



گزارش سامانه جامع مسکن اتاق تعاون ایران

تاریخ
مرداد ماه ۱۴۰۳



1-1 مقدمه

این ارزیابی با شرایط ذیل انجام شده است:

وب سایت	نسخه مورد بررسی
ASP.NET	وب سرویس مورد استفاده
Blackbox	نوع ارزیابی

1-2 ارزیابی سرویس

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

نام آسیب پذیری: ضعیف بودن CAPTCHA

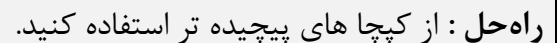
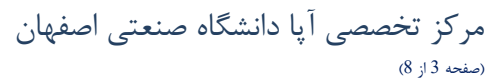
آدرس آسیب پذیر:

<https://iccmaskan.ir/Captchasp.aspx>

سطح خطر: CVSS v4.0 : Low : 3.5

توضیح مختصر: کپچا توسط ابزار tesseract قابل حل شدن است. در تمامی قسمت های وب سایت فقط از همین کپچا استفاده میشود. نحوه حل آن به صورت زیر میباشد:

```
curl https://iccmaskan.ir/Captchasp.aspx --output c.png -s &&  
tesseract c.png stdout -l eng --psm 8
```



آدرس آسیب پذیر:

سطح خطر: 5.4 : Medium : CVSS v4.0

مورد اول : <https://iccmaskan.ir/cp/ashx/uploadpic.ashx>

این مورد همواره مقدار 1- را در قسمت body برمیگرداند.

مورد دوم : <https://iccmaskan.ir/ashx/uploadpic.ashx>

اگر مقدار "requestid" بین 1 تا 5 باشد مقدار 1- همانند قسمت قبل باز گردانده میشود، در غیر اینصورت هیچ پاسخی در body وجود نخواهد داشت .

```
* upload completely sent off: 259 bytes
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
< HTTP/2 200
< date: Thu, 22 Aug 2024 13:23:00 GMT
< content-type: text/plain; charset=utf-8
< content-length: 2
< cache-control: private
< X-aspnet-version: 4.0.30319
< X-powered-by: ASP.NET
< X-xss-protection: 1; mode=block
< server: ArvanCloud
< server-timing: total;dur=185
< x-cache: BYPASS
< x-request-id: fc747e50aa1e077c2ad803dae42160ca
< x-sid: 2070
< accept-ranges: bytes
* Connection #0 to host iccmaskan.ir left intact
```

```
* upload completely sent off: 259 bytes
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
< HTTP/2 200
< date: Thu, 22 Aug 2024 13:23:37 GMT
< content-type: text/plain
< content-length: 0
< cache-control: private
< X-aspnet-version: 4.0.30319
< X-powered-by: ASP.NET
< X-xss-protection: 1; mode=block
< server: ArvanCloud
< server-timing: total;dur=19
< x-cache: BYPASS
< x-request-id: 9b9ecb23b3e28ae15b38d69fc4f74eff
< x-sid: 2070
< accept-ranges: bytes
* Connection #0 to host iccmaskan.ir left intact
```

هرچند فایل <https://iccmaskan.ir/script/uploadpic.js> اطلاعات بیشتری در این مورد به ما میدهد اما باز هم نحوه عملکرد این دو مورد نامشخص است و نمی توان تشخیص داد که فایل ها آپلود میشوند یا نه. در حالت کلی احتمال آپلود فایل های غیر مجاز وجود دارد.

راه حل : اگر از این نقاط استفاده ای نمیشود بهتر است در دسترس نباشند و یا اگر استفاده میشوند بهتر است کد وضعیت دقیق تری در خصوص مجاز بودن آپلود داده شود تا مانع آپلود های غیرمجاز شود.

نام آسیب پذیری: دسترسی به تصاویر حذف شده

آدرس آسیب پذیر:

<https://iccmaskan.ir/images/brand/3.png>
<https://iccmaskan.ir/images/ProjectPic/101.jpg>
<https://iccmaskan.ir/images/ProjectPic/102.jpg>

سطح خطر: CVSS v4.0 : LOW : 2.7

توضیح مختصر: به نظر میرسد در هنگام حذف پروژهای 101 و 102 و همچنین برند سوم، عکسهای آنها همچنان در سایت باقی مانده اند. که از طریق آدرسهای ذکر شده قابل دسترسی هستند.



راه حل: منابع مربوط به آبجکت های حذف شده باید از دسترس خارج شوند.

نام آسیب پذیری: در دسترس بودن فایل های js بلااستفاده

آدرس آسیب پذیر:

<https://iccmaskan.ir/script/global.js>
<https://iccmaskan.ir/script/uploadpic.js>
<https://iccmaskan.ir/script/news.js>

سطح خطر: 3.6 : LOW : CVSS v4.0

توضیح مختصر: بنظر میرسد این فایل ها مربوط به کارکرد هایی از سیستم بوده اند که دیگر وجود ندارند یا برای کاربر احراز هویت نشده قابل استفاده نیستند. از آنجایی که این اطلاعات به صورت عمومی در دسترس هستند، اطلاعاتی را در مورد نحوه عملکرد سیستم میدهند. به عنوان مثال کوکی zarparsbasket.

```
//===== Count product in Baket =====  
function countcookie() {  
  
    var city = getCookie("zarparsbasket");  
    var cn = city.split('&');  
  
    if (cn.length == 0 || cn == "" || cn == null) {  
        $(".a-basket span").html('0');  
    } else {  
        $(".a-basket span").html(cn.length);  
    }  
};
```



راه حل: اگر از این اسکریپت ها استفاده نمیشود و یا برای کاربران احراز هویت نشده استفاده نمی شود، بهتر است دسترسی به آنها نیز محدود باشد.

نام اشکال : مدیریت خطای زمان اجرا

آدرس آسیب پذیر:

تمامی URL ها .

سطح خطر: 2.9 : LOW : CVSS v4.0

توضیح مختصر: وبسایت هنگام برخورد با خطا (مثلا XSS یا مقادیر اشتباه) به صفحه ای منتقل میشود که مربوط به مدیریت خطای ASP.NET است. مانند آدرس های زیر :

<https://iccmaskan.ir/ashx/login.ashx?user=123123123&pass=3213213>
<https://iccmaskan.ir/<script>>

Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a <web.config> configuration file located in the root directory of the current web application. This <customErrors> tag should then have its <mode> attribute set to <Off>.

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the <defaultRedirect> attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

Web.Config Configuration File -->

```
<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configuration>
```

Web.Config Configuration File -->

```
<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
```

همچنین هنگام استفاده از نال بایت ، خطا توسط nginx مدیریت میشود.

400 Bad Request

nginx



راه حل : بهتر است بجای استفاده از صفحه خطای فریم ورک ها از یک صفحه خطای دلخواه استفاده شود تا اطلاعاتی از سرور فاش نشود. همچنین نال بایت باید توسط asp.net مدیریت شود.

نام اشکال : مدیریت نادرست url باعث عدم بارگیری منابع میشود

آدرس آسیب پذیر:

تمامی URL های وبسایت که به .aspx منتهی میشوند.

سطح خطر: -

توضیح مختصر: اگر هر مسیری به انتهای این URL ها اضافه شود باز هم آن URL باز میشود اما با توجه به تغییر مسیر، مرورگر تلاش میکند منابع را از مسیر جدید بارگیری کند که منجر به عدم لود آنها میشود. به عنوان مثال :

<https://iccmaskan.ir/default.aspx/any/random/url.anyextention>

یا مثلاً ممکن است کاربر اشتباهی آدرس زیر را وارد کند که منجر به لود نشدن کپچا میشود.

<https://iccmaskan.ir/login.aspx/>

راه حل : مسدود کردن چنین آدرس هایی یا هدایت کردن آن ها به آدرس اصلی .

نام اشکال : مجاز بودن فعال POST

آدرس آسیب پذیر:

اکثر URL ها.

سطح خطر: -

توضیح مختصر: در اکثر URL ها امکان POST وجود دارد. این را هم از بررسی فعل های مجاز در OPTION و هم از امتحان کردن POST میتوان دریافت.



```
curl -X POST -T ~/Pictures/random.png -b 'ASP.NET_SessionId=w13bpepahopdackwjrrfBe0' 'https://iccmaskan.ir/default.aspx'

<!DOCTYPE html>
<html>
<head><title>
سامانه مسکن اتاق تعاون ایران
</title><meta charset="utf-8" /><meta http-equiv="x-ua-compatible" content="ie=edge" /><meta name="description" /><meta name="viewport" content="width=device-width, initial-scale=1" />

<!-- Place favicon.ico in the root directory -->
<link rel="shortcut icon" type="image/x-icon" href="images/icon.png" /><link rel="apple-touch-icon" href="apple-touch-icon.png" />

<!-- All css files are included here. -->
<!-- Bootstrap framework main css -->
<link rel="stylesheet" href="css/bootstrap.min.css" />
<!-- Owl Carousel main css -->
<link rel="stylesheet" href="css/owl.carousel.min.css" /><link rel="stylesheet" href="css/owl.theme.default.min.css" />
<!-- This core.css file contains all plugings css file. -->
<link rel="stylesheet" href="css/core.css" />
<!-- Theme shortcodes/elements style -->
<link rel="stylesheet" href="css/shortcode/shortcodes.css" />
<!-- Theme main style -->
<link rel="stylesheet" href="style.css?ver=1" />
<!-- User style -->
<link rel="stylesheet" href="css/custom.css?ver=2" />

<!-- jquery latest version -->
<script src="js/vendor/jquery-1.12.0.min.js"></script>

<!-- Modernizr JS -->
<script src="js/vendor/modernizr-2.8.3.min.js"></script>

<!--BEGIN RAYCHAT CODE-->
<script type="text/javascript">!function(){function t(){var t=document.createElement("script");t.type="text/javascript",t.async=!0,localStorage.getItem("rayToken")?t.src="https://app.ra
ychat.io/scripts/js/+o+?ride="+localStorage.getItem("rayToken")+"&href="+window.location.href:t.src="https://app.raychat.io/scripts/js/+o+?href="+window.location.href;var e=document.getE
lementsByTagName("script")[0],e.parentNode.insertBefore(t,e)}var e=document,a=window,o="a9da6ba4-69c1-4681-be8b-42886e7fb736";"complete"==e.readyState?t():a.attachEvent?a.attachEvent("onloa
d",t):a.addEventListener("load",t,!1)}();</script>
<!--END RAYCHAT CODE-->

<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.4.1/font/bootstrap-icons.css" /></head>
<body>
<form method="post" action="default.aspx" id="form1">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="Qh60u1xPDNUPV8mXC904vQ3vJ0mqeuV+8zdJCMZmtV6xxTDPXaLa6PMghPXJiviyamaZoGPMwQ3hy0y/zxRfYV0PFckvf55SGYXZC5FWREys=" />
<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CA0B0334" />
</form>
</body>
</html>
```

راه حل : مسدود کردن POST به نقاطی که نیازی به POST ندارند.