۱-مقدمه

با عنایت به وظایف سازمان ملی استاندارد مبنی بر ارائه خدمات به صورت الکترونیک و با توجه به سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (سند افتا) ، با هدف حفظ و ارتقای امنیت اطلاعات سازمانی در سامانه های تخصصی سازمان، آزمون نفوذ پذیری به عنوان راهکاری موثر در امنیت اطلاعات و یافتن ریسک ها و مخاطرات سازمان و امکان سنجی میزان آمادگی شبکه در برابر حملات انجام گرفته است.

تست نفوذ یا ارزیابی امنیتی روشی است که توسط آن قادر خواهیم بود تا آسیب‌پذیری‌های موجود در نرم‌افزارها، شبکه، وب‌سایت و بانک‌های اطلاعاتی خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت سیستم خود را افزایش دهیم. این روش با استفاده از ارزیابی جنبه‌های مختلف امنیتی کمک می‌کند تا با کاهش دادن ریسک‌های امنیتی موجود، احتمال نفوذ غیرمجاز به شبکه را کاهش دهیم.

هدف از انجام تست نفوذ، یافتن آسیب‌پذیری در یک یا چند مورد از زمینه‌های زیر می‌باشد:

- امنیت تجهیزات فعال شبکه
- امنیت سیستم‌عامل‌ها
- امنیت سرویس‌های شبکه و بانک‌های اطلاعاتی
- امنیت برنامه‌های کاربردی و نرم‌افزارهای تحت شبکه، تحت وب و تحت موبایل

تست نفوذ را می‌توان از دیدگاه‌های متفاوتی بررسی نمود. براساس میزان اطلاعاتی که در اختیار تیم نفوذ است، می‌توان سه دسته White Box، Black Box و Gray Box را در نظر گرفت و از دیدگاه مکان انجام تست نفوذ بهInternal و External تقسیم نمود

رویکرد Black-Box ، Gray-Box و White-Box

تست نفوذ به روش‌های متفاوتی قابل انجام است. بیشترین تفاوت میان این روش‌ها، در میزان اطلاعات مرتبط با جزییات پیاده‌سازی سیستم در حال تست می‌باشد که در اختیار تیم تست نفوذ قرار داده می‌شود. با توجه به این موضوع تست نفوذ را می‌توان به سه دستهBlack-Box ، White – Box و Gray-Box تقسیم نمود.

تست Black-Box با فرض فقدان دانش قبلی از زیر ساختهایی است که قرار است مورد تست قرار گیرند. متخصصان باید پیش از آنالیز و بررسی، ابتدا مکان و گستره سیستم‌ها را بطور دقیق مشخص کنند. تست Black-Box در واقع شبیه‌سازی کردن حمله‌ای است که توسط نفوذگری انجام می‌شود که در ابتدا با سیستم آشنایی ندارد.

از سوی دیگر در تست White-Box اطلاعات ضروری مانند معماری شبکه، کدهای منبع، اطلاعات آدرس IP و شاید حتی دسترسی به بعضی از کلمات عبور،در اختیار تیم ارزیابی امنیتی قرار می‌گیرد. تست White-Box حمله‌ای را شبیه سازی می‌کند که ممکن است در اثر افشای اطلاعات محرمانه از شبکه داخلی یا حضور نفوذگر در داخل سازمان بوجود آید. تست White-Box دارای گستردگی وسیعی می‌باشد و محدوده آن شامل بررسی شبکه محلی تا جستجوی کامل منبع نرم افزارهای کاربردی به منظور کشف آسیب‌پذیری‌هایی که تا کنون از دید برنامه نویسان مخفی مانده است، می‌باشد.

روش های متنوع دیگری نیز وجود دارد که در واقع مابین دو روش ذکر شده در بالا قرار می‌گیرند که معمولا از آنها به تست های Gray-Box تعبیر می‌شود.

تست نفوذ External و Internal

تست External به انواع تست‌هایی اطلاق می‌شود که در خارج از محدوده سازمانی که قرار است مورد تست نفوذ قرار بگیرد، انجام می‌شود و تست‌های Internal در حوزه مکانی آن سازمان و در میان افرادی که آن سازمان فعالیت می‌کنند انجام می‌شود.

نوع اول در واقع سناریویی را بررسی می‌کند که مهاجم با دسترسی داشتن به منابع مورد نیاز خود، از جمله آدرس های IP که از سازمان مورد نظر در اختیار دارد و یا با در اختیار داشتن کد منبع نرم افزارهایی که در سازمان استفاده می‌شوند و در اینترنت موجود می باشند اقدام به پویش و کشف آسیب‌پذیری نماید.

در نوع دوم سناریویی بررسی می‌شود که مهاجم به هر طریق ممکن موفق به ورود به سازمان مورد نظر شده و با جمع آوری داده های مورد نظر اقدام به حمله می‌کند. با ورود به محدوده مکانی یک سازمان مهاجم می تواند سناریوهای مختلفی را پیاده سازی نماید. برای نمونه با استفاده از شبکه بی‌سیم داخلی و بررسی داده‌های به اشتراک گذاشته شده که می تواند اطلاعات کارمندان باشد، حدس زدن کلمات عبور اصلی برای مهاجم ساده‌تر خواهد شد.

۲- اقدامات سازمان ملی استاندارد در راستای بررسی میزان امنیت زیر ساخت ها و سامانه ها

در حال حاضر دریافت گواهینامه امنیتی دارای فرایندی زمان بر و پرهزینه است. که هزینه صدور این گواهینامه از هزینه خرید نرم افزار بسیار بیشتر است. از طرفی جهت اجرای آزمون نفوذ پذیری نیاز است تا بسته کامل سامانه شامل سورس کد نرم افزار، پایگاه داده و دیگر بخش ها به طور کامل در اختیار آزمون گر قرار گیرد تا مورد ارزیابی واقع شود. در صورتی که سیستم های سفارشی مشتری دارای اسناد بالا دستی، شرایط کاری پیچیده، مشکلات و نواقصی است که در زمان طراحی دیده شده، پیوسته در حال تغییر و بهبود است. عدم توجه به جزئیات در زمان طراحی و تولید، منجر به از بین رفتن اعتبار گواهینامه اخذ شده پس از تغییرات خواهد شد.

۲-۱ امنیت سامانه های تخصصی

تست نفوذ به صورت دوره ای از تمامی سامانه های تخصصی توسط کارشناسان فناوری اطلاعات سازمان انجام می شود. یکی از راهکار های برقراری امنیت متد OWASP [1] است. لیست Owasp top 10 ، آسیب پذیر ترین ریسک های امنیتی احتمالی و مشکلات امنیتی موجود در برنامه های کاربردی تحت وب را مشخص می کند. برخی از آسیب پذیری ها به شرح زیر است:

[1] Open Web Application Security Protocol Project

- **تزریق در دیتابیس[۲] (اجرای دستورات مخرب بر روی پایگاه داده)**

این حمله پرخطر ترین حمله ممکن است که هکر می تواند با اضافه کردن کدهایی به دستورات SQL اطلاعات مربوط به کاربران، مشخصات جداول، و داده ها را دستکاری کند و یا استخراج کند. به جهت تشخیص این گونه حمله ها روش های مختلفی وجود دارد. روش مورد استفاده مبتنی بر هوش مصنوعی است. ابتدا یک مدل یادگیر با ناظر ایجاد می شود. برای این کار کوئری ها به دو کلاس مخرب و غیر مخرب طبقه بندی می شود. ابتدا ویژگی های کوئری های مخرب و غیر مخرب استخراج می شود که از ۳۰ ویژگی استفاده می کنیم. سپس از شبکه عصبی مصنوعی MLP برای طبقه بندی کوئری ها به دو کلاس استفاده می شود.

ویژگی هایی استخراج شده از کوئری ها که قابلیت تفکیک پذیری کوئری مخرب از سالم را دارد به شرح زیر است:

۱- تعداد کاراکتر های غیر معمول (پرخطر) مانند : # /* ‘ “ || \\ = /**/ @@ --

۲- تعداد تکرار کاراکتر های منطقی مانند :

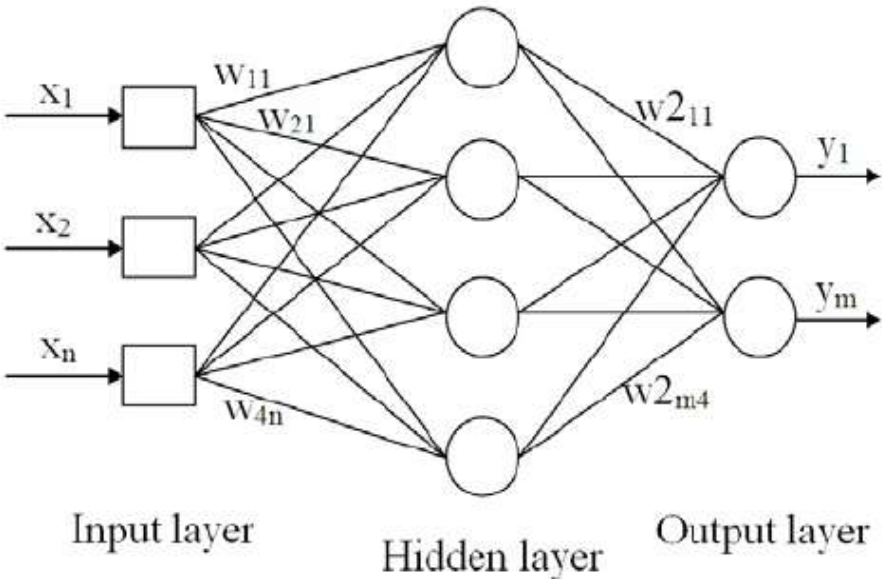
% ! / \ + - % ^ * : ; , _ { } @ ., [ ] ? = == < > != <= >= << >> | &

۳- عبارات پر خطر شناخته شده مانند: 1=1 , @=@ , or 1 , and 1

۴- طول کل کوئری (معمولا طول کوئری سالم کوتاه تر از کوئری مخرب است)

معماری شبکه عصبی نیز به شکل زیر است. تعداد گره های لایه ورودی ۴ می باشد (۴ ویژگی از هر کوئری استخراج شده است). تعداد گره لایه خروجی نیز ۲ می باشد (دو کلاس مخرب و سالم) تعداد لایه مخفی نیز به صورت تجربی ۴ در نظر گرفته می شود.

[2] SQL Injection



به دلیل اهمیت بالای دو سامانه زیر، آزمایشات مربوط به تشخیص تزریق SQL بر روی این دو سامانه انجام گرفته است.

۱- سامانه صدور مجوزهای کالاهای صادراتی و وارداتی

به جهت اهمیت ویژه ای که این سامانه (http://coc.isiri.gov.ir/) از لحاظ تعداد کاربر و دامنه وسیع خدماتی که ارائه می دهد، مانند دریافت اطلاعات از گمرک و ارسال نتایج ارزیابی گمرک به صورت بر خط، ارسال نتایج ارزیابی به ستاد مبارزه با قاچاق کالا و ارز به صورت بر خط بحث امنیت در این سامانه بسیار حائز اهمیت می باشد.

صدور کد استاندارد برای فرآورده های نفتی از جمله اقدامات مهم در این سامانه است که از لحاظ برقراری امنیت اطلاعات اهمیت ویژه ای دارد.

۲- سامانه بازرسی آسانسور (http://lift.isiri.gov.ir)

در زمینه صدور مجوز گواهی ایمنی آسانسور که در سطح ملی عمل می کند. شهرداری ها و ادارات کل استانی در این سامانه فعالیت می کنند. لذا از اهمیت بالایی به جهت امنیت برخوردار است.

پیاده سازی نیز در محیط نرم افزار متلب انجام گرفته است. که در یک باز مشخص زمانی کوئری های مربوط به دو سامانه بازرسی آسانسور و صدور مجوز کالاهای صادراتی و وارداتی انجام گرفته است. که نتیجه حاکی از آن

است عدم مشاهده کوئری مخرب می باشد. لذا می توان گفت که سامانه ها نسبت به حمله تزریق SQL مقاوم می باشند.

دیگر موارد امنیتی که در چاچوب OWASP می گنجد به شرح زیر می باشد.که در این خصوص بررسی ها و آزمون ها به صورت دوره ای برگزار می گردد.

- **شکستن احراز هویت و مدیریت نشست**
- **نکات ایمنی (احراز هویت کاربران سامانه)**
- **تنظیمات امنیتی (سرور)**
- **گزارش خدمات FTP ، DNS و SMTP را در سرور و شناسایی پورت های باز**
- **بررسی بروز رسانی نرم افزار از لحاظ تکنولوژی های طراحی و توسعه نرم افزار**
- **قرار گرفتن اطلاعات در معرض دید**

به طور نمونه در مورد سامانه صدور مجوزهای کالاهای صادراتی و وارداتی تمهیدات امنیتی از جمله کدگذاری اطلاعات در دیتابیس و نیز هنگام انتقال داده ها صورت می گیرد. همچنین در وب سرویسهای دریافت و ارسال اطلاعات احراز هویت توسط آدرس آی پی و نیز توکن صورت می گیرد تا امکان جعل آن به حداقل برسد. همچنین به منظور شناسایی و رفع مشکلات امنیتی این سامانه به صورت دوره ای توسط نرم افزارهای تست نفوذ و تست استرس تحت بررسی قرار گرفته و باگهای آن رفع می گردد. تست نفوذ به صورت دوره ای بر اساس ۳۲ تست استاندارد روی سامانه صورت می گیرد و امتیازات سامانه ها بر اساس استاندارد CVSS ثبت می شود تا میزان خطرپذیری سامانه ها مشخص شود که این مستندات برای سامانه ها موجود می باشد به عنوان مثال تست " عدم ذخیره داده‌های حساس سمت کاربر" که روی یکی از سامانه ها صورت گرفته است به شرح زیر می باشد:

مورد تست ۳: عدم ذخیره داده‌های حساس سمت کاربر[۱]

توصیف
برنامهٔ کاربردی نباید هیچ‌گونه دادهٔ حساسی را در وب اسکریپت‌ها، کوکی‌ها و فیلدهای مخفی[۲] ذخیره کند؛ به دلیل اینکه این اطلاعات برای کاربر قابل رؤیت و تغییر است. به‌عنوان مثال اگر مدیر بودن یا نبودن در سامانه توسط یک پرچم[۳] در کوکی مشخص شود، کاربر می‌تواند با تغییر این مقدار، دسترسی معادل مدیر به سامانه پیدا کند. البته، از آنجا که آزمون‌های مرتبط به کوکی، در مورد تست جداگانه‌ای بررسی می‌شود، از آوردن توضیحات مربوط به کوکی در این مرحله خودداری می‌شود.
وضعیت
Passed
رتبه‌بندی خطر بر اساس CVSS
۰/۰

Access Vector	Access Complexity	Authentication
Local	Medium	Single
Confidentialy Impact	**Integrity Impact**	**Availability Impact**
Partial	Partial	**Partial**

رتبه‌بندی خطر بر اساس OWASP
Low
شواهد اثبات
با وجه به اینکه اطلاعات مهمی در توکن ذخیره نمی شود.

علت

۲-۲ بررسی امنیت در زیر ساخت ها:

از لحاظ زیر ساخت و تجهیزات شبکه سازمان، سخت افزار ها دارای license معتبر بوده و نرم افزار آنتی ویروس نیز به صورت دوره ای به روز رسانی می شود. سیستم امنتی به صورت دولایه بوده و فایروال ها به صورت active- active می باشد که ضریب نفوذ را تا حد زیادی کاهش می دهد.

جمهوری اسلامی ایران
سازمان برنامه و بودجه کشور
امور صنعت، معدن، بازرگانی و ارتباطات

شماره: ۱۶۱۳۱۴۲
تاریخ: ۹۶/۱۰/۱۳

بنام خدا

گواهی موقت تائید و ثبت نرم افزار

نام فارسی: سامانه هوشمند مبادله اطلاعات (سیمانوین)

با استناد به مواد ۲۱ و ۲۲ و ۲۳ قانون "ارتقاء سلامت نظام اداری و مقابله با فساد"، مصوب ۱۳۹۰ مجلس شورای اسلامی، تحت شماره شناسایی زیر بطور موقت تائید و ثبت شد. مشخصات دارندگان حقوق مادی و معنوی (مالکان و پدیدآورندگان) در ظهر این گواهی مندرج است.

۳۰۰۳۹۰

توجه: این گواهی به علت تغییر در شاخص های ارزیابی تا تاریخ ۱۳۹۶/۱۲/۲۸ اعتبار دارد، بدیهی است متقاضی ملزم است بعد از این تاریخ، جهت اخذ مجدد گواهی با معیارهای جدید مصوب، به این امور مراجعه نماید.

حمید امانی همدانی
رئیس امور صنعت، معدن، بازرگانی و ارتباطات

این گواهی سندرسمی دولتی محسوب می شود و هرگونه جعل آن مستوجب پیگرد قانونی است

مشخصات دارندگان حقوق مادی (مالک / مالکان)

شخص حقوقی:

ردیف	نام شرکت	محل ثبت	شماره ثبت
۱	سامانه‌های هوشمند نسل سوم	تهران	۱۹۱۸۷۴

شخص حقیقی:

ردیف	نام و نام خانوادگی	شناسه ملی
۱	احمد مطلبی	۰۰۵۶۴۳۰۴۶۹

مشخصات دارندگان حقوق معنوی (پدیدآورنده / پدیدآورندگان)

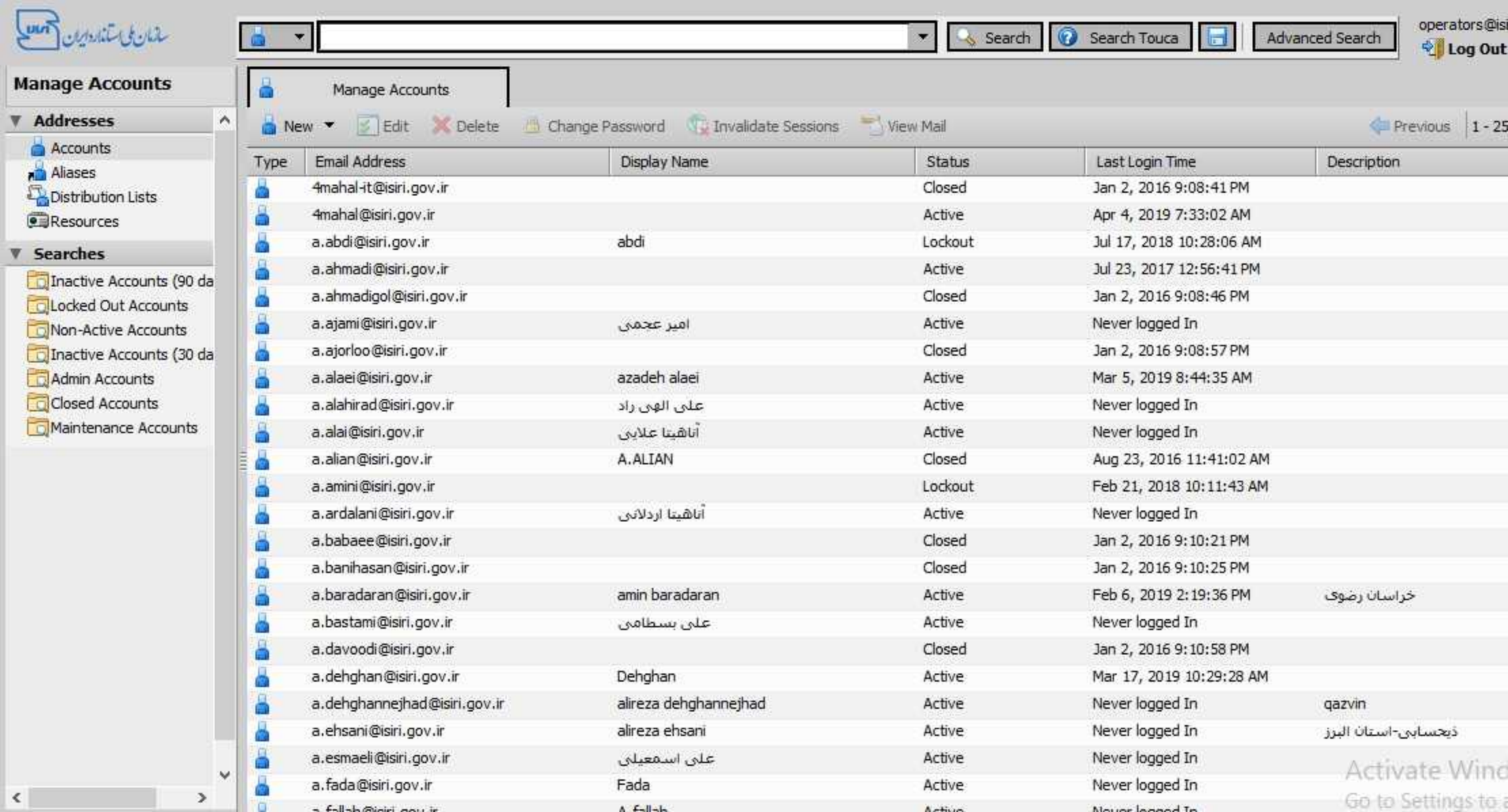
شخص حقوقی:

ردیف	نام شرکت	محل ثبت	شماره ثبت
۱	سامانه‌های هوشمند نسل سوم	تهران	۱۹۱۸۷۴

شخص حقیقی:

ردیف	نام و نام خانوادگی	شناسه ملی
۱	احمد مطلبی	۰۰۵۶۴۳۰۴۶۹

(توجه: اطلاعات مندرج در جداول فوق کاملاً جنبه خوداظهاری داشته و این امور هیچگونه مسئولیتی در این خصوص ندارد.)


Search
Search Touca
Advanced Search
operators@isi
Log Out
Manage Accounts
Addresses
Accounts
Aliases
Distribution Lists
Resources
Searches
Inactive Accounts (90 da
Locked Out Accounts
Non-Active Accounts
Inactive Accounts (30 da
Admin Accounts
Closed Accounts
Maintenance Accounts
Manage Accounts
New
Edit
Delete
Change Password
Invalidate Sessions
View Mail
Previous
1 - 25
Type
Email Address
Display Name
Status
Last Login Time
Description
4mahal-it@isiri.gov.ir
Closed
Jan 2, 2016 9:08:41 PM
4mahal@isiri.gov.ir
Active
Apr 4, 2019 7:33:02 AM
a.abdi@isiri.gov.ir
abdi
Lockout
Jul 17, 2018 10:28:06 AM
a.ahmadi@isiri.gov.ir
Active
Jul 23, 2017 12:56:41 PM
a.ahmadigol@isiri.gov.ir
Closed
Jan 2, 2016 9:08:46 PM
a.ajami@isiri.gov.ir
امیر عجمی
Active
Never logged In
a.ajorloo@isiri.gov.ir
Closed
Jan 2, 2016 9:08:57 PM
a.alaei@isiri.gov.ir
azadeh alaei
Active
Mar 5, 2019 8:44:35 AM
a.alahirad@isiri.gov.ir
علی الهی راد
Active
Never logged In
a.alai@isiri.gov.ir
آناهیتا علایی
Active
Never logged In
a.alian@isiri.gov.ir
A.ALIAN
Closed
Aug 23, 2016 11:41:02 AM
a.amini@isiri.gov.ir
Lockout
Feb 21, 2018 10:11:43 AM
a.ardalani@isiri.gov.ir
آناهیتا اردلانی
Active
Never logged In
a.babaee@isiri.gov.ir
Closed
Jan 2, 2016 9:10:21 PM
a.banihasan@isiri.gov.ir
Closed
Jan 2, 2016 9:10:25 PM
a.baradaran@isiri.gov.ir
amin baradaran
Active
Feb 6, 2019 2:19:36 PM
خراسان رضوی
a.bastami@isiri.gov.ir
علی بسطامی
Active
Never logged In
a.davoodi@isiri.gov.ir
Closed
Jan 2, 2016 9:10:58 PM
a.dehghan@isiri.gov.ir
Dehghan
Active
Mar 17, 2019 10:29:28 AM
a.dehghannejhad@isiri.gov.ir
alireza dehghannejhad
Active
Never logged In
qazvin
a.ehsani@isiri.gov.ir
alireza ehsani
Active
Never logged In
ذیحسابی-استان البرز
a.esmaeli@isiri.gov.ir
علی اسمعیلی
Active
Never logged In
a.fada@isiri.gov.ir
Fada
Active
Never logged In
Activate Wind
Go to Settings to a

شماره: ۶۳۹۵/۹۸/۴۰/۲۳۲

تاریخ: ۱۳۹۸/۲/۱۶

پیوست:

عادی

فاقد طبقه بندی

از : شرکت صنایع امنیت فضای تبادل اطلاعات صاایران

به : مدیر عامل محترم شرکت رایان نظم

موضوع : نتیجه آزمون نفوذپذیری سامانه یکپارچه توازن

دستاورد تولید

((شرکت صاافتا مرجع و پیشرو در صنایع امنیت با رویکرد ایجاد امنیت شناور و یکپارچه در راستای تحقق نیاز مشتری))

سلام علیکم

با صلوات بر محمد و آل محمد(ص) و با احترام،

به آگاهی می‌رساند سامانه یکپارچه توازن محصول شرکت رایان نظم مطابق روش آزمون مدلسازی تهدیدات و آزمون نفوذپذیری و به شماره آزمون RAYAN NAZM-AFTA-TAVAZON-01 توسط مرکز ارزیابی ایمنی و امنیتی این شرکت، مورد ارزیابی قرار گرفت و در زمان اجرای آزمون، آسیب‌پذیری مشاهده نگردید.

*** با توجه به اینکه در این آزمون الزامات امنیتی ستاد کل ن.م مورد بررسی قرار نگرفته است، این گزارش شامل تایید سطوح امنیتی ستاد کل ن.م نمی‌باشد.**

*** این گواهی مربوط به برنامه کاربردی بوده و ملاحظات امنیتی بستر و زیرساخت، شامل امنیت سیستم‌عامل، امنیت کلیه سرویس‌ها از جمله سرویس‌دهنده وب، الزامات کانال ارتباطی امن (SSL/TLS) و تنظیمات نامناسب امنیتی را شامل نمی‌گردد. بدیهی است اعمال کلیه پیکربندی‌های امن مربوط به محصول، بستر و زیرساخت بر عهده بهره‌بردار است.**

*** آزمون بر روی وب سایت با معادل درهم‌سازی شده ذیل انجام پذیرفته و هرگونه تغییر در سامانه فوق از شمول این گزارش خارج است.**

MD5 (RayanNazm.rar): 7e10c755fbe859edc8e4ddc40b1981b4

سرپرست شرکت صنایع امنیت فضای تبادل اطلاعات صاایران

کیانوش آزادی

تهران -میدان دوبنیاد - خیابان شهید لنگری - خیابان شهید تیموری
تلفن: ۲۲۹۸۲-۴۲۹۳۴۰۳۶ دورنگار: ۲۲۹۳۵۰۴۵
info@saafta.ir www.saafta.ir