Samt-git\Mars.UI\Controllers\ProductController.cs:1319
   lambda_method(Closure , ControllerBase , Object[] ) +247
   System.Web.Mvc.ReflectedActionDescriptor.Execute(ControllerContext controllerContext, IDictionary`2 parameters) +229
   System.Web.Mvc.ControllerActionInvoker.InvokeActionMethod(ControllerContext controllerContext, ActionDescriptor actionDescriptor, IDictionary`2 parameters) +35
   System.Web.Mvc.Async.AsyncControllerActionInvoker.<BeginInvokeSynchronousActionMethod>b__39(IAsyncResult asyncResult, ActionInvocation innerInvokeState) +39
   System.Web.Mvc.Async.WrappedAsyncResult`2.CallEndDelegate(IAsyncResult asyncResult) +77
   System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeActionMethod(IAsyncResult asyncResult) +42
   System.Web.Mvc.Async.AsyncInvocationWithFilters.<InvokeActionMethodFilterAsynchronouslyRecursive>b__3d() +72
   System.Web.Mvc.Async.<>c__DisplayClass46.<InvokeActionMethodFilterAsynchronouslyRecursive>b__3f() +396
   System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeActionMethodWithFilters(IAsyncResult asyncResult) +42
   System.Web.Mvc.Async.<>c__DisplayClass2b.<BeginInvokeAction>b__1c() +38
   System.Web.Mvc.Async.<>c__DisplayClass21.<BeginInvokeAction>b__1e(IAsyncResult asyncResult) +188
   System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeAction(IAsyncResult asyncResult) +38
   System.Web.Mvc.Controller.<BeginExecuteCore>b__1d(IAsyncResult asyncResult, ExecuteCoreState innerState) +32
   System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +73
   System.Web.Mvc.Controller.EndExecuteCore(IAsyncResult asyncResult) +52
   System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +39
   System.Web.Mvc.Controller.EndExecute(IAsyncResult asyncResult) +38
   System.Web.Mvc.MvcHandler.<BeginProcessRequest>b__5(IAsyncResult asyncResult, ProcessRequestState innerState) +46
   System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +73
   System.Web.Mvc.MvcHandler.EndProcessRequest(IAsyncResult asyncResult) +38
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +431
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +75
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +158
```

API:

https://esale.samt.ac.ir/Scripts/Custom/api.js

در فایل های سایت ، api هایی قابل مشاهده است که میتوان از آن در ssrf استفاده کرد.

```
//var apiUrl = "https://192.168.1.28:8890/";

var apiUrl = "https://apiesale.samt.ac.ir/";

//var apiUrl = "http://api.vesalbookshop.com";

// var apiUrl = "http://localhost:53287/";
```

APA-IUTCE