مرکز تخصصی

آپا

دانشگاه صنعتی اصفهان

(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

گزارش سامانه جامع مسکن اتاق تعاون ایران

تاریخ

مرداد ماه ۱۴۰۳

1-1 مقدمه

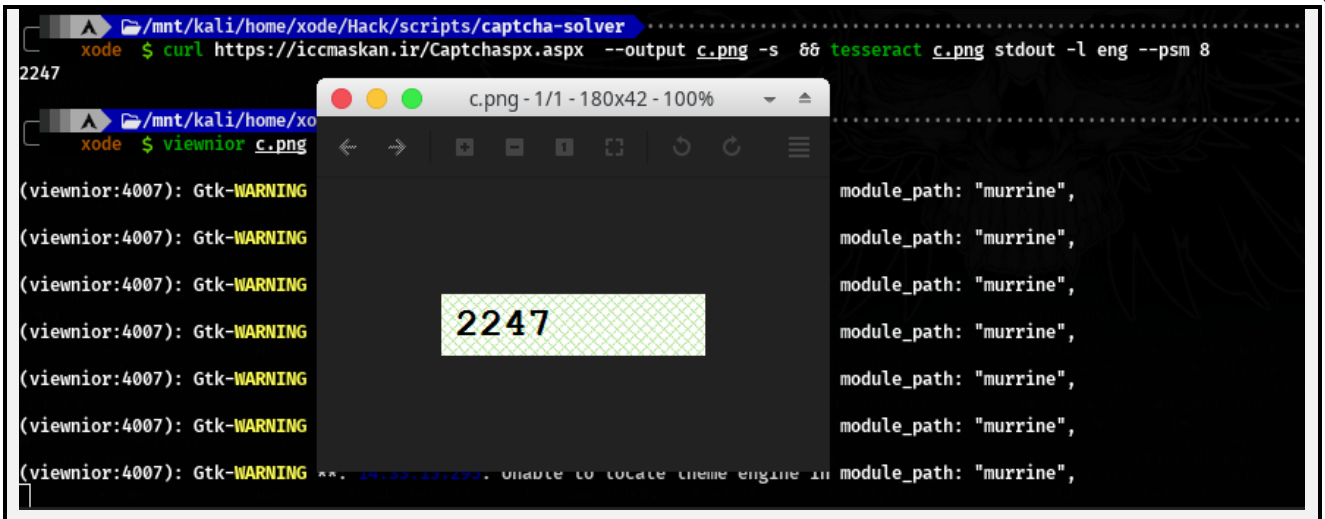
این ارزیابی با شرایط ذیل انجام شده است:

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

1-2 ارزیابی سرویس

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

نام آسیب‌پذیری: ضعیف بودن CAPTCHA
آدرس آسیب‌پذیر: https://iccmaskan.ir/Captchaspx.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/Captchaspx.aspx --output c.png -s && tesseract c.png stdout -l eng --psm 8`



راه‌حل : از کپچا های پیچیده تر استفاده کنید.

نام آسیب پذیری : وجود نقطه پایانی آپلود

آدرس آسیب‌پذیر:

https://iccmaskan.ir/cp/ashx/uploadpic.ashx
https://iccmaskan.ir/ashx/uploadpic.ashx

سطح خطر: CVSS v4.0 : Medium : 5.4

تو ضیح مختصر: دو نقطه پایانی برای آپلود عکس وجود دارد. هر دو نقطه به ازای تمامی درخوا ست کد و ضعیت 200 را باز می گردانند.

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

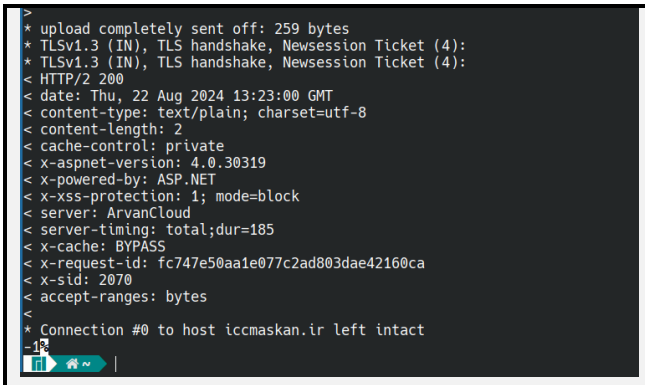
```
curl -X POST -F "requestid=1" -F "fileid=1" -b
'ASP.NET_SessionId=w13bpepafhopdackwjjrfbe0'
'https://iccmaskan.ir/cp/ashx/uploadpic.ashx'
```

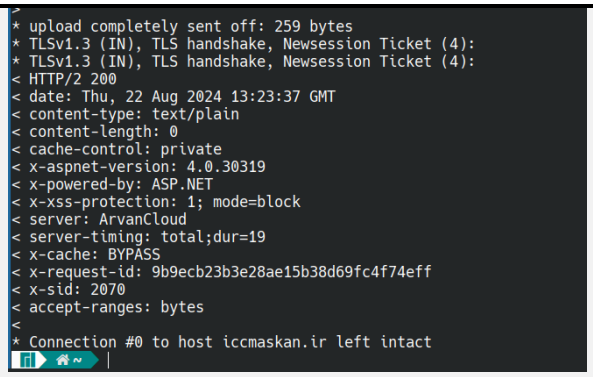
این مورد همواره مقدار 1- را در قسمت body برمیگرداند.

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

```
curl -X POST -F "requestid=5" -F "fileid=1"   -b
'ASP.NET_SessionId=w13bpepafhopdackwjjrfbe0'
'https://iccmaskan.ir/ashx/uploadpic.ashx'
```

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





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 اپلود میشوند یا نه. در حالت کلی احتمال آپلود فایل های غیر مجاز وجود دارد.

راه‌حل : اگر از این نقاط استفاده ای نمیشود بهتر است دردسترس 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 آسیب‌پذیر:

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 میر سد در هنگام حذف پروژه های 101 و 102 و همچنین برند سوم، عکس های آنها همچنان در سایت باقی مانده اند. که از طریق آدرس های ذکر شده قابل دسترسی هستند.

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

نام آسیب پذیری : در دسترس بودن فایل های js بلااستفاده

آدرس آسیب‌پذیر:

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

سطح خطر: CVSS v4.0 : LOW : 3.6

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 انجایی که این اطلاعات به صورت عمومی درسترس 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);
    };

};
```

راه‌حل : 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

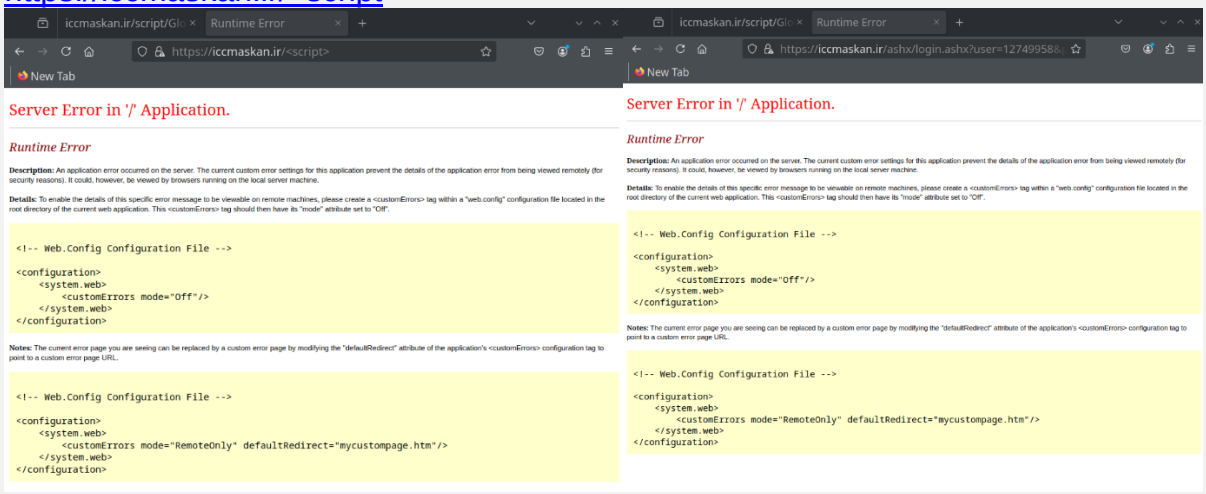
آدرس آسیب‌پذیر:

تمامی URL ها .

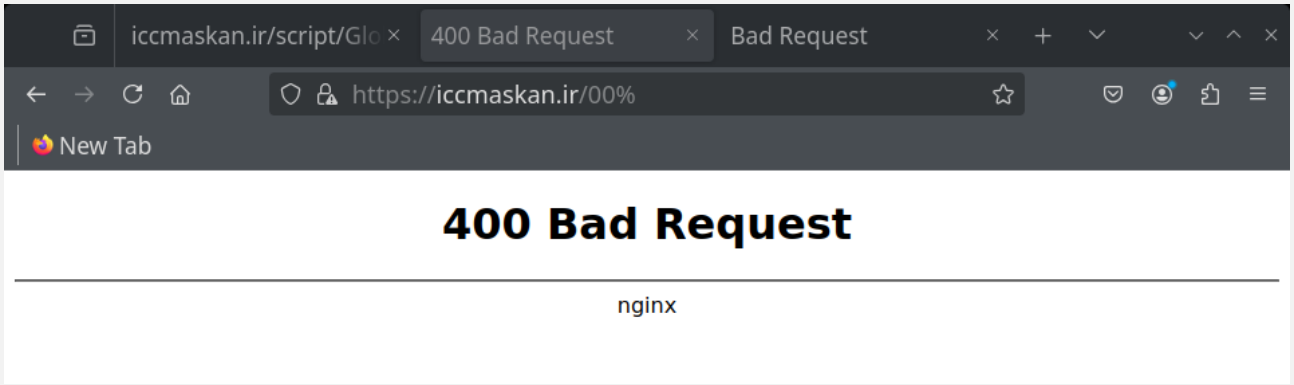
سطح خطر: CVSS v4.0 : LOW : 2.9

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>



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



راه‌حل : 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 آسیب‌پذیر: تمامی URL های وبسایت که به aspx. منتهی میشوند.
سطح خطر: -
تو ضیح 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 مثلا ممکن است کاربر اشتباهی آدرس زیر را وارد کند که منجر به لود نشدن کپچا میشود. https://iccmaskan.ir/login.aspx/
راه‌حل : مسدود کردن چنین آدرس هایی یا هدایت کردن آن ها به آدرس اصلی .

نام اشکال : مجاز بودن فعال POST
آدرس آسیب‌پذیر: 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=w13bpepafhopdackwjjrfbe0' '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 fremwork 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 contents 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+"?rid="+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="a96a6ba4-69c1-4681-be8b-42086e7fb736";"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="Qh60u1xPDNUPV8mXC9O4vQ3vJ0mqeuV+8zdJCMZmtV6xxTDPXaLa6PMghPXJivyamaZoGPMwQ3hyOy/zxRfYV0PFckvfS5SGYXZC5FWREys=" />

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CA0B0334" />
```

راه‌حل : مسدود کردن POST به نقاطی که نیازی به POST ندارند.