راهنمای اجرایی • نسخه ۱٫۰

مستند جامع
آزمون امنیت وب و API

نقشه راه، چک‌لیست و روش کوتاه تست

۳۴ مرحله • ۲۶۳ کنترل شماره‌دار

مستقل از مدل پروژه، نقش‌ها و فناوری

تهیه‌کننده: محمد ارباب بهار علی

09152399231

ASVS 4.0.3 • Secure Coding Practices 2.0.1 • OWASP Top 10:2025

تاریخ تدوین: ۲۰۲۶/۰۹/۰۷

راهنمای استفاده

این سند نسخه تجمیعی و اجرایی چک‌لیست‌ها و رودمپ گفتگو است. کنترل‌های تکراری ادغام و موارد اختصاصی پروژه به قواعد عمومی تبدیل شده‌اند. هیچ نقش، مسیر، ظرفیت یا فناوری مشخصی برای هدف فرض نشده است.

روش خواندن هر آیتم: عنوان کنترل؛ سپس اقدام آزمون و معیار قبولی کوتاه. ابزار و مرجع در ابتدای هر مرحله آمده است.

جدید: کنترل یا جزئیاتی که با دو PDF ارسالی نسبت به فهرست اولیه اضافه شد.

تکمیلی: جزئیات اجرایی افزوده؛ نقل مستقیم بند PDF نیست.

بدون برچسب: کنترل قبلی یا روش اجرایی رودمپ. برچسب‌ها نتیجه آزمون نیستند.

وضعیت نتیجه: آزمون‌نشده، قبول، مردود، نامرتبط با دلیل. نبود دسترسی به کد یا تنظیمات، «بررسی‌نشده» است؛ نه «قبول».

مرجع: V به بخش ASVS 4.0.3 و A به دسته Top 10:2025 اشاره دارد. نگاشت Top 10 موضوعی و تحلیلی است؛ برای هر یافته باید با علت واقعی تطبیق داده شود.

محدوده کامل بودن: این راهنما همه محورهای گفتگو را پوشش می‌دهد؛ جایگزین ثبت تک‌تک الزامات سطح انتخابی ASVS یا ادعای گواهی انطباق نیست. حدود عددی و الزامات دقیق از همان نسخه و سیاست مصوب استخراج شوند.

روش اثبات: پاسخ HTTP را با وضعیت واقعی داده، رفتار مرورگر یا شواهد کد تطبیق بده. هشدار اسکنر، بازتاب ورودی و بنر نسخه به‌تنهایی آسیب‌پذیری قطعی نیستند.

محیط اجرا: آزمون‌ها داخل محدوده مجاز باشند. همزمانی، کمبود فضا، خطای وابستگی، Restore و Smuggling در محیط مناسب و ایزوله اجرا شوند.

ترتیب اجرا و خروجی هر فاز

۱. محدوده و آماده‌سازی: دارایی مجاز، نسخه و ابزار آماده.

۲. شناسایی: دارایی و مسیر واقعی تأییدشده.

۳. زیرساخت و مرورگر: مواجهه عمومی، TLS، تنظیمات و اطلاعات افشاشده.

۴. هویت و مجوز: پوشش تمام جریان‌های ورود، نشست و دسترسی موجود.

۵. ورودی و پردازش: تزریق، Parser، مقصد، فایل و API.

۶. تمامیت و پایداری: منطق، همزمانی، داده، رمزنگاری و شرایط غیرعادی.

۷. بررسی داخلی: کد، دیتابیس، لاگ، وابستگی و استقرار.

۸. جمع‌بندی: Restore، کنترل پوشش، گزارش و بازآزمایی.

خروج از هر فاز: نتیجه، شاهد و موارد باز ثبت شده باشند. یافته دارای اثر فوری، پیش از ادامه آزمون وابسته تعیین تکلیف شود.

بررسی کد و مستندات، هر زمان دسترسی فراهم است، می‌تواند همزمان با آزمون رفتاری پیش برود.

چرخه کوتاه تست

۱. درخواست یا وضعیت سالم را ثبت کن.

۲. هر بار یک عامل مرتبط را تغییر بده.

۳. پاسخ، وضعیت داده و اثر عملی را مقایسه کن.

۴. شاهد را با شناسه کنترل ذخیره کن.

۵. نتیجه را ثبت و بعد از اصلاح دوباره همان آزمون را اجرا کن.

فهرست مراحل

مرحله ۱

محدوده و معیار ارزیابی

SCP: Introduction ؛ASVS: Assessment

ابزار / دسترسی: مستندات و مصاحبه

۱.۱. محدوده آزمون

فهرست دارایی و مجوز را تطبیق بده؛ فقط دارایی تأییدشده وارد آزمون شود.

۱.۲. نسخه و محیط

نسخه، تاریخ و محیط مستقر را ثبت کن؛ شواهد به نسخه مشخص متصل باشند.

۱.۳. سطح ASVS [جدید]

سطح هدف و بندهای قابل‌اعمال را تعیین کن؛ موارد نامرتبط دلیل داشته باشند.

۱.۴. دسترسی‌های آزمون

دسترسی‌های موجود را ثبت کن؛ نداشتن کد یا حساب، قبول تلقی نشود.

۱.۵. شواهد و نتیجه

برای هر کنترل درخواست، پاسخ و نتیجه ثبت کن؛ آزمون قابل‌تکرار باشد.

۱.۶. پاک‌سازی [جدید]

داده و تغییرات آزمایشی را فهرست کن؛ پس از ارزیابی حذف یا برگردانده شوند.

مرحله ۲

آماده‌سازی ابزار

روش اجرایی؛ مرتبط با ASVS: Assessment

ابزار / دسترسی: Burp Pro، Windows 11، Kali، Nmap

۲.۱. پروژه Burp

پروژه مستقل و Scope دقیق بساز؛ درخواست خارج از محدوده اسکن نشود.

۲.۲. مرورگر و HTTPS

ترافیک مرورگر آزمایشی را از Proxy عبور بده؛ درخواست و پاسخ HTTPS دیده شوند.

۲.۳. تفکیک نشست

نشست‌های آزمایشی را جدا کن؛ Cookie یک هویت وارد آزمون هویت دیگر نشود.

۲.۴. ثبت زمان و خروجی

ساعت و محل نگهداری شواهد را کنترل کن؛ رخدادها قابل‌تطبیق و فایل‌ها محافظت‌شده باشند.

۲.۵. کنترل شدت

نرخ درخواست و زمان اجرای اسکن را تنظیم کن؛ محدودیت‌های توافق‌شده رعایت شوند.

مرحله ۳

شناسایی غیرفعال

Top 10: A02؛ SCP: System Configuration

ابزار / دسترسی: Google، Shodan

۳.۱. ایندکس عمومی

صفحات، زیردامنه‌ها و مسیرهای عمومی را جست‌وجو کن؛ خروجی دارایی‌ها ثبت شود.

۳.۲. فایل و اطلاعات حساس

اسناد، Backup، تنظیمات و خطاهای ایندکس‌شده را بررسی کن؛ افشای واقعی با شاهد جدا شود.

۳.۳. سرویس‌های شناخته‌شده

رکورد IP، پورت، بنر و گواهی را بررسی کن؛ زمان مشاهده ثبت شود.

۳.۴. تعلق دارایی

نام و گواهی را با موجودی مجاز تطبیق بده؛ IP مشترک خودکار وارد محدوده نشود.

۳.۵. اعتبار نتیجه

سرنخ قدیمی را برای تأیید فعال علامت بزن؛ نبود نتیجه، نبود آسیب‌پذیری تلقی نشود.

مرحله ۴

شناسایی فعال و نقشه عملکرد

ASVS: V1.1؛ SCP: System Configuration؛ Top 10: A02، A06

ابزار / دسترسی: Nmap، Burp Proxy و Target

۴.۱. پورت و سرویس

پورت‌های محدوده را بررسی و سرویس را شناسایی کن؛ مواجهه عمومی با نیاز مصوب سازگار باشد.

۴.۲. دسترسی مستقیم

مسیرهای مستقیم و واسطه‌دار را مقایسه کن؛ محدودیت امنیتی از مسیر جایگزین دور نخورد.

۴.۳. درخواست‌های پایه

قابلیت‌های در دسترس را مرور کن؛ مسیر، متد، ورودی و قالب پاسخ ثبت شوند.

۴.۴. جریان هویت

ورود، خروج، بازیابی و تغییر وضعیت را ثبت کن؛ تمام مسیرهای هویتی پوشش داده شوند.

۴.۵. نقاط پردازش

آپلود، خروجی، URL ورودی و ارتباط خارجی را مشخص کن؛ هیچ نقطه ورود شناخته‌شده جا نماند.

۴.۶. مرز اعتماد [جدید]

معماری و جریان داده را با مستندات تطبیق بده؛ فرض‌های تأییدنشده مشخص بمانند.

مرحله ۵

معماری و توسعه امن

ASVS: V1؛ SCP: Introduction، General Coding؛ Top 10: A06

ابزار / دسترسی: مستندات، کد و مصاحبه

۵.۱. مدل تهدید

جریان‌های حساس و سوءاستفاده‌ها را مرور کن؛ کنترل متناظر و آزمون برای تهدیدها وجود داشته باشد.

۵.۲. نیازمندی امنیتی [جدید]

نیازمندی هر قابلیت را بررسی کن؛ رفتار مجاز و غیرمجاز صریح باشد.

۵.۳. کنترل متمرکز [جدید]

پیاده‌سازی ورود، مجوز و اعتبارسنجی را مرور کن؛ مسیر ضعیف یا کنترل تکراری ناسازگار نباشد.

۵.۴. چرخه توسعه [جدید]

مسئولیت، آموزش و بازبینی تغییرات را بررسی کن؛ امنیت در توسعه و نگهداری پوشش داده شود.

۵.۵. برون‌سپاری [جدید]

قرارداد و معیار پذیرش را بررسی کن؛ نیازمندی و روش ارزیابی امنیتی مشخص باشد.

۵.۶. تفکیک اعتماد [جدید]

مرز شبکه و سرویس را بررسی کن؛ بخش کم‌اعتماد به منابع حساس دسترسی نامحدود نداشته باشد.

مرحله ۶

زیرساخت و تنظیمات

ASVS: V1.14، V14؛ SCP: System Configuration؛ Top 10: A02

ابزار / دسترسی: Nmap، Burp، تنظیمات سرور

۶.۱. قابلیت‌های اضافی

سرویس‌ها و فایل‌های غیرضروری را فهرست کن؛ موارد بدون نیاز حذف یا محدود باشند.

۶.۲. حالت توسعه

خطا، کنسول و تنظیم محیط را بررسی کن؛ Debug در محیط عملیاتی غیرفعال باشد.

۶.۳. مستندات داخلی

دسترسی به مستندات API و مدیریت را بررسی کن؛ فقط مخاطب مجاز دسترسی داشته باشد.

۶.۴. فهرست پوشه

درخواست پوشه‌ها را بررسی کن؛ Directory Listing ناخواسته فعال نباشد.

۶.۵ متد HTTP

متدهای هر مسیر را تغییر بده؛ فقط متد موردنیاز با مجوز مناسب پذیرفته شود.

۶.۶. حساب اجرا [جدید]

مجوز سرویس و فرایند را مرور کن؛ سطح دسترسی بیش از نیاز نباشد.

۶.۷. تفکیک محیط [جدید]

حساب، شبکه و داده محیط‌ها را مقایسه کن؛ محیط ضعیف‌تر راه ورود به محیط حساس نباشد.

۶.۸. تمامیت تنظیمات [جدید]

تاریخچه و مجوز تغییر را بررسی کن؛ دست‌کاری تنظیم امنیتی قابل‌ردیابی باشد.

مرحله ۷

TLS و ارتباطات امن

ASVS: V9، V1.9؛ SCP: Communication Security؛ Top 10: A04

ابزار / دسترسی: ابزار TLS در Kali، Burp، تنظیمات

۷.۱. نسخه و Cipher

پروتکل‌ها و Cipherها را شناسایی کن؛ فقط گزینه‌های مجاز سیاست امنیتی فعال باشند.

۷.۲. گواهی

نام، تاریخ، زنجیره و اعتماد را بررسی کن؛ گواهی معتبر و متعلق به مقصد باشد.

۷.۳. اجبار HTTPS

مسیرهای حساس را با ارتباط ناامن بررسی کن؛ اطلاعات حساس روی کانال ناامن منتقل نشود.

۷.۴. شکست TLS [جدید]

در محیط تست شکست اعتبارسنجی ایجاد کن؛ اتصال به کانال ناامن برنگردد.

۷.۵. ارتباط داخلی [جدید]

اتصال سرویس، مدیریت و دیتابیس را مرور کن؛ هویت و محرمانگی ارتباط حساس حفظ شوند.

۷.۶. اعتماد گواهی [جدید]

کد اعتبارسنجی و CAهای مجاز را بررسی کن؛ پذیرش همه گواهی‌ها وجود نداشته باشد.

۷.۷. ابطال و ثبت خطا [جدید]

سازوکار ابطال و لاگ TLS را بررسی کن؛ شکست ارتباط قابل‌تشخیص باشد.

مرحله ۸

هدرها و افشای اطلاعات

ASVS: V14.3، V14.4؛ SCP: Data Protection؛ Top 10: A02، A05

ابزار / دسترسی: Burp، Developer Tools

۸.۱. CSP

هدر و منابع واقعی صفحه را مقایسه کن؛ سیاست اجرایی با نیازها محدود و سازگار باشد.

۸.۲. nonce و اجرا

پاسخ‌های تازه و اجرای اسکریپت آزمایشی را بررسی کن؛ nonce قابل‌حدس یا تکراری نباشد.

۸.۳. iframe

صفحه را در iframe محیط تست باز کن؛ نمایش خارج از سیاست مسدود شود.

۸.۴. HSTS و Referrer

هدرها را در پاسخ‌های مرتبط بررسی کن؛ ارتباط و ارسال Referrer داده حساس را افشا نکنند.

۸.۵. نوع محتوا [جدید]

Content-Type، charset و nosniff را بررسی کن؛ مرورگر نوع ناامن متفاوت تفسیر نکند.

۸.۶. دانلود [جدید]

Content-Disposition را متناسب با مصرف بررسی کن؛ فایل به‌شکل ناخواسته اجرا نشود.

۸.۷. خطا و بنر

پاسخ عادی و خطا را مقایسه کن؛ Stack trace، مسیر داخلی و نسخه غیرضروری افشا نشوند.

۸.۸. کد عمومی

HTML، JavaScript و Source Map را مرور کن؛ Secret و آدرس داخلی حساس وجود نداشته باشد.

۸.۹. فایل باقی‌مانده

Backup، تنظیمات، مخزن و فایل موقت را بررسی کن؛ دانلود عمومی ناخواسته ممکن نباشد.

۸.۱۰. robots و کامنت [جدید]

مسیر و متن عمومی را بررسی کن؛ robots.txt جایگزین کنترل دسترسی نشده باشد.

مرحله ۹

CORS و اعتماد به هدرها

ASVS: V14.5؛ SCP: Access Control؛ Top 10: A01، A02

ابزار / دسترسی: Burp Repeater، مرورگر، تنظیمات Proxy

۹.۱. CORS

Origin معتبر، غیرمجاز و null را مقایسه کن؛ خواندن پاسخ حساس فقط برای مبادی مجاز ممکن باشد.

۹.۲. credentials

سیاست Cookie و CORS را در مرورگر بررسی کن؛ Origin دلخواه به پاسخ احرازشده دسترسی نگیرد.

۹.۳. منابع مشترک

CORP و سیاست فایل‌ها را بررسی کن؛ اشتراک‌گذاری با نیاز واقعی سازگار باشد.

۹.۴. هدر Proxy

هدرهای انتقال IP و هویت را تغییر بده؛ فقط واسطه معتبر بتواند مقدار قابل‌اعتماد تعیین کند.

۹.۵. Origin و Referer [جدید]

هدر را حذف یا تغییر بده؛ احراز هویت و مجوز صرفاً به این مقادیر وابسته نباشند.

مرحله ۱۰

ورود و سیاست رمز

ASVS: V2.1، V2.2، V2.5؛ SCP: Authentication؛ Top 10: A07

ابزار / دسترسی: Burp Repeater، مرورگر، سیاست امنیتی

۱۰.۱. مسیرهای ورود

همه مسیرهای هویتی را مقایسه کن؛ مسیر جایگزین کنترل ضعیف‌تر نداشته باشد.

۱۰.۲. دورزدن ورود

حالت ناقص و Credential آزمایشی را بررسی کن؛ هیچ bypass فعال نباشد.

۱۰.۳. شناسایی حساب [جدید]

پیام، وضعیت و زمان حساب موجود و ناموجود را مقایسه کن؛ افشای قابل‌اتکا ایجاد نشود.

۱۰.۴. تلاش ناموفق

تلاش محدود و کنترل‌شده اجرا کن؛ مقابله با حدس رمز و قفل سوءاستفاده‌پذیر بررسی شود.

۱۰.۵. رمز بلند [جدید]

طول و ورودی Unicode را آزمون کن؛ رمز بی‌اطلاع کوتاه نشود و حدود سیاست رعایت شوند.

۱۰.۶. رمز افشاشده [جدید]

کنترل رمز رایج را بررسی کن؛ رمز ضعیف رد و رمز خام برای بررسی بیرونی افشا نشود.

۱۰.۷. رابط رمز [جدید]

Paste، Password Manager و نمایش موقت را بررسی کن؛ قابلیت امن ورود مسدود نشده باشد.

۱۰.۸. تغییر رمز [جدید]

درخواست را بدون احراز مجدد معتبر ارسال کن؛ تغییر حساس بدون اثبات هویت پذیرفته نشود.

۱۰.۹. سیاست سازگار [جدید]

قواعد رمز را با مبنای انتخابی تطبیق بده؛ توصیه‌های متعارض اسناد کورکورانه جمع نشوند.

۱۰.۱۰. حساب و اعلان [جدید]

حساب پیش‌فرض و اعلان امنیتی را بررسی کن؛ حساب ناخواسته فعال و تغییر حساس بی‌خبر نباشد.

مرحله ۱۱

بازیابی و فعال‌سازی

ASVS: V2.3، V2.5؛ SCP: Authentication؛ Top 10: A07

ابزار / دسترسی: Burp، کانال آزمایشی بازیابی

۱۱.۱. توکن اولیه [جدید]

کد فعال‌سازی را بررسی کن؛ تصادفی، محدود به حساب و کوتاه‌عمر باشد.

۱۱.۲. بازیابی [جدید]

توکن را تغییر، تکرار و پس از انقضا مصرف کن؛ فقط درخواست معتبر یک‌بار پذیرفته شود.

۱۱.۳. کانال بازیابی [جدید]

مقصد ارسال و تغییر آن را بررسی کن؛ بازیابی فقط به کانال تأییدشده برسد.

۱۱.۴. اطلاعات قدیمی [جدید]

پاسخ بازیابی را بررسی کن؛ رمز فعلی، Hint یا سؤال امنیتی ضعیف راه ورود نباشد.

۱۱.۵. رمز موقت [جدید]

اولین ورود را طی کن؛ رمز موقت بدون تغییر به Credential دائمی تبدیل نشود.

۱۱.۶. ابطال پس از بازیابی

Token قبلی را دوباره استفاده کن؛ سیاست ابطال در تمام مسیرها اعمال شود.

۱۱.۷. اعلان تغییر [جدید]

تغییر اطلاعات بازیابی را اجرا کن؛ مالک حساب اعلان بدون داده حساس دریافت کند.

مرحله ۱۲

MFA و OTP

ASVS: V2.6 تا V2.9، V4.3؛ SCP: Authentication؛ Top 10: A07

ابزار / دسترسی: Burp، ابزار یا عامل آزمایشی

۱۲.۱. نیاز به MFA [جدید]

سیاست و مسیرهای حساس را مقایسه کن؛ MFA لازم از مسیر جایگزین دور نخورد.

۱۲.۲. کد ثابت

کدهای آزمایشی و منطق تولید را بررسی کن؛ کد ثابت یا قابل‌پیش‌بینی پذیرفته نشود.

۱۲.۳. انقضا و اتصال [جدید]

کد را برای درخواست دیگر و پس از انقضا استفاده کن؛ پذیرش فقط در زمینه اصلی باشد.

۱۲.۴. مصرف مجدد [جدید]

کد مصرف‌شده را دوباره و همزمان ارسال کن؛ حداکثر یک مصرف موفق باشد.

۱۲.۵. تلاش و ارسال [جدید]

تلاش و ارسال مجدد محدود اجرا کن؛ سقف مؤثر و غیرقابل‌دورزدن باشد.

۱۲.۶. Seed و بازیابی [جدید]

ذخیره Seed و کد اضطراری را مرور کن؛ اطلاعات محفوظ و کد بازیابی یک‌بارمصرف باشد.

۱۲.۷. تعویض عامل [جدید]

تعویض، حذف و فقدان عامل را بررسی کن؛ احراز قوی، ابطال و اعلان اجرا شوند.

۱۲.۸. عامل سخت‌افزاری [جدید]

Challenge و تأیید کاربر را بررسی کن؛ پاسخ تازه و مرتبط با اقدام واقعی باشد.

۱۲.۹. عامل ضعیف [جدید]

سیاست SMS، ایمیل و Biometric را مرور کن؛ قدرت آن‌ها بیش از واقع فرض نشود.

مرحله ۱۳

نشست و Cookie

ASVS: V3.1 تا V3.4، V3.7؛ SCP: Session Management؛ Top 10: A07

ابزار / دسترسی: Burp، نشست‌های جدا، مرورگر

۱۳.۱. ایجاد نشست

شناسه پیش و پس از ورود را مقایسه کن؛ نشست تازه ایجاد و Fixation رد شود.

۱۳.۲. تصادفی‌بودن [جدید]

مولد نشست و طول آن را مرور کن؛ از CSPRNG و آنتروپی مناسب استفاده شود.

۱۳.۳. Cookie

Secure، HttpOnly، SameSite و Scope را بررسی کن؛ Credential فقط در زمینه لازم ارسال شود.

۱۳.۴. پیشوند و تکرار

قواعد __Host- و Cookie هم‌نام را بررسی کن؛ نشست مبهم یا همزمان ناخواسته صادر نشود.

۱۳.۵. افشای Token

URL، لاگ و خطا را بررسی کن؛ Token خام در محل ناامن نباشد.

۱۳.۶. خروج و تغییر

درخواست قدیمی را بعد از خروج یا تغییر حساس تکرار کن؛ ابطال مطابق سیاست اعمال شود.

۱۳.۷. Timeout [جدید]

پس از بی‌کاری و پایان عمر نشست درخواست بفرست؛ احراز مجدد مطابق سیاست لازم شود.

۱۳.۸. مدیریت دستگاه [جدید]

فهرست و ابطال نشست‌ها را بررسی کن؛ مالک بتواند با احراز معتبر نشست را لغو کند.

۱۳.۹. نشست ناقص [جدید]

در میانه بازیابی یا MFA درخواست حساس بفرست؛ دسترسی کامل داده نشود.

۱۳.۱۰. نشست نامعتبر

Token نامعتبر ارسال کن؛ خروج یا پاسخ منع معتبر باشد و خطای کنترل جریان بلعیده نشود.

مرحله ۱۴

Token و ورود یکپارچه

ASVS: V3.5، V3.6؛ Top 10: A07، A08

ابزار / دسترسی: Burp، کد و تنظیمات هویت

۱۴.۱. اعتبار Token

دست‌کاری امضا و توکن منقضی را بررسی کن؛ پذیرش بدون اعتبار رمزنگاری ممکن نباشد.

۱۴.۲. کلید fallback

تنظیمات ناقص را در تست بررسی کن؛ کلید ناامن پیش‌فرض فعال نشود.

۱۴.۳. تمدید

Refresh Token قبلی را پس از تمدید مصرف کن؛ Rotation و ابطال مطابق طراحی باشند.

۱۴.۴. reuse و همزمانی

مصرف مجدد و موازی را بررسی کن؛ خانواده و تراکنش طبق سیاست امن مدیریت شوند.

۱۴.۵. ذخیره Refresh

دیتابیس را بررسی کن؛ Token خام قابل‌بازیابی ذخیره نشده باشد.

۱۴.۶. Claims [تکمیلی]

iss، aud، exp، nbf و الگوریتم را تغییر بده؛ Token خارج از قرارداد رد شود.

۱۴.۷. OAuth و SSO [جدید]

ابطال مجوز و زمان احراز مجدد را بررسی کن؛ اعتماد منقضی ادامه پیدا نکند.

۱۴.۸. Flow هویت [تکمیلی]

در صورت کاربرد state، nonce، PKCE و Redirect URI را بررسی کن؛ پاسخ به جریان و مقصد معتبر متصل باشد.

مرحله ۱۵

کنترل دسترسی

ASVS: V4، V1.4؛ SCP: Access Control؛ Top 10: A01

ابزار / دسترسی: Burp Repeater، سیاست دسترسی و کد

۱۵.۱. درخواست مستقیم

عملیات را بدون نشست اجرا کن؛ منابع غیرعمومی مسدود باشند.

۱۵.۲. مرز هویت

درخواست را با هویت یا مجوز متفاوت تکرار کن؛ داده و عمل خارج از اختیار قابل‌دسترسی نباشد.

۱۵.۳. سطح رکورد

شناسه منبع را تغییر بده؛ ایجاد، خواندن، تغییر و حذف همگی مجوز مستقل داشته باشند.

۱۵.۴. فایل و خروجی

دانلود، گزارش، جست‌وجو و عملیات گروهی را بررسی کن؛ مسیر جانبی مجوز را دور نزند.

۱۵.۵. ویژگی مجوز

مالکیت و ویژگی امنیتی را در ورودی تغییر بده؛ کاربر مجوز خود را افزایش ندهد.

۱۵.۶. خطای مجوز [جدید]

شکست کنترل مجوز را در تست ایجاد کن؛ حالت پیش‌فرض منع دسترسی باشد.

۱۵.۷. تغییر وضعیت

مجوز یا وضعیت هویت را تغییر بده؛ اثر آن در همه نشست‌ها مطابق سیاست اعمال شود.

۱۵.۸. تفکیک وظایف [جدید]

سیاست عملیات پرارزش را بررسی کن؛ تأیید مستقل در صورت الزام قابل‌دورزدن نباشد.

۱۵.۹. ابزار و شاهد

از Repeater و هویت‌های مجاز آزمون استفاده کن؛ نتیجه با سیاست واقعی دسترسی مقایسه شود.

مرحله ۱۶

قواعد چرخه هویت و عملیات مدیریتی

ASVS: V4، V11؛ Top 10: A01، A06

ابزار / دسترسی: Burp، کد و داده آزمایشی

۱۶.۱. مجوز اجراکننده و هدف

قواعد عمل روی هویت دیگر یا خود را بررسی کن؛ فقط ترکیب مجاز پذیرفته شود.

۱۶.۲. ساخت هویت

شکست تخصیص مجوز را ایجاد کن؛ هویت نیمه‌کاره یا بیش‌ازحد مجاز باقی نماند.

۱۶.۳. عملیات متناقض

وضعیت‌های ناسازگار را همزمان ارسال کن؛ درخواست مبهم رد شود.

۱۶.۴. تغییر شناسه هویتی

مجوز، یکتایی و ابطال نشست را بررسی کن؛ تغییر معتبر و قابل‌حسابرسی باشد.

۱۶.۵. آثار وابسته

تغییر وضعیت را روی کارهای وابسته بررسی کن؛ مالکیت و سابقه مطابق سیاست حفظ شوند.

مرحله ۱۷

CSRF

ASVS: V4.2، V13.2؛ SCP: Session Management؛ Top 10: A01

ابزار / دسترسی: Burp و مرورگر

۱۷.۱. نقاط حساس

روش انتقال Credential را ثبت کن؛ عملیات مبتنی بر Cookie کنترل متناسب داشته باشد.

۱۷.۲. Token محافظ

Token را حذف، تغییر یا از نشست دیگر جایگزین کن؛ درخواست غیرمعتبر اجرا نشود.

۱۷.۳. Origin و روش ارسال

درخواست cross-origin را در مرورگر آزمایش کن؛ اثر تغییردهنده ناخواسته ایجاد نشود.

۱۷.۴. جریان بدون نشست [جدید]

ورود و عملیات عمومی حساس را بررسی کن؛ Login CSRF و سوءاستفاده خودکار مهار شوند.

۱۷.۵. اثبات اثر

وضعیت واقعی را پس از آزمون بررسی کن؛ صرف پاسخ موفق یا حذف Cookie اثبات نقص نباشد.

مرحله ۱۸

اعتبارسنجی ورودی

ASVS: V5.1؛ SCP: Input Validation؛ Top 10: A05، A10

ابزار / دسترسی: Burp Repeater، کد

۱۸.۱. نوع و حدود

نوع، طول، بازه، enum و خالی‌بودن را تغییر بده؛ داده خارج از قرارداد رد شود.

۱۸.۲. شناسه خراب

ورودی شناسه یا رمزشده نامعتبر بفرست؛ خطای کنترل‌شده و بدون اثر جانبی باشد.

۱۸.۳. قواعد مرتبط

ترکیب متناقض فیلدها و بازه زمانی بفرست؛ قاعده عملیاتی سمت سرور اجرا شود.

۱۸.۴. Unicode

ارقام، فاصله و Encoding را تغییر بده؛ تفسیر معتبر و یکسان باقی بماند.

۱۸.۵. HPP

پارامتر تکراری در منابع مختلف بفرست؛ تفاوت تفسیر کنترل امنیتی را دور نزند.

۱۸.۶. Mass Assignment [جدید]

فیلد اضافه امنیتی بفرست؛ فقط فیلدهای مجاز قابل‌تغییر باشند.

۱۸.۷. Canonicalization [جدید]

Encoding چندمرحله‌ای و Null Byte را بررسی کن؛ اعتبارسنجی پس از تفسیر معتبر انجام شود.

۱۸.۸. منابع خارجی [جدید]

ورودی فایل، سرویس و دیتابیس را مرور کن؛ داده غیرقابل‌اعتماد پیش از مصرف کنترل شود.

۱۸.۹. رد امن [جدید]

شکست اعتبارسنجی ایجاد کن؛ عملیات حساس و تغییر داده ادامه پیدا نکند.

مرحله ۱۹

XSS و خروجی

ASVS: V5.2، V5.3؛ SCP: Output Encoding؛ Top 10: A05

ابزار / دسترسی: Burp، مرورگر، کد

۱۹.۱. سه نوع XSS

مسیر بازتابی، ذخیره‌ای و DOM را بررسی کن؛ ورودی کاربر به اجرای کد ناخواسته نرسد.

۱۹.۲. نمایش متن

جزئیات، پیام و لاگ را بررسی کن؛ داده به‌صورت متن یا HTML پاک‌سازی‌شده نمایش یابد.

۱۹.۳. Encoding زمینه‌ای [جدید]

خروجی HTML، Attribute، URL و JavaScript را مرور کن؛ Encoder متناسب با مفسر باشد.

۱۹.۴. Rich Text [جدید]

پاک‌سازی محتوای مجاز را بررسی کن؛ محتوای اجرایی حذف و متن لازم حفظ شود.

۱۹.۵. قالب قابل‌اسکریپت [جدید]

SVG، Markdown و سبک ورودی را بررسی کن؛ اجرای خارج از سیاست ممکن نباشد.

۱۹.۶. اجرای پویا [جدید]

مصرف eval و رشته اجرایی را مرور کن؛ داده غیرقابل‌اعتماد مستقیم اجرا نشود.

۱۹.۷. تأیید یافته

اثر را در مرورگر ثبت کن؛ بازتاب متن و ویرایش دستی پاسخ، اثبات XSS برنامه نیست.

مرحله ۲۰

تزریق در مفسرها

ASVS: V5.2، V5.3؛ SCP: Output Encoding، Database؛ Top 10: A05

ابزار / دسترسی: Burp، بررسی Query و کد

۲۰.۱. SQL Injection

ورودی مؤثر بر Query را تغییر و کد را مرور کن؛ داده از ساختار فرمان جدا باشد.

۲۰.۲. ORM و NoSQL [جدید]

فیلتر و عملگرهای ورودی را بررسی کن؛ ساختار دلخواه به Query تحمیل نشود.

۲۰.۳. مرتب‌سازی پویا [جدید]

نام فیلد و جهت مرتب‌سازی را تغییر بده؛ فقط گزینه‌های Allowlist پذیرفته شوند.

۲۰.۴. فرمان سیستم [جدید]

ورودی مؤثر بر Command و Argument را بررسی کن؛ فرمان یا گزینه ناخواسته اجرا نشود.

۲۰.۵. LDAP و XML [جدید]

نقاط دارای مفسر مربوط را بررسی کن؛ ورودی ساختار LDAP، XPath یا XML را تغییر ندهد.

۲۰.۶. ایمیل [جدید]

فیلدهای پیام و Header را بررسی کن؛ تزریق SMTP یا IMAP ممکن نباشد.

۲۰.۷. قالب و JSON [جدید]

Template و Parser را مرور کن؛ ورودی به عبارت اجرایی یا ساختار ناخواسته تبدیل نشود.

۲۰.۸. CRLF

ورودی مؤثر بر Header را تغییر بده؛ Header یا پاسخ اضافی ساخته نشود.

مرحله ۲۱

Deserialization

ASVS: V5.5، V1.5؛ Top 10: A08، A02

ابزار / دسترسی: Burp، تنظیمات Parser و کد

۲۱.۱. نوع شیء [جدید]

نوع‌های ورودی را بررسی کن؛ داده نتواند کلاس دلخواه یا رفتار اجرایی بسازد.

۲۱.۲. تمامیت [جدید]

داده سریال‌شده نیازمند اعتماد را دست‌کاری کن؛ تغییر بدون اصالت رد شود.

۲۱.۳. XXE [جدید]

دسترسی XML Parser به منبع خارجی کنترل‌شده را بررسی کن؛ دریافت غیرمجاز رخ ندهد.

۲۱.۴. Parser استاندارد [جدید]

مصرف JSON، XML و YAML را مرور کن؛ تنظیمات امن و نبود eval تأیید شوند.

۲۱.۵. محدودیت پردازش [تکمیلی]

عمق و حجم ورودی را در تست افزایش بده؛ مصرف منابع و خطا کنترل‌شده باشند.

مرحله ۲۲

SSRF و مسیرها

ASVS: V5.1، V5.2.6، V12.3، V12.6؛ Top 10: A01، A05

ابزار / دسترسی: Burp، مقصد آزمایشی کنترل‌شده، کد

۲۲.۱. مقصد خروجی

URL و metadata مؤثر بر درخواست را تغییر بده؛ مقصد فقط در Allowlist باشد.

۲۲.۲. مرز اتصال

DNS و IP هنگام اتصال را بررسی کن؛ مقصد غیرمجاز پشت نام مجاز پنهان نشود.

۲۲.۳. Redirect و Proxy

مسیر تغییر مقصد را بررسی کن؛ هر گام از سیاست خروجی پیروی کند.

۲۲.۴. دریافت Credential

درخواست‌های اولیه و احراز سرویس را مرور کن؛ همان محافظ مقصد اعمال شود.

۲۲.۵. ساختار URL

پورت، scheme، credential و مسیر مبهم را بررسی کن؛ تفسیر ناامن پذیرفته نشود.

۲۲.۶. تفاوت Parser [جدید]

تفسیر مقصد در اجزا را مقایسه کن؛ اختلاف آن‌ها راه دورزدن نباشد.

۲۲.۷. Open Redirect [جدید]

مقصد هدایت را تغییر بده؛ فقط مسیر امن یا مقصد مجاز پذیرفته شود.

۲۲.۸. Traversal

مسیر نسبی، مطلق و Encoding را بررسی کن؛ فایل خارج از محدوده قابل‌دسترسی نباشد.

۲۲.۹. LFI و RFI [جدید]

مسیر فایل یا منبع خارجی را تغییر بده؛ Include غیرمجاز و افشای مسیر رخ ندهد.

مرحله ۲۳

آپلود و دانلود

ASVS: V12، V1.12؛ SCP: File Management؛ Top 10: A01، A02، A05، A06

ابزار / دسترسی: Burp، فایل‌های آزمایشی بی‌خطر، تنظیمات

۲۳.۱. مجوز فایل

آپلود و دانلود را با زمینه دسترسی متفاوت اجرا کن؛ فقط عمل مجاز انجام شود.

۲۳.۲. نوع واقعی

پسوند، MIME و محتوای فایل را ناسازگار کن؛ نوع غیرمجاز رد شود.

۲۳.۳. نام فایل

نام و مسیر غیرعادی ارسال کن؛ نام امن تولید و مسیر کاربر مستقیم مصرف نشود.

۲۳.۴. حجم

مرز حجم مصوب را آزمون کن؛ کنترل پیش از پردازش پرهزینه اجرا شود.

۲۳.۵. سهمیه [جدید]

تعداد و مجموع اندازه را بررسی کن؛ یک هویت فضای نامحدود مصرف نکند.

۲۳.۶. آرشیو [جدید]

حجم بازشده، تعداد و مسیر داخل آرشیو را بررسی کن؛ استخراج محدود به محدوده امن باشد.

۲۳.۷. اسکن محتوا [جدید]

سازوکار ضدبدافزار را با نمونه آزمون استاندارد بررسی کن؛ فایل مردود منتشر نشود.

۲۳.۸. ذخیره [جدید]

محل و مجوز را مرور کن؛ فایل کاربر مجوز اجرای کد نداشته باشد.

۲۳.۹. نمایش [جدید]

فایل قابل‌اسکریپت را باز کن؛ Origin اصلی در معرض اجرای ناخواسته قرار نگیرد.

۲۳.۱۰. RFD [جدید]

نام و Header خروجی را تغییر بده؛ دانلود بازتابی به فایل اجرایی ناامن تبدیل نشود.

مرحله ۲۴

API و پروتکل‌ها

ASVS: V13؛ Top 10: A01، A02، A05، A06، A08

ابزار / دسترسی: Burp، قرارداد API، کد

۲۴.۱. مجوز API

مسیر، متد و منبع را تغییر بده؛ کنترل در سطح عملیات و داده اعمال شود.

۲۴.۲. قرارداد پیام [جدید]

نوع محتوا، Schema و فیلد مفقود را آزمون کن؛ درخواست خارج از قرارداد رد شود.

۲۴.۳. Secret در URL

Query و مسیر را مرور کن؛ Token یا داده حساس در URL نباشد.

۲۴.۴. تفسیر یکسان [جدید]

Encoding و Parser اجزا را مقایسه کن؛ پیام معنای امنیتی متفاوت نگیرد.

۲۴.۵. تمامیت انتقال [جدید]

TLS و امضای لازم را بررسی کن؛ پیام حساس در انتقال قابل‌تغییر نباشد.

۲۴.۶. GraphQL [جدید]

عمق، مقدار و هزینه Query را محدود آزمون کن؛ مجوز در منطق و محدودیت منابع مؤثر باشد.

۲۴.۷. SOAP [جدید]

XSD، اعتبار فیلد و امضای لازم را بررسی کن؛ پیام نامعتبر قبل از پردازش رد شود.

مرحله ۲۵

منطق و همزمانی

ASVS: V11، V1.11؛ SCP: General Coding؛ Top 10: A06، A10

ابزار / دسترسی: Burp Repeater، محیط تست، مشاهده داده

۲۵.۱. ترتیب مراحل

مرحله را حذف یا جابه‌جا کن؛ فقط گذار مجاز پردازش شود.

۲۵.۲. تکرار

یک عملیات را دوباره اجرا کن؛ اثر ناخواسته یا رکورد تکراری ایجاد نشود.

۲۵.۳. اتمیک‌بودن

میان مراحل خطا ایجاد کن؛ عملیات کامل شود یا به وضعیت معتبر قبلی برگردد.

۲۵.۴. قفل و صف

درخواست محدود همزمان اجرا کن؛ صف و استقلال پردازش مطابق سیاست باشند.

۲۵.۵. TOCTOU [جدید]

شرط را بین بررسی و اجرا تغییر بده؛ تصمیم بر وضعیت معتبر و هماهنگ متکی باشد.

۲۵.۶. منابع مشترک [جدید]

حالت مشترک و همزمانی را مرور کن؛ دسترسی بدون هماهنگی داده را خراب نکند.

۲۵.۷. سقف کسب‌وکار [جدید]

تعداد و سرعت عملیات را بررسی کن؛ محدودیت واقعی در سرور اعمال شود.

۲۵.۸. رفتار غیرعادی [جدید]

عملیات خارج از ترتیب ایجاد کن؛ رخداد مهم ثبت و در صورت نیاز هشدار داده شود.

۲۵.۹. قطع و تکرار [تکمیلی]

ارتباط را قطع و درخواست را تکرار کن؛ اثر حساس دوباره ایجاد نشود.

مرحله ۲۶

داده و Cache

ASVS: V6.1، V8؛ SCP: Data Protection؛ Top 10: A01، A02، A04

ابزار / دسترسی: مرورگر، Burp، تنظیمات Cache و داده

۲۶.۱. طبقه‌بندی [جدید]

داده و مصرف آن را مرور کن؛ سطح حفاظت و ضرورت نگهداری مشخص باشد.

۲۶.۲. رمزنگاری داده

ذخیره داده حساس را بررسی کن؛ محرمانگی و تمامیت مطابق سیاست حفظ شوند.

۲۶.۳. حداقل داده [جدید]

پاسخ و جمع‌آوری را مرور کن؛ فقط داده لازم در اختیار مخاطب مجاز باشد.

۲۶.۴. Cache واسطه [جدید]

پاسخ را میان زمینه‌های دسترسی مقایسه کن؛ داده حساس بین هویت‌ها نشت نکند.

۲۶.۵. Cache مرورگر [جدید]

Header و رفتار بازگشت صفحه را بررسی کن؛ محتوای حساس ناخواسته باقی نماند.

۲۶.۶. Storage [جدید]

Cookie، localStorage، sessionStorage و IndexedDB را بررسی کن؛ Secret ناامن ذخیره نشود.

۲۶.۷. خروج و ابطال [جدید]

پس از خروج یا تغییر مجوز داده را بخوان؛ DOM و Cache مطابق سیاست پاک یا باطل شوند.

۲۶.۸. حذف و خروجی [جدید]

چرخه حذف، Export و مدت نگهداری را بررسی کن؛ سیاست داده واقعاً اجرا شود.

۲۶.۹. رضایت و حسابرسی [جدید]

اطلاع‌رسانی و ثبت دسترسی را مرور کن؛ مصرف داده شفاف و دسترسی حساس قابل‌پیگیری باشد.

۲۶.۱۰. نسخه موقت [جدید]

فایل و نسخه واسط را بررسی کن؛ پس از رفع نیاز حذف یا محافظت شوند.

مرحله ۲۷

رمزنگاری و Secrets

ASVS: V2.4، V2.10، V6؛ SCP: Cryptographic Practices؛ Top 10: A04، A07، A08

ابزار / دسترسی: کد، تنظیمات، مخزن Secrets

۲۷.۱. ذخیره رمز [جدید]

Hash و Salt را بررسی کن؛ تابع تخصصی و هزینه مناسب، نه Hash سریع یا رمز برگشت‌پذیر، استفاده شود.

۲۷.۲ Pepper [جدید]

در صورت استفاده محل نگهداری را بررسی کن؛ Secret از مخزن Hash جدا و محافظت‌شده باشد.

۲۷.۳. الگوریتم

کتابخانه و روش رمزنگاری را مرور کن؛ طراحی اختصاصی ناامن یا الگوریتم ضعیف نباشد.

۲۷.۴ IV و nonce [جدید]

تولید و مصرف را بررسی کن؛ الزامات تازگی و یکتایی الگوریتم رعایت شوند.

۲۷.۵. تمامیت رمز [جدید]

Ciphertext را در تست تغییر بده؛ تغییر بدون اصالت پذیرفته نشود.

۲۷.۶ Oracle و زمان [جدید]

پاسخ خطا و مقایسه Secret را بررسی کن؛ جزئیات قابل‌سوءاستفاده افشا نشوند.

۲۷.۷. تصادفی امن

مولد رمز موقت و مقدار غیرقابل‌حدس را مرور کن؛ CSPRNG استفاده شود.

۲۷.۸. چرخه کلید [جدید]

تولید، دسترسی، چرخش و امحا را بررسی کن؛ کلید قابل‌مدیریت و قابل‌جایگزینی باشد.

۲۷.۹. حفاظت کلید [جدید]

Vault یا سازوکار معادل را بررسی کن؛ سطح حفاظت با نیاز و سطح ارزیابی سازگار باشد.

۲۷.۱۰ Secret مخزن

کد، تنظیمات و تاریخچه را بررسی کن؛ Secret افشاشده چرخانده و دسترسی آن لغو شود.

۲۷.۱۱ HMAC و Replay

امضای درخواست و تازگی را بررسی کن؛ تغییر method/path/body و تکرار پیام معتبر پذیرفته نشود.

۲۷.۱۲. هویت سرویس [جدید]

حساب و مجوز اتصال را بررسی کن؛ Credential پیش‌فرض یا دسترسی بیش از نیاز نباشد.

مرحله ۲۸

دیتابیس و تمامیت داده

ASVS: V1.2، V5.3، V9، V11؛ SCP: Database Security؛ Top 10: A01، A02، A05، A10

ابزار / دسترسی: تنظیمات، کد دسترسی داده، دیتابیس تست

۲۸.۱. حساب اتصال [جدید]

مجوزها را مرور کن؛ برنامه دسترسی مدیریتی غیرضروری نداشته باشد.

۲۸.۲. تفکیک اعتبار [جدید]

Credential مرزهای اعتماد را مقایسه کن؛ اشتراک حساب مانع تفکیک مجوز نشود.

۲۸.۳. Connection String

محل ذخیره و TLS را بررسی کن؛ Credential افشا و اتصال حساس ناامن نباشد.

۲۸.۴. امکانات پیش‌فرض [جدید]

حساب، Schema و سرویس اضافی را مرور کن؛ فقط موارد لازم فعال باشند.

۲۸.۵. Query و تراکنش

پارامتری‌بودن و Rollback را بررسی کن؛ تزریق و وضعیت نیمه‌کاره رخ ندهند.

۲۸.۶. Index و migration

Schema مستقر را با تغییرات لازم مقایسه کن؛ Constraint لازم واقعاً فعال باشد.

۲۸.۷. آزادسازی اتصال [جدید]

خطا و خروج زودهنگام ایجاد کن؛ Connection و تراکنش رهاشده باقی نمانند.

۲۸.۸. ظرفیت

حجم، رشد و سقف فایل را بررسی کن؛ محدودیت شناخته‌شده و هشدار ظرفیت وجود داشته باشد.

مرحله ۲۹

منابع و Exception

ASVS: V7.4، V11، V12.1؛ SCP: Error Handling؛ Top 10: A06، A10

ابزار / دسترسی: محیط تست، Burp، پایش منابع

۲۹.۱. سقف ورودی

بدنه و صفحه‌بندی نزدیک مرز ارسال کن؛ محدودیت قبل از مصرف سنگین اجرا شود.

۲۹.۲. نرخ و صف

درخواست محدود و افزایشی بفرست؛ سقف و پاسخ کنترل‌شده مؤثر باشند.

۲۹.۳. Timeout و Retry [جدید]

وابستگی را کند یا قطع کن؛ انتظار و تکرار نامحدود رخ ندهد.

۲۹.۴. شکست امن [جدید]

خطای کنترل امنیتی ایجاد کن؛ دسترسی باز و موفقیت کاذب برنگردد.

۲۹.۵. Exception سراسری

خطای مدیریت‌نشده در تست ایجاد کن؛ پاسخ عمومی و شناسه پیگیری ارائه شود.

۲۹.۶. آزادسازی [جدید]

مسیر خطا را بررسی کن؛ قفل، فایل، اتصال و حافظه آزاد شوند.

۲۹.۷. پایداری [جدید]

CPU، RAM و دیسک را پایش کن؛ شرایط غیرعادی به مصرف کنترل‌نشده منجر نشوند.

مرحله ۳۰

پردازش HTTP

مرتبط با ASVS: V13.1، V14؛ Top 10: A02

ابزار / دسترسی: محیط ایزوله، Burp، تنظیمات واسطه‌ها

۳۰.۱. زنجیره واقعی

اجزای دریافت تا پردازش را ثبت کن؛ نتیجه به کل مسیر مستقر متصل باشد.

۳۰.۲. طول پیام

تعارض طول و Header تکراری را در تست بررسی کن؛ درخواست مبهم به تفسیر متفاوت نرسد.

۳۰.۳. تبدیل پروتکل

مرز نسخه‌های HTTP را بررسی کن؛ تبدیل، کنترل امنیتی را دور نزند.

۳۰.۴. Desynchronization

مصرف بدنه و اتصال پایدار را بررسی کن؛ مرز درخواست‌های متوالی مخلوط نشود.

۳۰.۵. Keep-Alive

رفتار قطع و استفاده مجدد اتصال را ثبت کن؛ راهکار رفع در کل زنجیره مؤثر باشد.

مرحله ۳۱

لاگ، حسابرسی و هشدار

ASVS: V7، V1.7، V11؛ SCP: Error Handling and Logging؛ Top 10: A08، A09، A10

ابزار / دسترسی: رخداد آزمایشی، لاگ، تنظیمات هشدار

۳۱.۱. پوشش رخداد

ورود، منع دسترسی و تغییر حساس ایجاد کن؛ رخداد موفق و ناموفق لازم ثبت شوند.

۳۱.۲. خطاهای امنیتی [جدید]

خطای ورودی، Parser، TLS و رمزنگاری ایجاد کن؛ رخداد مرتبط قابل‌پیگیری باشد.

۳۱.۳. هویت و هدف

ثبت اجراکننده و هدف را بررسی کن؛ دو هویت جابه‌جا نشده باشند.

۳۱.۴. User-Agent

مقدار مرورگر و هدر انتقالی را مقایسه کن؛ داده تشخیصی صحیح و غیرقابل‌اتکا برای مجوز باشد.

۳۱.۵. داده حساس

متن لاگ را بررسی کن؛ رمز و Token خام ثبت نشده باشند.

۳۱.۶. Log Injection [جدید]

ورودی شامل جداکننده و markup بفرست؛ رخداد جعلی یا اجرای محتوای ناامن ایجاد نشود.

۳۱.۷. زمان و پیگیری [جدید]

ساعت و شناسه ارتباط رخدادها را بررسی کن؛ توالی قابل‌بازسازی باشد.

۳۱.۸. تمامیت و آرشیو

تغییر و حذف آزمایشی را بررسی کن؛ سابقه و نتیجه صحت مستقل قابل‌تشخیص باشند.

۳۱.۹. شکست لاگ

مقصد اصلی را در تست قطع کن؛ fallback امن و علت شکست ثبت شود.

۳۱.۱۰. حفاظت و نگهداری [جدید]

مجوز، انتقال و سقف لاگ را بررسی کن؛ خواندن، تغییر و رشد نامحدود ممکن نباشند.

۳۱.۱۱. هشدار عملی

رخداد واجد شرط ایجاد کن؛ هشدار به مقصد مسئول برسد و قابل‌اقدام باشد.

مرحله ۳۲

کد، حافظه و زنجیره تأمین

ASVS: V5.4، V8.3.6، V10، V14.2؛ SCP: Memory، General Coding؛ Top 10: A03، A08، A10

ابزار / دسترسی: بازبینی کد، تحلیل وابستگی، تنظیمات Build

۳۲.۱. وابستگی

نسخه‌ها و SBOM را تطبیق بده؛ بسته آسیب‌پذیر یا بدون پشتیبانی تعیین تکلیف شده باشد.

۳۲.۲. منشأ بسته [جدید]

مخزن و دریافت بسته را بررسی کن؛ کد از منبع تأییدنشده اجرا نشود.

۳۲.۳. کد پنهان [جدید]

حساب، کلید، زمان و مسیرهای مخفی را مرور کن؛ Backdoor و منطق مخرب وجود نداشته باشند.

۳۲.۴. Phone-home [جدید]

ارتباط و مجوز جمع‌آوری داده را بررسی کن؛ مصرف پنهان یا بیش از نیاز نباشد.

۳۲.۵. حافظه Native [جدید]

Buffer، پایان رشته و مرز حلقه را بررسی کن؛ خواندن یا نوشتن خارج از محدوده رخ ندهد.

۳۲.۶. عدد و Format [جدید]

Cast، علامت، دقت و Format String را بررسی کن؛ خطای عددی یا تفسیر ورودی ناامن نباشد.

۳۲.۷. عمر منابع [جدید]

مقداردهی و آزادسازی را مرور کن؛ داده اولیه نامشخص و منابع رهاشده وجود نداشته باشند.

۳۲.۸. داده در حافظه [جدید]

عمر Secret را بررسی کن؛ در حد امکان Runtime بعد از نیاز پاک شود.

۳۲.۹. حفاظت اجرا [جدید]

تنظیم Compiler، ایزوله‌سازی و افزایش مجوز را بررسی کن؛ حفاظت‌ها فعال و مجوز موقت باشد.

مرحله ۳۳

Build و استقرار

ASVS: V1.10، V1.14، V10.3، V14.1؛ SCP: General Coding؛ Top 10: A03، A08

ابزار / دسترسی: مخزن، Pipeline، Artifact و تنظیمات

۳۳.۱. ردیابی تغییر [جدید]

هویت و درخواست تغییر را تطبیق بده؛ هر تغییر حساس قابل‌انتساب باشد.

۳۳.۲. Pipeline

دسترسی و Secrets را بررسی کن؛ مرحله غیرمجاز Artifact را تغییر ندهد.

۳۳.۳. Build تکرارپذیر [جدید]

فرایند ساخت و استقرار را مرور کن؛ خروجی از ورودی و تنظیمات مشخص ساخته شود.

۳۳.۴. کنترل خودکار [جدید]

Gateهای امنیتی را بررسی کن؛ وابستگی و تنظیم ناامن واکنش تعریف‌شده داشته باشند.

۳۳.۵. تطبیق نسخه

Artifact و محیط مستقر را مقایسه کن؛ اصلاحات بررسی‌شده واقعاً منتشر شده باشند.

۳۳.۶. به‌روزرسانی [جدید]

کانال دریافت و امضا را بررسی کن؛ بسته دست‌کاری‌شده نصب یا اجرا نشود.

۳۳.۷. SRI [جدید]

Asset خارجی قابل‌اعمال را بررسی کن؛ تمامیت آن پیش از مصرف کنترل شود.

۳۳.۸. دامنه رهاشده [جدید]

وابستگی DNS و سرویس خارجی را مرور کن؛ مقصد رهاشده قابل‌تصاحب باقی نماند.

مرحله ۳۴

Backup و پایان ارزیابی

ASVS: V8.1، V14.1؛ Assessment: Top 10: A02، A04، A10

ابزار / دسترسی: Backup، محیط Restore، شواهد

۳۴.۱. پوشش Backup [جدید]

داده و تنظیمات ضروری را تطبیق بده؛ اجزای لازم برای بازیابی پوشش داده شوند.

۳۴.۲. حفاظت Backup [جدید]

مجوز و تمامیت را بررسی کن؛ نسخه پشتیبان قابل‌خواندن یا حذف غیرمجاز نباشد.

۳۴.۳. Restore [جدید]

بازیابی را در محیط تست اجرا کن؛ داده و کنترل امنیتی کامل و در زمان مصوب برگردند.

۳۴.۴. Runbook [جدید]

دستورالعمل را اجرا یا مرور کن؛ بازیابی وابسته به دانش ثبت‌نشده نباشد.

۳۴.۵. کنترل پوشش

تمام شناسه‌های سند را مرور کن؛ مورد بی‌نتیجه بدون توضیح باقی نماند.

۳۴.۶. گزارش

محل، اثر، شاهد و اصلاح را ثبت کن؛ شدت به اثر واقعی متکی باشد.

۳۴.۷. بازآزمایی

آزمون اولیه و مسیرهای مرتبط را تکرار کن؛ اصلاح مؤثر و دورزدن شناخته‌شده بسته باشد.

۳۴.۸. پاک‌سازی نهایی

داده، فایل و تغییر آزمایشی را حذف کن؛ محیط به وضعیت توافق‌شده بازگردد.

ضمیمه ۱ • شروع Google و Shodan

عبارت DOMAIN و محدوده شبکه را فقط با هدف مجاز جایگزین کن. هر عبارت جدا اجرا شود.

```
site:DOMAIN
site:DOMAIN inurl:login
site:DOMAIN inurl:admin
site:DOMAIN inurl:swagger
site:DOMAIN intitle:"index of"
site:DOMAIN filetype:pdf
site:DOMAIN "stack trace"
site:DOMAIN "appsettings.json"
```

در Shodan، از نام میزبان یا گواهی شروع کن؛ IP و پورت فقط پس از تأیید تعلق وارد تست فعال شوند.

```
hostname:DOMAIN
ssl.cert.subject.cn:DOMAIN
net:AUTHORIZED_CIDR
```

برای هر سرنخ: منبع، زمان مشاهده، دامنه یا IP، شرح مشاهده و وضعیت تأیید را ثبت کن. فایل با نام حساس ممکن است صرفاً در متن ذکر شده باشد.

ضمیمه ۲ • روش عمومی Burp

۱. در Proxy و HTTP History، درخواست سالم را پیدا کن.

۲. درخواست را به Repeater بفرست و پاسخ پایه را نگه دار.

۳. فقط عامل مرتبط با آزمون را تغییر بده؛ سپس پاسخ و اثر واقعی را بررسی کن.

۴. برای آزمون دسترسی، زمینه هویت را جدا نگه دار؛ برای کنترل مرورگر، نتیجه را در مرورگر تأیید کن.

۵. اسکن فعال را فقط روی مسیر انتخاب‌شده و داخل محدوده اجرا کن؛ یافته را دستی تأیید کن.

ضمیمه ۳ • ثبت نتیجه هر کنترل

۱. شناسه کنترل و عنوان: .....

۲. دارایی، مسیر و نسخه: .....

۳. تاریخ، محیط و سطح دسترسی: .....

۴. پیش‌شرط و درخواست پایه: .....

۵. تغییر اعمال‌شده و مراحل تکرار: .....

۶. نتیجه مورد انتظار: .....

۷. نتیجه مشاهده‌شده و شاهد: .....

۸. وضعیت: آزمون‌نشده / قبول / مردود / نامرتبط با دلیل

۹. اثر، شدت و مرجع مرتبط: .....

۱۰. اصلاح و مسئول پیگیری: .....

۱۱. نسخه و نتیجه بازآزمایی: .....

نام‌گذاری پیشنهادی شاهد: شناسه کنترل + تاریخ + نوع شاهد. اطلاعات ورود و داده حساس را پیش از اشتراک‌گذاری پاک یا ماسک کن.

نکات تفسیر نتیجه

۱. پاسخ ۲۰۰ به‌تنهایی موفقیت عملیات نیست؛ تغییر وضعیت را بررسی کن.

۲. پاسخ ۴۰۳ به‌تنهایی کافی نیست؛ اثر جانبی یا مسیر جایگزین را بررسی کن.

۳. نبود هشدار Burp اثبات امنیت نیست.

۴. مخفی‌کردن فناوری جایگزین رفع آسیب‌پذیری نیست.

۵. حضور HEAD، HTTP/1.1 یا OPTIONS به‌تنهایی نقص نیست.

۶. CSP Report-Only فقط گزارش می‌دهد؛ آن را سیاست مسدودکننده محسوب نکن.

۷. نتیجه عمومی نامرتبط با فناوری موجود، با دلیل کنار گذاشته شود.

ضمیمه ۴ • مرجع‌ها و اختلاف اسناد

۱. فایل Client Check List(1).txt: سابقه کنترل‌ها و اصلاحات کلاینت؛ تأیید تازه نسخه مستقر نیست.

۲. فایل backend Check List(1).txt: کنترل‌ها، موارد باز و نیازمند تأیید بک‌اند؛ قواعد اختصاصی در این سند عمومی شده‌اند.

۳. OWASP Application Security Verification Standard 4.0.3: مبنای V1 تا V14 و راهنمای ارزیابی.

۴. OWASP Secure Coding Practices، نسخه 2.0.1، دسامبر ۲۰۲۲: مبنای SCP و کنترل‌های توسعه امن.

۵. OWASP Top 10:2025: نگاشت موضوعی ریسک‌ها، نه فهرست کامل روش‌های تست.

ASVS 4.0.3 در این سند به‌دلیل نسخه فایل ارسالی استفاده شده و ادعای آخرین نسخه نیست.

توصیه‌های SCP درباره تغییر دوره‌ای رمز، محدودیت Paste و منع نشست همزمان با ASVS یکسان نیستند. این‌ها الزام عمومی تجمیعی نشده‌اند؛ مبنای انتخابی و استثنای سیاست باید ثبت شود.

سقف حجم، طول رمز، نرخ و عمر نشست از سیاست و سطح انتخابی تعیین شوند؛ عدد اختصاصی فایل قبلی به همه پروژه‌ها تعمیم داده نشده است.

OWASP Top 10:2025

ASVS v4.0.3

OWASP Secure Coding Practices

Shodan Filters

Google Search Operators

ضمیمه ۵ • نگاشت Top 10:2025

۱. A01 — کنترل دسترسی شکسته: مجوز، جداسازی داده، CSRF و کنترل مقصد.

۲. A02 — پیکربندی ناامن: سرویس، وب‌سرور، مرورگر و واسطه‌ها.

۳. A03 — شکست زنجیره تأمین: منشأ بسته، وابستگی و Pipeline.

۴. A04 — شکست رمزنگاری: TLS، کلید، Secret و حفاظت داده.

۵. A05 — تزریق: ورودی به مفسر، Query، قالب یا خروجی اجرایی.

۶. A06 — طراحی ناامن: جریان کسب‌وکار، سهمیه و کنترل سوءاستفاده.

۷. A07 — شکست احراز هویت: ورود، بازیابی، MFA، نشست و Token.

۸. A08 — شکست تمامیت نرم‌افزار یا داده: امضا، Artifact، پیام و Deserialization.

۹. A09 — شکست لاگ و هشدار: ثبت، حفاظت، تشخیص و اطلاع‌رسانی رخداد.

۱۰. A10 — مدیریت نادرست شرایط استثنایی: خطا، شکست امن، پاک‌سازی و وضعیت ناسازگار.

> یک کنترل ممکن است چند دسته را پوشش دهد. برچسب دسته به‌تنهایی شدت یافته را تعیین نمی‌کند؛ علت، مسیر سوءاستفاده و اثر واقعی باید ثبت شوند.