



پروژه آزمون نفوذپذیری - موزه بانک ملی ایران

گزارش آزمون نفوذ museum.bmi.ir سامانه

museum.bmi.ir-Website-Pentest-Report-R1.0

شناسه سند:

محرمانه

طبقه بندي سند:

R1.0

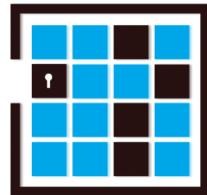
شماره نگارش:

99/03/07

تاریخ آخرین ویرایش:

۶

تعداد صفحات:



شرکت مهندسی امن گسترش پیام پرداز

تهران خیابان شریعتی، بالاتر از پل سیدخدان، خیابان مجتبایی، کوچه دایانا، کوچه بروجردی، پلاک 44، طبقه سوم - واحد 6

www.AmnGostar-co.ir

این مستند حاوی اطلاعات حساس شرکت تجارت الکترونیکی ارتباط فردا بوده و می‌بایست بر اساس دستورالعمل‌های امنیتی سازمان، اقدامات لازم برای محافظت از آن در برابر افشای غیرمجاز صورت پذیرد.



به عنوان حداقل اقدامات امنیتی لازم الاجرا برای محافظت از اطلاعات ارایه شده در این سند، می‌بایست اطلاعات موجود در سند حاضر تنها در صورت نیاز منتشر شده و همچنین از محفظه مناسبی که دارای قفل بوده یا هر مکانی که در برابر سرقت، دسترسی‌های غیر عمدی و افشاگری غیر مجاز، به قدر کافی مصون باشد برای نگهداری از آن استفاده گردد.

سوابق تغییرات سند

ردیف	شماره نگارش	تیم تست نفوذ	تاریخ تهییه	تأیید کنند(ه/گان)	تاریخ تأیید	تعداد صفحات
1	R1.0	تیم تست نفوذ	99/03/01	مدیریت پروژه	99/03/07	۶۶

قدوین سند

شرح تغییر:



فهرست مطالب

5	1. مقدمه
5	1.1. معرفی
5	1.2. مشخصات زیر ساختی
6	2. رویکرد اجرایی
8	3. ابزار مورد استفاده
9	4. خلاصه مدیریتی
10	5. آسیب پذیری ها
11	5.1. آسیب پذیری های HIGH
11	ورود به پنل ادمین به عنوان کاربر test
14	آسیب پذیری Privilege scalation
16	آسیب پذیری SQL Injection
21	5.2. آسیب پذیری های MEDIUM
21	آسیب پذیری Logout functionality
23	آسیب پذیری Stack trace
25	دسترسی به فایل Log
30	آسیب پذیری Character injection
32	آسیب پذیری Full path disclosure
35	5.3. آسیب پذیری های Low
35	استفاده از نسخه آسیب پذیر Bootstrap 3.3.7
37	استفاده از نسخه آسیب پذیر JQuery 3.3.1
39	استفاده از نسخه آسیب پذیر Net Framework 4.0.30319
41	آسیب پذیری Error Handling
43	استفاده از نسخه آسیب پذیر IIS 10
45	در دسترس بودن پنل Admin
47	فعال بودن متدهای DEBUG
49	عدم فعال سازی HSTS
50	عدم استفاده از مکانیزم امنیتی Lockout
51	آسیب پذیری نسخه TLS مورد استفاده
53	ارسال ViewState بدون رمزنگاری



55	6. توصیه های امنیتی
55	6.۱. اعمال کردن DENSEC
56	6.۲. حذف سرآیند X-POWERED-BY از پاسخ سرور
57	7. اقدامات انجام شده
57	7.۱. بررسی آسیب پذیری XSS
58	7.۲. بررسی آسیب پذیری CLICK JACKING
59	7.۳. بررسی آسیب پذیری HPP
60	7.۴. بررسی آسیب پذیری IIS TILDE
60	7.۵. تلاش برای شناسایی فایروال سامانه
61	7.۶. بررسی اسناد و فایل های سامانه در بستر اینترنت با استفاده از ابزار FOCA
62	7.۷. بررسی سامانه با استفاده از ابزار WHATWEB
65	7.۸. اسکن سامانه با ابزار NMAP



۱. مقدمه

آزمون نفوذ و انجام ارزیابی های امنیتی لازم جهت شناسایی آسیب پذیری ها و نیز بررسی اطمینان از صحت پیاده سازی کنترل های امنیتی با هدف مقابله و جلوگیری از حملات هکرها به عنوان یکی از روش های متدائل در حفظ امنیت سازمان ها مطرح است.

شایان ذکر است به منظور بهره برداری از مزایای فوق، بانک ملی ایران اقدام به اجرای پروژه آزمون نفوذپذیری سامانه های خود نموده است. در راستای پروژه مزبور، در این سند گزارش ارزیابی ها و آزمون نفوذ انجام شده برای سامانه museum.bmi.ir رائے می شود.

۱.۱. معرفی

سامانه museum.bmi.ir یکی از سامانه های بانک ملی است که دارای پلتفرم تحت وب می باشد. بانک ملی ایران در ۱۷ شهریور ۱۳۰۷ به موجب "قانون تأسیس بانک ملی ایران" مصوب ۱۴ اردیبهشت ۱۳۰۶ تأسیس و آغاز به کار کرد و در ۲۰ شهریور ۱۳۰۷ طی مراسمی رسمی افتتاح شد. در ابتدای تأسیس، بانک قادر ساختمانی بود که آن را مختص به خود ساخته باشد، اما در ۲۵ تیر ماه سال ۱۳۱۲ ساختمان شعبه و ادارات مرکزی شروع و در سوم اردیبهشت ماه سال ۱۳۱۵ افتتاح گردید.

۲. مشخصات زیر ساختی

System Name	Museum
Test URL	https://museum.bmi.ir
IP Address	89.235.65.239
Framework	Microsoft ASP.NET



2 رویکرد اجرایی

رویکرد آزمون نفوذ مبنی بر کشف و مرتفع سازی مشکلات امنیتی در مقابل تهدیدات داخلی و خارجی از طریق بکارگیری معیارهای صحیح ارزیابی تمرکز دارد و رسیدن به سطوح بالای قابلیت اعتماد به سیستم در راستای منافع کسب و کار را مدد نظر قرار می‌دهد.

با توجه به اینکه سامانه museum.bmi.ir برنامه کاربردی تحت وب می‌باشد متداول‌ترین OWASP به عنوان مرجع در این پروژه مدنظر بوده که می‌توان گفت کاملترین و مناسب‌ترین متادارزیابی امنیتی و آزمون نفوذ در حوزه برنامه‌های کاربردی تحت وب می‌باشد. به منظور اطمینان از جامعیت آزمون‌های انجام شده، سعی گردیده است تمامی موارد OWASP Testing Guide مورد بررسی قرار گیرد. علاوه بر موارد فوق، دانش فنی و تجربه کارشناسان تیم آزمون نفوذ نیز در انجام پروژه‌ها مدنظر قرار گرفته است.

روش انجام آزمون نفوذ به صورت جعبه سیاه و دسترسی نفوذگر در کمترین سطح و در حد یک کاربر عادی سامانه و بدون هیچ اکانت کاربری بوده.

در این راستا پس از شناسایی سامانه هدف، پویش آسیب‌پذیری‌ها بصورت خودکار و دستی با استفاده از ابزارهای مورد نیاز انجام گردید. اهم اقدامات انجام شده در آزمون نفوذ به شرح زیر می‌باشد:

(1) شناسایی و جمع‌آوری اطلاعات- برخی از تکنیک‌های مورد استفاده در این آزمون:

- شناسایی پورت‌ها و نقاط ورود برنامه‌ی کاربردی
- آزمون برای FINGERPRINT برنامه‌ی کاربردی تحت وب
- تحلیل کدهای خطأ
- کاوش با استفاده از روبات‌ها، اسپایدرها و کراولرها و ...

(2) پویش سامانه با استفاده از ابزار خودکار

(3) بررسی خروجی ابزار مورد استفاده

(4) بررسی دستی سامانه و انجام آزمون‌های مختلف از جمله:

- آزمون مدیریت پیکربندی
- آزمون تصدیق اصالت



• آزمون بررسی مجوزهای دسترسی

• آزمون مدیریت نشست

• آزمون اعتبار و صحت داده

• آزمون سریز بافر

• آزمون مجوز نادرست فایل‌ها و دایرکتوری‌ها

• ... و ...

(5) بررسی سناریوهای اختصاصی سامانه

(6) و ...



۳. ابزار مورد استفاده

برخی از ابزارهای تخصصی مورد استفاده در ارزیابی امنیتی و آزمون نفوذ عبارتند از:

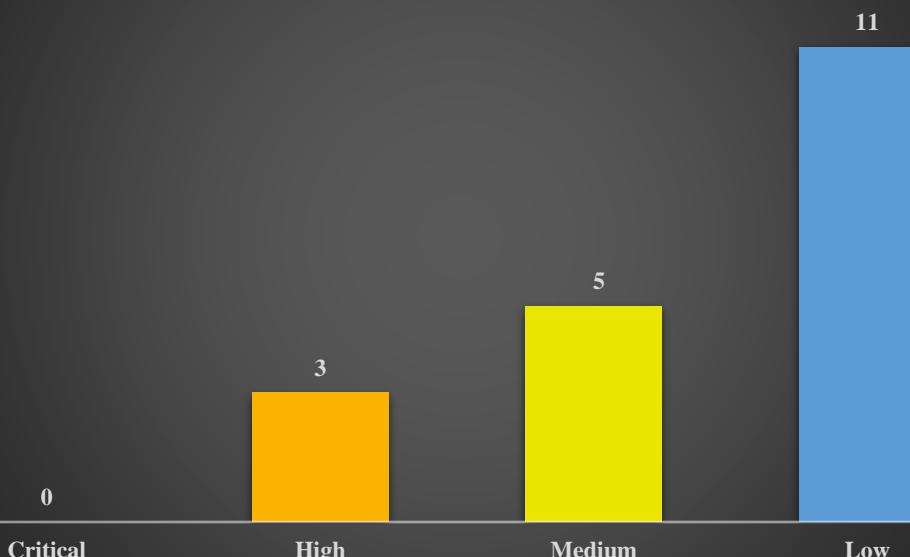
- Nmap •
- Net Sparker •
- SQLmap •
- Acunetix •
- BurpSuite •
- Python Scripts •
- Whatweb •
- Wafw00f •



4. خلاصه مدیریتی

سامانه museum.bmi.ir یکی از سامانه های بانک ملی ایران است که دارای پلتفرم تحت وب می باشد. انجام آزمون نفوذ به روش جعبه سیاه و سطح دسترسی و آگاهی تیم نفوذگر در کمترین سطح سامانه بوده است. همچنین همان گونه که پیشتر بیان شد بر مبنای رویکرد آزمون نفوذ، علاوه بر بررسی آسیب پذیری های عمومی، فرآیندهای سامانه شناسایی گردیده تا امکان بررسی سناریوهای اختصاصی برای سامانه میسر گردد. در نهایت بر مبنای کنترل های OWASP و سناریوهای اختصاصی انجام شده، وضعیت آسیب پذیری های کشف شده برای این سامانه به شرح زیر می باشد.

آسیب پذیری های شناسایی شده به تفکیک درجه اهمیت





5. آسیب پذیری ها

آسیب پذیری های شناسایی شده در سامانه به تفکیک درجه اهمیت عبارتند از:

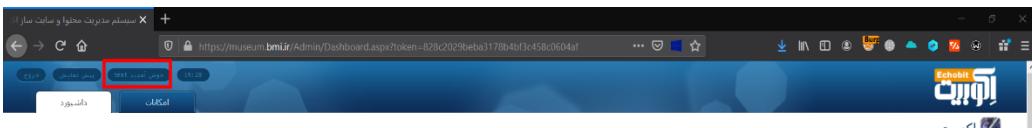
- آسیب پذیری با درجه اهمیت Critical: ۰ عدد
- آسیب پذیری با درجه اهمیت High: ۳ عدد
- آسیب پذیری با درجه اهمیت Medium: ۵ عدد
- آسیب پذیری با درجه اهمیت Low: 11 عدد

در ادامه توضیحات لازم در خصوص آسیب پذیری های شناسایی شده، شرح، حوزه تاثیر، شدت اثر و در نهایت راهکار

برطرف سازی آنها در قالب جداول زیر ارائه شده است.



1.5. آسیب پذیری های High

عنوان آسیب پذیری	شرح آسیب پذیری	شناسه آسیب پذیری																																	
ورود به پنل ادمین به عنوان کاربر test	ورود به پنل ادمین یا حتی پنل کاربران دیگر، آسیب پذیری بسیار خطرناکی می باشد که مشکلات بسیار زیادی برای سامانه ایجاد خواهد نمود. یک فرد مهاجم با ورود غیر مجاز به پنل مدیریت قادر خواهد بود تا تمامی سامانه را در دست گرفته و اقدام به دستکاری داده ها و یا تغییر سامانه نماید. همچنین با کاوش در منوهای مختلف با ساختار کلی و پیکربندی سامانه آشنا خواهد شد.	عنوان آسیب پذیری																																	
High (AV:N/AC:L/Au:N/C:P/I:P/A:P) – 7.5	درجه اهمیت																																		
Web Application	حوزه تاثیر																																		
URL: https://museum.bmi.ir/Admin/LoginPage.aspx	سیستم های آسیب پذیر (IP&URL)																																		
هنگام بررسی پنل ورودی ادمین، با وارد نمودن مقدار test به عنوان نام کاربری و همچنین به عنوان پسورد، به عنوان کاربر test به پنل ادمین وارد شده و به بررسی بیشتر در این خصوص پرداخته شد. (توجه نمایید که برای تست کردن موارد امنیتی دیگر اقدام به تغییر رمز عبور این اکانت نموده و در حال حاضر پسورد اکانت مذکور Test@1234 می باشد).	روند بررسی																																		
 <p>The screenshot shows the 'Admin' dashboard of the museum website. A red box highlights the 'نام کاربری' (Username) input field where 'test' has been entered. The dashboard also displays a table of recent logins and a sidebar menu.</p> <table border="1" data-bbox="230 1718 865 1965"> <thead> <tr> <th>تاریخ</th> <th>نام و سمت</th> <th>ردیف</th> </tr> </thead> <tbody> <tr><td>14:39 1399/02/28</td><td>علی هاشمی</td><td>1</td></tr> <tr><td>18:43 1398/12/12</td><td>علی هاشمی</td><td>2</td></tr> <tr><td>18:43 1398/12/12</td><td>علی هاشمی</td><td>3</td></tr> <tr><td>09:46 1398/11/16</td><td>علی هاشمی</td><td>4</td></tr> <tr><td>09:37 1398/11/16</td><td>علی هاشمی</td><td>5</td></tr> <tr><td>09:32 1398/11/16</td><td>علی هاشمی</td><td>6</td></tr> <tr><td>09:32 1398/11/16</td><td>علی هاشمی</td><td>7</td></tr> <tr><td>09:32 1398/11/16</td><td>علی هاشمی</td><td>8</td></tr> <tr><td>09:32 1398/11/16</td><td>علی هاشمی</td><td>9</td></tr> <tr><td>09:32 1398/11/16</td><td>علی هاشمی</td><td>10</td></tr> </tbody> </table>	تاریخ	نام و سمت	ردیف	14:39 1399/02/28	علی هاشمی	1	18:43 1398/12/12	علی هاشمی	2	18:43 1398/12/12	علی هاشمی	3	09:46 1398/11/16	علی هاشمی	4	09:37 1398/11/16	علی هاشمی	5	09:32 1398/11/16	علی هاشمی	6	09:32 1398/11/16	علی هاشمی	7	09:32 1398/11/16	علی هاشمی	8	09:32 1398/11/16	علی هاشمی	9	09:32 1398/11/16	علی هاشمی	10	 <p>The screenshot shows the 'Recent Changes' section of the dashboard. It features a large black rectangular redaction box covering several rows of data, likely containing sensitive information.</p>	
تاریخ	نام و سمت	ردیف																																	
14:39 1399/02/28	علی هاشمی	1																																	
18:43 1398/12/12	علی هاشمی	2																																	
18:43 1398/12/12	علی هاشمی	3																																	
09:46 1398/11/16	علی هاشمی	4																																	
09:37 1398/11/16	علی هاشمی	5																																	
09:32 1398/11/16	علی هاشمی	6																																	
09:32 1398/11/16	علی هاشمی	7																																	
09:32 1398/11/16	علی هاشمی	8																																	
09:32 1398/11/16	علی هاشمی	9																																	
09:32 1398/11/16	علی هاشمی	10																																	



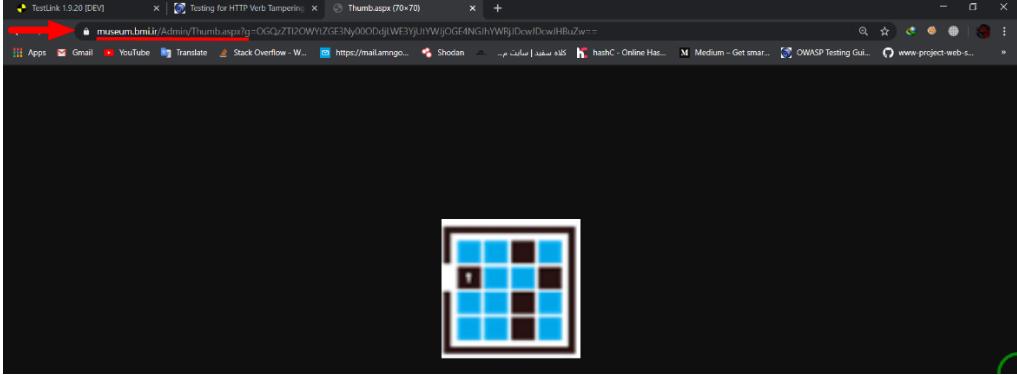
و سپس مشاهده گردید که این کاربر دسترسی برای ایجاد یا ویرایش برخی از فایل‌ها و تنظیمات را دارد.

در ادامه اقدام به آپلود عکس در سامانه گردید.

همانطور که مشاهده می‌نمایید تصویر با موفقیت بارگذاری گردید و کلیک بر روی گزینه انتشار در سامانه ثبت گردید.

در ادامه با یک مرورگر دیگر که به اکانت مدیریت لایکن نبود، اقدام به مشاهده تصویر نموده که تصویر مربوطه در دسترس بوده و تصویر با موفقیت کامل در سامانه قرار گرفت. (به دلیل عدم ایجاد تداخل در سامانه، تصویر پس از ضبط POC‌های مربوطه حذف گردید.)

	<p>پروژه آزمون نفوذپذیری - موزه بانک ملی ایران</p> <p>موزه بانک ملی ایران</p>	
---	---	---

	<ul style="list-style-type: none"> - این حساب کاربری در صورت عدم نیاز به صورت کامل غیرفعال گردد. - در صورت نیاز برای وجود حساب کاربری test، حتماً پسورد مناسب برای آن در نظر گرفته شود تا به راحتی نتوان وارد این حساب کاربری شد. 	<p>راهکار</p>
--	---	---------------



Vul-Museum-Website-H-02

شناسه آسیب پذیری

عنوان آسیب پذیری	آسیب پذیری
شرح آسیب پذیری	<p>این آسیب پذیری زمانی رخ میدهد که یک کاربر محدود، که توانایی استفاده از برخی امکانات سامانه را در حالت عادی ندارد، با توجه به شرایطی خاص، قادر به ارتقا سطح دسترسی خود باشد به نحوی که بتواند از امکانات و موارد فوق الذکر استفاده نماید.</p> <p>مهاجم می تواند با ارتقا سطح دسترسی خود، تنها با یک حساب محدود، دست به اقدامات تخریب گردن در سامانه بزند. برای مثال تنها کاربر admin قادر به ایجاد یا حذف حساب کاربری می باشد، و این کار را از طریق منوی کاربران، قسمت ایجاد کاربر جدید، انجام میدهد. حال در نظر بگیرید این قابلیت در منوی کاربران عادی وجود ندارد، حال اگر کاربری بتواند با پیدا کردن آدرس صفحه مذکور، به آدرس admin/users/adduser و بتواند بدون داشتن دسترسی و اجازه کافی، وارد آدرس مربوطه گردد و اقدام به اضافه نمودن یک کاربر به سامانه نماید، در این صورت آسیب پذیری Privilege Scalation رخ داده است.</p>
درجه اهمیت	High <u>(AV:N/AC:L/Au:N/C:P/I:P/A:P)</u> – 7.5
حوزه تاثیر	Web Application
سیستم‌های آسیب‌پذیر (IP&URL)	URL: https://museum.bmi.ir/Admin/Controls.aspx https://museum.bmi.ir/Admin/Plugins.aspx
روند بررسی	با بررسی قبلی که بر روی حساب کاربری test داشتم، متوجه شدم که منو ها و امکانات خاصی در اختیار این دارد، اما با توجه به مسیرهای یافت شده در فایل log و تلاش برای باز کردن لینک های مربوطه مانند صفحه کنترل، مشاهده گردید که با وارد کردن آدرس مربوطه در URL و اضافه کردن token مربوط به حساب کاربری test صفحه ای که در هیچ یک از منوهای کاربری test وجود نداشت برای این کاربر در



دسترس قرار گرفته و میتوان با استفاده از این امکانات اقدام به تغییراتی در سامانه نماید
که در حالت عادی دسترسی برای این کار ندارد.

همچنین با توجه به مسیر دیگری که از فایل LogFile.txt استخراج گردید، به قسمتی در خصوص مدیریت فایل های Plugin در سامانه رسیدیم.

سپس اقدام به آپلود چندین Plugin در سامانه نمودیم.

- مجوز های دسترسی صفحات مختلف، با Token کاربر چک شده و در صورتی که کاربر مجوز استفاده از صفحه یا قابلیت خاصی را نداشت، آن صفحه در دسترس وی قرار نگیرد.

راهکار



Vul-Museum-Website-H-03		شناسه آسیب پذیری
عنوان آسیب پذیری	آسیب پذیری	
آسیب پذیری SQL Injection	<p>آسیب پذیری SQL Injection مربوط به دیتابیس و ارتباط با آن می باشد. در این آسیب پذیری مهاجم قادرخواهد بود تا با دیتابیس سامانه ارتباط برقرار نموده و دستورات خود را به زبان SQL وارد نموده و از سرور پاسخ آن را دریافت نماید، این ارتباط می تواند به صورت مستقیم، از طریق خطاهای دریافتی از سمت دیتابیس یا به صورت بلایند و بر اساس منطق کاری دیتابیس باشد. زمانی که مهاجم قادر به برقراری ارتباط با دیتابیس یک سامانه باشد، عملاً تمامی منابع و داده های سامانه را در دست خواهد داشت.</p> <p>این آسیب پذیری می تواند منجر به کشف ایمیل ها، نام های کاربری و پسورد ها، موجودی حساب، شماره حساب، اطلاعات شخصی و اطلاعات مهم دیگری از کاربران و کارمندان سازمان گردد. همچنین مهاجم ممکن است اقدام به ویرایش یا حذف و حتی اضافه نمودن اطلاعات به سامانه نماید و یا دیتابیس را به طور کامل حذف نماید، همچنین در برخی شرایط، مهاجم قادر خواهد بود با استفاده از دستورات SQL اقدام به خواندن فایل ها، تغییر محتوا صفحات، آپلود فایل مخرب و ... بر روی سامانه نماید.</p>	شرح آسیب پذیری
High <u>(AV:N/AC:L/Au:N/C:C/I:C/A:C)</u> – 10.0		درجه اهمیت
Web Application		حوزه تاثیر
URL: https://museum.bmi.ir/s/Fa/22/?keyword=		سیستم های آسیب پذیر (IP&URL)
در حین بررسی، با صفحه ای مواجه شدیم که اخبار موجود در سامانه را بر اساس کلیدواژه ای دریافتی به کاربر نمایش می دهد، این کار به وسیله پارامتر keyword در URL سامانه انجام می گردد. سپس برای بررسی این پارامتر با دیتابیس یک علامت ' در انتهای مقدار این پارامتر قرار گرفت و مشاهده گردید که یک خطای Stack Trace به		روند بررسی



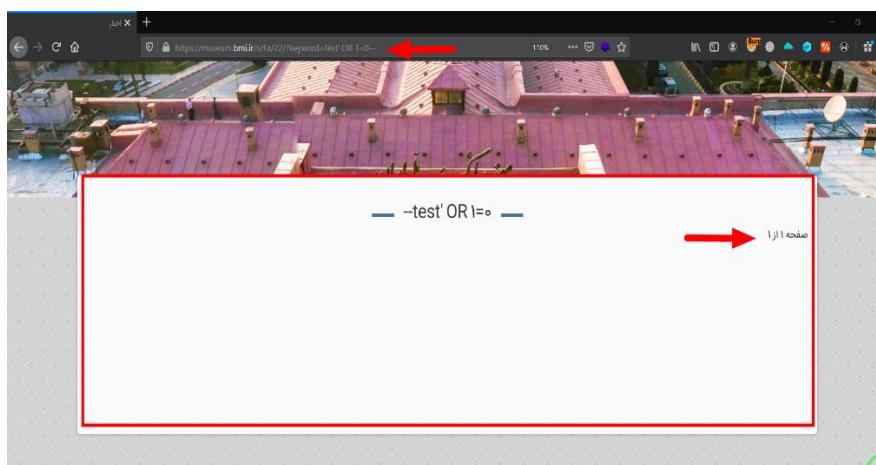
وجود آمد که از دلیل خطای ایجاد شده، متوجه گردیده که این پارامتر با دیتابیس در ارتباط بوده و خطای مربوطه نیز به دلیل عدم اعتبارستن جی مناسب رخ داده است.

سپس ادامه این روند به دو روش بررسی گردید که به شرح زیر می باشد:

ابتدا با استفاده از کوئری $OR 1=0$ اقدام به بررسی سامانه نموده و همانطور که در

تصویر نیز مشخص است، سامانه بدون خطا بارگذاری گردید اما هیچ خبری نیز نمایش

داده نشد.



سپس مقدار شرط را با استفاده از کوئیری `OR 1=1` برابر `True` قرارداده و مشاهده گردید که تمامی اخبار سامانه به دلیل `True` بودن شرط، در صفحه نمایش داده شد.



بازدید آقای فریاد، مدیر کل موزه

در روش دوم تلاش گردید تا تعداد ستون های دیتابیس با استفاده از کوئری ORDER BY

به دست آید، همانطور که در تصویر مشاهده می گردد، با قرار دادن مقدار 1 صفحه

بدون مشکل بارگذاری می گردد اما با قرار دادن مقدار 100 خطای رخ میدهد که بیانگر

این موضوع می باشد که تعداد ستون های وارد شده بیش از تعداد ستون های موجود می

باشد.

با مقداد صحیح

مرفه بانک ملی ایران

test ORDER BY 1

صفحه ۱ از ۱

و با مقدار ناصحیح



The ORDER BY position number 100 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException. The ORDER BY position number 100 is out of range of the number of items in the select list.

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:

```
[SqlException (0x80131904): The ORDER BY position number 100 is out of range of the number of items in the select list.] System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3986108 System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736 System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +90 System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +137 System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption, System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyn System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 t System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +83 System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301 System.Data.SqlClient.SqlCommand.ExecuteReader() +157
```

با کاهش مقدار 100 به 50 همچنان خطأ وجود داشت و سپس مقدار به 25 و پس از

آن 20 کاهش پیدا کرد و خطأ همچنان وجود داشت، اما با وارد کردن مقدار 15 صفحه

مربوطه بارگذاری گردید و خطأ همچنان وجود داشت، نهایتاً سامانه با مقدار 18

بارگذاری گردید در حالی که با مقدار 19 خطأ رخ میداد و از همین رو متوجه شدیم که

سامانه دارای 18 ستون می باشد.

همانطور که مشاهده می گردد با مقدار 19، سامانه بارگذاری نگردید.

The ORDER BY position number 19 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException. The ORDER BY position number 19 is out of range of the number of items in the select list.

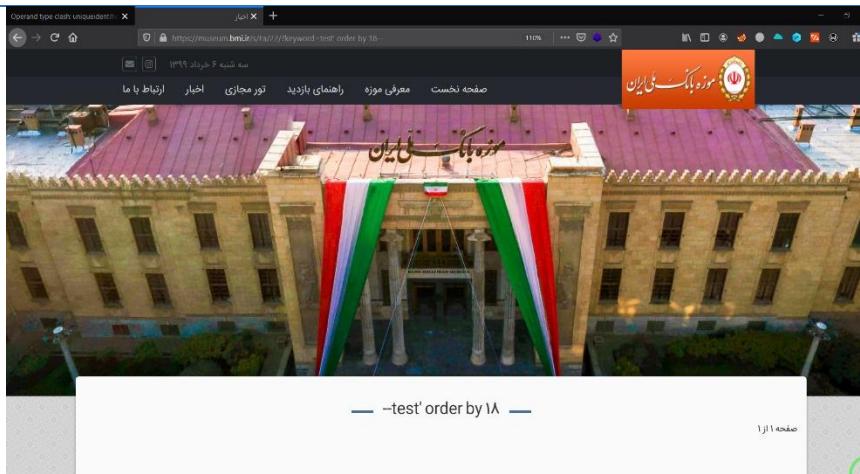
Source Error:

```
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:

```
[SqlException (0x80131904): The ORDER BY position number 19 is out of range of the number of items in the select list.] System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3986108 System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +736 System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +90 System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +137 System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParam System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyn System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task`1 result, Boolean asyn System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +83 System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +301 System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301 System.Data.SqlClient.SqlCommand.ExecuteReader() +157 echobit.core.SQLServerDB.RunSelectQuery(String _query) in D:\[Projects]\Echobit\Code\echobitlib\Core\SQLServerDB.cs:70 echobit.core.CMSArchive.GetArchiveItems_Published(String BL_ArchiveUID, Int32 TopCount, String BL_ArchiveCatUID, String keyword) in D:\[Projects]\Echobit\Code\echobit UserControls_ArchiveFullList.BindProperties2Elements() +314 UserControls_ArchiveFullList.Page_Load(Object sender, EventArgs e) +93 System.Web.UI.Control.OnLoad(EventArgs e) +106 System.Web.UI.Control.LoadRecursive() +162 System.Web.UI.Control.LoadRecursive() +162 System.Web.UI.Control.LoadRecursive() +162 System.Web.UI.Control.LoadRecursive() +162
```

و سپس با مقدار 18 بارگذاری گردید.



مطابق هماهنگی های انجام شده با کارفرمای محترم، به دلیل مسائل امنیتی، ادامه این روند مجاز نبوده و از ادامه این فرآیند صرف نظر گردید.

- علاوه بر بهروزرسانی دیتابیس خود به آخرین نسخه و نصب پچ های امنیتی راه کارهای زیر نیز پیشنهاد می گردد:

- استفاده از Prepared Statements با استفاده از استفاده از Parameterized Queries
- استفاده از Stored Procedures ها
- استفاده از روشن Whitelist Input Validation و مسدود سازی کاراکتر های غیر مجاز
- استفاده از روشن Escaping برای تمامی Input های دریافتی از کاربر
- استفاده از مکانیزم های بازدارنده در WAF

راهکار



2.5 آسیب پذیری های Medium

Vul-Museum-Website-M-01		شناسه آسیب پذیری
عنوان آسیب پذیری	آسیب پذیری	
	<p>در این آسیب پذیری که معمولاً به دلیل اعمال نادرست مکانیزم حذف token یا session رخ میدهد، پس از خروج کاربر از اکانت کاربری، نشست همچنان معتر بوده و مهاجم می‌توان با استفاده از این نشست که استفاده کننده اصلی آن اقدام به خروج از حساب کاربری خود نموده دست به اقداماتی از طریق حساب کاربری فرد مذکور بزند.</p> <p>این آسیب پذیری با توجه به سطح دسترسی حساب کاربری مربوطه و مدت زمان اعتبار نشست دارای اهمیت متفاوت خواهد بود.</p>	شرح آسیب پذیری
	<p>Medium <u>(AV:N/AC:L/Au:N/C:N/I:P/A:N)</u> – 5.0</p> <p>Web Application</p>	درجه اهمیت
	<p>URL: https://museum.bmi.ir/Admin/Dashboard.aspx</p> <p>ابتدا وارد حساب کاربری مربوطه شده و سپس اقدام به تغییر رمز عبور می‌نماییم.</p>	حوزه تاثیر
	<p>سیستم‌های آسیب‌پذیر (IP&URL)</p> <p>روند بررسی</p> <p>سپس درخواست تغییر پسورد را با استفاده از ابزار burpsuite به بخش repeater ارسال نموده و از اکانت کاربری خارج می‌شویم.</p>	

	پروژه آزمون نفوذپذیری - موزه بانک ملی ایران موزه بانک ملی ایران	
---	--	---

Burp Suite Professional v2.0.11beta - museum.bmi.ir - licensed to Milan

Target: https://museum.bmi.ir

Request

```
POST AdminChangeUserInfo.aspx?Token=828c2029beba3178b4bf3c458c0604f HTTP/1.1
Host: museum.bmi.ir
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 676
Origin: https://museum.bmi.ir
Connection: close
Referer: https://museum.bmi.ir/AdminChangeUserInfo.aspx?Token=828c2029beba3178b4bf3c458c0604f
id
Cookie: mainpageTabNumber=4; ASP.NET_SessionId=jyjmbn0ee250ox15d10ek;
MyAppCookie=1CA824D87F7FBC5CAAA4CC9C637FB9013034328C8FD8623B3775647F7CDAB
D104AF5004C8785E327C74956D00105F10CF3F88737D83B84047730F6C319DAB754BD772842
E89976D9EAC451EAB517A014BDB08E283882A8468522248C8CDE173B8E8F4E8639D6339D2
0A747BA340E39AD5A88A84FCCDF9FB977B6C2A283BE15A4243E86A17289FE318BF94C397
105986875997AB5883AE43F
```

Response

Raw

پس از خروج از حساب، اقدام به ارسال دستور ضبط شده در repeater نموده و مشاهده

می گردد که دستور با موفقیت اجرا گردید.

Burp Suite Professional v2.0.11beta - museum.bmi.ir - licensed to Milan

Target: https://museum.bmi.ir

Request

```
POST AdminChangeUserInfo.aspx?Token=828c2029beba3178b4bf3c458c0604f HTTP/1.1
Host: museum.bmi.ir
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 676
Origin: https://museum.bmi.ir
Connection: close
Referer: https://museum.bmi.ir/AdminChangeUserInfo.aspx?Token=828c2029beba3178b4bf3c458c0604f
Done
```

Response

Raw Headers HTML Render ViewState

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: Fri, 31 Jan 1980 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
X-Powered-By: ASP.NET
Date: Mon, 18 May 2020 07:32:50 GMT
Content-Length: 4111
```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

پس از انجام این مراحل با پسورد جدید وارد اکانت کاربری شده و تایید گردید که پسورد عوض شده است.

- نشست یا توکن و تمامی اطلاعات مربوط به آن پس از خروج از حساب کاربری به طور کامل غیر قابل استفاده گردد.

راهکار



Vul-Museum-Website-M-02		شناسه آسیب پذیری
آسیب پذیری	عنوان آسیب پذیری	
<p>در حالت عادی، این صفحات نباید برای کاربران عادی سامانه به نمایش درآید، توجه نمایید که این خطاهای ممکن است حاوی اطلاعات حساس، قطعات کد، مسیرهای سیستمی و بسیاری اطلاعات مهم دیگر باشند.</p>		
Medium <u>(AV:N/AC:L/Au:N/C:P/I:N/A:N)</u> – 5.0		
Web Application		
URL: https://museum.bmi.ir/s/MainFa/1/		
<p>با وارد کردن هر مقداری به شکل تگ HTML در URL صفحه، خطایی به شرح زیر نمایش داده می‌شود: (همانطور که مشاهده می‌گردد، علاوه بر قطعات کد، نسخه‌ی Microsoft داده است که صورت کامل مشخص می‌باشد.)</p>		
 <p>Server Error in '/' Application. A potentially dangerous Request.Path value was detected from the client (>). Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code. Exception Details: System.Web.HttpException: A potentially dangerous Request.Path value was detected from the client (>). 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: [HttpException (0x80004005): A potentially dangerous Request.Path value was detected from the client (>).] System.Web.HttpRequest.ValidateInputIfRequiredByConfig() +11981492 System.Web.PipelineStepManager.ValidateHelper(HttpContext context) +52 Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0</p>		
<p>همچنین برای پارامتر g مقداری تصادفی به صورت Base64 قرار داده شد که نتیجه آن نیز به شکل خطای زیر می‌باشد.</p>		
 <p>Server Error in '/' Application. Index was outside the bounds of the array. Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code. Exception Details: System.IndexOutOfRangeException: Index was outside the bounds of the array. 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: [IndexOutOfRangeException: Index was outside the bounds of the array.] System.Web.HttpRequest.ValidateInputIfRequiredByConfig() +11981494 System.Web.UI.Control.OnLoadRecursive(Control sender, EventArgs e) +106 System.Web.UI.Control.OnLoadRecursive() +48 System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +3785 Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0</p>		



همچنین یک نمونه دیگر از این مشکل که توسط اسکنر NetSoparker شناسایی گردید،

منجر به افشاری اطلاعات حساس گردید که شامل IP داخلی سیستم مدیریت کننده سرور

می باشد.

- استفاده از صفحات خطای شخصی سازی شده در سامانه

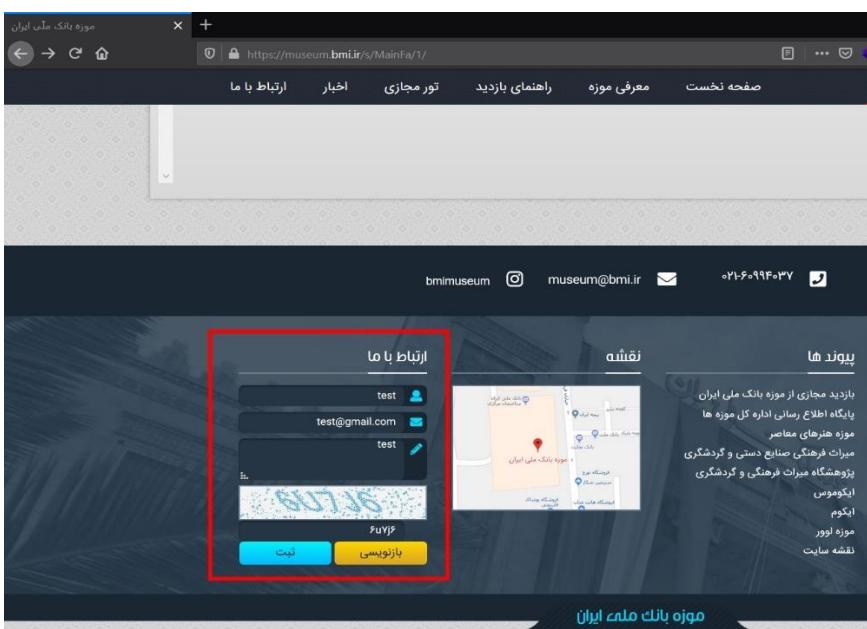
- رفع خطاهاي پيغامه نويسي، از طریق قرار دادن Exception ها در کد های

تا در صورت بروز خطأ، بر اساس Exception نوشته شده، وند Back-end

برنامه ادامه بارد.

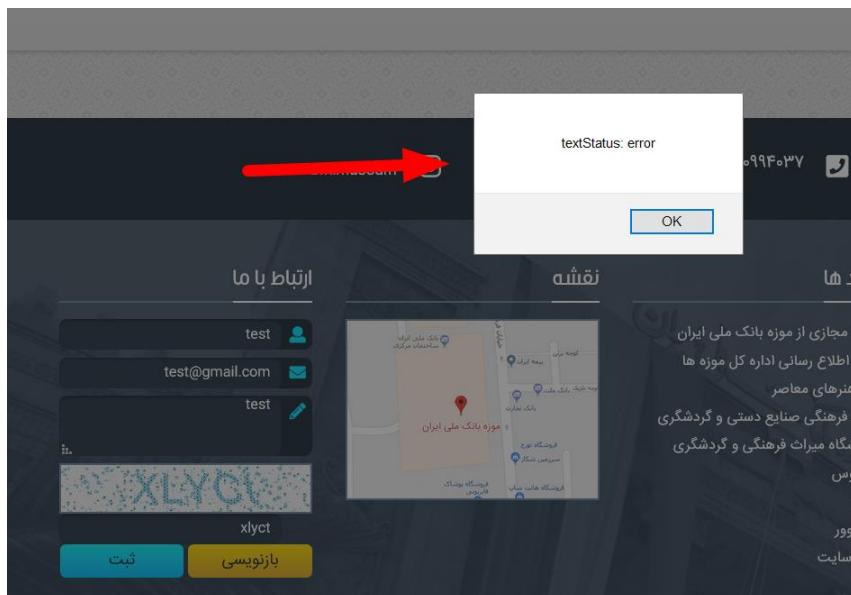
راهکار



عنوان آسیب پذیری	عنوان آسیب	شناسه آسیب پذیری
فایل لگ حاوی اطلاعات بسیار زیادی از جمله فعالیت های انجام شده، قطعات کد و خطاهای، تلاش های کاربران برای ورود، یوزر نیم و پسورد و اطلاعات ارزشمند دیگری می باشد. این فایل تنها باید برای مالک سامانه یا مسئول مربوطه قابل دسترسی باشد، در صورت رعایت نکردن مکانیزم های امنیتی مناسب در جهت محافظت از این فایل، مهاجم با دستیابی به این فایل می تواند اقدام به استفاده از اطلاعات موجود در فایل در جهت آسیب رساندن به سامانه نماید.	شرح آسیب پذیری	فایل لگ حاوی اطلاعات بسیار زیادی از جمله فعالیت های انجام شده، قطعات کد و خطاهای، تلاش های کاربران برای ورود، یوزر نیم و پسورد و اطلاعات ارزشمند دیگری می باشد. این فایل تنها باید برای مالک سامانه یا مسئول مربوطه قابل دسترسی باشد، در صورت رعایت نکردن مکانیزم های امنیتی مناسب در جهت محافظت از این فایل، مهاجم با دستیابی به این فایل می تواند اقدام به استفاده از اطلاعات موجود در فایل در جهت آسیب رساندن به سامانه نماید.
Medium (AV:N/AC:L/Au:N/C:P/I:N/A:N) – 5.0	درجه اهمیت	Web Application
URL: https://museum.bmi.ir/Admin/WriteFolder/LogFile.txt	سیستم های آسیب پذیر (IP&URL)	هنگام بررسی قسمت مربوط به ارتباط به ما در انتهای صفحه اول سامانه، اطلاعات در فیلد ها وارد و اقدام به ارسال پیغام گردید.
	روند بررسی	

	پروژه آزمون نفوذپذیری - موزه بانک ملی ایران موزه بانک ملی ایران	
---	--	---

پس از کلیک بر روی دکمه ثبت، با خطایی به شرح زیر مواجه شدیم.



پس از مواجهه با این خطا، اقدام به بررسی درخواست مربوطه به وسیله ابزار BurpSuit نموده و مشاهده گردید که در پاسخ دریافتی از سمت سرور، خطایی دریافت می گردد که اشاره به آدرس خاصی در سامانه دارد.

Request

```
GET /MainFa.aspx?ps=f&ajaxparam=PostComment$SS$test$SS$test@gmail.com$SS$test$SS$info@asmanfaraz.ir$SS$lyct$SS$7dbebdd7-0700-4bfc-975c-75ea0ea4b0b4 HTTP/1.1
Host: museum.bmi.ir
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/plain, */*;q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: https://museum.bmi.ir/MainFa/
Cookie: mainpagetabnumber=4; ASP.NET_SessionId=zseas42wzqwpd5cpj1qyn0jt
```

Response

```
HTTP/1.1 500 Internal Server Error
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: Fri, 01 Jan 1990 08:00:00 GMT
X-Frame-Options: SAMEORIGIN
X-Powered-By: ASP.NET
Date: Tue, 19 May 2020 06:52:52 GMT
Connection: close
Content-Length: 8286

<!DOCTYPE html>
<html>
<head>
<title>Access to the path 'E:\WebSite\museum\BMI\Admin\WriteFolder\LogFolder\LogFile.txt' is denied.</title>
<meta name="viewport" content="width=device-width">
<style>
body {font-family:'Verdana';font-weight:normal;font-size:.7em;color:black}
p {font-family:'Verdana';font-weight:normal;color:black;margin-top:-5px}
b {font-family:'Verdana';font-weight:bold;color:black;margin-top:-5px}
H1 { font-family:'Verdana';font-weight:normal;font-size:18pt;color:red }
H2 { font-family:'Verdana';font-weight:normal;font-size:14pt;color:maroon }
pre {font-family:'Consolas','Lucida
```

با وارد کردن آدرس مربوطه در مرورگر، صفحه مربوطه که حاوی log های سامانه می باشد، بدون هیچ مکانیزم امنیتی پیشگیرانه ای باز شد.



با پرسی این فایل اطلاعاتی به دست آمد که به شرح زیر می‌پاشد:

۱- یورت مورد استفاده در Loacal host

2- نام کاربری و پسورد و همچنین آدرس میل سرور

```
12/26/2018 10:03:28 PM Mailhost:93.126.21.30 Username: no-reply, Encoded: 123456 System.Net.SmtpException: Failure sending mail. ---> System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 93.126.21.30:25  
at System.Net.Sockets.Socket.DoConnect(EndPoint endPointSnapshot, SocketAddress socketAddress)  
at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket socket, IPAddress address, ConnectSocketState state, IAsyncResult asyncResult, Exception e)  
--- End of inner exception stack trace ---  
at System.Net.ServicePoint.GetConnection(PooledStream PooledStream, Object owner, Boolean async, IPAddress address, Socket s, Socket abortSocket, Socket s, Int32 abortSocket6)  
at System.Net.PooledStream.AsyncGetConnection(IObjectWrapper owningObject, Boolean async, GeneralIAsyncResultDelegate asyncCallback)  
at System.Net.ConnectionPointCollection.AsyncGetConnection(IObjectWrapper owningObject, GeneralIAsyncResultDelegate asyncCallback, Int32 creationTimeout)  
at System.Net.ServicePoint.GetAsync(IPEndPoint endPoint, Int32 creationTimeout)  
at System.Net.Mail.SmtpClient.get_ConnectionPoint()  
at System.Net.Mail.SmtpClient.Send(MailMessage message)  
--- End of inner exception stack trace ---  
at System.Net.Mail.SmtpClient.Send(MailMessage message)  
at Echobit.core.MailSender.Send(ArrayList ToAddresses, String Subject, String Body) in D:\[Projects]\Echobit\EchobitLib\Core\MailSender.cs:line 162
```

با بررسی IP مربوطه مشخص گردید که این ارتباط از شهر اصفهان انجام گردیده و موفقیت آمیز

نیز نبوده است.

اطلاعات دیتاپس - 3



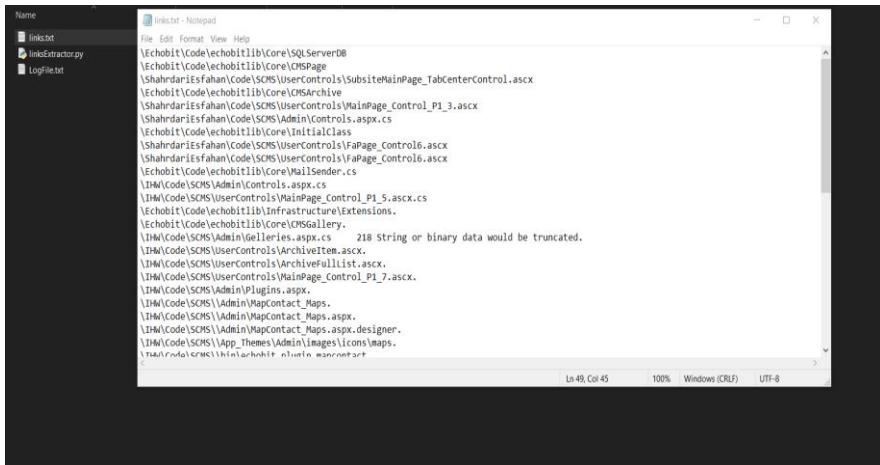
```

at System.Data.SqlClient.SqlInternalConnectionTds.LoginNoFailover(ServerInfo serverInfo, String newPassword, Boolean redirectedUserInstance, SqlConnection
connectionOptions, TimeoutTimer timeout)
at System.Data.SqlClient.SqlInternalConnectionTds.OpenLoginEnlist(SqlConnection owningObject, TimeoutTimer timeout, SqlConnectionString connectionOptions,
redirectedUserInstance)
at System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, Object providerInfo, Stri
ng newPassword, Boolean redirectedUserInstance)
at System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, Object poolGroupProviderInfo, DbConnectionPool pool, DbConnecti
onFactory info)
at System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnectionPool pool, DbConnection owningObject, DbConnectionOptions options, String
providerConnectionString, DbConnection owningConnection, DbConnectionPool pool, DbConnectionOptions options)
at System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject)
at System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject)
at System.Data.ProviderBase.DbConnectionFactory.GetConnection(DbConnection owningObject)
at System.Data.ProviderBase.DbConnectionPool.GetConnection(DbConnection owningConnection)
at System.Data.ProviderBase.DbConnectionFactory.GetConnection(DbConnection outerConnection, DbConnectionFactory connectionFactory)
at System.Data.SqlClient.SqlConnection.Open()
at D:\Projects\ShahrdariEsfahan\Code\SCMS\UserControls\FaPage_Control6.BindPropertiesElements() in d:\[Projects]\ShahrdariEsfahan\Code\SCMS\UserControls\FaPage_Control6.aspx.cs:line 66
Cannot open database "SCMS" requested by the login. The login failed.
Login failed for user 'CIO\wali'.
-----
```

9/6/2015 11:15:14 AM
at System.Web.UI.TemplateParser.ProcessException(Exception ex)
at System.Web.UI.TemplateParser.HandlePostParse()

4- لینک های مهم

تمامی لینک های داخل فایل log به شرح زیر برای بررسی بیشتر استخراج گردید.



توجه نمایید که برخی از لینک های مربوطه منجر به دسترسی به صفحاتی شدند که در حالت عادی دسترسی به آنها امکان پذیر نبود و با بدست آوردن مسیر آن از داخل فایل log به آن دسترسی پیدا کرده.

- با توجه به اینکه رسیدن به این فایل، نتیجه‌ی یک خطای اشتباه در سامانه بود، لذا تمامی خطاهای سامانه باید شخصی سازی گردد و از انتشار هرگونه اطلاعات در پاسخ‌های خطای سرور جلوگیری به عمل آید.

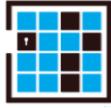
راهکار

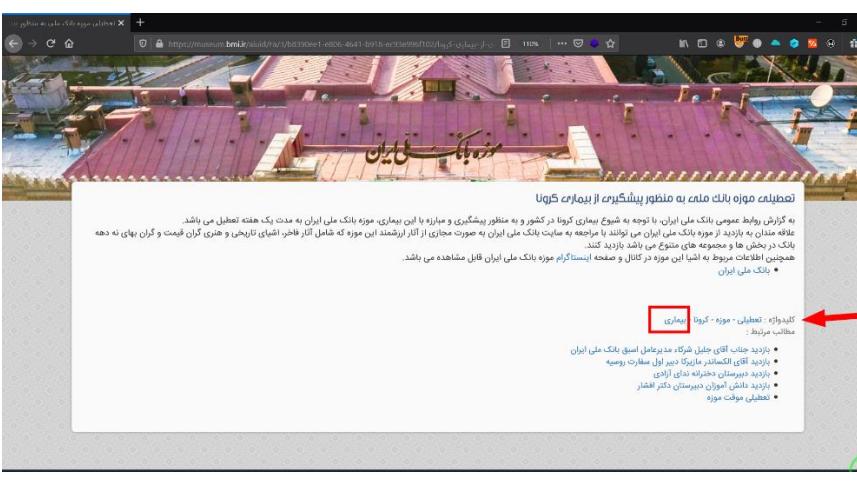


- ایجاد یک مکانیزم امنیتی مناسب جهت کنترل دسترسی به فایل های سیستم، چنین فایلی نباید

برای کاربران عادی در دسترس باشد. (با اینکه دسترسی نوشتن در این فایل وجود نداشت، اما تنها

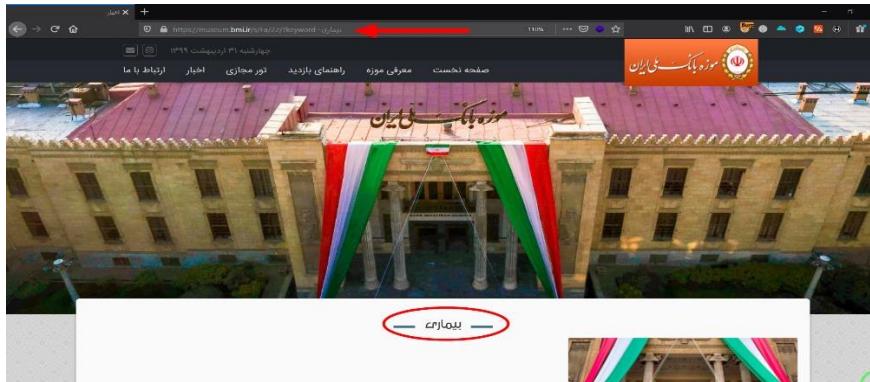
قابلیت خواندن به افشاء اطلاعات زیادی انجامید.)



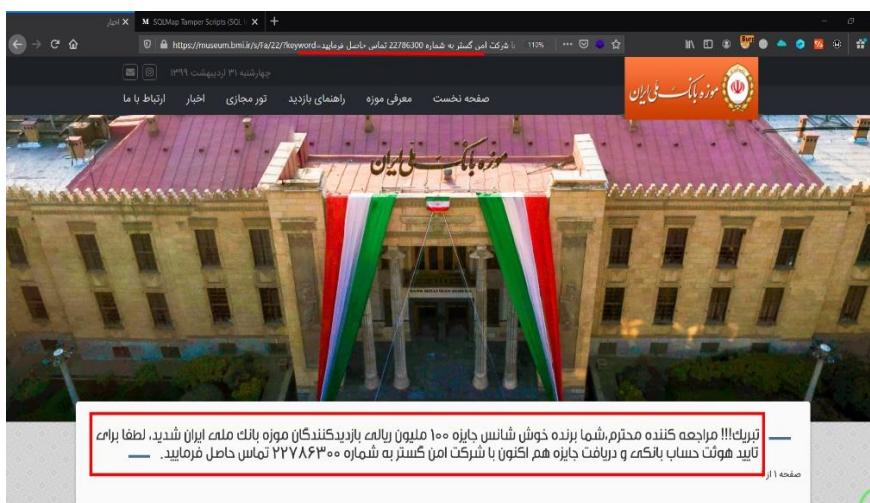
Vul-Museum-Website-M-04		شناسه آسیب پذیری
عنوان آسیب پذیری	آسیب پذیری	
شرح آسیب پذیری	<p>این آسیب پذیری میتواند متن مورد نظر مهاجم را به صورت مستقیم بر روی صفحه نماید دهد. شاید در نگاه اول چنین آسیب پذیری زیاد مهم به نظر نرسد، اما وقتی متن دلخواه مهاجم در قالب و چهارچوب سامانه اصلی نمایش داده می شود، اعتبار زیادی به متن مربوطه میدهد و مهاجم می تواند از آن برای فریب کاربران و حتی افرادی که کاربر سامانه نمی باشند نیز استفاده نمیاد. اهمیت این آسیب پذیری رابطه مستقیمی با اهمیت و کسب کار سامانه آسیب پذیر دارد و از آنجایی که در حال حاضر اسن آسیب پذیری بر روی سامانه بانکی معتبر کشف گردیده، از اهمیت بسیار بالایی برخوردار می باشد.</p>	
درجه اهمیت	Medium <u>(AV:N/AC:L/Au:N/C:N/I:P/A:N)</u> – 5.0	
حوزه تاثیر	Web Application	
سیستم‌های آسیب‌پذیر (IP&URL)	URL: https://museum.bmi.ir/s/Fa/22/?keyword=Vulnerable_parameter	
روند بررسی	با مراجعه به قسمت خبری سامانه موزه بانک ملی، در زیر اخبار و تصاویر، قسمتی به نام کلید واژه وجود داشت که به عنوان راهی برای یافتن مطالب مشابه استفاده می گردد.	 <p>The screenshot shows a search result page for 'Vulnerable parameter'. The result is a news item from the 'News' section. The headline reads: 'تقطیعات موزه بانک ملی به اینترنت پیشکشی از بیمه‌ها کلوب' (Cut-offs from the National Museum to the Internet). The text of the news item discusses the implementation of new rules regarding the use of the term 'cut-off' in contracts, which has led to some confusion and potential legal issues. A red arrow points to the word 'کلوب' (Club) in the text, which is highlighted in red.</p>



با کلیک بر روی این لینک به صفحه ای مانند صفحه نتیجه جستجو هدایت شده که موضوع مربوطه جستجو شده و نتیجه آن نمایش داده شده، اما متن مورد جستجو که در لینک به پارامتر keyword ارسال گردیده است، به صورت مستقیم بر روی صفحه چاپ گردیده است.



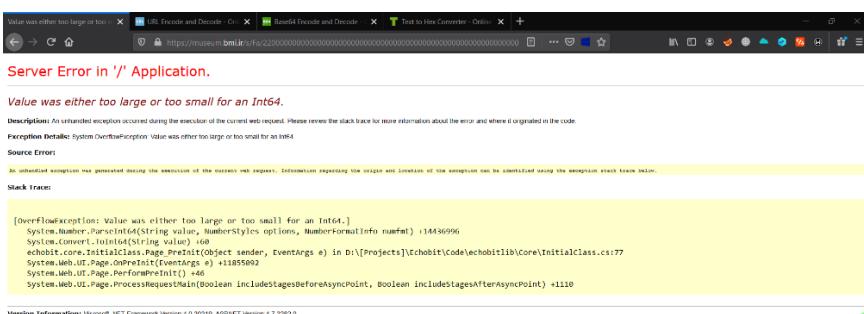
سپس اقدام به تزییق متن مورد نظر خود در این پارامتر نموده و همانطور که مشاهده می گردد، متن ساختگی به صراحت بر روی صفحه سامانه قابل مشاهده می باشد.



- بهترین و مطمئن ترین راه، عدم نمایش مستقیم متن گرفته شده از کاربر بر روی صفحات سامانه می باشد. بهتر است از کلمات آماده ای نظیر "چنین کلید وژه ای یافت نشد." و... استفاده گردد.

راهکار



Vul-Museum-Website-M-05		شناسه آسیب پذیری
عنوان آسیب پذیری	آسیب پذیری	Full path disclosure
شرح آسیب پذیری	در این آسیب پذیری، مهاجم میتواند در یک صفحه خطای Stack Trace یا آدرس کامل از قسمتی از سامانه به دست آورد، این آدرس محل دقیقی از محل وقوع مشکل یا خطای را به مهاجم نشان میدهد، این آدرس کامل بوده و حتی درایو یا پارتیشنی که سامانه بر روی آن در حال اجرا می باشد را نشان می دهد. این اطلاعات برای مهاجم بسیار حیاتی بوده و می تواند مهاجم را برای آسیب رساندن به سامانه یا کشف آسیب پذیری های بیشتر راهنمایی نماید.	آسیب پذیری
درجه اهمیت	Medium (AV:N/AC:L/Au:N/C:P/I:N/A:N) – 5.0	
حوزه تاثیر	Web Application	
سیستم‌های آسیب‌پذیر (IP&URL)	URL: https://museum.bmi.ir/s/MainFa/1/	
روند بررسی	با تغییر در URL و مقادیر ارسالی به سمت سرور، با خطاهای Stack Trace بسیاری در سامانه مواجه شدیم، اما برخی از این خطاهای دارای مسیر کاملی از قسمتی از سامانه یا کد قابل اجرای آن به شرح زیر می باشد.(این خطا به دلیل وارد کردن مقدار عددی بسیار بزرگ در URL سامانه رخ داد)	با تغییر در URL و مقادیر ارسالی به سمت سرور، با خطاهای Stack Trace بسیاری در سامانه مواجه شدیم، اما برخی از این خطاهای دارای مسیر کاملی از قسمتی از سامانه یا کد قابل اجرای آن به شرح زیر می باشد.(این خطا به دلیل وارد کردن مقدار عددی بسیار بزرگ در URL سامانه رخ داد)
 <p>Server Error in '/' Application. Value was either too large or too small for an Int64. Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code. Exception Details: System.OverflowException: Value was either too large or too small for an Int64 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: [OverflowException: Value was either too large or too small for an Int64.] System.Number.Int64FromDouble(Double value, NumberStyles options, NumberFormatInfo numfmt) +10436996 System.Convert.ToInt64(Int64 value) +0 echobit.core.InitialClass.Page.PreInit(Object sender, EventArgs e) in D:\[Projects]\echobit\code\echobit\lib\Core\InitialClass.cs:77 System.Web.UI.Page.OnPreInit(EventArgs e) +11855892 System.Web.UI.Page.PerformPreInit() +46 System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1110 Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0</p>		روند بررسی



همانطور که ملاحظه می نمایید علاوه بر اطلاعات مهم (نسخه دقیق .NET)

و قطعات کد منتشر شده در صفحه، مسیر خاصی از سامانه،

به صورت کامل قابل مشاهده می باشد.

همچنین در هنگام استفاده از قسمت "ارتباط با ما" در انتهای صفحه، با خطای Stack

زیر مواجه شده:

Access to the path 'E:\WebSite\museum\BMI\Admin\WriteFolder\LogFolder\LogFile.txt' is denied.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.UnauthorizedAccessException: Access to the path 'E:\WebSite\museum\BMI\Admin\WriteFolder\LogFolder\LogFile.txt' is denied.

ASP.NET is not authorized to access the requested resource. Consider granting access rights to the resource to the ASP.NET request identity. ASP.NET has a base process identity (typically IIS/IIS APPPOOL) on IIS 6 or Network Service on IIS 7, and the configured application pool identity on IIS 7.5 that is used if the application is impersonating. If the application is impersonating via <identity impersonate="true">, the identity will be the anonymous user (typically IUSR_MACHINENAME) or the authenticated request user. To grant ASP.NET access to a file, right-click the file in File Explorer, choose "Properties" and select the Security tab. Click "Add" to add the appropriate user or group. Highlight the ASP.NET account, and check the boxes for the desired access.

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:

```
[UnauthorisedAccessException: Access to the path 'E:\WebSite\museum\BMI\Admin\WriteFolder\LogFolder\LogFile.txt' is denied.]  
System.IO._Internal.WriteFile(Int32 errorCode, String maybeFullPath) +417  
System.IO.FileStream._Init(String path, FileMode mode, FileAccess access, Int32 rights, FileShare share, Int32 bufferSize, FileOptions options, SECURITY_ATTRIBUTES& securityAttrs, Boolean bFromProxy, Boolean useLongPath) +123  
System.IO.FileStream..ctor(String path, FileMode mode, FileAccess access, FileShare share, Int32 bufferSize, FileOptions options, String msgPath, Boolean bFromProxy, Boolean useLongPath) +103  
System.IO.StreamWriter..ctor(String path, Boolean append, Encoding encoding, Int32 bufferSize, Boolean checkHost) +103  
System.IO.StreamWriter..ctor(String path) +59  
echoHabit.core.ErrorHandling.Setup(Exception ex) in D:\[Projects]\echoHabit\Code\echoHabitLib\Core\ErrorHandling.cs:48  
echoHabit.ul.FaultSendComment(String toEmailAddress, String UserFullname, String Desc, String UserEmail, String captchaText, String captchaID) +665  
echoHabit.ul.FaultSendComment(String toEmailAddress, String UserFullname, String Desc, String UserEmail, String captchaText, String captchaID) +665  
Mainfa.Page_Load(Object sender, EventArgs e) +279  
System.Web.UI.Control.OnLoad(EventArgs e) +106  
System.Web.UI.Control.LoadRecursive() +68  
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +3785
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3202.0

این خطای اشاره به آدرس کامل فایلی به نام LogFile.txt دارد و همانطور که در

گزارش مطرح شده است، با استفاده از این مسیر به دست آمده، به فایل Log سیستم

دسترسی پیدا نموده و در ادامه با استخراج مسیرهایی از این فایل، توانستیم به صفحاتی

از پنل مدیریت دسترسی پیدا نماییم که در حالت عادی قابل دسترس نمی باشد.

همچنین در قسمتی از سامانه، با وارد کردن مقدار عدد 1 در پارامتری که باید مقدار

قرار بگیرد با خطای مواجه شدیم که باز هم مسیری کامل به نمایش درآمد.

Server Error in '/' Application.

Invalid length for a Base-64 char array or string.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.FormatException: Invalid length for a Base-64 char array or string.

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:

```
[FormatException: Invalid length for a Base-64 char array or string.]  
System.Convert.FromBase64CharPtr(Char* inputptr, Int32 inputlength, Byte* startDestIntPtr, Int32 destLength) +802  
System.Convert.FromBase64String(String s) +48  
echoHabit.core.CMSGallery.DecodeGalleryParam(String Param) in D:\[Projects]\echoHabit\Code\echoHabitLib\Core\CMSGallery.cs:264  
CMSGallery.DecodeGalleryParam() +608  
System.Web.UI.Control.OnLoad(EventArgs e) +106  
System.Web.UI.Control.LoadRecursive() +68  
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +3785
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3202.0



- استفاده از صفحات خطای شخصی سازی شده در سامانه

- رفع خطاهای برنامه نویسی از طریق قرار دادن Exception ها در کد های

Back-end تا در صورت بروز خطا، بر اساس Exception نوشته شده روند

برنامه ادامه یابد.

راهکار



3.5 آسیب پذیری های Low

Vul-Museum-Website-L-01	شناسه آسیب پذیری
استفاده از نسخه آسیب پذیر Bootstrap 3.3.7	عنوان آسیب پذیری
یک فریم ورک محبوب است که به کمک آن می‌توان صفحات وب واکنش گرا طراحی کرد. اما ممکن است برخی از توابع استفاده شده در این فریم ورک آسیب پذیر باشند. در این نسخه از Bootstrap، توابع زیادی وجود دارند که مهاجم می‌تواند با مقدار دهی به آنها در صورت عدم کنترل ورودی‌ها یا دور زدن مکانیزم‌های امنیتی مربوطه اقدام به حملات XSS نماید.	شرح آسیب پذیری
حملات XSS می‌توانند منجر به سرقت اطلاعات کاربر، تغییر محتویات صفحه، هدایت کاربر به صفحات دیگر و... گردد.	
میانگین امتیاز این آسیب پذیری‌ها که تعداد آنها به 6 عدد می‌رسد، برابر 4.3 می‌باشد.	
Low	درجه اهمیت
Web Application	حوزه تاثیر
URL: https://museum.bmi.ir/s/MainFa/1/	sistemi‌های آسیب‌پذیر (IP&URL)
با استفاده از افزونه Wappalyzer مشخص گردید که سامانه از نسخه 3.3.7 فریم ورک استفاده می‌نماید.	روند بررسی



همچنین با بررسی این نسخه در اینترنت تعداد ۶ آسیب پذیری XSS برای این نسخه به شرح زیر یافت گردید.

Getbootstrap » Bootstrap » 3.3.7 : Security Vulnerabilities

Cpe Name:cpe:/a:getbootstrap:bootstrap/3.3.7

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By: CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-8331 79		XSS		2019-02-20	2019-06-11	4.3	None	Remote	Medium	Not required	None	Partial	None
In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.														
2	CVE-2018-20677 79		XSS		2019-01-09	2019-06-11	4.3	None	Remote	Medium	Not required	None	Partial	None
In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.														
3	CVE-2018-20676 79		XSS		2019-01-09	2019-06-11	4.3	None	Remote	Medium	Not required	None	Partial	None
In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.														
4	CVE-2018-14042 79		XSS		2018-07-13	2019-05-10	4.3	None	Remote	Medium	Not required	None	Partial	None
In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.														
5	CVE-2018-14040 79		XSS		2018-07-13	2019-05-10	4.3	None	Remote	Medium	Not required	None	Partial	None
In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.														
6	CVE-2016-10735 79		XSS		2019-01-09	2019-06-11	4.3	None	Remote	Medium	Not required	None	Partial	None
In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.														
Total number of vulnerabilities : 6 Page : 1 (This Page)														

ارتقا Bootstrap به آخرین نسخه آن -

راهکار

شناسه آسیب
پذیری

Vul-Museum-Website-L-02

عنوان آسیب پذیری	استفاده از نسخه آسیب پذیر JQuery 3.3.1
شرح آسیب پذیری	<p>JQuery یک کتابخانه از جاوا اسکریپت است که پیمایش اسناد HTML، رسیدگی به رویدادها، متحرک سازی و تعاملات AJAX را به منظور توسعه سریع وب تسهیل می کند. اما ممکن است برخی از توابع و کلاس های استفاده شده در این کتابخانه آسیب پذیر باشند. در این نسخه از JQuery، به دلیل مشکلی که در Object.prototype وجود دارد، می توان از jQuery.extend سو استفاده نمود که مهاجم را قادر می سازد تا در صورت عدم کنترل ورودی ها یا دور زدن مکانیزم های امنیتی مربوطه اقدام به حملات XSS نماید.</p> <p>حملات XSS می توانند منجر به سرقت اطلاعات کاربر، تغییر محتویات صفحه، هدایت کاربر به صفحات دیگر و... گردد.</p> <p>میانگین امتیاز این آسیب پذیری برابر 4.3 می باشد.</p>
درجه اهمیت	Low
حوزه تاثیر	Web Application
سیستم های آسیب پذیر (IP & URL)	URL: https://museum.bmi.ir/s/MainFa/1/
روند بورسی	با استفاده از افزونه Wappalyzer مشخص گردید که سامانه از نسخه 3.3.1 کتابخانه JQuery استفاده می نماید.



Wappalyzer

Web frameworks

Microsoft ASP.NET

Miscellaneous

Swiper Slider

Web servers

IIS IIS

JavaScript graphics

particles.js

Operating systems

Windows Server

JavaScript libraries

jQuery 3.3.1

Lightbox

UI frameworks

Bootstrap 3.3.7

animate.css

همچنین با بررسی این نسخه در اینترنت یک آسیب پذیری XSS برای این نسخه به شرح زیر یافت گردید.

Jquery » JQuery » 3.3.1 : Security Vulnerabilities

Cpe Name:cpe:/a:jquery:jquery:3.3.1

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-11358	79	XSS	2019-04-19 2019-06-12	4.3			None	Remote	Medium	Not required	None	Partial	None

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable `_proto_` property, it could extend the native `Object.prototype`.

Total number of vulnerabilities : 1 Page : [1](#) (This Page)

- ارتقا JQuery به آخرین نسخه آن

راهکار



Vul-Museum-Website-L-03		شناسه آسیب پذیری
استفاده از نسخه آسیب پذیر .Net Framework 4.0.30319	عنوان آسیب پذیری	
<p>NET Framework. یک فریم ورک مت Shankl از مجموعه ای از رابط های ماربردی برنامه نویسی و یک کتابخانه مشترک از کدها است. اما ممکن است برخی از توابع استفاده شده در این فریم روک آسیب پذیر باشند. در این نسخه از NET Framework، به دلیل مشکلات بسیاری که وجود دارد، مهاجم را قادر خواهد بود تا در صورت عدم کنترل ورودی ها یا دور زدن مکانیزم های امنیتی مربوطه اقدام به حملات مختلفی از جمله DOS، Exec Code و جمع آوری اطلاعات نماید.</p> <p>حملات DOS می تواند منجر به از دسترس خارج شدن سامانه به طور کامل، یا کند شدن شدید آن گردد.</p> <p>حملات Exec Code نیز به مهاجم اجازه اجرای کد از راه دور را می دهد.</p> <p>میانگین امتیاز اکثر این آسیب پذیری ها که تعداد آنها 58 عدد می باشد، برابر 9.3 می باشد.</p>	شرح آسیب پذیری	
Low	درجه اهمیت	
Web Application	حوزه تاثیر	
URL: https://museum.bmi.ir/s/MainFa/1/	سیستم های آسیب پذیر (IP & URL)	
با استفاده از افزونه Whatruns مشخص گردید که سامانه از نسخه 4.0.30319 فریم ورک.NET استفاده می نماید.	روند بررسی	



What runs museum.bmi.ir?

CMS

Particles JS

Web Framework

Bootstrap

Programming Language

ASP.NET 4.0.30319

Gallery

Lightbox

Javascript Graphics

WOW

Javascript Frameworks

jQuery 3.3.1

همچنین با بررسی این نسخه در اینترنت آسیب پذیری های فراوانی برای این نسخه به

شرح زیر یافت گردید.

Microsoft » .NET Framework » 4.0 : Security Vulnerabilities

Cve Number: CVE-2015-4622 119 Exec Code Overflow Mem. Corr. 2015-12-09 2019-05-19 None Remote Medium Not required Complete Complete Complete

The Windows font library in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT Gold and R1; Office 2007 SP3; Office 2010 SP2; Word Viewer; .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6; Skype for Business 2016; Lync 2010; Lync 2013 SP1; Live Meeting 2007 Console; and Silverlight 5 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corrupted Vulnerability."

Cve Number: CVE-2015-4622 28 Exec Code 2015-11-11 2018-10-12 None Remote Medium Not required None Partial None

Cross-site scripting (XSS) vulnerability in Microsoft .NET Framework 4.0, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka ".NET Elevation of Privilege Vulnerability."

Cve Number: CVE-2015-4628 200 Info 2015-11-11 2018-10-12 None Remote Medium Not required Partial None None

The XML-DTD parser in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to read arbitrary files via an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, aka ".NET Information Disclosure Vulnerability."

Cve Number: CVE-2015-4644 118 Exec Code Overflow Bypass 2015-09-14 2018-10-12 None Remote Medium Not required Complete Complete Complete

Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 improperly counts objects before performing an array copy, which allows remote attackers to (1) execute arbitrary code via a crafted XAML browser application (XBAP) or (2) bypasses Microsoft .NET Framework application, aka ".NET Execution of Privilege Vulnerability."

Cve Number: CVE-2015-4644 20 Exec Code 2015-08-14 2019-05-19 None Remote Medium Not required Complete Complete Complete

Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT Gold and R1; Office 2007 SP3 and 2010 SP2; Live Meeting 2007 Console; Lync 2010; Lync 2013 Attendee; Lync 2013 SP1; Lync Basic 2013 SP1; Silverlight before 5.1.40728; and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka "TrueType Font Parsing Vulnerability," a different vulnerability than CVE-2015-2453.

Cve Number: CVE-2015-4642 20 Exec Code 2015-08-14 2019-05-12 None Remote Medium Not required Complete Complete Complete

Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT Gold and R1; Office 2007 SP3 and 2010 SP2; Live Meeting 2007 Console; Lync 2010; Lync 2013 Attendee; Lync 2013 SP1; Lync Basic 2013 SP1; Silverlight before 5.1.40728; and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted OpenType font, aka "OpenType Font Parsing Vulnerability."

Cve Number: CVE-2015-4660 20 Exec Code 2015-08-14 2019-05-17 None Remote Medium Not required Complete Complete Complete

ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT Gold and R1; and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka "OpenType Font Parsing Vulnerability."

Cve Number: CVE-2015-4656 20 Exec Code 2015-08-14 2019-05-15 None Remote Medium Not required Complete Complete Complete

Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT Gold and R1; Windows 10; and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka "TrueType Font Parsing Vulnerability," a different vulnerability than CVE-2015-2455.

Cve Number: CVE-2015-4655 20 Exec Code 2015-08-14 2019-05-15 None Remote Medium Not required Complete Complete Complete

- نصب آخرین به روز رسانی ها و پچ های امنیتی

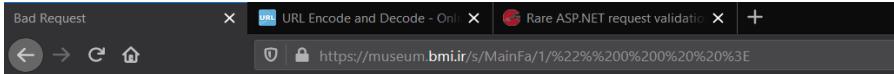
- غیرفعال کردن نمایش بنر سرور در پاسخ ها و صفحات خطای سامانه.

راهکار

Vul-Museum-Website-L-04

شناسه آسیب پذیری

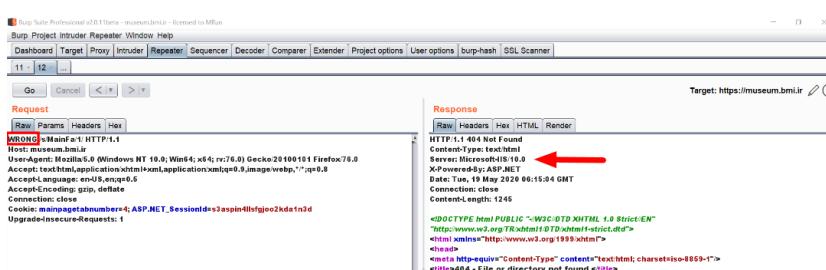


عنوان آسیب پذیری	آسیب پذیری
<p>خطاهای در صفحات وب علاوه بر اینکه نشان دهنده عدم کارکرد صحیح قسمتی از کد می باشد، ممکن است اطلاعات بسیار مهم و حساسی را افشا نماید، در یک صفحه خطای ممکن است، نوع و نسخه سرور، مسیرهای مهم، توابع استفاده شده، قسمتی از کد و ... نشان داده شود و این موضوع کمک بسیار بزرگی به مهاجم برای بررسی دقیقتر سامانه در جهت یافتن آسیب پذیری ها می نماید.</p> <p>همچنین دلیل و چگونگی ایجاد خطای آگاهی زیادی از نحوه کارکرد سامانه به مهاجم می دهد و همین امر باعث ترغیب بیشتر مهاجم برای تلاش در جهت آسیب رساندن به سامانه می گردد.</p> <p>درجه اهمیت این آسیب پذیری وابسته به تاثیر آن در سامانه و میزان اطلاعات نمایش داده شده می باشد.</p>	شرح آسیب پذیری
Low	درجه اهمیت
Web Application	حوزه تاثیر
URL: https://museum.bmi.ir/s/MainFa/1/	سیستم‌های آسیب‌پذیر (IP&URL)
همانطور که در تصویر زیر قابل مشاهده می باشد، با دستکاری URL سامانه، به خطایی در خصوص اشکال در URL برخورد نمودیم:	 <p>Bad Request - Invalid URL</p> <p>HTTP Error 400. The request URL is invalid.</p> <p>همچنین با تغییر ورژن در درخواست HTTP ارسالی به 3.0 با خطای زیر مواجه شدیم:</p>



<p>Version Not Supported</p> <hr/> <p>HTTP Error 505. The HTTP Version in the request is not supported.</p> <p>استفاده از Custom Error Page ها برای خطا های سری 400 و 500 -</p> <p>رفع خطاهای برنامه نویسی از طریق قرار دادن Exception ها در کد های Back-Exception تا در صورت بروز خطا، بر اساس end نوشته شده روند برنامه ادامه یابد.</p> <p style="text-align: right;">راهکار</p>



Vul-Museum-Website-L-05		شناسه آسیب پذیری
عنوان آسیب پذیری	استفاده از نسخه آسیب پذیر 10 IIS	
شرح آسیب پذیری	<p>در صورت استفاده از یک وب سرور خاص، لازم است تا همیشه از آخرين به روز رسانی ها استفاده گردد تا از آسیب پذیری های شناخته شده جلوگیری به عمل آید، توجه نمایید که وجود آسیب پذیری در سامانه حتی با وجود مکانیزم های امنیتی مناسب باز هم بسیار خطر آفرین می باشد، زیرا مهاجم ممکن است با روش خاصی این مکانیزم های امنیتی را دور زده و به سامانه آسیب برساند، لذا رفع کامل آسیب پذیری همیشه بهترین راهکار می باشد.</p> <p>البته باید توجه گردد که در این آسیب پذیری بحث اصلی افشاری نوع و نسخه وب سرور مورد استفاده می باید که باید از مهاجم مخفی بماند.</p>	
درجه اهمیت	Low	
حوزه تاثیر	Web Application	
sistems های آسیب پذیر (IP&URL)	URL: https://museum.bmi.ir/s/MainFa/1/	
روند بررسی	<p>با تغییر متند درخواست از GET به WRONG با خطای مبنی بر وجود نداشتن این صفحه مواجه شدیم که در پاسخ دریافتی از سمت سرور، نوع و نسخه وب سرور به شرح زیر مشخص می باشد:</p> 	



همچنین با بررسی این نسخه در اینترنت یک آسیب پذیری برای این نسخه به شرح زیر یافت گردید.

CVE-2020-0645 Detail

Current Description

A tampering vulnerability exists when Microsoft IIS Server improperly handles malformed request headers, aka 'Microsoft IIS Server Tampering Vulnerability'.

Source: MITRE

[View Analysis Description](#)

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.X Severity and Metrics:



Base Score: 7.5 HIGH

Vector:

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

QUICK INFO

CVE Dictionary Entry:

CVE-2020-0645

NVD Published Date:

03/12/2020

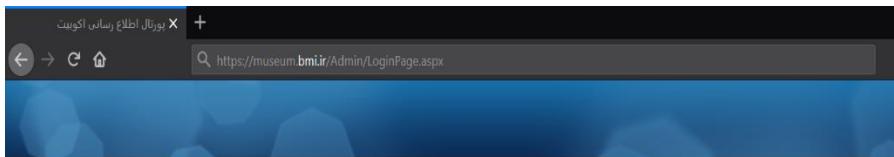
NVD Last Modified:

03/16/2020

- نصب آخرین به روز رسانی ها و پچ های امنیتی
- غیر فعال کردن نمایش نوع و نسخه سرور در پاسخ ها و صفحات خطای سامانه.

راهکار

**Vul-Museum-Website-L-06****شناسه آسیب پذیری**

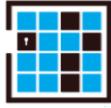
عنوان آسیب پذیری	در دسترس بودن پنل Admin
شرح آسیب پذیری	<p>پنل Admin یکی از مهمترین قسمت های سامانه می باشد که مالک سامانه و مدیران آن می توانند برای ورود به سامانه و ایجاد تغییرات در آن و بررسی داده ها از آن استفاده نمایند. این پنل باید در محلی غیر قبل دسترس و غیر قبل حدس برای مهاجمان قرار گیرد تا از دیدن آنها پنهان بماند، زیرا مهاجم با یافتن صفحه ورودی این پنل مهم، قطعاً اقدام به تلاش های فراوان برای وارد شدن به این بخش از سامانه می نماید، و در صورت ورود به پنل مدیریتی، اختیار کامل سامانه را به دست خواهد گرفت.</p>
درجه اهمیت	Low
حوزه تاثیر	Web Application
سیستم های آسیب پذیر (IP & URL)	<p>URL: https://museum.bmi.ir/Admin/LoginPage.aspx</p> <p>تیم تست نفوذ، در جهت یافتن صفحه ورودی ادمین، در انتهای آدرس سامانه کلمه Admin را اضافه نموده و مشاهده گردید که به آدرس museum.bmi.ir/Admin/LoginPage.aspx ریدایرکت شد. که این آدرس پنل ورودی می باشد.</p>
روند بررسی	
	



- پیشنهاد می گردد صفحه ورودی ادمین به آدرسی غیر قابل حدس زدن برای مهاجمان منتقل گردد و با استفاده از مسیرهای پیشفرض نتوان آن را یافت.

- همانطور که دیده شد با وارد کردن مقدار Admin در انتهای آدرس سامانه، به صفحه ورودی ریدایرکت شدیم، پیشنهاد می گردد، چنین ریدایرکت هایی از سامانه حذف گردد تا مهاجم نتواند به راحتی این صفحه را بیابد.

راهکار



Vul-Museum-Website-L-07		شناسه آسیب پذیری
عنوان آسیب پذیری	فعال بودن متدهای DEBUG	
شرح آسیب پذیری	<p>متدهای HTTP برای برقراری ارتباط با سرور مورد نیاز می باشند، اما از برخی از این متدها به صورت عمومی استفاده نمی گردد و استفاده از این متدها برای محافظت از سامانه غیرفعال می گردد.</p> <p>متدهای Debug یکی از این متدها می باشد که هیچ کاربری نباید اجازه استفاده از این متدها در سامانه داشته باشد، با این متد در سامانه، فرد مهاجم می تواند با سو استفاده از این متد اقدام به ویرایش سامانه نماید.</p>	
درجه اهمیت	Low	
حوزه تاثیر	Web Application	
sistemi های آسیب پذیر (IP&URL)	URL: https://museum.bmi.ir/panorama/master_mus	
روند بررسی	<p>متدهای مختلف بر روی سامانه تست گردید و تمامی متدهای غیر مجاز، غیرفعال بودند، اما در آدرس paorama/master_mus برای این آدرس غیرفعال نبوده و همانطور که قابل مشاهده می باشد، سامانه به ما پاسخ 200 در خصوص استفاده از متد DEBUG را بر میگرداند.</p>	
راهکار	<p>- در صورت عدم ضرورت استفاده از این متد در این بخش از سامانه، نسبت به غیرفعال نمودن این متد در سامانه با اضافه کردن /تغییر مقدار زیر در فایل web.config اقدام نمایید:</p>	



```
<compilation
    debug="false"
/>
```



Vul- Museum-Website-L-08		شناسه آسیب پذیری
HSTS عدم فعال سازی	عنوان آسیب پذیری	
<p>در صورت فعل نبودن این مکانیزم امنیتی در سامانه، فرد مهاجم می تواند حین انتقال یک کاربر از پروتکل HTTP به HTTPS درخواست را به سرقت برد و با پاسخی ساختگی به آن درخواست پاسخ دهد و عملاً یک حمله مرد میانی رخ خواهد داد، این حمله به SSL Stripping attack نیز معروف است. همچنین ممکن است اطلاعاتی نظیر کوکی در ابتدای کار به کاربر اختصاص داده شود و به دلیل وجود ارتباط نا امن اولیه، تمامی اطلاعات توسط مهاجم قابل دسترس و س استفاده خواهد بود.</p>		شرح آسیب پذیری
Low		درجه اهمیت
Web Application		حوزه تاثیر
URL: https://museum.bmi.ir/		sistemi های آسیب پذیر (IP&URL)
<p>اسکنر NetSparker با توجه به بررسی پاسخ های دریافتی از سمت سرور، متوجه این موضوع گردیده که مکانیزم امنیتی HSTS بر روی سامانه فعل نمی باشد.</p> <p>HTTP Strict Transport Security (HSTS) Policy Not Enabled</p> <p>LOW</p> <p>Certainty : [REDACTED] URL : https://museum.bmi.ir/</p> <p>Vulnerability Details Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled. The target website is being served from not only HTTP but also HTTPS and it lacks of HSTS policy implementation. HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTP (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion. When a web application issues HSTS Policy to user agents, conformant user agents behave as follows: Automatically turn any insecure links referencing the web application into secure links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.) If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), show an error message and do not allow the user to access the web application.</p> <p>CLASSIFICATION OWASP 2013 A6 OWASP 2017 A3 CAPEC 217 ISO27001 A14.1.2</p>		روند بررسی
<p>- اضافه کردن سرآیند Strict-Transport-Security به پاسخ سرور. به شکل زیر میتوانید این سرآیند را به پاسخ سرور اضافه نمایید:</p> <p>Strict-Transport-Security:max-age=31536000; includeSubDomains; preload</p>		راهکار



Vul- Museum-Website-L-09		شناسه آسیب پذیری
عنوان آسیب پذیری	عدم استفاده از مکانیزم امنیتی Lockout	
شرح آسیب پذیری	این مکانیزم امنیتی پس از تعداد زیادی تلاش ناموفق برای ورود به اکانت کاربری، اکانت مذکور یا فرد مهاجم را برای مدتی مسدود می نماید تا از حملات حدس پسورد جلوگیری به عمل آید، با توجه به عدم تنظیم این مکانیزم امنیتی فرد مهاجم قادر خواهد بود تا با تست پسورد های مختلف برای یک اکانت کاربری، اقدام به حدس پسورد نماید.	
درجه اهمیت	Low	
حوزه تاثیر	Web Application	
sistems های آسیب پذیر (IP&URL)	URL: https://museum.bmi.ir/Admin/LoginPage.aspx	
روند بررسی	تقریبا 20 تلاش ناموفق برای اکانت کاربری test صورت گرفت و پس از آن مشاهده گردید که نه تنها اکانت مذکور lockout نگردیده است، بلکه متخصص تست نفوذ نیز همچنان قادر به ادامه تست می باشد.	
راهکار	- اعمال محدودیت برای تلاش های ناموفق جهت ورود به پنل مربوطه که با توجه به سیاست های سازمان تنظیم می گردد. (برای مثال، بعد از 3 تلاش ناموفق، اکانت مذکور 15 دقیقه غیرفعال گردد.)	



Vul-Museum-Website-L-010

شناسه آسیب پذیری

عنوان آسیب پذیری	آسیب پذیری نسخه TLS مورد استفاده
شرح آسیب پذیری	<p>آسیب‌پذیری و ضعف پروتکل TLSv1 مدت زیادی است که در بستر اینترنت وجود دارد. در حملات Poodle، مهاجم می‌تواند با سوءاستفاده از ضعف موجود در این پروتکل به ترافیک رمزنشده کاربر دسترسی پیدا کند. به این منظور مهاجم ابتدا ارتباط کاربر را به نحوی تغییر می‌دهد که در آن برای رمزگاری از پروتکل قدیمی TLSv1 استفاده کند؛ این امر با استفاده از این ویژگی انجام می‌گیرد که در صورت بروز خطا در برقراری یک ارتباط رمزگاری شده، کارگزار یا سرویس گیرنده (در اینجا مرورگر وب) سعی در ایجاد ارتباط با یک پروتکل قدیمی می‌کند.</p>
درجه اهمیت	Medium
حوزه تاثیر	Web Application
sistemi hâri آسیب پذیر (IP&URL)	URL: https://museum.bmi.ir
روند بررسی	طبق گزارش ابزار ssl labs که در تصویر زیر قابل مشاهده است، این وبسایت از نسخه‌های ۱.۰ و ۱.۱ پروتکل TLS پشتیبانی می‌کند. لازم به ذکر است که این مسئله به این معنی نیست که از نسخه به روز TLS استفاده نمی‌شود. در حال حاضر نسخه TLS 1.3 نیز بر روی سرور فعال می‌باشد. ولی فعال نگاه داشتن نسخه قدیمی TLS باعث بروز این آسیب‌پذیری گردیده است.



You are here: Home > Projects > SSL Server Test > museum.bmi.ir

SSL Report: museum.bmi.ir (89.235.65.239)

Assessed on: Mon, 18 May 2020 12:21:14 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating: **B**

Category	Score
Certificate	100
Protocol Support	~70
Key Exchange	100
Cipher Strength	100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

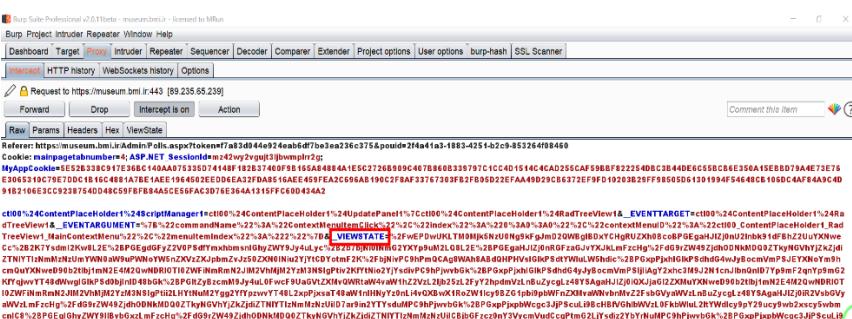
This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO»](#)

- در وب سرور IIS وارد فایل web.config شده و requireSSL="false" را به requireSSL="True" تغییر دهید.

- غیر فعال کردن تمام نسخه های TLS قدیمی تر از 1.2 در وب سرور

راهکار



شناسه آسیب پذیری	
عنوان آسیب پذیری	ارسال ViewState بدون رمزگاری
شرح آسیب پذیری	<p>در این مورد، سورس صفحه به صورت مستقیم به سمت سرور ارسال شده و این موضوع ممکن است برای مهاجم نقطه ای باشد تا با بررسی مقادیر ارسال شده، آنها را دستکاری نموده و نهایتاً به نتیجه ای خاص یا آسیب پذیری دیگری دست پیدا کند.</p> <p>لذا ارسال ViewState به صورت متن واضح (یا کد شده توسط الگوریتم Base64) ایده مناسبی نمی باشد.</p>
درجه اهمیت	Medium
حوزه تاثیر	Web Application
sistemi های آسیب پذیر (IP&URL)	<p>URL: https://museum.bmi.ir/Admin</p> <p>همانطور که قابل ملاحظه می باشد، در قسمتی از سامانه، در درخواست ارسالی به سمت سرور، پارامتری به نام ViewState در حال ارسال می باشد:</p> 
روند بررسی	<p>با بررسی این قطعه در سایت Syberchief URL Decode گردیده و سپس Base64 Decode UTF-8 استاندارد سازی شده تا بتوان متون فارسی داخل آن را نیز مشاهده نمود.</p>



6. توصیه های امنیتی

1.6. اعمال کردن DENSEC

DNSSEC یک تکنولوژی می باشد که برای محافظت در برابر حملات، توسعه پیدا کرده است . با این وجود برای از بین بردن آسیب پذیری های مربوطه، DNSSEC باید در هر مرحله از فرایند تحلیل نام، توسعه پیدا کند. Sign کردن Root Zone یک قدم ضروری در فرایند تحلیل نام می باشد. نکته مهم درباره DNSSEC این است که این تکنولوژی داده ها را رمزگذاری نمی کند و تنها اعتبار آدرس سایت را مورد بررسی قرار می دهد. همان طور که در تصویر زیر مشاهده می شود، عدم وجود DNSSEC در سایت viewdns.info نیز مورد تائید قرار گرفته است.



The screenshot shows the ViewDNS.info interface with the URL <http://viewdns.info/Tools/DNSSEC>. The main content area displays the following text:

```
DNSSEC test result for museum.bmi.ir
=====
✖ This domain DOES NOT have DNSSEC enabled.
```



2.6 حذف سرآیند X-Powered-By از پاسخ سرور

پیشنهاد می‌گردد به منظور پنهان سازی ساختار سامانه و عدم راهنمایی فرد مهاجم برای آسیب رساندن به سامانه، اطلاعات سرور را از دید عموم پنهان سازید.

همانطور که در تصویر زیر مشاهده می‌گردد، این سرآیند در پاسخ سرور وجود دارد.

Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render ViewState
GET /s/MainFa/1 HTTP/1.1 Host: museum.bmi.ir User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Cookie: mainpagetabnumber=4; ASP.NET_SessionId=bqibt4naa2hcbbt3epnbs4wy Upgrade-Insecure-Requests: 1	HTTP/1.1 200 OK Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Content-Type: text/html; charset=utf-8 Expires: Fri, 01 Jan 1990 00:00:00 GMT X-Frame-Options: SAMEORIGIN X-Powered-By: ASP.NET  Date: Sun, 17 May 2020 08:17:49 GMT Connection: close Content-Length: 108604

7. اقدامات انجام شده

7.1. XSS بررسی آسیب پذیری

برای بررسی آسیب پذیری XSS اقدام به تست Payload های مختلفی در پارامترها و مقادیر مختلفی گردید. تقریباً تمامی تلاش ها به عنوان درخواست خطرناک شناسایی گردید و از اجرای آن جلوگیری به عمل آمد.

A potentially dangerous Request.QueryString value was detected from the client (p=%26%233e%3b).

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 (p=%26%233e%).

Source Error:

```
[No relevant source lines]
```

Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\ed2ef2cf\479ce676\App_Web_h2eewm11.0.cs Line: 0

Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was detected from the client (p=%26%233e%).]
System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11969159
System.Web.HttpRequest.ValidateHttpValueCollection(HttpValueCollection collection, RequestValidationSource requestCollection) +200
System.Web.HttpRequest.get_QueryString() +69
System.Web.UI.Page.DeterminePostBackMode() +85
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9458
System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +345
System.Web.UI.Page.ProcessRequest() +75
System.Web.UI.Page.ProcessRequest(HttpContext context) +78
ASP.mainfa_aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\ed2ef2cf\479ce676\App_Web_h2eewm11.0...
System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +790
System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +195
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +88]
```

Version Information: Microsoft .NET Framework Version: 4.0.30319; ASP.NET Version: 4.7.3282.0



2.7 بررسی آسیب پذیری Click Jacking

برای بررسی آسیب پذیری Click Jacking در سامانه، با استفاده از کد زیر، تلاشی برای ایجاد یک از سامانه

گردید:

```
1 <html>
2   <head>
3     <title>Clickjack test page</title>
4   </head>
5   <body>
6     <p>Website is vulnerable to clickjacking!</p>
7     <iframe src="https://museum.bmi.ir/s/MainFa/1/" width="500" height="500"></iframe>
8   </body>
9 </html>
```



که نتیجه آن عدم آسیب پذیری سامانه بود

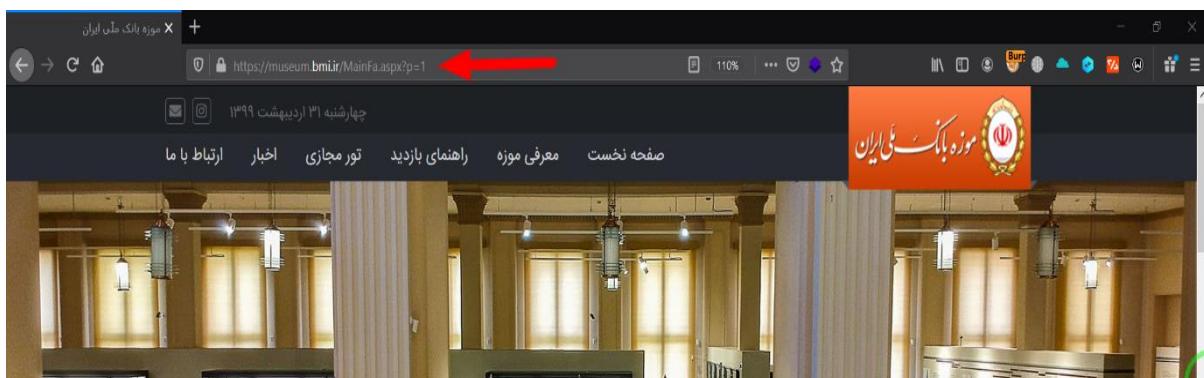
Is website vulnerable to clickjacking?



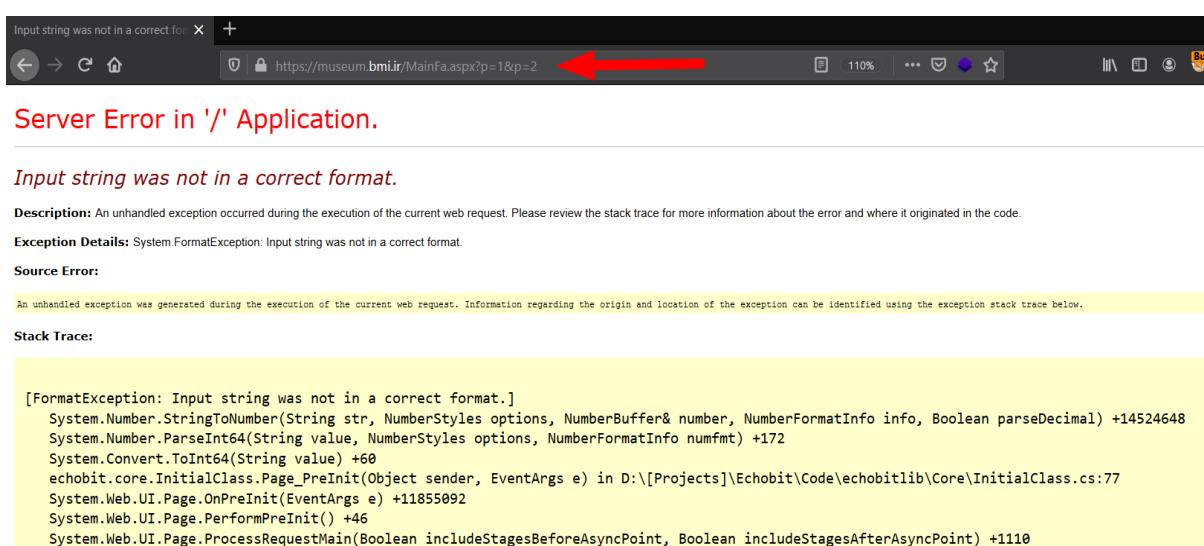
3.7 بررسی آسیب پذیری HPP

برای بررسی آسیب پذیری HPP در سامانه، ابتدا بررسی گردید که چگونه با متغیرها در URL برخورد می شود.

در حالت عادی صفحه به صورت زیر بارگذاری می شود.



سپس با تغییر در URL HPP با خطای زیر مواجه گردیده:



Server Error in '/' Application.

Input string was not in a correct format.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.FormatException: Input string was not in a correct format.

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:

```
[FormatException: Input string was not in a correct format.]  
System.Number.StringToNumber(String str, NumberStyles options, NumberBuffer& number, NumberFormatInfo info, Boolean parseDecimal) +14524648  
System.Number.ParseInt64(String value, NumberStyles options, NumberFormatInfo numfmt) +172  
System.Convert.ToInt64(String value) +60  
echobit.core.InitialClass.Page_PreInit(Object sender, EventArgs e) in D:\[Projects]\Echobit\Code\echobitlib\Core\InitialClass.cs:77  
System.Web.UI.Page.OnPreInit(EventArgs e) +11855092  
System.Web.UI.Page.PerformPreInit() +46  
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1110
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3282.0

با توجه به نتیجه فوق، آسیب پذیری HPP در سامانه وجود ندارد.



4.7 آسیب پذیری، سے، IIS Tilde

سامانه با استفاده از این‌ارا Shortname iis تست گردید و آسیب پذیری در این خصوص شناسایی نشد.

```
root@kali:~/Downloads/IIS-ShortName-Scanner# java -jar iis_shortname_scanner.jar https://museum.bmi.ir/
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=true
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by IISShortNameScanner.IIS_ShortName_Scanner (file:/root/Downloads/IIS-ShortName-Scanner/iis_shortname_scanner.jar)
        to field sun.net.www.protocol.https.HttpsURLConnectionImpl.delegate
WARNING: Please consider reporting this to the maintainers of IISShortNameScanner.IIS_ShortName_Scanner
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
# IIS Short Name (8.3) Scanner version 2.3.9 (05 February 2017) - scan initiated 2020/05/19 03:54:45
Target: https://museum.bmi.ir/
[_] Result: Not vulnerable or no item was found. It was not possible to get proper/different error messages from the server. Check the inputs and try again.
[_] Extra information:
[_] Number of sent requests: 144
```

۵.۷ تلاش برای شناسایی فایروال سامانه

همانطور که مشاهده می شود در جهت شناسایی فایروال مورد استفاده در سامانه از ابزار Wafw00f استفاده گردید و فایروال این سامانه RequestValidationMode (Microsoft) تشخیص داده شد.



6.7. بررسی اسناد و فایل های سامانه در بستر اینترنت با استفاده از ابزار FOCA

سامانه با استفاده از ابزار FOCA برای شناسایی و یافتن اسنادی همچون فایل های اکسل، فایل های متی و... و همچنین یافتن شبکه ها و آی پی های مرتبط با سامانه که در بستر اینترنت قابل دسترسی می باشند (به صورت ناخواسته) مورد پویش قرار گرفته و هیچ فایل و سند مهمی یافت نشد.

The screenshot shows the FOCA Open Source 3.4.7.0 application window. The left sidebar displays a tree view of the target website's structure under the domain 'museum.bmi.ir'. The 'Network' section shows 'Clients (0)', 'Servers (2)' including '89.0.0.0' and 'Unknown Servers', and a link to 'https://museum.bmi.ir'. The 'Domains' section shows 'bmi.ir' with a link to 'https://museum.bmi.ir'. The 'Document Analysis' section is collapsed. The main pane features a red cartoon character logo with the text 'Foca OPEN SOURCE'. To the right of the logo are sections for 'Search engines' (Google, Bing, DuckDuckGo) and 'Extensions' (checkboxes for doc, docx, sxl, sxw, odp, ppt, pps, ppsx, ods, wpd, xls, xlsx, odg, rtf, All, None). Below these are tabs for 'Custom search' and 'Search All'. A large table below lists log entries with columns for Time, Source, Severity, and Message. The log entries are:

Time	Source	Severity	Message
12:10:13...	ShodanSearch	medium	Found IP Information 89.235.64.67
12:10:14...	IPBingSearch	medium	[BingWeb] Found domain bmi.ir in IP 89.235.64.67
12:10:24...	IPBingSearch	medium	BingWeb search finished successfully!!
12:10:24...	ShodanSearch	medium	Shodan search finished successfully!!
12:15:12...	Crawling	medium	Domain found: museum.bmi.ir

At the bottom of the log pane are buttons for 'Settings', 'Deactivate AutoScroll', 'Clear', and 'Save log to File'. A message at the bottom states 'Subdomains search for https://museum.bmi.ir finished'.



7.7 بررسی سامانه با استفاده از ابزار WhatWeb

سامانه با ابزار WhatWeb تست گردیده و نتیجه آن به شرح زیر می باشد:

```
root@kali:~# whatweb -a 3 -v https://museum.bmi.ir/
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
WhatWeb report for https://museum.bmi.ir/
Status   : 302 Found
Title    : Object moved
IP       : 89.235.65.239
Country  : IRAN (ISLAMIC REPUBLIC OF), IR

Summary  : X-Frame-Options[SAMEORIGIN], Cookies[ASP.NET_SessionId], RedirectLocation[/s/MainFa/1/], ASP.NET, X-Powered-By[ASP.NET], HttpOnly[ASP.NET_SessionId]

Detected Plugins:
[ ASP.NET ]
  ASP.NET is a free web framework that enables great Web applications. Used by millions of developers, it runs some of the biggest sites in the world.

  Google Dorks: (2)
  Website      : https://www.asp.net/

[ Cookies ]
  Display the names of cookies in the HTTP headers. The values are not returned to save on space.

  String      : ASP.NET_SessionId

[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More Info: http://en.wikipedia.org/wiki/HTTP_cookie

  String      : ASP.NET_SessionId

[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and 302

  String      : /s/MainFa/1/ (from location)

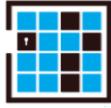
[ X-Frame-Options ]
  This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info: http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx

  String      : SAMEORIGIN

[ X-Powered-By ]
  X-Powered-By HTTP header

  String      : ASP.NET (from x-powered-by string)

HTTP Headers:
  HTTP/1.1 302 Found
  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
  Pragma: no-cache
  Content-Type: text/html; charset=utf-8
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
  Expires: Fri, 01 Jan 1990 00:00:00 GMT
  Location: /s/MainFa/1/
  Set-Cookie: ASP.NET_SessionId=cyt2eh2syxjaqetbqcd3di4b; path=/; secure; HttpOnly
  X-Frame-Options: SAMEORIGIN
  X-Powered-By: ASP.NET
  Date: Tue, 26 May 2020 06:14:32 GMT
  Connection: close
  Content-Length: 129
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
```



```
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
WhatWeb report for https://museum.bmi.ir/s/MainFa/1/
Status   : 200 OK
Title    : موزه بانک ملی ایران
IP      : 89.235.65.239
Country  : IRAN (ISLAMIC REPUBLIC OF), IR

Summary  : X-Frame-Options[SAMEORIGIN], Cookies[ASP.NET_SessionId], Bootstrap[3.3.7], JQuery[3.3.1], ASP.NET, MetaGenerator[EchoBit], Script[text/javascript], X-Powered-By[ASP.NET], Lightbox, Email[info@asmanfaraz.ir,museum@museum.bmi.ir], HttpOnly[ASP.NET_SessionId]

Detected Plugins:
[ ASP.NET ]
  ASP.NET is a free web framework that enables great Web applications. Used by millions of developers, it runs some of the biggest sites in the world.
    Google Dorks: (2)
    Website     : https://www.asp.net/

[ Bootstrap ]
  Bootstrap is an open source toolkit for developing with HTML, CSS, and JS.
    Version     : 3.3.7
    Version     : 3.3.7
    Website     : https://getbootstrap.com/

[ Cookies ]
  Display the names of cookies in the HTTP headers. The values are not returned to save on space.
    String      : ASP.NET_SessionId

[ Email ]
  Extract email addresses. Find valid email address and

[ Lightbox ]
  Javascript for nice image popups

[ MetaGenerator ]
  This plugin identifies meta generator tags and extracts its value.

[ JQuery ]
  A fast, concise, JavaScript that simplifies how to traverse HTML documents, handle events, perform animations, and add AJAX.

[ Bootstrap ]
  Bootstrap is an open source toolkit for developing with HTML, CSS, and JS.
    Version     : 3.3.7
    Version     : 3.3.7
    Website     : https://getbootstrap.com/

[ Cookies ]
  Display the names of cookies in the HTTP headers. The values are not returned to save on space.
    String      : ASP.NET_SessionId

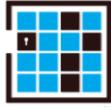
[ Email ]
  Extract email addresses. Find valid email address and

[ Lightbox ]
  Javascript for nice image popups

[ MetaGenerator ]
  This plugin identifies meta generator tags and extracts its value.
```



```
[ value. ]  
[ KaliLinux Share : EchoBit ]  
[ String : EchoBit ]  
[ Script ]  
This plugin detects instances of script HTML elements and  
returns the script language/type.  
[ String : text/javascript ]  
[ X-Frame-Options ]  
This plugin retrieves the X-Frame-Options value from the  
HTTP header. - More Info:  
http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx  
[ String : SAMEORIGIN ]  
[ X-Powered-By ]  
X-Powered-By HTTP header  
[ String : ASP.NET (from x-powered-by string) ]  
HTTP Headers:  
HTTP/1.1 200 OK  
Cache-Control: no-cache, no-store, max-age=0, must-revalidate  
Pragma: no-cache  
Content-Type: text/html; charset=utf-8  
Expires: Fri, 01 Jan 1990 00:00:00 GMT  
Set-Cookie: ASP.NET_SessionId=yyquxauri2qgkbgiofrfxtwb; path=/; secure; HttpOnly  
X-Frame-Options: SAMEORIGIN  
X-Powered-By: ASP.NET  
Date: Tue, 26 May 2020 06:14:34 GMT  
Connection: close  
Content-Length: 107999
```



8.7 اسکن سامانه با ابزار Nmap

سامانه با ابزار nmap هم به صورت کامل و هم به صورت دقیق تر بر روی پورت های مهم صورت گرفت و نهایتاً تنها پورت 443 بر روی سامانه به صورت باز شناسایی گردید.

```
root@kali:~# nmap -Pn -p- -vv 89.235.65.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-26 03:05 EDT
Initiating Parallel DNS resolution of 1 host. at 03:05
Completed Parallel DNS resolution of 1 host. at 03:05, 9.25s elapsed
Initiating SYN Stealth Scan at 03:05
Scanning 89.235.65.239 [65535 ports]
Discovered open port 443/tcp on 89.235.65.239
SYN Stealth Scan Timing: About 5.39% done; ETC: 03:15 (0:09:04 remaining)
SYN Stealth Scan Timing: About 7.64% done; ETC: 03:19 (0:12:18 remaining)
SYN Stealth Scan Timing: About 12.20% done; ETC: 03:20 (0:13:04 remaining)
SYN Stealth Scan Timing: About 13.94% done; ETC: 03:22 (0:14:18 remaining)
SYN Stealth Scan Timing: About 18.32% done; ETC: 03:21 (0:13:13 remaining)
SYN Stealth Scan Timing: About 22.59% done; ETC: 03:21 (0:12:13 remaining)
SYN Stealth Scan Timing: About 27.55% done; ETC: 03:20 (0:10:42 remaining)
SYN Stealth Scan Timing: About 33.56% done; ETC: 03:19 (0:09:03 remaining)
SYN Stealth Scan Timing: About 39.11% done; ETC: 03:18 (0:07:53 remaining)
SYN Stealth Scan Timing: About 43.49% done; ETC: 03:18 (0:07:14 remaining)
SYN Stealth Scan Timing: About 48.93% done; ETC: 03:18 (0:06:26 remaining)
SYN Stealth Scan Timing: About 54.43% done; ETC: 03:17 (0:05:35 remaining)
SYN Stealth Scan Timing: About 62.08% done; ETC: 03:18 (0:04:52 remaining)
SYN Stealth Scan Timing: About 68.75% done; ETC: 03:19 (0:04:13 remaining)
SYN Stealth Scan Timing: About 74.54% done; ETC: 03:18 (0:03:20 remaining)
SYN Stealth Scan Timing: About 79.48% done; ETC: 03:18 (0:02:40 remaining)
SYN Stealth Scan Timing: About 86.25% done; ETC: 03:20 (0:02:01 remaining)
SYN Stealth Scan Timing: About 91.83% done; ETC: 03:20 (0:01:13 remaining)
Completed SYN Stealth Scan at 03:21, 928.39s elapsed (65535 total ports)
Nmap scan report for 89.235.65.239
Host is up, received user-set (0.066s latency).
Scanned at 2020-05-26 03:05:43 EDT for 928s
Not shown: 65534 filtered ports
Reason: 65534 no-responses
PORT      STATE SERVICE REASON
443/tcp    open  https   syn-ack ttl 128
Unknown:0/0
Read data files from: /usr/bin/../share/nmap
```

همچنین با این اسکنر بررسی گردید تا نوع و سیستم عامل وب سرور مشخص گردد که تنها نوع و نسخه مورد استفاده از آن یافت شد و ابزار قادر به شناسایی سیستم عامل نگردید.



```
root@kali:~# nmap -p 443 -sV -o 89.235.65.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-26 03:03 EDT
Nmap scan report for 89.235.65.239
Host is up (0.017s latency).

PORT      STATE SERVICE VERSION
443/tcp    open  ssl/http Microsoft IIS httpd 10.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp_sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT V24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds
```