بسمه تعالی

شرح توان مندی‌ها در حوزه‌ی آزمون نفوذپذیری

شرکت داده پردازان آبشار

نسخه‌ی عمومی

تاریخچه‌ی سند

نسخه	تاریخ	تهیه‌کنندگان	مرورکنندگان	طبقه‌بندی	توضیحات
۱,۰	سه‌شنبه/۱۳۹۲/۰۵/۱۵	مهران طریحی	علی مجدزاده کوهبنانی	عمومی	ایجاد سند

این صفحه به‌عمد خالی گذاشته شده است.

فهرست مطالب

۰) مقدمه

شرکت داده پردازان آبشار پیشرو در ارائه‌ی خدمات ارزیابی آسیب‌پذیری[۱] و آزمون نفوذپذیری[۲] در حوزه‌های شبکه، برنامه‌های کاربردی مبتنی بر میزکاری[۳]، برنامه‌های کاربردی وب[۴] و همچنین آزمون‌های نفوذپذیری فیزیکی و مهندسی اجتماعی، بر اساس استانداردهای بین‌المللی است. گروه‌بندی خدمات به شرح زیر است:

۱. آزمون نفوذپذیری شبکه؛
۲. آزمون نفوذپذیری برنامه‌های مبتنی بر میزکاری؛
۳. آزمون نفوذپذیری برنامه‌های کاربردی وب؛
۴. آزمون نفوذپذیری فیزیکی و مهندسی اجتماعی[۵]؛

پس از تشریح هر یک از انواع خدمات آزمون نفوذپذیری، فهرستی از سوابق کاری مرتبط در این حوزه نیز در ادامه‌ی مستند اراده شده است.

۱) آزمون نفوذپذیری شبکه

آزمون نفوذپذیری شبکه به منظور کشف آسیب‌پذیری‌ها، سوء استفاده و نفوذ به تجهیزات فعال شبکه شامل سوییچ‌ها و مسیریاب‌ها، تجهیزات امنیتی شامل دیواره‌ی آتش[۶]، سامانه‌ی تشخیص و جلوگیری از نفوذ[۷] و ...، و همچنین سرورها و میزبان‌های شبکه صورت می‌گیرد. این آزمون از طریق بستر شبکه‌های عمومی مانند اینترنت، شبکه‌های اختصاصی و همچنین شبکه‌ی داخلی سازمان می‌تواند انجام شود. علاوه بر این، رویکرد آزمون می‌تواند مبتنی بر موارد زیر باشد:

- بدون داشتن اطلاعات (جعبه سیاه)[۸]؛
- با دارا بودن بخشی از اطلاعات (جعبه خاکستری)[۹]؛
- با دارا بودن اطلاعات کامل از شبکه (جعبه سفید)[۱۰]؛

۱-۱) روش‌شناسی آزمون نفوذپذیری شبکه

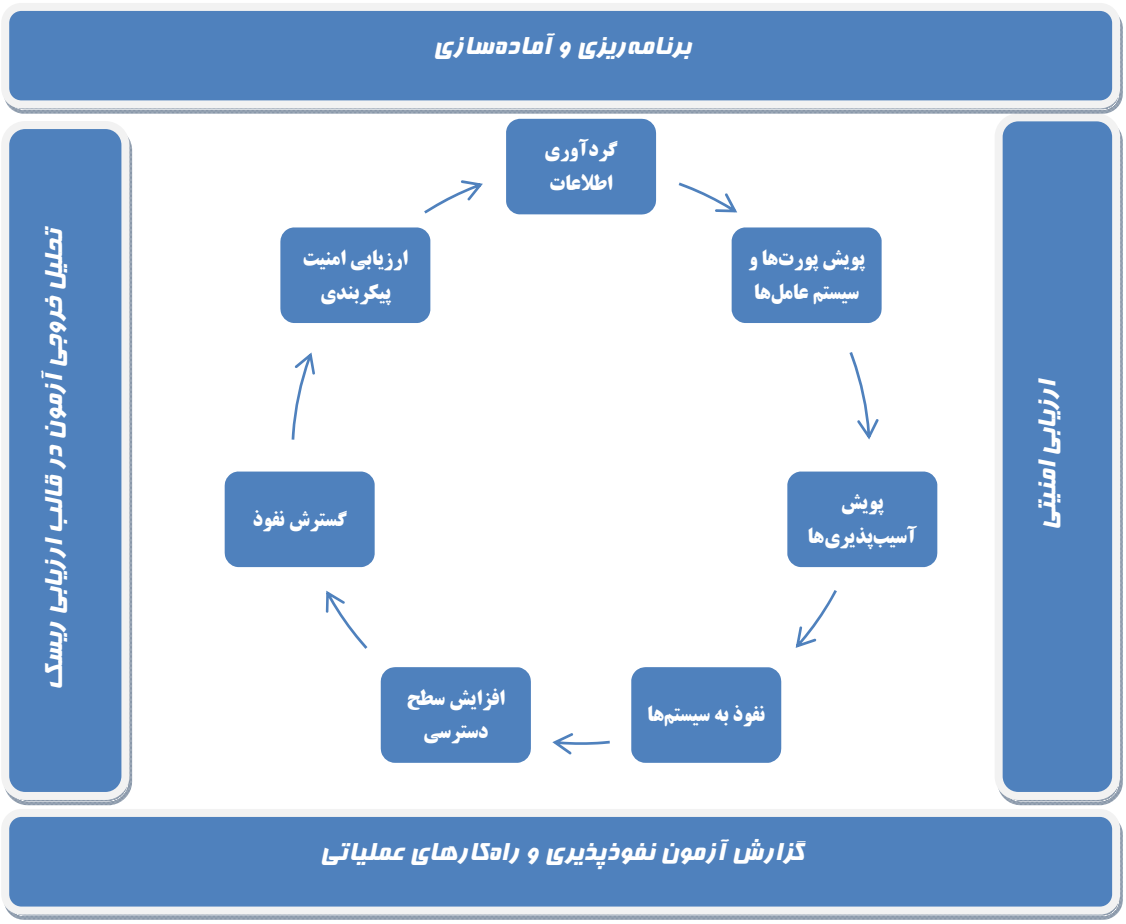
روش‌شناسی[۱] مورد استفاده در آزمون نفوذپذیری شبکه، روش‌شناسی سفارشی‌شده‌ی[۲] شرکت داده پردازان آبشار است که بیشتر مبتنی بر روش‌شناسی ISSAF[۳] است. روش‌شناسی آزمون نفوذپذیری شرکت آبشار مشتمل بر چهار فاز و هفت گام ارزیابی است. فازهای آزمون عبارتند از:

---

[1] Vulnerability Assessment
[2] Penetration Testing
[3] Desktop
[4] Web Application
[5] Social Engineering
[6] Firewall
[7] Intrusion Detection & Prevention System
[8] Black Box
[9] Grey Box
[10] White Box

۱. برنامه‌ریزی و آماده‌سازی
۲. ارزیابی امنیتی
۳. گزارش آزمون نفوذپذیری و ارائه‌ی راه‌کارهای عملیاتی
۴. تحلیل خروجی آزمون در قالب ارزیابی ریسک

شکل زیر روش‌شناسی آزمون نفوذپذیری را نمایش می‌دهد.



شکل ۱ روش‌شناسی آزمون نفوذپذیری شبکه

[1] Methodology
[2] Customized
[3] Information Systems Security Assessment Framework

۱-۱-۱) فاز اول - برنامه‌ریزی و آماده سازی

این فاز دربردارنده‌ی اقدامات اولیه به منظور انجام آزمون نفوذپذیری است و مهم‌ترین بخش آن انعقاد قرارداد آزمون نفوذپذیری و مشخص کردن محدوده‌ی پروژه و همچنین نوع انجام آزمون می‌باشد. فعالیت‌هایی که در این فاز انجام می‌پذیرد عبارتند از:

- مشخص کردن نفرات تماس از هر یک از دو تیم آزمون‌گر و سازمان؛
- برگزاری جلسات مربوط به شناسایی محدوده‌ی پروژه و نحوه‌ی انجام آزمون؛
- موافقت در رابطه با موارد آزمون و مفاد قرارداد؛
- آماده‌سازی تیم‌پروژه، برنامه‌ریزی زمانی و مدیریت پروژه؛

۱-۱-۲) فاز دوم – ارزیابی امنیتی

این فاز دربردارنده‌ی گام‌هایی است که به طور عملی، انجام آزمون نفوذپذیری را دربر دارد. این گام‌ها به صورت مدل لایه‌ای در نظر گرفته شده‌اند و با پیشرفت در هر گام، سطح دسترسی نیز به همان نسبت افزایش می‌یابد. گام‌های این فاز عبارتند از:

۱. گرد آوری اطلاعات
۲. پویش پورت‌ها و سیستم‌عامل‌ها
۳. پویش آسیب‌پذیری‌ها
۴. نفوذ به سیستم‌ها
۵. افزایش سطح دسترسی
۶. گسترش نفوذ
۷. ارزیابی امنیت پیکربندی

در ادامه هر یک از گام‌های فاز ارزیابی امنیتی تشریح می‌شوند.

گردآوری اطلاعات

گردآوری اطلاعات یکی از اساسی‌ترین گام‌ها در راستای انجام آزمون نفوذپذیری است. بدست آوردن اطلاعات در این گام ممکن است هم به شکل فنی و هم به شکل غیر فنی انجام شود. با توجه به اینکه نوع آزمون جعبه سفید یا جعبه سیاه در نظر گرفته شود ممکن است نیاز به کسب اطلاعاتی از سمت سازمان انجام شود که این اطلاعات ممکن است با استفاده از مطالعه‌ی مستندات، مصاحبه و یا از طرق دیگر کسب شود. در هر حال بخش دیگری از فرآیند گردآوری اطلاعات به صورت فنی و با استفاده از روش‌ها و ابزارهای مناسب حاصل خواهد شد. در صورتی که آزمون نفوذپذیری از روی شبکه‌ی اینترنت انجام شود امکان استفاده از منابع اطلاعاتی موجود در اینترنت (مانند گوگل) نیز میسر بوده و در این گام مورد استفاده قرار خواهد گرفت.

پویش پورت‌ها و سیستم‌عامل‌ها

پس از انجام گام اول و گردآوری اطلاعات اولیه، در این گام، تمامی اطلاعات مورد نیاز در رابطه با اهداف بدست خواهند آمد. این گام از یک رهیافت کاملاً فنی تبعیت کرده و هدف آن شناخت وضعیت کاملی از شبکه‌ی هدف می‌باشد. بسیاری از ابزارها و برنامه‌های

سودمند در این گام مورد استفاده قرار خواهند گرفت تا بتوانند اطلاعات فنی مورد نیاز را از سیستم‌های هدف جمع‌آوری نمایند. فعالیت‌هایی که در این گام انجام می‌شوند عبارتند از:

- مشخص‌کردن میزبان‌های زنده؛
- پویش پورت‌ها و سرویس‌ها؛
- نگاشت شبکه ؛
- مشخص کردن سرویس‌های حیاتی؛
- شناسایی سیستم‌عامل‌ها؛

این گام، نقاط ضعیف و قابل دسترسی در شبکه را شناسایی کرده و تأثیر زیادی در طرح حمله خواهد داشت.

پویش آسیب‌پذیری‌ها

در این گام فعالیت‌هایی انجام می‌پذیرد که زمینه را برای نفوذ به اهداف فراهم می‌کند. این فعالیت‌ها عبارتند از:

- شناسایی سرویس‌های آسیب‌پذیر با استفاده از کشف نسخه و اطلاعات مربوط به سرویس و پیام‌ها؛
- پویش آسیب‌پذیری‌ها به منظور کشف آسیب‌پذیری‌ها و نقاط ضعف؛
- تحلیل نتایج پویش آسیب‌پذیری و انطباق با اطلاعات بدست آمده از گام‌ها قبلی؛
- بررسی و دسته‌بندی آسیب‌پذیری‌های بدست آمده؛
- شناسایی مسیرهای حمله و سناریوی‌های نفوذ؛

نفوذ به سیستم‌ها

در این گام با توجه به اطلاعات بدست آمده از گام‌های قبلی اقدام به نفوذ به سیستم‌ها خواهد شد و سعی بر آن خواهد بود که بیشترین سطح دسترسی فراهم شود. مجموعه‌ای از کدها و اکسپلویت‌های عمومی و اختصاصی در این گام مورد استفاده قرار خواهند گرفت. اطلاعاتی که در این قسمت بدست خواهد آمد سابقه‌نگاری خواهد شد و در فاز تهیه‌ی گزارش مورد استناد قرار خواهد گرفت.

افزایش سطح دسترسی

چنانچه به هر دلیل سطح دسترسی پس از نفوذ به سیستم محدود باشد در این گام تلاش خواهد شد تا با افزایش سطح دسترسی به کلیه‌ی منابع سیستم دسترسی پیدا کرده و تمهیدات امنیتی محدودکننده‌ی کاربر از بین بروند. هدف از انجام این گام ایجاد دسترسی در سطح مدیر سیستم است.

گسترش نفوذ

پس از نفوذ به سیستم‌ها و بررسی اطلاعات بدست آمده از آنها، طرح‌های حمله گسترش داده شده و با استفاده از سیستم‌های تحت نفوذ این امکان وجود خواهد داشت که دیگر سیستم‌ها نیز مورد حمله قرار گیرند. از این‌رو با تحلیل اطلاعات بدست آمده از

سیستم‌های قربانی و با استفاده از آنها، دامنه‌ی حمله، گسترده شده و بقیه‌ی سیستم‌ها نیز در صورت امکان مورد نفوذ قرار خواهند گرفت.

ارزیابی امنیت پیکربندی

این گام که معمولاً در انتهای گام‌های اصلی ارزیابی امنیتی انجام می‌شود رویکردی مبتنی بر جعبه سفید داشته و با همکاری و تعامل سازمان کلیه‌ی پیکربندی‌های مربوط به تجهیزات شبکه و سرویس‌ها (در صورت موجود بودن در محدوده‌ی پروژه) مورد بازبینی امنیتی قرار گرفته و ضعف پیکربندی در آنها به همراه گزارش راه‌کارهای عملیاتی ارائه می‌شود. ذکر این نکته حائز اهمیت است که بسیاری از این ضعف‌های پیکربندی در فرآیند آزمون نفوذپذیری کشف نشده و غیر قابل دسترسی خواهد بود ولیکن امکان سوءاستفاده از آنها توسط نفوذگران در شرایط مختلف محتمل خواهد بود به عنوان مثال در صورت دسترسی فیزیکی به تجهیزات یا غیره.

۱-۱-۳) فاز سوم - گزارش آزمون نفوذپذیری و ارائه‌ی راه‌کارهای عملیاتی

هدف از انجام این فاز تهیه‌ی گزارش آزمون نفوذپذیری و همچنین راه‌کارهای عملیاتی، در رابطه با امن‌سازی ضعف‌ها و آسیب‌پذیری‌های بدست آمده از نتایج آزمون نفوذپذیری است. گزارش آزمون نفوذپذیری مشتمل بر موارد زیر است:

- مقدمه – شامل خلاصه‌ی مدیریتی و محدوده‌ی پروژه؛
- روش‌شناسی آزمون – شامل توصیف و شرح روش‌شناسی آزمون نفوذپذیری؛
- پویش پورت‌ها و سرویس‌ها - دربردارنده‌ی نتایج حاصل از پویش پورت‌ها و سرویس‌ها؛
- پویش آسیب پذیری‌ها – دربردارنده‌ی نتایج حاصل از پویش آسیب‌پذیری‌ها؛
- نفوذها – شامل چندین نمونه از نفوذهای انجام شده توسط تیم آزمون‌گر به عنوان اثبات مفاهیم و آسیب‌پذیری‌ها؛

در گزارش راه‌کارهای عملیاتی، کلیه‌ی اقداماتی که جهت امن‌سازی ضعف‌ها و آسیب‌پذیری‌ها بدست آمده که در گزارش آزمون نفوذپذیری تشریح شده‌اند، بیان می‌شوند. همچنین، در صورتی که ارزیابی امنیت پیکربندی نیز به عنوان گام هفتم از فاز ارزیابی امنیتی انجام شده باشد، اقدامات لازم جهت امن‌سازی پیکربندی تجهیزات و سرویس‌ها نیز در گزارش راه‌کارهای عملیاتی تشریح خواهد شد.

۱-۱-۴) فاز چهارم – تحلیل خروجی آزمون نفوذپذیری در قالب ارزیابی ریسک

در این فاز نتایج آزمون نفوذپذیری که در فاز دوم بدست آمده و در فاز سوم مستندسازی شده است در قالب مفهوم ارزیابی ریسک به منظور بهره‌مندی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات[1] مورد استفاده قرار خواهد گرفت. ذکر این نکته حائز اهمیت است که استفاده از نتایج آزمون نفوذپذیری در قالب مفاهیم ارزیابی ریسک ارتباط مناسبی میان بخش‌های سیستمی و فنی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات ایجاد می‌کند.

[1] Information Security Management System (ISMS)

۲) آزمون نفوذپذیری برنامه‌های کاربردی مبتنی بر میزکاری

آزمون نفوذپذیری برنامه‌های کاربردی مبتنی بر میزکار در هر دو حالت تک‌کاربره و مبتنی بر شبکه پوشش داده می‌شود. آزمون نفوذپذیری برنامه‌های کاربردی مبتنی بر میزکاری در شرکت داده پردازان آبشار مبتنی بر استاندارد CLASP[1] انجام می‌شود.

۲-۱) روش‌شناسی آزمون نفوذپذیری برنامه‌های کاربردی مبتنی بر میزکاری

مجموعه‌ای از مؤلفه‌های فرآیندی مبتنی بر نقش‌ها و فعالیت‌های موجود در چرخه‌ی تکامل نرم‌افزار که در هسته‌ی خود، دربرگیرنده‌ی روش‌هایی شناخته شده جهت ایجاد امنیت در چرخه‌ی تکامل نرم‌افزار به شکلی ساخت‌یافته، تکرارپذیر و اندازش‌پذیر است.

فرآیند CLASP از طریق پنج دیدگاه کلی ارائه شده است که هر کدام از این دیدگاه‌ها به مجموعه‌ای از فعالیت‌ها تقسیم می‌شوند. هر یک از فعالیت‌ها نیز به نوبه‌ی خود دربرگیرنده‌ی مؤلفه‌های فرآیند می‌باشند. دیدگاه‌ها عبارتند از:

- دیدگاه مفاهیم ـ شناخت چگونگی تعامل مؤلفه‌های فرآیند CLASP و چگونگی اعمال دیدگاه‌های دوم تا پنجم.
- دیدگاه مبتنی‌بر نقش ـ ایجاد نقش‌های مورد نیاز در پروژه‌ی امنیت‌محور مورد نظر و کاربرد آن‌ها در دیدگاه‌های سوم تا پنجم.
- دیدگاه فعالیت‌ـارزیابی ـ ارزیابی فعالیت‌های بیست‌وچهارگانه و امنیت‌محور CLASP در راستای سنجش تناسب آن‌ها برای دیدگاه چهارم.
- دیدگاه فعالیت‌ـپیاده‌سازی ـ اجرای زیرمجموعه‌ای از فعالیت‌های بیست‌وچهارگانه‌ی CLASP که در دیدگاه سوم انتخاب شده‌اند.
- دیدگاه نفوذپذیری ـ یکپارچه‌سازی راه‌حل‌های مربوط‌به انواع مشکلات در دیدگاه‌های سوم و چهارم.

CLASP نفوذپذیری امنیتی را در قالب رخنه‌ای در محیطی نرم‌افزاری تعریف می‌کند که به مهاجم امکان دسترسی ممتاز در متن سامانه‌ی کاربر، بهره‌برداری از عملیات آن، تسلط بر داده‌های موجود در آن و/یا کسب اعتمادی است که در حالت عادی به مهاجم اعطا نمی‌گردد، را فراهم می‌آورد.

نفوذپذیری امنیتی در نرم‌افزار زمانی رخ می‌دهد که هر بخشی از آن امکان نقض خط‌مشی امنیتی مرتبط را فراهم آورد. CLASP اقدام به تعیین یک‌صد و چهار گونه‌ی مشکل می‌نماید که پایه‌ی نفوذپذیری‌های امنیتی در متن برنامه‌ی نرم‌افزار را شکل می‌دهند. هر گونه‌ی مشکل، ترکیبی از مشکلاتی است که با ایجاد شرایط امنیتی خاصی، منجر به ایجاد یک نفوذپذیری در متن برنامه می‌گردد.

[1] Comprehensive Lightweight Application Security Process

۳) آزمون نفوذپذیری برنامه‌های کاربردی وب

با توجه به اهمیت استفاده از بستر اینترنت و توسعه‌ی برنامه‌های کاربردی وب، نیاز به برقراری امنیت این دسته از برنامه‌های کاربردی که مبتنی بر بستر وب می‌باشند، بیش از پیش آشکار است. شمار زیادی از خسارات واره به شرکت‌ها و سازمان‌ها در حوزه‌ی فناوری اطلاعات مبتنی بر همین دسته از حملات است. شرکت داده پردازان آبشار با دارا بودن نیروهای متخصص و کارآمد و استفاده از روش‌ها، ابزارها، فناوری‌ها، دانش به‌روز در این زمینه و همچنین دارا بودن سوابق درخشان، تمامی خدمات مربوط به این حوزه را به شکل مطلوب ارائه می‌نماید.

روش‌شناسی آزمون نفوذپذیری برنامه‌های کاربردی وب مبتنی بر روش‌شناسی OWASP[1] انجام می‌شود که در ادامه به صورت مختصر تشریح می‌شود.

۲-۱) روش‌شناسی آزمون نفوذپذیری برنامه‌های کاربردی وب

آزمون‌های وب آن دسته از آزمون‌هایی را شامل می‌شود که به طور تخصصی مبتنی بر فضای وب بوده و با پروتکل‌ها، فناوری‌ها و نیازمندی‌های این بستر سازگار است. فهرست این آزمون‌ها به صورت مشروح در جدول ۱ ارائه شده است. تعداد این آزمون‌ها ۶۶ عدد بوده که در قالب ده گروه تقسیم‌بندی شده‌اند.

جدول ۱ فهرست مجموعه آزمون‌های OWASP

Information Gathering
OWASP-IG-001 - 4.2.1 Spiders, Robots and Crawlers - N.A.
OWASP-IG-002 - 4.2.2 Search Engine Discovery/Reconnaissance - N.A.
OWASP-IG-003 - 4.2.3 Identify application entry points - N.A.
OWASP-IG-004 - 4.2.4 Testing for Web Application Fingerprint - N.A.
OWASP-IG-005 - 4.2.5 Application Discovery - N.A.
OWASP-IG-006 - 4.2.6 Analysis of Error Codes - Information Disclosure
Configuration Management Testing
OWASP-CM-001 - 4.3.1 SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) - SSL Weakness
OWASP-CM-002 - 4.3.2 DB Listener Testing - DB Listener weak
OWASP-CM-003 - 4.3.3 Infrastructure Configuration Management Testing - Infrastructure Configuration management weakness
OWASP-CM-004 - 4.3.4 Application Configuration Management Testing - Application Configuration management weakness
OWASP-CM-005 - 4.3.5 Testing for File Extensions Handling - File extensions handling
OWASP-CM-006 - 4.3.6 Old, backup and unreferenced files - Old, backup and unreferenced files
OWASP-CM-007 - 4.3.7 Infrastructure and Application Admin Interfaces - Access to Admin interfaces
OWASP-CM-008 - 4.3.8 Testing for HTTP Methods and XST - HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing
OWASP-AT-001 - 4.4.1 Credentials transport over an encrypted channel - Credentials transport over an encrypted channel
OWASP-AT-002 - 4.4.2 Testing for user enumeration - User enumeration
OWASP-AT-003 - 4.4.3 Testing for Guessable (Dictionary) User Account - Guessable user account
OWASP-AT-004 - 4.4.4 Brute Force Testing - Credentials Brute forcing

[1] Open Web Application Security Project

OWASP-AT-005 - 4.4.5 Testing for bypassing authentication schema - Bypassing authentication schema
OWASP-AT-006 - 4.4.6 Testing for vulnerable remember password and pwd reset - Vulnerable remember password, weak pwd reset
OWASP-AT-007 - 4.4.7 Testing for Logout and Browser Cache Management - - Logout function not properly implemented, browser cache weakness
OWASP-AT-008 - 4.4.8 Testing for CAPTCHA - Weak Captcha implementation
OWASP-AT-009 - 4.4.9 Testing Multiple Factors Authentication - Weak Multiple Factors Authentication
OWASP-AT-010 - 4.4.10 Testing for Race Conditions - Race Conditions vulnerability
Session Management
OWASP-SM-001 - 4.5.1 Testing for Session Management Schema - Bypassing Session Management Schema, Weak Session Token
OWASP-SM-002 - 4.5.2 Testing for Cookies attributes - Cookies are set not ‘HTTP Only’, ‘Secure’, and no time validity
OWASP-SM-003 - 4.5.3 Testing for Session Fixation - Session Fixation
OWASP-SM-004 - 4.5.4 Testing for Exposed Session Variables - Exposed sensitive session variables
OWASP-SM-005 - 4.5.5 Testing for CSRF – CSRF
Authorization Testing
OWASP-AZ-001 - 4.6.1 Testing for Path Traversal - Path Traversal
OWASP-AZ-002 - 4.6.2 Testing for bypassing authorization schema - Bypassing authorization schema
OWASP-AZ-003 - 4.6.3 Testing for Privilege Escalation - Privilege Escalation
Business logic testing
OWASP-BL-001 - 4.7 Testing for Business Logic - Bypassable business logic
Data Validation Testing
OWASP-DV-001 - 4.8.1 Testing for Reflected Cross Site Scripting - Reflected XSS
OWASP-DV-002 - 4.8.2 Testing for Stored Cross Site Scripting - Stored XSS
OWASP-DV-003 - 4.8.3 Testing for DOM based Cross Site Scripting - DOM XSS
OWASP-DV-004 - 4.8.4 Testing for Cross Site Flashing - Cross Site Flashing
OWASP-DV-005 - 4.8.5 SQL Injection - SQL Injection
OWASP-DV-006 - 4.8.6 LDAP Injection - LDAP Injection
OWASP-DV-007 - 4.8.7 ORM Injection - ORM Injection
OWASP-DV-008 - 4.8.8 XML Injection - XML Injection
OWASP-DV-009 - 4.8.9 SSI Injection - SSI Injection
OWASP-DV-010 - 4.8.10 XPath Injection - XPath Injection
OWASP-DV-011 - 4.8.11 IMAP/SMTP Injection - IMAP/SMTP Injection
OWASP-DV-012 - 4.8.12 Code Injection - Code Injection
OWASP-DV-013 - 4.8.13 OS Commanding - OS Commanding
OWASP-DV-014 - 4.8.14 Buffer overflow - Buffer overflow
OWASP-DV-015 - 4.8.15 Incubated vulnerability - Incubated vulnerability
OWASP-DV-016 - 4.8.16 Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling
Denial of Service Testing
OWASP-DS-001 - 4.9.1 Testing for SQL Wildcard Attacks - SQL Wildcard vulnerability
OWASP-DS-002 - 4.9.2 Locking Customer Accounts - Locking Customer Accounts
OWASP-DS-003 - 4.9.3 Testing for DoS Buffer Overflows - Buffer Overflows
OWASP-DS-004 - 4.9.4 User Specified Object Allocation - User Specified Object Allocation
OWASP-DS-005 - 4.9.5 User Input as a Loop Counter - User Input as a Loop Counter
OWASP-DS-006 - 4.9.6 Writing User Provided Data to Disk - Writing User Provided Data to Disk

OWASP-DS-007 - 4.9.7 Failure to Release Resources - Failure to Release Resources OWASP-DS-008 - 4.9.8 Storing too Much Data in Session - Storing too Much Data in Session
Web Services Testing
OWASP-WS-001 - 4.10.1 WS Information Gathering - N.A. OWASP-WS-002 - 4.10.2 Testing WSDL - WSDL Weakness OWASP-WS-003 - 4.10.3 XML Structural Testing - Weak XML Structure OWASP-WS-004 - 4.10.4 XML content-level Testing - XML content-level OWASP-WS-005 - 4.10.5 HTTP GET parameters/REST Testing - WS HTTP GET parameters/REST OWASP-WS-006 - 4.10.6 Naughty SOAP attachments - WS Naughty SOAP attachments OWASP-WS-007 - 4.10.7 Replay Testing - WS Replay Testing
Ajax Testing
OWASP-AJ-001 - 4.11.1 AJAX Vulnerabilities - N.A. OWASP-AJ-002 - 4.11.2 AJAX Testing - AJAX weakness

۲-۱-۱) آزمون‌های شناسایی و گردآوری اطلاعات

هدف از این دسته از آزمون‌ها، شناسایی و کشف اطلاعات درباره‌ی اهداف مورد آزمون با استفاده از روش‌های مختلف است. هر چه اطلاعات بیشتری در این فاز بدست بیاید در بخش‌های بعدی مورد استفاده واقع می‌شود. به منظور انجام این دسته از آزمون‌ها از طیف وسیعی از ابزارها و روش‌ها شامل پویش‌گرهای وب، بررسی‌های دستی، استفاده از موتورهای جستجو، بررسی پیغام‌های خطای برنامه و غیره استفاده می‌شود.

۲-۱-۲) آزمون‌های مدیریت پیکربندی

این مجموعه از آزمون‌های به منظور سنجش وضعیت پیکربندی و معماری مورد استفاده قرار می‌گیرد. اطلاعاتی مانند کد برنامه، متدهای HTTP، SSL/TLS و غیره مورد آزمون قرار می‌گیرند. لازم به ذکر است که بخش اعظمی از آزمون‌های این بخش باید به صورت جعبه سفید انجام شوند مانند تحلیل کد برنامه، مدیریت پیکربندی زیرساخت و غیره.

۲-۱-۳) آزمون‌های احراز هویت

این دسته از آزمون‌ها به منظور مشخص کردن نحوه‌ی احراز هویت کاربر/کاربران توسط سایت و همچنین امکان انجام حملاتی مانند پویش کاربران، دور زدن احراز هویت، نام‌های کاربری قابل حدس، مکانیزم‌های احراز هویت و غیره انجام می‌شود.

۲-۱-۴) آزمون‌های مدیریت نشست[1]

این گروه از آزمون‌ها، مدیریت نشست در برنامه‌ی کاربردی وب را بررسی می‌کنند که شامل مواردی مانند طرح مدیریت نشست، ویژگی‌های کوکی‌ها، متغیرهای نشست، امکان اجرای حملات CSRF[2] و غیره می‌باشد.

[1] Session
[2] Cross-Site Request Forgery

۲-۱-۵) آزمون‌های مجوزدهی

این گروه از آزمون‌ها به منظور بررسی مجوزدهی منابع به کاربران و یا سیستم‌ها انجام می‌شود. آزمون مجوزدهی به معنی آگاهی از فرآیند کارکردی مربوطه و استفاده از اطلاعات بدست آمده در جهت از بین بردن و یا دور زدن فرآیند مجوزدهی است. این مجموعه از آزمون‌ها شامل مواردی مانند: پیمایش مسیرها، امکان دور زدن مکانیزم‌های مجوزدهی و امکان افزایش سطح دسترسی است.

۲-۱-۶) آزمون منطق کاری سایت

این دسته از آزمون‌ها، منطق کارکردی سایت و برنامه‌ی کاربردی وب را مورد بررسی قرار می‌دهند. به عنوان مثال در صورتی که منطق کاری برنامه‌ی کاربردی به صورتی طراحی شده باشد که گام‌های ۱، ۲ و ۳ به ترتیب پشت‌سرهم اجرا شوند ولیکن در عمل بعد از گام ۱، فراخوانی گام ۳ انجام شود چه اتفاقی می‌افتد؟ این دسته از آزمون‌ها عموماً حالات غیرمتداول را در منطق برنامه بررسی می‌کنند.

۲-۱-۷) آزمون‌های اعتبارسنجی داده‌ها

این گروه از آزمون‌ها که یکی از متداول‌ترین ضعف‌های امنیتی در برنامه‌های کاربری وب را پوشش می‌دهند به منظور مشخص کردن متغیرها و پارامترهایی است که به صورت مناسب اعتبارسنجی نشده و در نتیجه پتانسیل اجرای حملات گوناگون را بر روی سایت و یا برنامه‌ی کاربردی وب بوجود خواهند آورد. این دسته از آزمون‌ها شامل مواردی هستند مانند: کلیه آزمون‌های مربوط به حملات XSS[1]، کلیه‌ی حالات ممکن برای تزریق[2] شامل SQL, XML, Command و غیره و همچنین سرریزهای بافر[3].

۲-۱-۸) آزمون‌های منع خدمت

هدف از این دسته از آزمون‌ها از کار انداختن سرور و یا سرویس مربوطه با استفاده از مکانیزم‌های وب می‌باشد. لازم به ذکر است که با توجه به ماهیت و نوع خدمات، اجرای این گونه آزمون‌ها نیازمند هماهنگی و اقدامات مقتضی است زیرا امکان قطعی و از کار افتادن سرویس‌ها و خدمات وجود خواهد داشت.

۲-۱-۹) آزمون‌های وب سرویس

این گروه از آزمون‌ها به منظور بررسی وب‌سرویس‌ها در نظر گرفته شده‌اند. هدف از این دسته از آزمون‌ها شناسایی متدها، توابع و سرویس‌های ارائه شده توسط وب‌سرویس و همچنین بررسی امکان ارسال پارامترهای غیرمتعارف به آنها و اجرای حملات بعدی است.

۲-۱-۱۰) آزمون‌های آژاکس[4]

تکنولوژی آژاکس که به منظور ارتقای سطح کیفی برنامه‌های کاربردی با بهره‌گیری از فناوری جاوااسکریپت بدست آمده است همانند برنامه‌های سنتی وب، تمامی آسیب‌پذیری‌های محتمل در فضای وب را به همراه دارد. از جمله اصلی‌ترین این آسیب‌پذیری‌ها، اجرای حملات CSRF است.

[1] Cross-Site Scripting
[2] Injection
[3] Buffer Overflow
[4] AJAX

۴) آزمون نفوذپذیری فیزیکی و مهندسی اجتماعی

آزمون نفوذپذیری فیزیکی و مهندسی اجتماعی یکی از انواع مهم آزمون‌ها می‌باشد که توجه مناسبی به آن نشده و اهمیت و ابعاد گوناگون آن به شکل مناسبی درک نشده است. ضعف و آسیب‌پذیری‌های مربوط به پرسنل و کارکنان در سازمان‌ها یک از شدیدترین آسیب‌پذیری‌ها بوده و حلقه‌ی ضعیف زنجیره‌ی امنیت شناخته شده است. از این رو، ارزیابی و آزمون‌های فیزیکی و همچنین مهندسی اجتماعی بیش از پیش حائز اهمیت است.

در این زمینه، شرکت داده پردازان آبشار با بهره‌گیری از روش‌های نوین مهندسی اجتماعی مثل SEVER[1] و همچنین استفاده از متدها و ابزارهای به‌روز از پیش‌گامان این گونه از آزمون‌های نفوذپذیری است. علاوه بر این، با توجه به مشخصات خاص و ویژگی‌های متمایز این گونه از آزمون‌ها، الزامات و راه‌کارهای مرتبط با فضای فرهنگی و بومی کشور به شکل مناسبی در روش‌شناسی این آزمون‌ها لحاظ گردیده است.

[1] Social Engineering Vulnerability Evaluation and Recommendation (SEVER)