

مرکز تخصصی  
ای سی  
دانشگاه صنعتی اصفهان



(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

**ارزیابی امنیتی سامانه معاونین توسعه**

**دانشگاه‌های علوم پزشکی کشور**

مربوط به :

شرکت فرادید رایان افزار

(محرمانه)

آبان‌ماه ۱۳۹۸



## مقدمه

این گزارش بنا به درخواست شرکت مهندسی "فرادید رایان افزار" توسط مرکز تخصصی آ‌پا دانشگاه صنعتی اصفهان تهیه شده است. نتایج ارزیابی نشان‌دهنده وجود آسیب‌پذیری با سطح خطر بالا می‌باشد. هدف اصلی این گزارش، اعلام مجموعه آسیب‌پذیری‌های شناسایی شده در سامانه مورد نظر جهت رفع و ارتقاء امنیت می‌باشد. در گزارش ارزیابی امنیتی علاوه بر آسیب‌پذیری برنامه کاربردی تحت وب، به تعدادی از آسیب‌پذیری‌های ماشین سرویس‌دهنده نیز اشاره شده است. آسیب‌پذیری‌های ماشین سرویس‌دهنده صرفاً جنبه آگاهی‌رسانی داشته و در صدور گواهی موثر نیستند.

این ارزیابی با شرایط ذیل انجام شده است:

سامانه تحت ارزیابی	سامانه معاونین توسعه دانشگاه‌های علوم پزشکی کشور
نوع کارگزار وب	IIS/10
فناوری توسعه	DNN v. 09.04.01 (22)
پایگاه داده	Microsoft SQL Server 2017
سیستم‌عامل	Microsoft Windows Server 2016 Standard
نوع ارزیابی	آزمون نفوذپذیری جعبه‌سیاه با سطح دسترسی کاربر
زمان ارزیابی	
شرایط ارزیابی	ارزیابی در محل فیزیکی سرویس‌دهنده انجام شده است.

## ارزیابی سرویس‌دهنده و برنامه‌های کاربردی

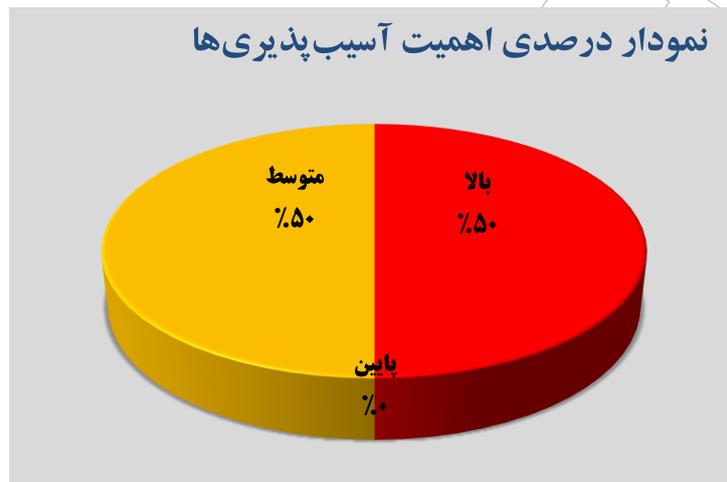
➤ ارزیابی‌ها نشان می‌دهد که پورت‌های زیر بر روی ماشین سرویس‌دهنده باز می‌باشند (صرفاً جهت آگاهی):

ردیف	شماره پورت	سرویس
۱	80/tcp	http
۲	135/tcp	msrpc
۳	139/tcp	smb
۴	445/tcp	cifs

➤ وضعیت آسیب‌پذیری‌های کشف شده عبارتند از:

تعداد	درجه آسیب‌پذیری
۲	بالا
۲	متوسط
۰	پایین

نمودار درصدی اهمیت آسیب‌پذیری‌ها



APARI

بررسی‌های انجام گرفته نشان می‌دهد که در برنامه کاربردی تحت‌وب "سامانه معاونین توسعه دانشگاه‌های علوم پزشکی کشور"، آسیب‌پذیری‌های زیر وجود دارند:

### نام آسیب‌پذیری: کنترل دسترسی نامناسب

#### آدرس‌های آسیب‌پذیر:

- /DesktopModules/Faradid-EntForms/ViewForm.aspx?&sid=....

#### سطح خطر: بالا

**توضیح مختصر:** عدم کنترل دسترسی مناسب به صفحات مختلف وب سایت می‌تواند منجر به افشای اطلاعات محرمانه یک سیستم شود. باید تمامی داده‌ها و صفحات هنگام بارگذاری بررسی شوند که آیا کاربر جاری مجاز به مشاهده این اطلاعات می‌باشد؟ عدم کنترل دسترسی مناسب می‌تواند سیستم را با چالش‌های حفظ حریم خصوصی نیز روبه‌رو کند.

**راه‌حل:** بررسی دسترسی‌ها در هنگام پاسخ به درخواست‌ها.

**اثبات:** در این سامانه صفحه مربوط به چاپ اطلاعات کارت ورود دچار ضعف امنیتی است. با دستکاری پارامترهای موجود در لینک صفحه می‌توان به اطلاعات کارت ورود دیگر کاربران دست یافت.

Name	Domain	Path	Expires	LastAccessed	Value	HttpOnly	SameSite
ASPKANONYMOUS	192.168.20...	/	Sat, 11 Jan 2020 15...	Sat, 09 Nov 2019 05:48:32 GMT	qq7JIZfOJusOxAvMakY2hu77e8uIQ2UyZbXQGEuI5F91aBNIWg_R2by7X8kamZis_RBD...	true	Unset
RequestVerificationToken	192.168.20...	/	Session	Sat, 09 Nov 2019 05:48:32 GMT	ufqDcgZu5ZWQzjpVKIIZTDhUu9FxtNupIB7ISD3Q9wpAgzC9nW_-ULT9FubzADk6E...	true	Unset
ASP.NET_SessionId	192.168.20...	/	Session	Sat, 09 Nov 2019 05:48:32 GMT	dmtk00v05oj4nynbcypdfxou	true	Unset
authentication	192.168.20...	/	Session	Sat, 09 Nov 2019 05:48:32 GMT		true	Unset
dnn_IsMobile	192.168.20...	/	Session	Sat, 09 Nov 2019 05:48:32 GMT	False	true	Unset
FFCurPage	192.168.20...	/	Mon, 09 Nov 2020	Sat, 09 Nov 2019 05:48:32 GMT	1	true	Unset



### نام آسیب‌پذیری: ارسال نام کاربری و رمز عبور به صورت فاش

آدرس آسیب‌پذیر:

- /

سطح خطر: بالا

**توضیح مختصر:** فرم login به صورت رمز نشده از سمت کاربر به سوی سرور فرستاده می‌شود. در نتیجه رمز کاربران به صورت فاش از بستر اینترنت عبور می‌کند و در صورت شنود شبکه رمز کاربران فاش خواهد شد.

**راه‌حل:** استفاده از https به جای http

### نام آسیب‌پذیری: بارگذاری فایل کنترل نشده

آدرس آسیب‌پذیر:

- /API/InternalServices/FileUpload/UploadFromLocal

سطح خطر: متوسط

**توضیح مختصر:** بارگذاری فایل روی کارگزار سامانه می‌تواند باعث شود سامانه با مخاطراتی رو به رو شود. زیرا ممکن است فایل‌های آلوده به بدافزار روی سامانه قرار گیرند. برای کاهش این مخاطرات باید کنترل‌هایی در سمت کلاینت و کارگزار انجام شود. یکی از این کنترل‌ها بررسی نوع فایل می‌باشد.

**راه‌حل:** علاوه بر پسوند فایل‌ها باید سرآیند فایل نیز بررسی شود.



## نام آسیب پذیری: خطای کنترل نشده

### آدرس‌های آسیب پذیر:

- /
- /WebResource.axd
- /ScriptResource.axd
- /desktopmodules/DNNArticleLightboxContentPlugin/Thumbnail.ashx
- /Default.aspx
- /Home/AppointmentRequest/

### سطح خطر: متوسط

توضیح مختصر: طبق ارزیابی انجام شده مشخص گردید، صفحات زیر حاوی پیغام‌های error/warning می‌باشند. این صفحات ممکن است اطلاعات حساسی را فاش نمایند. به‌علاوه این اطلاعات ممکن است محل ذخیره‌ی فایلی که باعث ایجاد استثناء مدیریت نشده است را نیز نشان دهد. این اطلاعات فاش شده می‌تواند به مهاجم برای اجرای موفق حملات بعدی کمک نماید.

راه‌حل: پیشنهاد می‌گردد کد منبع صفحه مربوطه مورد بازبینی قرار گیرد. همچنین صفحه خطا دلخواه برای نمایش به کاربر پیاده‌سازی گردد. استفاده از روش واحد برای handling خطاها که حاوی هیچ‌گونه اطلاعاتی همچون مکان قرارگیری فایلی که خطا در آن رخ داده است نباشد.

### اثبات آسیب پذیری:

تنها برای مدیران قابل نمایش است

```
DotNetNuke.Services.Exceptions.ModuleLoadException: View or function 'dbo.EFV_ConferencesRequest' has more column names specified than columns defined. Could not use view or function 'dbo.EFV_aYce3a9bF4' because of binding errors. --> System.Data.SqlClient.SqlException: View or function 'dbo.EFV_ConferencesRequest' has more column names specified than columns defined. Could not use view or function 'dbo.EFV_aYce3a9bF4' because of binding errors.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady) at System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() at System.Data.SqlClient.SqlDataReader.get_MetaData() at System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption, Boolean shouldCacheForAlwaysEncrypted) at System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyncWrite, Boolean inRetry, SqlDataReader ds, Boolean describeParameterEncryptionRequest) at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean& usedCache, Boolean asyncWrite, Boolean inRetry) at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) at System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) at System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior) at
```