پروپوزال پویش امنیتی و کشف آسیب‌پذیری‌ها در:

سامانه‌های دانشگاه امام صادق (ع)

92.242.196.0/23

77.104.103.0/24 (*.isu.ac.ir)

مهرماه ۱۳۹۷

فهرست مطالب

۱. مقدمه ۱

۱-۱. رویکرد Black-Box، Gray-Box و White-Box ۱

۱-۲. تست نفوذ External و Internal ۲

۲. رویکرد ارزیابی امنیتی و آزمون نفوذ ۳

۲-۱. تست‌های امنیتی بر اساس استاندارد OWASP ASVS 3.0.1 ..... ۳

۳. برآورد زمان و قیمت ۶

۱. مقدمه

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

تست نفوذ را می‌توان از دیدگاه‌های متفاوتی بررسی نمود. بر اساس 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 به Internal و External تقسیم نمود.

۱–۱. 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 دسته Black-Box، White-Box و Gray-Box تقسیم نمود.

تست Black-Box با فرض فقدان دانش قبلی از زیرساخت‌هایی است که قرار است مورد تست قرار گیرند. متخصصان باید پیش از آنالیز و بررسی، ابتدا مکان و گستره سیستم‌ها را به‌طور دقیق مشخص کنند. تست Black-Box درواقع 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 شبیه‌سازی می‌کند که ممکن است در اثر افشای اطلاعات محرمانه از شبکه داخلی یا حضور نفوذگر در داخل سازمان به وجود آید. تست White-Box دارای گستردگی وسیعی می‌باشد و محدوده آن شامل بررسی شبکه محلی تا جستجوی کامل منبع نرم‌افزارهای کاربردی به‌منظور کشف آسیب‌پذیری‌هایی که تاکنون از دید برنامه نویسان مخفی مانده است، می‌باشد.

روش‌های متنوع دیگری نیز وجود دارد که درواقع مابین دو روش ذکرشده در بالا قرار می‌گیرند که معمولاً از آن‌ها به تست‌های Gray-Box تعبیر می‌شود.

۱–۲. 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 در آن سازمان فعالیت می‌کنند انجام می‌شود.

نوع اول درواقع سناریویی را بررسی می‌کند که مهاجم با دسترسی داشتن به منابع موردنیاز خود، ازجمله آدرس‌های IP که از سازمان موردنظر در اختیار دارد و یا با در اختیار داشتن کد منبع نرم‌افزارهایی که در سازمان استفاده می‌شوند و در اینترنت موجود می‌باشند اقدام به پویش و کشف آسیب‌پذیری نماید.

در نوع دوم سناریویی بررسی می‌شود که مهاجم به هر طریق ممکن موفق به ورود به سازمان موردنظر شده و با جمع‌آوری داده‌های موردنظر اقدام به حمله می‌کند. با ورود به محدوده مکانی یک سازمان مهاجم می‌تواند سناریوهای مختلفی را پیاده‌سازی نماید. برای نمونه با استفاده از شبکه بی‌سیم داخلی و بررسی داده‌های به اشتراک گذاشته شده که می‌تواند اطلاعات کارمندان باشد، حدس زدن کلمات عبور اصلی برای مهاجم ساده‌تر خواهد شد.

۲. رویکرد ارزیابی امنیتی و آزمون نفوذ

در حالت کلی، رویکرد تیم آزمون نفوذ، به چهار فاز کلی زیر تقسیم می‌گردد:

شناخت: در این فاز بیشتر فعالیت‌های لازم برای شناخت محیط، اهداف، نیازمندی‌های امنیتی و میزان تلاش لازم برای ارزیابی برنامه و شبکه بسته به سطح دسترسی موجود در هر آزمون، تعیین می‌گردد.

شناسایی آسیب‌پذیری‌ها: در این فاز آسیب‌پذیری‌های امنیتی شناسایی و ارزش‌گذاری می‌گردند.

بهره‌برداری: در این فاز تلاش برای نفوذ به سطوح مختلف برنامه و رسیدن به اهداف تعیین‌شده به‌وسیله آسیب‌پذیری‌های پیداشده، صورت می‌پذیرد.

مستندسازی و ارائه راهکارهای امن‌سازی: در این فاز نتایج مستند شده از فازهای قبل ارائه می‌گردد. همچنین راهکارها به‌منظور رفع آسیب‌پذیری نیز بیان می‌گردند.

۲–۱. تست‌های امنیتی بر اساس استاندارد OWASP ASVS 3.0.1

شناسایی آسیب‌پذیری‌ها مهم‌ترین مرحله در انجام آزمون نفوذ است. در این فاز با توجه به سطح ارزیابی و منابع در دسترس، آزمونگر اقدام به شناسایی آسیب‌پذیری‌ها می‌نماید. این کار اغلب با استفاده از ابزارهای پویشگر خودکار، نیمه‌خودکار و بررسی‌های دستی با رویکردهای متفاوت انجام می‌شود. تست‌های امنیتی با به‌کارگیری متدولوژی‌های مختلف تست نفوذ و بر اساس استاندارد OWASP ASVS 3.0.1[۱] که آخرین نسخه از این استاندارد است و در ماه ژوئن ۲۰۱۶ ارائه‌شده، انجام می‌شود و در لینک زیر قابل دریافت است.

https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

به‌طورکلی این استاندارد، شامل دسته‌های زیر است که بسته به سطح امنیتی موردنظر، جزئیات هر دسته متفاوت خواهد بود.

۱. معماری، طراحی و مدل تهدید

- در سطح اول، اطمینان از اینکه تمامی اجزاء برنامه، شناسایی شده‌اند و برای وجود تمامی آن‌ها دلیلی وجود دارد.
- در سطح دوم، اطمینان از اینکه معماری تعریف شده است و کد ارائه شده، پایبند به معماری است.
- در سطح سوم، اطمینان از اینکه معماری و طراحی، مؤثر و کاربردی باشند.

[۱] OWASP Application Security Verification Standard_3.0.1

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران – خیابان حافظ – ابتدای خیابان رشت – سمت چپ (درب فارابی دانشگاه صنعتی امیرکبیر) – پلاک ۳۵۰ – ساختمان مرکز تحقیقات پردازش‌های فوق سریع – طبقه همکف – مرکز پژوهشی آپا
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۲. نیازمندی‌های وارسی احراز هویت

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده می‌کند:

- هویت دیجیتال ارسال کننده ارتباط را وارسی می‌کند.
- تنها افراد مجاز قادر به تصدیق هویت هستند و اطلاعات محرمانه به‌صورت امن انتقال پیدا خواهند کرد.

۳. نیازمندی‌های وارسی مدیریت نشست

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای مدیریت نشست زیر را برآورده می‌کند:

- نشست‌ها از یکدیگر مستقل هستند و نمی‌توان آن‌ها را حدس زد یا به اشتراک گذاشت.
- نشست‌ها در زمانی که دوره آن‌ها تمام شده و دیگر موردنیاز نیستند، باید باطل شوند.

۴. نیازمندی‌های وارسی کنترل دسترسی

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده کند:

- افرادی که به منابع دسترسی دارند باید دارای مجوز این کار باشند.
- کاربران به‌خوبی به مجموعه‌ای خوش-تعریف از قوانین و سطح دسترسی‌ها مرتبط شده‌اند.
- ابرداده مربوط به قوانین و مجوزها از دست‌کاری محافظت شده است.

۵. نیازمندی‌های وارسی و رسیدگی به ورودی‌های مخرب

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده کند:

- همه ورودی‌ها به‌درستی اعتبارسنجی شده‌اند و برای هدف موردنظر مناسب هستند.
- به داده‌های دریافتی از موجودیت خارجی یا سرویس‌گیرنده‌ها نباید اعتماد کرد.

۶. نیازمندی‌های وارسی رمزنگاری

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده کند:

- دسترسی به کلید، در یک راه امن مدیریت می‌شود.
- یک مولد عدد تصادفی مناسب در زمان نیاز مورد استفاده قرار گرفته است.

۷. نیازمندی‌های وارسی ثبت وقایع و مدیریت خطاها

هدف اصلی مدیریت خطا و ثبت وقایع این است که یک واکنش مناسبی از طرف کاربر، مدیر و یا تیم پاسخ‌گو فراهم آورده شود. وقایع اغلب اطلاعات حساسی است که باید محافظت شوند و در مورد اطلاعاتی که به حریم خصوصی افراد ربط دارد باید با توجه به قانون‌های حفظ حریم خصوصی انجام شود.

۸. نیازمندی‌های وارسی محافظت داده

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای محافظت داده زیر را برآورده کند:

- محرمانگی: یعنی افراد غیرمجاز نباید اطلاعات را مشاهده کنند.
- صحت: داده‌ها نباید توسط افراد غیرمجاز دست‌کاری شوند.
- در دسترس بودن: داده‌ها باید برای افراد مجاز در دسترس باشند.

۹. نیازمندی‌های وارسی امنیت ارتباطات

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده کند:

- داده‌های حساس با پروتکل TLS انتقال داده می‌شوند.
- الگوریتم‌ها و دنباله‌های رمز قوی در همه موارد استفاده می‌شوند.

۱۰. نیازمندی‌های وارسی پیکربندی امن HTTP

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده کند:

- تنظیمات امنیتی برنامه سرویس‌دهنده به‌درستی پیکربندی شده است.
- پاسخ‌های HTTP شامل یک مجموعه کاراکترهای امن می‌شوند.

۱۱. نیازمندی‌های وارسی کنترل‌های مخرب

بررسی دقیق کد برنامه و عملکرد آن به‌طوری‌که بمب‌های منطقی در آن نباشد و همچنین کدهای مخربی در آن وجود نداشته باشد. این مورد بدون دسترسی به کد برنامه نمی‌تواند به‌صورت کامل انجام شود.

۱۲. نیازمندی‌های وارسی منابع و فایل‌ها

اطمینان از اینکه یک برنامه کاربردی وارسی شده، نیازمندی‌های سطح بالای زیر را برآورده کند:

- داده‌های غیرقابل‌اعتماد باید بر همین اساس و در روشی امن به کار گرفته شوند.
- منابع غیرقابل‌اعتماد در خارج از فایل ریشه و با مجوزهای محدود قرار می‌گیرند.

۱۳. پیکربندی

اطمینان از اینکه یک برنامه وارسی شده، موارد زیر را دارا می‌باشد:

- به‌روزرسانی کتابخانه‌ها و پلتفرم‌ها
- در پیکربندی پیش‌فرض خودش، امن است.

موارد دیگری هم شامل برنامه‌های موبایل و وب‌سرویس وجود دارد که در بالا بیان نشده است.

۳. برآورد زمان و قیمت

تست نفوذ سامانه‌های وب:

طبق بررسی اولیه مشخص شده است که این دامنه به‌صورت تقریبی دارای ۲۵ زیر دامنه مختلف در محدوده 77.104.103.0/24 است که باید مورد ارزیابی قرار گیرند. زمان‌بندی پیشنهادی برای تست Black-Box سامانه‌های وب موردنظر (*.isu.ac.ir) که در محدوده 77.104.103.0/24 قرار دارند، به‌صورت زیر می‌باشد:

نوع فعالیت	زمان‌بندی برحسب روز کاری											
	۵	۱۰	۲۰	۳۰	۴۰	۵۰	۶۰	۷۰	۸۰	۹۰	۱۰۰	۱۱۰	۱۲۰
شناخت سیستم													
شناسایی آسیب‌پذیری‌ها و نفوذ													
مستندسازی و ارائه راهکارهای ارتقای امنیت													

برآورد قیمت برای تست Black-Box سامانه‌های موردنظر، به‌صورت زیر می‌باشد:

	برنامه موردنظر	نفر/ساعت	هزینه (میلیون تومان)
۱	شناخت سیستم‌ها، تجزیه و تحلیل معماری سامانه‌های نرم‌افزاری و سرویس‌ها	۷۰	۴,۲
۲	پویش آسیب‌پذیری‌ها و جمع‌آوری شواهد	۹۰۰	۵۴
۳	تجزیه و تحلیل نتایج و آماده‌سازی گزارش و ارائه راهکارهای امن‌سازی	۶۰۰	۳۶
	مجموع		**۹۴,۲**
	سربار دانشگاه (٪۲۰)		**۱۸,۸۴**
	جمع کل		**۱۱۳,۰۴**

تست نفوذ شبکه:

زمان‌بندی برای تست Black-Box و internal شبکه موردنظر با محدوده 92.242.196.0/23 و 77.104.103.0/24، به‌صورت زیر می‌باشد:

نوع فعالیت	زمان‌بندی برحسب روز کاری													
	۵	۱۰	۱۵	۲۰	۲۵	۳۰	۳۵	۴۰	۴۵	۵۰	۵۵	۶۰	۶۵	۷۰
شناخت سیستم														
شناسایی آسیب‌پذیری‌ها و نفوذ														
مستندسازی و ارائه راهکارهای ارتقای امنیت														

برآورد قیمت برای تست Black-Box و internal شبکه موردنظر، به‌صورت زیر می‌باشد:

	برنامه موردنظر	نفر/ساعت	هزینه (میلیون تومان)
۱	شناخت سیستم‌ها، تجزیه و تحلیل معماری سامانه‌های نرم‌افزاری و سرویس‌ها	۶۰	۳,۶
۲	پویش آسیب‌پذیری‌ها و جمع‌آوری شواهد	۲۵۰	۱۵
۳	تجزیه و تحلیل نتایج و آماده‌سازی گزارش و ارائه راهکارهای امن‌سازی	۱۵۰	۹
	مجموع		**۲۷,۶**
	سربار دانشگاه (۲۰٪)		**۵,۵۲**
	جمع کل		**۳۳,۱۲**