OWASP Mobile Application Security Verification Standard 1.3

OWASP Open Web Application Security Project | Standard

MASVS

Mobile Application Security Verification Standard

(Persian Translation)

Carlos Holguera, Bernhard Müller,
Sven Schleier and Jeroen Willemsen

Version 1.3

OWASP Mobile Application Security Verification Standard

Version 1.3 May 13, 2021

Table of Content

پیشگفتار

انقلاب‌های فناورانه می‌توانند به‌سرعت اتفاق بیفتند. کمتر از یک دهه قبل، گوشی‌های هوشمند دستگاه‌های سنگین و عجیب با صفحه‌کلیدهای کوچک و ابزاری گران قیمت برای کاربران تجاری با دانش بالا بودند. امروزه، گوشی‌های هوشمند یک بخش ضروری از زندگی ما را تشکیل می‌دهند. ما برای اطلاعات، مسیریابی و ارتباطات به آنها وابسته شده‌ایم و آنها، هم در زندگی تجاری و هم در زندگی اجتماعی ما حاضر هستند.

هر تکنولوژی جدید خطرات امنیتی جدیدی را به‌وجود می‌آورد و یکی از چالش‌های عمده‌ای که صنعت امنیت با آن مواجه است، وفق یافتن با این تغییرات است. همواره جبهه‌ی دفاعی چند قدم عقب‌تر است. برای مثال، واکنش پیش‌فرض خیلی از افراد، به‌کارگیری شیوه‌های قدیمی در انجام کارها است: گوشی‌های هوشمند همانند کامپیوترهای کوچک و برنامه‌های کاربردی موبایل دقیقا همانند نرم‌افزارهای کلاسیک هستند، بنابراین به‌طور حتم باید بتوان نتیجه گرفت که الزامات امنیتی گوشی‌های هوشمند و کامپیوترها یکسان است. اما این فرضیه درست نیست. سیستم‌عامل‌های گوشی‌های هوشمند و کامپیوترهای رومیزی با یکدیگر متفاوت هستند و برنامه‌های کاربردی موبایل نیز با برنامه‌های تحت وب تفاوت دارند. برای مثال، شیوه‌ی کلاسیک مبتنی بر امضاء، کاربردی جهت پویش ویروس در سیستم‌عامل‌های نوین موبایل ندارد؛ این شیوه نه تنها با مدل توزیع شده‌ی برنامه‌ی کاربردی موبایل ناسازگار است، بلکه به‌دلیل محدودیت‌های sandboxing، از نظر فنی نیز غیرممکن می‌باشد. همچنین بعضی از انواع آسیب‌پذیری مانند سرریز بافر و مشکلات XSS، مطابقت کم‌تری با برنامه‌های عادی حوزه‌ی موبایل دارند و بیش‌تر در برنامه‌های کامپیوتری و برنامه‌های تحت وب موضوعیت پیدا می‌کنند (البته با در نظر گرفتن استثنائات).

با گذشت زمان، صنعت ما درک بهتری از مخاطرات و تهدیدات در حوزه‌ی موبایل پیدا کرده است. همانطور که مشخص است، موضوع امنیت موبایل، تماما درخصوص محافظت از داده است: برنامه‌ها، اطلاعات خصوصی ما شامل تصاویر، فایل‌های ضبط‌شده‌ی صوتی، یادداشت‌ها، اطلاعات حساب، اطلاعات تجاری، موقعیت مکانی و بسیاری چیزهای دیگر را ذخیره می‌کنند. آنها همانند کاربرانی که ما را جهت انجام خدماتی که روزانه استفاده می‌کنیم به سرویس‌ها متصل می‌کنند، و همانند مراکز ارتباطاتی که همه‌ی پیام‌های مبادله شده ما با دیگران را پردازش می‌کنند، عمل می‌نمایند. برای دسترسی بدون فیلتر به زندگی شخصی یک فرد فقط کافی است گوشی هوشمند او را تحت کنترل بگیرید. وقتی در نظر داشته باشیم که دستگاه‌های تلفن همراه به‌راحتی گم شده و یا سرقت می‌شوند و تعداد بدافزارهای موبایل رو به افزایش هستند، نیاز به حفاظت از داده‌ها بیشتر مشخص می‌شود.

بنابراین یک استاندارد امنیتی برای برنامه‌های کاربردی موبایل، باید بر چگونگی مدیریت، ذخیره و حفاظت از اطلاعات حساس توسط برنامه‌های موبایل تمرکز کند. اگرچه سیستم‌عامل‌های مدرن موبایل مانند iOS و اندروید، هایAPI خوبی برای ذخیره امن داده‌ها و ارتباطات امن پیشنهاد داده‌اند، اما برای موثر واقع‌شدن، هاAPI باید به‌طور صحیح پیاده‌سازی و استفاده شوند. ذخیره‌سازی داده، ارتباطات بین برنامه‌ای، استفاده مناسب از هایAPI رمزنگاری و ارتباطات امن شبکه تنها بخشی از جنبه‌هایی هستند که نیاز به توجه دقیق دارند.

پرسش مهمی که به موافقت همگانی در صنعت نیاز دارد این است که در حفاظت از محرمانگی و صحت داده تا کجا باید پیش رفت. به‌عنوان مثال، اغلب ما موافق هستیم که یک برنامه‌ی کاربردی موبایل باید گواهی سرور را در مبادله TLS اعتبارسنجی نماید. اما در مورد سازوکار امنیتی SSL pinning certificate چطور؟ آیا عدم استفاده از آن منجر به بروز آسیب‌پذیری می‌شود؟ آیا استفاده از این سازوکار باید در برنامه‌هایی که داده‌های حساس مدیریت می‌کنند الزام گردد؟ یا ممکن است حتی نتیجه‌ی معکوس دهد؟ آیا نیاز داریم تا داده‌های ذخیره‌شده در پایگاه‌های داده‌ی SQLite را حتی اگر سیستم‌عامل، برنامه را محصور کند، رمز کنیم؟ چیزی که برای یک برنامه مناسب است ممکن است برای برنامه‌ای دیگر ناکارآمد باشد. MASVS تلاشی است برای استانداردسازی این الزامات با بهره‌گیری از سطوح وارسی متناسب با سناریوهای تهدیدات متنوع.

علاوه‌بر این، ظهور بدافزار root و ابزارهای مدیریت از راه دور باعث ایجاد آگاهی در مورد این واقعیت شده است که خود سیستم‌عامل‌های موبایل دارای رخنه‌های امنیتی قابل بهره‌برداری هستند، درنتیجه استراتژی‌های کانتینریزاسیون برای محافظت بیشتر از داده‌های حساس و جلوگیری از دست‌کاری در سمت کاربر، به‌صورت فزاینده‌ای مورد استفاده قرار می‌گیرند. اینجاست که همه چیز پیچیده می‌شود. ویژگی‌های امنیتی مربوط به سخت‌افزار و راهکارهای کانتینریزاسیون در سطح سیستم‌عامل مانند Work for Android و Knox Samsung وجود دارند اما به‌طور یکنواخت برای دستگاه‌های مختلف در دسترس نیستند. یک راهکار موقت، امکان پیاده‌سازی معیارهای محافظتی مبتنی بر نرم‌افزار است اما متاسفانه هیچ استاندارد یا فرآیند تستی برای وارسی چنین محافظت‌هایی وجود ندارد.

نتیجه آنکه، گزارشات آزمون امنیت برنامه‌ی کاربردی موبایل همه‌جا قابل‌دسترس هستند؛ برای مثال برخی آزمونگرها عدم مبهم‌سازی(Obfuscation) کد یا تشخیص root بودن دستگاه در یک برنامه‌ی کاربردی اندروید را به‌عنوان «حفره‌ی امنیتی» گزارش می‌کنند. از طرف دیگر، معیارهای دیگری مانند رمزنگاری رشته، تشخیص debugger یا مبهم‌سازی(Obfuscation) جریان کنترل برنامه، اجباری در نظر گرفته نمی‌شوند. از آنجایی که تاب‌آوری یک مفهوم صفر و یکی نیست و این نوع دیدگاه به مسائل نیز منطقی نمی‌باشد: این وابسته به تهدیدات مشخص در سمت کاربر است که باید با آن مقابله شود. محافظت‌های نرم‌افزاری بی‌فایده نیستند اما نهایتا ممکن است دور زده شوند، درنتیجه هیچ‌گاه نباید به‌عنوان جایگزینی برای کنترل‌های امنیتی استفاده شوند.

هدف کلی استاندارد MASVS، ارائه‌ی مبانی اولیه برای امنیت برنامه‌ی کاربردی موبایل (استاندارد سطح-MASVS یک)، همچنین دربرگیرنده‌ی معیارهای دفاع در عمق (استاندارد سطح-MASVS دو) و محافظت‌هایی در برابر تهدیدات سمت کاربر (استاندارد مهندسی-MASVS معکوس) است. MASVS به‌دنبال دستیابی به موارد زیر است:

- فراهم آوردن الزامات برای معمارهای نرم‌افزار و توسعه‌دهندگانی که به‌دنبال توسعه‌ی امن برنامه‌های کاربردی موبایل هستند؛
- پیشنهاد یک استاندارد صنعتی که بتواند در بازبینی‌های امنیتی برنامه‌ی کاربردی موبایل، مورد آزمون قرار گیرد؛
- تبیین نقش سازوکارهای محافظتی نرم‌افزار در امنیت برنامه‌های کاربردی موبایل و تهیه‌ی الزامات به‌منظور وارسی میزان موثر بودن آنها؛
- ارائه‌ی توصیه‌های ویژه، متناظر با هر یک از سطوح امنیتی برای کاربردهای گوناگون.

می‌دانیم که دستیابی به رضایت 100٪ در صنعت غیرممکن است. با این‌وجود امیدواریم که استاندارد MASVS در فراهم آوردن دستورالعمل راهنما در همه‌ی مراحل توسعه و آزمون برنامه‌ی کاربردی موبایل مفید واقع شود. MASVS به‌عنوان یک استاندارد متن‌باز، در طول زمان تکامل پیدا خواهد کرد و در همین راستا از هر پیشنهاد و مشارکتی استقبال می‌کنیم.

توسط Mueller Bernhard

درباره‌ی استاندارد

به استاندارد وارسی امنیت برنامه‌ی کاربردی موبایل (MASVS) نسخه 1.1 خوش آمدید. MASVS یک تلاش جمعی برای برپاسازی چارچوبی از الزامات امنیتی مربوط به طراحی، توسعه و آزمون برنامه‌های کاربردی امن موبایل بر روی iOS و اندروید است.

MASVS نقطه اوج یک تلاش جمعی و بازخورد صنعت است. ما انتظار داریم که این استاندارد در طی زمان تکامل پیدا کرده و از بازخورد اجتماع استقبال می‌کنیم.

بهترین راه برای ارتباط با ما از طریق کانال Slack پروژه موبایل OWASP است: https://owasp.slack.com/messages/project-mobile_omtg/details/ .

حساب‌های کاربری می توانند در این آدرس ایجاد شوند: https://owasp.slack.com/join/shared_invite/zt-g398htpy-AZ40HOM1WUOZguJKbblqkw#/.

حق تکثیر و مجوز

تشکر و قدردانی

رهبر پروژه	نویسنده اصلی	مشارکت کنندگان و ویراستاران
Carlos and Schleier Sven Holguera	Bernhard Sven Mueller, Schleier, Jeroen Willemsen Carlos and Holguera	Jeroen Artem, Bachevsky Ali, Elderov Aleksey, Mesheryakov Antukh, Alexander Chilcutt, Will Cheney, Ben Clochard, Damien Boer, de Jon-Anthoney Beckers, Dewhurst, Ryan Denis, Ratchenko Delgado, Manuel Corbiaux, Stephen Langkemper, Sjoerd Grossman, Josh Glezman, Anton Gardiner, Ben @empty_jack, @PierrickV, Martelloni, Roberto Marsicano, Martin Marangoni, Henrique Vin□cius Sejpal, Abhinav Ruiz, Javier Rafii, Mehrad Orobator, Andrew Potapenko, Julia Shrivastava, Anant Soni, Nikhil Singh, Prabhant Sharma, Yogesh Seys, Stefaan Wierzbicki Lukasz Thomas, Pauchard Temmar, Abdessamad Stillavato, Francesco

زبان	مترجمان و ویراستاران
چینی (سنتی)	Wang Leo Hu, Henry Chien, Lex Chi, Peter
چینی (ساده‌شده)	S Jack Zang, Harold Peng, Bob
فارسی	Mehran Mazhari, Alireza Omidvar, Mahsa Azhirak, Dorna Akbari, Bardiya Salimian, Hamed Atefinia, Ramin Khoshdel Milad Seifalinia,
فرانسوی	(Review) Dong Christian Aftahi, Abderrahmane Szkudlarek, Romuald
آلمانی	(Review) Schleier Sven Gr□nitz, Rocco
هندی	Shah Vikrant Sinha, Kumar Devendra Dave, Parag Kunwar, Atul Kumar, Ritesh Sharma, Mukesh
ژاپنی	(Review) Okada Riotaro Takeyama, Koki
کره‌ای	Sung Jiyeon Han, Jiyou Cho, Jeongwon Jeon, Youngjae
روسی	Dmitry Tereshin (Review), Egor Oprya (Review), Vladislav Chelnokov Martynov, Eugen Maxim, Gall (Review)
اسپانیایی	Holguera Carlos Marsicano, Martin
پرتغالی (برزیلی)	Galves Fernando Ariza, Maur□cio Araujo, Rodrigo Junior, Humberto Polastro, Mateus
پرتغالی	Dias S□nia Fontes, Luis Gomes, Filipa Nogueira, Fernando Mota, Filipa Ana

این سند به‌عنوان یک fork از استاندارد وارسی برنامه‌ی کاربردی موبایل نوشته شده توسط Manico Jim آغاز شده است.

حامیان

با اینکه هر دو استاندارد MASVS و MSTG به‌طور داوطلبانه توسط جامعه تولید و نگهداری می‌شوند، اما گاهی اوقات به اندکی کمک خارجی نیاز است. بنابراین، از حامیان مالی‌مان بخاطر فراهم آوردن بودجه برای استخدام ویراستارهای فنی تشکر می‌کنیم. توجه داشته باشید که حمایت مالی آنان محتوای استاندارد MASVS یا MSTG را تحت تأثیر قرار نمی‌دهد. بسته‌های حمایت مالی در Wiki Project OWASP شرح داده‌شده‌اند.

نیکوکاران محترم

در ادامه مایلیم از Chapter Area Bay OWASP به خاطر حمایتشان قدردانی نماییم. در پایان مایلیم از تمام کسانی که کتاب را از Leanpub خریداری کرده و ما را حمایت کردند تشکر و قدردانی نماییم.

استاندارد وارسی امنیت برنامه‌ی کاربردی موبایل

از استاندارد MASVS می‌توان برای ایجاد سطحی از اطمینان در امنیت برنامه‌های کاربردی موبایل استفاده نمود. الزامات با در نظر گرفتن رسیدن به اهداف زیر توسعه داده شده‌اند:

- استفاده به‌عنوان معیار اندازه‌گیری - به‌منظور ارائه‌ی استاندارد امنیتی که بوسیله‌ی آن برنامه‌های کاربردی موجود موبایل بتوانند توسط توسعه‌دهندگان و مالکان آن‌ها مقایسه شوند؛
- استفاده به‌عنوان راهنما - به‌منظور ارائه‌ی راهنمایی در طول تمام مراحل توسعه و تست برنامه‌ی کاربردی موبایل؛
- قابل استفاده بودن در مدت تهیه - به‌منظور ارائه‌ی مبنایی برای وارسی امنیت برنامه‌ی کاربردی موبایل.

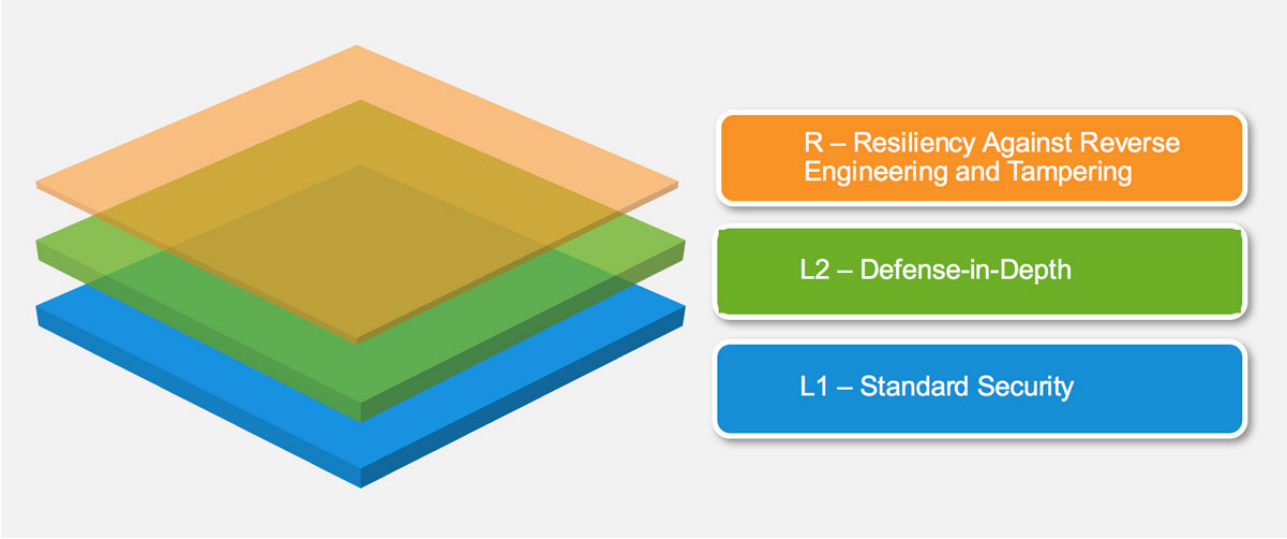
مدل AppSec موبایل

استاندارد MASVS دو سطح وارسی امنیت (MASVS-L1 و MASVS-L2) را در کنار مجموعه‌ای از الزامات تاب‌آوری مهندسی معکوس (MASVS-R)، تعریف می‌کند. MASVS-L1 شامل الزامات کلی امنیتی است که برای همه‌ی برنامه‌های کاربردی موبایل توصیه شده‌اند، درحالی‌که MASVS-L2 باید برای برنامه‌هایی که با داده‌های بسیار حساس سر و کار دارند اعمال شود. MASVS-R کنترل‌های محافظتی بیشتری را نیز پوشش می‌دهد و در صورتی می‌تواند اعمال شود که هدف از طراحی، جلوگیری از تهدیدات سمت کاربر باشد.

نتیجه انجام الزامات موجود در MASVS-L1 یک برنامه امن می‌شود که بهترین رویه‌های امنیتی را دنبال می‌کند و از آسیب‌پذیری‌های رایج ضرری نمی‌بیند. MASVS-L2 نیز کنترل‌های دفاع در عمق بیشتری از قبیل SSL pinning را می‌افزاید که نتیجه آن برنامه ای مقاوم در برابر حملات پیچیده می‌باشد - با این فرض که کنترل‌های امنیتی سیستم‌عامل موبایل دست‌نخورده باشد و کاربر نهایی به‌عنوان دشمنی بالقوه در نظر گرفته نشده باشد. انجام تمامی الزامات محافظتی در MASVS-R و یا زیرمجموعه‌هایی از آن، به جلوگیری از تهدیدات خاص سمت کاربر، درجایی که کاربر نهایی مخرب یا سیستم‌عامل موبایل در معرض خطر باشد، کمک می‌کند.

الف: اگرچه ما پیاده‌سازی کنترل‌های موجود در MASVS-L1 را در هر برنامه‌ای توصیه می‌کنیم، اما پیاده‌سازی کردن یا نکردن آن در نهایت باید یک تصمیم مخاطره محور باشد که توسط صاحبان کسب‌وکار گرفته می‌شود.

ب: توجه داشته باشید که کنترل‌های محافظت نرم‌افزار که در MASVS-R فهرست شده‌اند و در راهنمای آزمون امنیت موبایل OWASP شرح داده‌شده‌اند، در نهایت می‌توانند دور زده شوند و هیچ‌گاه نباید به‌عنوان جایگزینی برای کنترل‌های امنیتی، مورداستفاده قرار گیرند. در عوض، هدف آن افزودن کنترل‌های محافظتی تهدیدات خاص به برنامه‌های کاربردی است که الزامات استاندارد MASVS در MASVS-L1 یا MASVS-L2 را نیز انجام می‌دهد.



ساختار سند

بخش نخست استاندارد MASVS شامل توضیحاتی در خصوص مدل امنیت و سطوح وارسی در دسترس می‌باشد، که با توصیه‌هایی در خصوص نحوه‌ی استفاده عملی از استاندارد همراه شده است. جزئیات الزامات امنیتی، به همراه نگاشت آنها به سطوح وارسی، در بخش دوم فهرست شده‌اند. الزامات ها بر اساس اهداف/چارچوب فنی به هشت دسته (V1 تا V8) طبقه‌بندی‌شده‌اند. نام‌گذاری زیر در کل استاندارد MASVS و MSTG استفاده شده است.

- طبقه‌بندی الزامات: MASVS-Vx، به‌عنوان‌مثال: MASVS-V2 ذخیره‌سازی داده و حریم خصوصی
- الزام: MASVS-Vx.y، به‌عنوان‌مثال: MASVS-V2.2 هیچ اطلاعات حساسی در لاگ‌های برنامه نوشته نشده است.

جزئیات سطوح وارسی

MASVS-L1: امنیت استاندارد

برنامه‌ی کاربردی موبایلی که استاندارد MASVS-L1 را کسب می‌کند به بهترین رویه‌های امنیتی برنامه‌ی کاربردی موبایل پایبند می‌شود. این موضوع، الزامات پایه‌ای در خصوص کیفیت کد، مدیریت داده‌های حساس و تعامل با محیط موبایل را محقق می‌کند. به‌منظور وارسی کنترل‌های امنیتی باید یک فرآیند آزمون طی شود. این سطح برای همه‌ی برنامه‌های کاربردی موبایل مناسب است.

MASVS-L2: دفاع در عمق

MASVS-L2 کنترل‌های امنیتی پیشرفته‌ای را ارائه می‌دهد که فراتر از الزامات استاندارد است. برای تحقق الزامات MASVS-L2 باید یک مدل تهدید وجود داشته باشد و امنیت بایستی بخش جدایی‌ناپذیری از معماری و طراحی برنامه کاربردی موبایل باشد. بر اساس مدل تهدید، باید موارد کنترلی مناسبی در MASVS-L2 انتخاب و با موفقیت پیاده‌سازی می‌شدند. این سطح برای برنامه‌های کاربردی که داده‌های بسیار حساس را مدیریت می‌کنند، مانند برنامه‌های بانکی موبایل مناسب است.

MASVS-R: تاب‌آوری در برابر مهندسی معکوس و دست‌کاری

برنامه‌ی کاربردی دارای فناوری امنیتی پیشرفته و به روز است، همچنین در برابر حملات خاص و شناخته‌شده‌ی سمت کاربر مانند دست‌کاری، تعدیل یا مهندسی معکوس برای استخراج کد یا داده‌های حساس، منعطف است. چنین برنامه‌ای از ویژگی‌های امنیتی سخت‌افزاری یا تکنیک‌های قوی و تایید شده‌ی محافظت از نرم‌افزار بهره می‌گیرد. MASVS-R در برنامه‌های کاربردی که داده‌های بسیار حساس را مدیریت می‌کنند، کاربرد دارد و می‌تواند به‌عنوان وسیله‌ای برای محافظت از مالکیت معنوی یا اثبات دست‌کاری یک برنامه‌ی کاربردی، مورد استفاده قرار گیرد.

کاربرد توصیه‌شده

برنامه‌های کاربردی را می‌توان بر اساس ارزیابی مخاطره قبلی و سطح کلی امنیت موردنیاز، مطابق با MASVS سطح L1 یا L2 وارسی نمود. L1 برای همه‌ی برنامه‌های موبایل قابل‌اجرا است، درحالی‌که L2 به‌طورکلی برای برنامه‌های کاربردی‌ای توصیه می‌شود که داده یا کاربرد حساس‌تری را مدیریت می‌نمایند. MASVS-R (یا بخش‌هایی از آن) را می‌توان برای اثبات تاب‌آوری در برابر تهدیدات خاص، مانند بسته‌بندی مجدد یا استخراج داده‌های حساس و افزون بر آن در وارسی امنیتی مناسب استفاده نمود.

به‌طور خلاصه، انواع وارسی‌های موجود، به‌شرح زیر می‌باشند:

- MASVS-L1
- MASVS-L1+R
- MASVS-L2
- MASVS-L2+R

ترکیب‌های مختلف، درجه‌های متفاوتی از امنیت و تاب‌آوری را منعکس می‌کنند. هدف آن است که امکان تاب‌آوری فراهم گردد: برای مثال، یک بازی موبایل ممکن است اضافه کردن کنترل‌های امنیتی ،MASVS-L2 مانند احراز هویت دو عاملی را به دلایل مرتبط با کاربردپذیری تضمین نکند، اما نیاز تجاری شدیدی برای جلوگیری از دست‌کاری داشته‌باشد.

کدام نوع وارسی باید انتخاب گردد

پیاده‌سازی الزامات MASVS L2 باعث افزایش امنیت می‌شود، درعین‌حال که هزینه‌ی توسعه را افزایش می‌دهد و به‌طور بالقوه تجربه‌ی کاربر نهایی را بدتر می‌کند (این همان فرآیند قدیمی است که در آن چیزی را به ازای چیز دیگری از دست می‌دهیم). سطح دو به‌طورکلی زمانی باید برای برنامه‌های کاربردی به‌کار گرفته شود که موازنه‌ی بین مخاطره و هزینه منطقی باشد (به‌عنوان‌مثال، ضرر بالقوه ناشی از به‌خطر انداختن محرمانگی یا یکپارچگی بالاتر از هزینه‌ی ایجادشده به‌واسطه‌ی کنترل‌های امنیتی اضافی است). ارزیابی مخاطره باید نخستین گام پیش از به‌کارگیری استاندارد MASVS باشد.

مثال‌ها

MASVS-L1

- همه‌ی برنامه‌های کاربردی موبایل. MASVS-L1 بهترین رویه‌های موجود که تاثیری منطقی بر هزینه‌ی توسعه و تجربه کاربری را به همراه دارد، فهرست می‌کند. الزامات موجود در MASVS-L1 را برای هر برنامه‌ای که واجد شرایط سطوح بالاتر نیست، اعمال نمایید.

MASVS-L2

- صنعت خدمات بهداشت و درمان: برنامه‌های موبایل که اطلاعات شخصی قابل‌شناسایی را ذخیره می‌نمایند، می‌توانند در سرقت هویت، پرداخت‌های جعلی یا انواع طرح‌های کلاه‌برداری مورداستفاده قرار گیرند. در بخش خدمات بهداشت و درمان ایالات‌متحده، ملاحظات قانونی مطلوب، شامل قانون انتقال و پاسخ‌گویی الکترونیک بیمه‌ی سلامت (HIPAA)، حریم خصوصی، امنیت، قوانین اعلان رخنه و قانون ایمنی بیمار است.
- صنعت مالی: برنامه‌های کاربردی که دسترسی به اطلاعات بسیار حساس مانند شماره‌ی کارت‌های اعتباری و اطلاعات شخصی دارند و یا به کاربر اجازه‌ی انتقال وجه می‌دهند. این برنامه‌های کاربردی، کنترل‌های امنیتی بیشتری را برای جلوگیری از کلاه‌برداری ضمانت می‌کنند. برنامه‌های مالی باید مطابقت با استاندارد امنیت داده‌ی صنعت پرداخت کارتی (PCI DSS)، قانون Bliley Leech Gramm و قانون Sarbanes-Oxley (SOX) را تضمین کنند.

L1+R MASVS

- برنامه‌های کاربردی موبایل که در آن‌ها حفاظت از مالکیت معنوی (IP) یک هدف تجاری است. کنترل‌های تاب‌آوری فهرست شده در MASVS-R می‌توانند برای دشوار نمودن دستیابی به کد منبع اصلی و جلوگیری از دست‌کاری یا کرک شدن استفاده شوند.
- صنعت بازی: بازی‌هایی با نیاز ضروری به مقابله با تعدیل و تقلب، همانند بازی‌های آنلاین رقابتی. تقلب مسئله‌ی مهمی در بازی‌های آنلاین است چراکه تعداد زیاد متقلبان منجر به نارضایتی بازیکنان دیگر می‌شود و در نهایت می‌تواند موجب شکست یک بازی گردد. MASVS-R کنترل‌های پایه‌ای ضد دست‌کاری را فراهم می‌آورد که به دشوار سازی فرآیند تقلب کمک می‌کند و افزایش تلاش متقلبان را به‌همراه دارد.

L2+R MASVS

- صنعت مالی: برنامه‌های کاربردی بانکداری آنلاین که به کاربر امکان انتقال وجوه را می‌دهند، محیطی هستند که در آن‌ها روش‌هایی همچون تزریق کد و انجام فرآیند بانکی با استفاده از دستگاه‌های آلوده شده، مخاطره آمیز است. در این مورد، کنترل‌های موجود در MASVS-R می‌توانند به‌عنوان مانعی برای دست‌کاری و به دنبال آن افزایش فشار بر روی سازندگان بدافزار، به‌کار گرفته شوند.
- همه‌ی برنامه‌های موبایل که با توجه به طراحی‌شان، نیاز به ذخیره‌ی داده‌های حساس در دستگاه همراه دارند و درعین‌حال باید از طیف گسترده‌ای از دستگاه‌ها و نسخه‌های سیستم‌عامل پشتیبانی کنند. در این حالت، می‌توان از کنترل‌های تاب‌آوری به‌عنوان یک تکنیک دفاع در عمق برای دشوار نمودن تلاش مهاجمانی استفاده نمود که قصد استخراج داده‌های حساس را دارند.
- برنامه‌هایی که دارای خریدهای درون برنامه‌ای هستند باید به‌طور ایده‌آل از کنترل‌های سمت سرور و MASVS-L2 برای محافظت از محتوای پرداخت استفاده نمایند. اما مواردی ممکن است وجود داشته باشند که امکان محافظت از سمت سرور وجود نداشته باشد. در آن موارد، کنترل‌های استاندارد MASVS-R باید به‌منظور دشوار سازی مهندسی معکوس و دست‌کاری برنامه اعمال شوند.

ارزیابی و گواهی

دیدگاه OWASP در مورد گواهینامه‌های استاندارد MASVS و نمادهای اعتماد الکترونیکی

OWASP، به‌عنوان یک سازمان غیرانتفاعی بی‌طرف، هیچ فروشنده، ممیز یا نرم‌افزاری را تأیید نمی‌نماید.

کلیه‌ی دعاوی ضمانتی، نمادهای اعتماد الکترونیکی یا گواهینامه‌ها به‌طور رسمی موردبررسی، ثبت یا تأیید OWASP قرار نگرفته‌اند، بنابراین یک سازمان با اتکا بر چنین دیدگاهی بایستی نسبت به اعتماد به هر شخص ثالث یا هر نماد اعتماد الکترونیکی مدعی ارائه‌ی گواهینامه‌ی (M)ASVS هوشیار باشد.

این موضوع نباید سازمان‌ها را از ارائه‌ی چنین خدمات ضمانتی‌ای مادامی‌که ادعای ارائه‌ی گواهینامهٔ رسمی OWASP را نمی‌کنند، بازدارد.

راهنمای صدور گواهینامه برای برنامه‌های کاربردی موبایل

روش توصیه‌شده به‌منظور وارسی انطباق یک برنامه‌ی کاربردی موبایل با استاندارد MASVS، انجام بازبینی به شیوه‌ی «کتاب‌باز» است، به این معنی که به آزمونگرها اجازه‌ی دسترسی به منابع کلیدی از جمله معماران و توسعه‌دهندگان برنامه‌ی کاربردی، مستندات پروژه، کد منبع و دسترسی تأیید شده به پایانه شامل دسترسی به حداقل یک حساب کاربری برای هر نقش، داده می‌شود.

لازم به ذکر است که استاندارد MASVS تنها امنیت (سمت کاربر) برنامه‌ی کاربردی موبایل و ارتباطات شبکه‌ای بین برنامه‌ی کاربردی و پایانه‌های راه دور، همچنین تعداد کمی از الزامات اولیه و کلی مربوط به احراز هویت کاربر و مدیریت نشست را پوشش می‌دهد. این استاندارد شامل الزامات مشخصی برای سرویس‌های از راه دور (مثلاً سرویس‌های وب) مربوط به برنامه‌ی کاربردی می‌باشد، به‌طوری‌که مجموعه‌ی محدودی از الزامات کلی مربوط به مدیریت نشست و احراز هویت را در برمی‌گیرد. بااین‌حال، بخش V1 استاندارد MASVS مشخص می‌نماید که خدمات از راه دور، باید تحت پوشش مدل تهدید کلی قرار بگیرند و با استانداردهای مناسبی همچون ASVS OWASP وارسی شوند.

سازمان صادرکننده‌ی گواهینامه باید در هر گزارش، دامنه‌ی وارسی (به‌ویژه اگر مؤلفه‌ی کلیدی خارج از محدوده باشد) و خلاصه‌ای از یافته‌های وارسی شامل آزمون‌های موفق و ناموفق، به همراه راه‌حل‌های روشن در مورد چگونگی برطرف کردن آزمون‌های ناموفق را ارائه دهد. تهیه و نگهداری اوراق کاری حاوی جزئیات، تصاویر ضبط‌شده یا فیلم‌ها، قطعه کدهای بهره‌برداری مطمئن و قابل تکرار از آسیب‌پذیری، سوابق الکترونیکی آزمون مانند لاگ‌های شنود پروکسی و یادداشت‌های مربوطه مانند لیست پاک‌سازی، رویه‌ی استاندارد در صنعت شناخته می‌شود. اجرای یک ابزار و گزارش نقص‌ها به‌تنهایی کافی نیست؛ این امر شواهد کافی در مورد اینکه همه‌ی آسیب‌های در سطح صدور گواهینامه آزمایش شده‌اند و یا اینکه آیا این عمل به‌درستی انجام شده است، ارائه نمی‌دهد. در صورت بروز اختلاف، باید شواهد حمایتی کافی وجود داشته باشد تا مورد آزمایش قرار گرفتن هر الزام وارسی شده را اثبات نماید.

استفاده از راهنمای آزمون امنیت موبایل OWASP (استاندارد MSTG)

استاندارد MSTG OWASP دستورالعملی برای آزمون امنیت برنامه‌های کاربردی موبایل است. این استاندارد فرآیندهای فنی را به‌منظور وارسی الزامات فهرست شده در استاندارد MASVS شرح می‌دهد. استاندارد MSTG شامل فهرستی از موارد آزمون است که هرکدام به یک الزام در استاندارد MASVS نگاشت شده‌اند. الزامات استاندارد MASVS، سطح بالا و کلی هستند درحالی‌که استاندارد MSTG بر پایه‌ی هر سیستم‌عامل موبایل، توصیه‌ها و فرآیندهای آزمون را به‌طور عمیق ارائه می‌دهد.

نقش ابزارهای خودکار آزمون امنیتی

استفاده از پویشگرهای کد منبع و ابزارهای آزمون جعبه سیاه برای افزایش کارایی در هر زمان ممکنی توصیه می‌شود. با این حال، امکان وارسی الزامات استاندارد MASVS با استفاده از ابزارهای خودکار، به‌تنهایی امکان‌پذیر نیست. هر برنامه‌ی کاربردی موبایل متفاوت است و درک معماری کلی، منطق تجاری و مشکلات فنی تکنولوژی‌ها و فریمورک‌های استفاده‌شده در آن، یک الزام ضروری برای وارسی امنیت برنامهٔ کاربردی است.

سایر کاربردها

به‌عنوان راهنمای تفصیلی معماری امنیتی

یکی از کاربردهای رایج استاندارد وارسی امنیت برنامه‌ی کاربردی موبایل، فراهم آوردن منبعی برای معماران امنیت است. دو چارچوب مهم معماری امنیت، SABSA یا TOGAF، بسیاری از اطلاعاتی که برای تکمیل بازبینی‌های معماری امنیت برنامه‌های کاربردی موبایل ضروری است را در خود جای نداده‌اند. استاندارد MASVS می‌تواند برای پر کردن این‌گونه خلاءها مورد استفاده قرار گیرد و به معماران امنیت این اجازه را بدهد تا کنترل‌های بهتری را نسبت به آسیب‌های رایج برنامه‌های کاربردی موبایل اتخاذ نمایند.

به‌عنوان جایگزینی برای فهرست ملاحظات کدنویسی امن

بسیاری از سازمان‌ها می‌توانند با انتخاب یکی از دو سطح استاندارد MASVS یا انشعاب گرفتن از آن و ایجاد تغییر در دامنه‌ای خاص متناسب با سطح مخاطره‌ی هر برنامه، از این استاندارد بهره‌مند گردند. ما از این نوع انشعاب تا هر زمانی که قابلیت ردیابی حفظ گرد استقبال می‌کنیم، بنابراین اگر یک برنامه‌ی کاربردی الزام 4.1 را محقق ساخته باشد، این بدان معنا است که با تکامل استاندارد نسخه‌های منشعب نیز آن الزام را رعایت می‌کنند.

به‌عنوان پایه‌ای برای روش‌شناسی آزمون امنیتی

یک شیوه‌ی ارزنده‌ی آزمون امنیت برنامه‌ی کاربردی موبایل باید تمامی الزامات فهرست شده در استاندارد MASVS را پوشش دهد. راهنمای آزمون امنیتی موبایل OWASP (MSTG) موارد آزمون جعبه سیاه و جعبه سفید را برای هر الزام وارسی تشریح می نماید.

به‌عنوان راهنمایی برای انجام خودکار آزمون‌های واحد و یکپارچگی

استاندارد MASVS به‌استثنای الزامات معماری، بسیار آزمون‌پذیر طراحی شده است. آزمون‌های واحد، یکپارچه‌سازی و پذیرش، می‌توانند به‌صورت خودکار و مبتنی بر الزامات استاندارد MASVS، در چرخه‌ی پیوسته‌ی توسعه گنجانده شوند. این امر نه تنها آگاهی توسعه‌دهنده را نسبت به امنیت افزایش می‌دهد، بلکه کیفیت کلی برنامه‌های کاربردی حاصله را بهبود می‌بخشد و تعداد یافته‌ها را حین آزمون امنیت، در فاز قبل از عرضه به بازار کاهش می‌دهد.

برای آموزش توسعه ایمن

استاندارد MASVS می‌تواند برای تعریف مشخصه‌های یک برنامه‌ی کاربردی موبایل ایمن استفاده شود. بسیاری از دوره‌های «کد نویسی ایمن» در واقع همان دوره‌های هک قانونمند با نکات اندکی از کد نویسی هستند. این مورد به توسعه‌دهندگان کمکی نمی‌کند. در عوض، دوره‌های توسعه‌ی ایمن، به‌جای مثلاً «10 مشکل امنیتی رایج در کد نویسی»، می‌توانند از استاندارد MASVS، با تمرکز قوی بر کنترل‌های کنشگرایانه استفاده کنند.

V1: الزامات معماری، طراحی و مدل‌سازی تهدید

هدف کنترل

در یک دنیای ایده‌آل، امنیت در تمام مراحل توسعه‌ی برنامه باید در نظر گرفته شود. اما در واقعیت، امنیت اغلب در مرحله‌ی آخر چرخه‌ی حیات توسعه‌ی نرم‌افزار موردتوجه قرار می‌گیرد. علاوه‌بر کنترل‌های فنی، استاندارد وارسی امنیت برنامه‌ی کاربردی موبایل، نیاز به ایجاد فرایندهایی دارد که بتوان از مورد توجه بودن امنیت در زمان برنامه‌ریزی معماری برنامه‌ی موبایل و شناخت وظیفه‌مندی‌های اصلی و امنیتی مؤلفه‌ها اطمینان حاصل نمود. از آنجایی که بسیاری از برنامه‌های موبایل به‌عنوان سرویس‌دهنده از راه دور عمل می‌کنند، باید از اعمال استانداردهای امنیتی مناسب برای آن سرویس‌ها اطمینان حاصل نمود - تست برنامه‌ی موبایل در محیط ایزوله کافی نیست.

دسته‌بندی V1، الزامات مرتبط با فاز معماری و طراحی برنامه‌ی کاربردی موبایل را فهرست می‌نماید. به این ترتیب، این تنها دسته‌بندی‌ای است که به موارد آزمون فنی در راهنمای آزمودن برنامه‌ی کاربردی موبایل OWASP نگاشت نمی‌شود. برای پوشش موضوعاتی مانند مدل‌سازی تهدید، چرخه‌ی حیات توسعه‌ی امن نرم‌افزار و مدیریت کلید، خوانندگان MASVS باید به پروژه‌های مرتبط با OWASP و یا سایر استانداردهای ارائه‌شده در زیر مراجعه نمایند.

الزامات وارسی امنیت

الزامات سطح یک و دو از استاندارد وارسی امنیت برنامه‌های کاربردی موبایل به‌صورت زیر فهرست شده‌اند.

#	MSTG-ID	شرح	سطح یک	سطح دو
1.1	MSTG-ARCH-1	تمامی مؤلفه‌های برنامه‌ی کاربردی مورد نیاز شناسایی و شناخته‌شده‌اند.	x	x
1.2	MSTG-ARCH-2	کنترل‌های امنیتی هرگز فقط در سمت مشتری اعمال نمی‌شوند، بلکه در نقاط انتهایی مرتبط به کنترل از راه دور نیز اعمال می‌گردد.	x	x
1.3	MSTG-ARCH-3	یک معماری سطح بالا در برنامه‌ی کاربردی موبایل و تمامی سرویس‌های متصل به آن تعریف شده‌است و امنیت در آن معماری در نظر گرفته شده‌است.	x	x
1.4	MSTG-ARCH-4	داده‌هایی که در برنامه‌ی کاربردی موبایل حساس در نظر گرفته شده‌اند، به‌وضوح شناسایی شده‌اند.	x	x
1.5	MSTG-ARCH-5	تمامی مؤلفه‌های برنامه‌ی کاربردی موبایل بر اساس عملکرد امنیتی و یا تجاری که ارائه می‌کنند، مشخص شده‌اند.		x
1.6	MSTG-ARCH-6	مدل‌سازی تهدیدی که برای برنامه‌ی کاربردی موبایل و تمامی سرویس‌های مرتبط از راه دور ایجاد شده است، تهدیدات بالقوه و اقدامات متقابل را شناسایی می‌نماید.		x
1.7	MSTG-ARCH-7	تمامی کنترل‌های امنیتی به‌صورت متمرکز پیاده‌سازی شده‌اند.		x
1.8	MSTG-ARCH-8	یک خط‌مشی صریح برای نحوهی مدیریت کلیدهای رمزنگاری (در صورت وجود) و چرخه‌ی عمر کلیدهای رمزنگاری اعمال می‌شود. در حالت ایده آل، از یک استاندارد مدیریت کلید همانند NIST SP 800-57 پیروی نمایید.		x
1.9	MSTG-ARCH-9	یک سازوکار برای اجرای بروز رسانی برنامه‌ی کاربردی موبایل وجود دارد.		x
1.10	MSTG-ARCH-10	امنیت در تمامی مراحل چرخه‌ی حیات توسعه‌ی نرم‌افزار در نظر گرفته شده‌است.		x
1.11	MSTG-ARCH-11	یک سیاست افشای مسئولیت‌پذیرانه‌ی (آسیب‌پذیری) در حال اجرا است و به‌طور مؤثری اعمال می‌شود.		x
1.12	MSTG-ARCH-12	برنامه‌ی کاربردی موبایل باید با قوانین و مقررات حفظ حریم خصوصی مطابقت داشته باشد.	x	x

مراجع

برای دریافت اطلاعات بیشتر به آدرس‌های زیر مراجعه نمایید:

- ده تهدید برتر موبایل (OWASP) - تهدید رتبهی دهم (عملکرد نامربوط) - https://owasp.org/www-project-mobile-top-10/2016-risks/m10-extraneous-functionality
- مدلسازی تهدید (OWASP) - https://owasp.org/www-community/Application_Threat_Modeling
- راهنمای چرخه‌ی حیات توسعه‌ی امن نرم‌افزار (OWASP) - https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets_excluded/Secure_SDLC_Cheat_Sheet.md
- راهنمای چرخه‌ی حیات توسعه‌ی نرم‌افزار مایکروسافت - https://www.microsoft.com/en-us/sdl/

- استاندارد NIST (SP 800-57) - https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
- (security.txt) - https://securitytxt.org

V2: الزامات ذخیره‌سازی داده و حریم خصوصی

هدف کنترل

حفاظت از داده‌های حساس، از قبیل ابزارهای احراز هویت و اطلاعات خصوصی، یک نقطه تمرکز کلیدی در امنیت موبایل است. در مرحله‌ی اول اگر مکانیزم‌های سیستم عامل همانند IPC به‌طور نامناسب استفاده شوند، ممکن است اطلاعات حساس به طور سهوی در معرض دسترسی سایر برنامه‌های کاربردی موجود بر روی همان دستگاه قرار گیرند. همچنین ممکن است که داده‌ها به‌طور اشتباه بر روی حافظه ابری، پشتیبان یا حافظه نهان صفحه‌کلید نشت کنند. علاوه‌بر این، دستگاه‌های موبایل در مقایسه با سایر انواع دستگاه‌ها می‌توانند راحت‌تر مفقود شده یا مورد سرقت قرار بگیرند، بنابراین سناریوی دسترسی فیزیکی یک شخص متخاصم محتمل‌تر است. در این صورت یک سری محافظت‌های اضافی می‌توانند پیاده‌سازی شوند تا دسترسی به داده‌ها دشوارتر گردد. توجه داشته باشید که از آنجایی که MASVS بر برنامه‌ی کاربردی متمرکز می‌باشد، این استاندارد سیاست‌های الزام شده سطح دستگاه توسط MDM را تحت پوشش قرار نمی‌دهد.

تعریف داده حساس

داده‌ی حساس در چارچوب MASVS هم مربوط به ابزارهای احراز هویت کاربر است و هم هرگونه داده دیگر که در یک چارچوب خاص حساس در نظر گرفته می‌شود، مانند:

- اطلاعات قابل شناسایی خصوصی که(PII) می‌توانند توسط سرقت هویت مورد سوء استفاده قرار بگیرند: شماره‌های تأمین اجتماعی، شماره‌های کارت اعتباری، شماره‌های حساب بانکی و اطلاعات بهداشتی.
- اطلاعات بسیار حساس که در صورت به‌خطر افتادن می‌توانند منجر به آسیب به سابقهی شخصی یا خسارت‌های مالی شوند.
- هرگونه داده‌ای که باید توسط قانون و یا به‌دلایل مورد قبول محافظت شود.

الزامات وارسی امنیت

حجم زیادی از مشکلات افشای اطلاعات می‌توانند با پیروی از قوانین ساده‌ای پیشگیری شوند. بیشتر کنترل‌های فهرست شده در این فصل برای تمام سطوح تایید الزامی هستند.

#	MSTG-ID	شرح	سطح یک	سطح دو
2.1	MSTG-STORAGE-1	نیاز است تا از امکانات ذخیره‌سازی احراز هویت سیستم از قبیل ،PII ابزارهای تصدیق هویت کاربر یا کلیدهای رمزنگاری به طور مناسب استفاده شده باشند.	x	x
2.2	MSTG-STORAGE-2	هیچ اطلاعات حساسی نباید خارج از کانتینر برنامه یا امکانات ذخیره‌سازی ابزارهای احراز هویت سیستم ذخیره‌سازی شود.	x	x
2.3	MSTG-STORAGE-3	هیچ اطلاعات حساسی نباید در لاگ‌های برنامه‌ها نوشته شود.	x	x
2.4	MSTG-STORAGE-4	هیچ اطلاعات حساسی نباید با اشخاص ثالث به اشتراک گذاشته شود مگر اینکه بخشی ضروری از معماری باشد.	x	x
2.5	MSTG-STORAGE-5	حافظه کش صفحه‌کلید برای ورودی‌های متنی که شامل اطلاعات حساس است غیر فعال شده باشد.	x	x
2.6	MSTG-STORAGE-6	هیچ اطلاعات حساسی توسط مکانیزم IPC فاش نشود.	x	x
2.7	MSTG-STORAGE-7	هیچ اطلاعات حساسی از قبیل کلمات عبور یا پین‌ها توسط رابط کاربری فاش نشوند.	x	x
2.8	MSTG-STORAGE-8	هیچ اطلاعات حساسی در فایل‌های پشتیبان تولید شده توسط سیستم عامل موبایل وجود نداشته باشد.		x
2.9	MSTG-STORAGE-9	وقتی برنامه‌ی کاربردی وارد پس‌زمینه می‌شود باید اطلاعات حساس را از view ها پاک کند.		x
2.10	MSTG-STORAGE-10	برنامه‌ی کاربردی اطلاعات حساس را بیش از میزان ضروری در حافظه نگهداری نکند و حافظه پس از استفاده صریحا پاک شود.		x
2.11	MSTG-STORAGE-11	برنامه کاربردی یک سیاست device-access-security حداقلی را الزامی نماید. از جمله الزام کاربر به تنظیم یک کد عبور دستگاه.		x
2.12	MSTG-STORAGE-12	برنامه‌ی کاربردی کاربر را در مورد انواع اطلاعات شخصی قابل شناسایی پردازش شده و همچنین بهترین شیوه‌های امنیتی که کاربر باید در استفاده از برنامه دنبال نماید، آموزش دهد.		x

#	MSTG-ID	شرح	سطح یک	سطح دو
2.13	MSTG-STORAGE-13	هیچ داده حساسی نباید به طور محلی بر روی دستگاه موبایل ذخیره‌سازی شود. بلکه داده در موقع نیاز باید از یک پایانه‌ی راه دور دریافت شده و فقط در حافظه‌ی غیر دائم ذخیره‌سازی شود.		x
2.14	MSTG-STORAGE-14	اگر هنوز لازم است که داده‌ی حساس به طور محلی ذخیره‌سازی شود، باید توسط یک کلید مشتق شده از حافظه ذخیره سازی پشتیبانی شده به‌صورت سخت‌افزاری رمزنگاری شده که نیازمند تصدیق هویت است.		x
2.15	MSTG-STORAGE-15	حافظه ذخیره‌سازی محلی برنامه‌ی کاربردی باید بعد از تعداد زیادی تلاش ناموفق برای تصدیق هویت پاکسازی شود.		x

منابع

راهنمای وارسی امنیتی موبایل ،OWASP دستورالعمل‌هایی مفصل را برای تایید الزامات لیست شده در این بخش، فراهم می کند.

- اندروید: تست محل ذخیره‌سازی داده - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05d-Testing-Data-Storage.md
- iOS: تست محل ذخیره‌سازی داده - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06d-Testing-Data-Storage.md

همچنین برای اطلاعات بیشتر مشاهده کنید:

- OWASP Top 10 Mobile: M1 (استفاده‌ی نادرست از پلتفرم) - https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage
- OWASP Top 10 Mobile: M2 (ذخیره‌ی ناامن داده) - https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage
- CWE 117 (خنثی سازی خروجی‌های اشتباه برای لاگ ها) - https://cwe.mitre.org/data/definitions/117.html
- CWE 200 (افشای اطلاعات) - https://cwe.mitre.org/data/definitions/200.html
- CWE 276 (دسترسی‌های پیشفرض نادرست) - https://cwe.mitre.org/data/definitions/276.html
- CWE 311 (عدم رمزنگاری داده‌های حساس) - https://cwe.mitre.org/data/definitions/311.html
- CWE 312 (ذخیره‌سازی داده‌های حساس به صورت متن آشکار) - https://cwe.mitre.org/data/definitions/312.html
- CWE 316 (ذخیره‌سازی داده‌های حساس به‌صورت متن آشکار در حافظه‌ی موقت) - https://cwe.mitre.org/data/definitions/316.html
- CWE 359 (افشای اطلاعات خصوصی (نقش حریم خصوصی)) - https://cwe.mitre.org/data/definitions/359.html
- CWE 522 (محافظت ناکافی از احراز هویت) - https://cwe.mitre.org/data/definitions/522.html
- CWE 524 (افشای اطلاعات از طریق حافظه کش) - https://cwe.mitre.org/data/definitions/524.html
- CWE 530 (افشای فایل‌های پشتیبان در محیط کنترل بدون تعین سطح دسترسی) - https://cwe.mitre.org/data/definitions/530.html
- CWE 532 (افشای اطلاعات از طریق فایل‌های لاگ) - https://cwe.mitre.org/data/definitions/532.html
- CWE 534 (افشای اطلاعات از طریق فایل‌های لاگ اشکال زدایی) - https://cwe.mitre.org/data/definitions/534.html
- CWE 634 (ضعف‌های ناشی از پردازش سیستمی) - https://cwe.mitre.org/data/definitions/634.html
- CWE 798 (استفاده از احراز هویت به‌صورت هارد کد شده) - https://cwe.mitre.org/data/definitions/798.html
- CWE 921 (ذخیره‌سازی اطلاعات حساس در مکانیزمی بدون کنترل دسترسی) - https://cwe.mitre.org/data/definitions/921.html
- CWE 922 (ذخیره‌سازی ناایمن اطلاعات حساس) - https://cwe.mitre.org/data/definitions/922.html

V3: الزامات رمزنگاری

هدف کنترل

رمزنگاری یک جزء ضروری در حفاظت از داده‌ی ذخیره شده در گوشی موبایل می‌باشد. همچنین این دسته بندی، جایی است که ممکن است همه چیز به شکل وحشتناکی اشتباه پیش برود، به خصوص هنگامی که از قردادهای استاندارد پیروی نشود. هدف کنترل‌ها در این بخش این است که اطمینان حاصل کنند برنامه وارسی شده، از رمزنگاری طبق بهترین روش‌های صنعتی استفاده می‌کند، که شامل موارد زیر می‌شود:

- استفاده از کتابخانه‌های رمزنگاری ثابت شده؛
- انتخاب و پیکربندی مناسب اصول ابتدایی رمزنگاری؛
- تولید یک عدد تصادفی مناسب هرگاه که تصادفی بودن مورد نیاز است؛

الزامات وارسی امنیت

#	MSTG-ID	شرح	سطح یک	سطح دو
3.1	MSTG-CRYPTO-1	برنامه بر رمزنگاری متقارن با کلیدهای هاردکد شده، به عنوان تنها روش رمزگذاری، تکیه نمی کند.	x	x
3.2	MSTG-CRYPTO-2	برنامه از پیاده سازی‌های به اثبات رسیده‌ی ابتدایی رمزنگاری استفاده می‌کند.	x	x
3.3	MSTG-CRYPTO-3	برنامه از اصول ابتدایی رمزنگاری استفاده می کند که برای استفاده خاص مناسب هستند و با پارامترهایی که به بهترین روش‌های صنعتی پایبند هستند، پیکربندی شده‌اند.	x	x
3.4	MSTG-CRYPTO-4	برنامه از پروتکل‌ها یا الگوریتم‌های رمزنگاری که به دلایل امنیتی به طور گسترده منسوخ شناخته شده‌اند، استفاده نمی کند.	x	x
3.5	MSTG-CRYPTO-5	برنامه از کلید رمزنگاری یکسان برای چندین عمل، استفاده نمی کند.	x	x
3.6	MSTG-CRYPTO-6	تمام مقدارهای تصادفی با استفاده از یک تولید کننده عدد تصادفی به‌طورکافی امن تولید شده‌اند.	x	x

منابع

راهنمای وارسی امنیتی موبایل OWASP، دستورالعمل‌هایی مفصل برای تایید الزامات لیست شده در این بخش، فراهم می کند.

- Android: تست رمزنگاری - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05e-Testing-Cryptography.md
- iOS: تست رمزنگاری - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06e-Testing-Cryptography.md

برای اطلاعات بیشتر همچنین مشاهده کنید:

- OWASP Top Mobile 10: M5 (رمزنگاری نامناسب) - https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography
- CWE 310 (مشکلات رمزنگاری) - https://cwe.mitre.org/data/definitions/310.html
- CWE 321 (استفاده از کلید رمزنگاری هاردکد شده) - https://cwe.mitre.org/data/definitions/321.html
- CWE 326 (قدرت رمزنگاری ناکافی) - https://cwe.mitre.org/data/definitions/326.html
- CWE 327 (استفاده از الگوهای رمزنگاری پرخطر یا منقضی شده) - https://cwe.mitre.org/data/definitions/327.html
- CWE 329 (عدم استفاده از IV تصادفی به‌همراه حالت CBC) - https://cwe.mitre.org/data/definitions/329.html
- CWE 330 (استفاده از مقادیر تصادفی نامناسب) - https://cwe.mitre.org/data/definitions/330.html
- CWE 337 (جستجو قابل حدس در PRNG) - https://cwe.mitre.org/data/definitions/337.html
- CWE 338 (استفاده از رمزنگاری ضعیف تولید کننده‌ی جعلی اعداد تصادفی (PRNG)) - https://cwe.mitre.org/data/definitions/338.html

V4: الزامات تصدیق هویت و مدیریت نشست

هدف کنترل

در بیشتر موارد، ورود کاربران به یک سرویس از راه‌دور بخشی جدایی ناپذیر از معماری کلی برنامه موبایل است. حتی اگر بیشتر منطق در پایانه رخ دهد. MASVS برخی الزامات پایه در مورد چگونگی مدیریت نشست‌ها و حساب‌های کاربری را تعریف می‌نماید.

الزامات وارسی امنیت

#	شناسه-آزمون امنیتی برنامه‌ی کاربردی موبایل	شرح	سطح یک	سطح دو
4.1	MSTG-AUTH-1	اگر برنامه‌ی کاربردی برای کاربران، دسترسی به یک سرویس از راه‌دور را فراهم می‌کند، نوعی تصدیق هویت همانند نام کاربری و کلمه عبور باید در پایانه‌ی راه‌دور انجام شود.	x	x
4.2	MSTG-AUTH-2	اگر از مدیریت نشست حالت مند (stateful) استفاده شده است، پایانه‌ی راه دور باید بدون ارسال احراز هویت کاربر از شناسه‌های نشست تولید شده به‌طور تصادفی برای تصدیق هویت درخواست‌های سمت کاربر استفاده کند.	x	x
4.3	MSTG-AUTH-3	اگر از تصدیق هویت مبتنی بر توکن بدون حالت (stateless) استفاده شده است، سرور باید توکنی را ارائه دهد که توسط یک الگوریتم امن امضا شده باشد.	x	x
4.4	MSTG-AUTH-4	وقتی کاربر از سیستم خارج می‌شود، پایانه‌ی راه‌دور نشست فعلی را پایان می‌دهد.	x	x
4.5	MSTG-AUTH-5	یک سیاست کلمه عبور وجود دارد و در سمت پایانه‌ی راه‌دور اعمال می‌شود.	x	x
4.6	MSTG-AUTH-6	پایانه‌ی راه‌دور مکانیزمی را برای محافظت در برابر وارد کردن اطلاعات احراز هویت نادرست به دفعات زیاد پیاده‌سازی می‌کند.	x	x
4.7	MSTG-AUTH-7	نشست‌ها پس از مدتی عدم فعالیت یا منقضی شدن توکن‌های دسترسی در سمت پایانه‌ی راه‌دور نامعتبر می‌شوند.	x	x
4.8	MSTG-AUTH-8	تصدیق هویت بیومتریک نباید محدود به یک رویداد باشد (به‌عنوان نمونه استفاده از یک API که تنها True و False را باز می‌گرداند). به‌جای این، باید بر اساس گشودن keychain یا keystore باشد.		x
4.9	MSTG-AUTH-9	مرحله دومی از تصدیق هویت در پایانه‌ی راه‌دور وجود داشته باشد و الزامات تصدیق هویت دو مرحله‌ای همواره الزامی باشند.		x
4.10	MSTG-AUTH-10	تراکنش‌های حساس نیازمند تصدیق هویت مرحله به مرحله باشند.		x
4.11	MSTG-AUTH-11	برنامه‌ی کاربردی کاربر را نسبت به تمام فعالیت‌های ورود به سیستم با حساب وی آگاه می‌سازد. کاربران قادرند لیستی از دستگاه‌هایی که از آن‌ها برای دسترسی به حساب استفاده شده است را مشاهده کنند و دستگاه‌های خاصی را مسدود نمایند.		x
4.12	MSTG-AUTH-12	مدل‌های صدور مجوز باید در سمت پایانه‌ی راه‌دور تعریف شده و اجباری شوند.	x	x

منابع

راهنمای وارسی امنیتی موبایل OWASP، دستورالعمل‌هایی مفصل برای تایید الزامات لیست شده در این بخش، فراهم می‌کند.

- عمومی: احراز هویت و مدیریت نشست - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04e-Testing-Authentication-and-Session-Management.md
- Android: تست احراز هویت داخلی - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05f-Testing-Local-Authentication.md
- iOS: تست احراز هویت داخلی - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06f-Testing-Local-Authentication.md

برای اطلاعات بیشتر همچنین مشاهده کنید:

- OWASP Mobile Top 10: M4 (احراز هویت نا امن) - https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication
- OWASP Mobile Top 10: M6 (سطح درسترسی نا امن) - https://owasp.org/www-project-mobile-top-10/2016-risks/m6-insecure-authorization
- CWE 287 (احراز هویت نامناسب) - https://cwe.mitre.org/data/definitions/287.html

- CWE 307 (اعمال نامناسب منع دسترسی برای تلاش‌های زیاد) - https://cwe.mitre.org/data/definitions/307.html
- CWE 308 (استفاده از تایید هویت تک مرحله‌ای) - https://cwe.mitre.org/data/definitions/308.html
- CWE 521 (الزامات کلمه عبور ضعیف) - https://cwe.mitre.org/data/definitions/521.html
- CWE 604 (احراز هویت سمت کاربر) - https://cwe.mitre.org/data/definitions/604.html
- CWE 613 (انقضای نامناسب نشست) - https://cwe.mitre.org/data/definitions/613.html

V5: الزامات ارتباطات شبکه

هدف کنترل

هدف کنترل‌های فهرست شده در این بخش، این است که از محرمانگی و یکپارچگی اطلاعات مبادله شده میان برنامه موبایل و پایانه‌های سرویس از راه دور، اطمینان حاصل گردد. در حداقل شرایط، یک برنامه موبایل باید کانالی امن و رمزنگاری شده برای ارتباطات شبکه با استفاده از پروتکل TLS با تنظیمات مناسب، ایجاد کند. سطح دو، اقدامات اضافی دفاع عمیق، مانند SSL pinning را لیست می‌کند.

الزامات وارسی امنیت

#	MSTG-ID	شرح	سطح یک	سطح دو
5.1	MSTG-NETWORK-1	داده با استفاده از TLS روی شبکه رمزگذاری می‌شود. کانال امن در طول برنامه، همواره استفاده می‌شود.	x	x
5.2	MSTG-NETWORK-2	تنظیمات TLS با بهترین روش‌های حال حاضر مطابقت دارند، و یا اگر سیستم عامل موبایل از استانداردهای پیشنهادی پشتیبانی نمی‌کند، تنظیمات TLS تا جای ممکن با آنها مشابهت داشته باشد.	x	x
5.3	MSTG-NETWORK-3	برنامه، گواهینامه X.509 پایانه از راه‌دور را هنگامی که کانال امن ایجاد شود، وارسی می‌کند. تنها گواهینامه‌های امضا شده توسط CA مطمئن قابل قبول می‌باشند.	x	x
5.4	MSTG-NETWORK-4	برنامه یا از Store Certificate خودش استفاده می‌کند، یا گواهینامه‌ی پایانه یا کلید عمومی را پین می‌کند، و متعاقبا اتصالات به پایانه‌هایی که گواهینامه یا کلید متفاوتی دارند را ایجاد نمی‌کند، حتی اگر آن گواهینامه توسط CA مطمئن امضا شده باشد.		x
5.5	MSTG-NETWORK-5	برنامه تنها بر یک کانال ناامن ارتباطی (ایمیل یا پیامک) برای عملیات‌های بسیار مهم مانند ثبت نام‌ها و بازگردانی حساب، تکیه نمی‌کند.		x
5.6	MSTG-NETWORK-6	برنامه تنها بر کتابخانه‌های امنیت و اتصال که به روز می‌باشند، متکی می‌باشد.		x

منابع

راهنمای وارسی امنیتی موبایل ،OWASP دستورالعمل‌هایی مفصل برای تایید الزامات لیست شده در این بخش، فراهم می‌کند.

- عمومی: تست ارتباطات شبکه - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04f-Testing-Network-Communication.md
- Android: تست ارتباطات شبکه - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05g-Testing-Network-Communication.md
- iOS: تست ارتباطات شبکه - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06g-Testing-Network-Communication.md

برای اطلاعات بیشتر، مشاهده کنید:

- OWASP Mobile Top 10: M3 (ارتباطات نا امن) - https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication
- CWE 295 (اعتبار سنجی نادرست گواهی نامه) - https://cwe.mitre.org/data/definitions/295.html
- CWE 296 (پیروی ناصحیح از زنجیره‌ی اطمینان گواهی نامه) - https://cwe.mitre.org/data/definitions/296.html
- CWE 297 (صحت سنجی نادرست گواهینامه با میزبان اشتباه) - https://cwe.mitre.org/data/definitions/297.html
- CWE 298 (اشتباه در اعتبار سنجی انقضاء گواهی نامه) - https://cwe.mitre.org/data/definitions/298.html
- CWE 308 (استفاده از احراز هویت یک مرحله‌ای) - https://cwe.mitre.org/data/definitions/308.html
- CWE 319 (انتقال اطلاعات مهم به صورت متنی واضح) - https://cwe.mitre.org/data/definitions/319.html
- CWE 326 (استحکام ناکافی در رمزنگاری) - https://cwe.mitre.org/data/definitions/326.html
- CWE 327 (استفاده از الگوی رمزنگاری منقضی شده یا پرخطر) - https://cwe.mitre.org/data/definitions/327.html
- CWE 780 (استفاده از الگوی RSA بدون OAEP) - https://cwe.mitre.org/data/definitions/780.html
- CWE 940 (اشتباه در صحت سنجی منبع کانال ارتباطی) - https://cwe.mitre.org/data/definitions/940.html
- CWE 941 (مشخص سازی اشتباه منبع در یک کانال ارتباطی) - https://cwe.mitre.org/data/definitions/941.html

V6: الزامات تعامل با پلتفرم

هدف کنترل

کنترل‌های این گروه، اطمینان حاصل می‌کنند که برنامه‌ی کاربردی از API مربوط به پلتفرم و مؤلفه‌های استاندارد به‌صورت امن استفاده می‌کند. علاوه‌براین، این کنترل‌ها ارتباطات بین برنامه‌های کاربردی (IPC) را کنترل می‌نماید.

الزامات وارسی امنیت

#	MSTG-ID	توضیحات	سطح یک	سطح دو
6.1	MSTG-PLATFORM-1	برنامه‌ی کاربردی تنها به حداقل دسترسی‌های ضروری نیاز داشته باشد.	x	x
6.2	MSTG-PLATFORM-2	تمام ورودی‌ها از منابع خارجی و کاربر، اعتبارسنجی شده و اگر ضروری بود به خوبی بررسی شوند. این شامل داده‌های دریافت شده از رابط کاربری، مکانیزم‌های IPC از قبیل intent ها، URL های اختصاصی و منابع شبکه می‌باشد.	x	x
6.3	MSTG-PLATFORM-3	برنامه‌ی کاربردی عملکردهای حساس را از طریق طرح‌های URL اختصاصی صادر نمی‌کند. مگر اینکه این مکانیزم‌ها به درستی محافظت شده باشند.	x	x
6.4	MSTG-PLATFORM-4	برنامه‌ی کاربردی عملکرد حساس را از طریق امکانات IPC صادر نمی‌کند. مگر اینکه این مکانیزم‌ها به درستی محافظت شده باشند.	x	x
6.5	MSTG-PLATFORM-5	جاوا اسکریپت در WebView ها غیر فعال شده است. مگر اینکه به صراحت موردنیاز باشد.	x	x
6.6	MSTG-PLATFORM-6	WebView ها طوری پیکربندی شده‌اند که تنها حداقل کنترل کننده‌های پروتکل مورد نیاز را مجاز بدانند (به‌طور ایده‌آل تنها HTTPS پشتیبانی شود). کنترل کننده‌های پروتکل به‌طور بالقوه خطرناک از قبیل file ، tel و app-id غیر فعال باشند.	x	x
6.7	MSTG-PLATFORM-7	اگر متدهای داخلی برنامه در WebView ها قابل دیدن هستند، بررسی کنید که WebView تنها جاوا اسکریپت قرار داده شده در بسته برنامه‌ی کاربردی را پردازش می‌کند.	x	x
6.8	MSTG-PLATFORM-8	Object توالی‌سازی)Deserialization اشیاء) در صورت وجود داشتن توسط API های امن توالی‌سازی پیاده‌سازی شده باشد.	x	x
6.9	MSTG-PLATFORM-9	برنامه‌ی کاربردی از خود در برابر حملات پوشاندن صفحه نمایش محافظت می‌کند. (فقط سیستم عامل اندروید)		x
6.10	MSTG-PLATFORM-10	حافظه‌ی نهان، حافظه‌ی ذخیره‌سازی و منابع بارگذاری شده در WebView، (جاوا اسکریپت و غیره) باید قبل از نابود شدن WebView پاک شوند.		x
6.11	MSTG-PLATFORM-11	وارسی کنید که برنامه‌ی کاربردی در هنگام وارد کردن اطلاعات (فقط سیستم عامل iOS) حساس، از استفاده صفحه کلیدهای شخص ثالث جلوگیری می‌کند.		x

منابع

راهنمای وارسی امنیتی موبایل OWASP، دستورالعمل‌هایی مفصل برای تایید الزامات لیست شده در این بخش، فراهم می‌کند.

- Android: تست تعامل با پلتفورم - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing-Platform-Interaction.md
- iOS: تست تعامل با پلتفورم - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md

برای اطلاعات بیشتر همچنین مشاهده کنید:

- OWASP Mobile Top 10: M1 (استفاده‌ی نادرست از پلتفورم) - https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage
- OWASP Mobile Top 10: M7 (کیفیت پایین کد) - https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality
- CWE 20 (اعتبارسنجی نادرست ورودی) - https://cwe.mitre.org/data/definitions/20.html
- CWE 79 (خنثی سازی نادرست ورودی‌ها در حین تولید صفحات وب) - https://cwe.mitre.org/data/definitions/79.html
- CWE 200 (افشای اطلاعات) - https://cwe.mitre.org/data/definitions/200.html
- CWE 250 (اجرا با سطح دسترسی غیرضروری) - https://cwe.mitre.org/data/definitions/250.html

- CWE 672 (بهره‌برداری از یک منبع بعد از منقضی شدن یا آزاد سازی آن) - https://cwe.mitre.org/data/definitions/672.html
- CWE 749 (افشای متدها و توابع خطرناک) - https://cwe.mitre.org/data/definitions/749.html
- CWE 772 (فراموش کردن آزادسازی یک منبع پس از اتمام عمر مفید) - https://cwe.mitre.org/data/definitions/772.html
- CWE 920 (اعمال نادرست جلوگیری از مصرف قدرت) - https://cwe.mitre.org/data/definitions/920.html
- CWE 925 (اعمال ناصحیح صحت سنجی هدف با منتشر کردن دریافت کننده‌ها) - https://cwe.mitre.org/data/definitions/925.html
- CWE 926 (صدور نادرست اجزای برنامه‌ی اندرویدی) - https://cwe.mitre.org/data/definitions/926.html
- CWE 927 (استفاده از Intent Implicit برای ارتباطات حساس) - https://cwe.mitre.org/data/definitions/927.html
- CWE 939 (تعیین سطح دسترسی نادرست در کنترل کننده‌های طرح‌های اختصاصی (URL - https://cwe.mitre.org/data/definitions/939.html

V7: الزامات کیفیت کد و تنظیمات ساخت

هدف کنترل

هدف از این کنترل، این است که اطمینان حاصل گردد شیوه‌های کد نویسی امنیتی پایه در توسعه‌ی برنامه رعایت می‌شوند و امکانات امنیتی رایگان که توسط کامپایلر ارائه می‌شوند، فعال می‌باشند.

الزامات وارسی امنیت

#	MSTG-ID	شرح	سطح یک	سطح دو
7.1	MSTG-CODE-1	برنامه توسط گواهینامه‌ی معتبر امضا و تامین شده است که در آن از کلید خصوصی به درستی محافظت شده است.	x	x
7.2	MSTG-CODE-2	برنامه در حالت انتشار ساخته شده است، همراه با تنظیمات مناسب برای ساخت یک انتشار (به‌عنوان مثال غیر قابل دیباگ بودن)	x	x
7.3	MSTG-CODE-3	علائم اشکال زدایی از باینری‌های بومی حذف شده‌اند.	x	x
7.4	MSTG-CODE-4	کد اشکال زدایی و کد دستیار توسعه دهنده حذف شده باشد (به‌عنوان نمونه: کد آزمایشی، درب‌های پشتی، تنظیمات مخفی)، و برنامه استثنائات یا پیغام‌های اشکال زدایی طولانی را ثبت نمی‌کند.	x	x
7.5	MSTG-CODE-5	تمامی مؤلفه‌های شخص ثالث مورد استفاده‌ی برنامه‌ی موبایل، همچون کتابخانه‌ها و چارچوب‌ها، شناسایی شده‌اند، و برای داشتن آسیب‌پذیری‌های شناخته شده بررسی می‌شوند.	x	x
7.6	MSTG-CODE-6	برنامه استثنائات احتمالی را رسیدگی کرده و آنها را مدیریت می‌کند.	x	x
7.7	MSTG-CODE-7	منطق مدیریت استثناء در کنترل‌های امنیتی، به‌صورت پیش‌فرض، دسترسی را منع می‌کند.	x	x
7.8	MSTG-CODE-8	در کد مدیریت نشده، حافظه، به‌صورت ایمن اختصاص یافته، آزاد شده و استفاده می‌شود.	x	x
7.9	MSTG-CODE-9	امکانات امنیتی رایگان ارائه شده توسط زنجیره ابزار، همچون کوچک سازی byte-code، محافظت از پشته، پشتیبانی از PIE و شمارنده ارجاع خودکار، فعال می‌باشند.	x	x

منابع

راهنمای وارسی امنیتی موبایل OWASP، دستورالعمل‌هایی مفصل برای تایید الزامات لیست شده در این بخش، فراهم می‌کند.

- Android: تست تنظیمات ساخت و کیفیت کد - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05i-Testing-Code-Quality-and-Build-Settings.md
- iOS: تست تنظیمات ساخت و کیفیت کد - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06i-Testing-Code-Quality-and-Build-Settings.md

برای اطلاعات بیشتر، مشاهده کنید:

- OWASP Top Mobile 10: M7 (کیفیت ضعیف کد) - https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality
- CWE 20 (اعتبار سنجی نادرست ورودی) - https://cwe.mitre.org/data/definitions/20.html
- CWE 89 (اعمال نادرست خنثی سازی عناصر خاص که در فرمان‌های SQL استفاده می‌شوند) - https://cwe.mitre.org/data/definitions/89.html
- CWE 95 (اعمال نادرست خنثی سازی مستقیم در ارزیابی پویای کد (Eval)) - https://cwe.mitre.org/data/definitions/95.html
- CWE 119 (محدودسازی نادرست عملگرها در محدوده‌ی بافر حافظه) - https://cwe.mitre.org/data/definitions/119.html
- CWE 215 (افشای اطلاعات از طریق اطلاعات عیب‌یابی) - https://cwe.mitre.org/data/definitions/215.html
- CWE 388 (7PK - استثنائات) - https://cwe.mitre.org/data/definitions/388.html
- CWE 489 (بقایای عیب یابی کد) - https://cwe.mitre.org/data/definitions/489.html
- CWE 502 (پاک‌سازی داده‌های نامطمئن) - https://cwe.mitre.org/data/definitions/502.html
- CWE 511 (بمب‌های منطقی/زمانی) - https://cwe.mitre.org/data/definitions/511.html
- CWE 656 (توجه به امنیت در بی توجهی) - https://cwe.mitre.org/data/definitions/656.html
- CWE 676 (استفاده‌ی بالقوه‌ی توابع خطرناک) - https://cwe.mitre.org/data/definitions/676.html
- CWE 937 (OWASP Top Ten 2013 دسته‌بندی A9 - استفاده از آسیب‌پذیری‌های شناخته شده) - https://cwe.mitre.org/data/definitions/937.html

V8: الزامات انعطاف‌پذیری

هدف کنترل

این بخش معیارهای دفاع در عمق توصیه شده برای برنامه‌های کاربردی که اطلاعات حساس را پردازش کرده یا دسترسی به عملکرد یا اطلاعات حساس را فراهم می‌کنند را پوشش می‌دهد. نبود این کنترل‌ها باعث ایجاد آسیب‌پذیری نمی‌شود بلکه این کنترل‌ها به‌منظور افزایش انعطاف‌پذیری برنامه‌ی کاربردی در مقابل مهندسی معکوس و حملات خاص سمت کاربر در نظر گرفته شده‌اند.

کنترل‌های این بخش باید بنابه‌نیاز و بر اساس ارزیابی خطرات به‌وجود آمده توسط دستکاری غیرمجاز برنامه و یا مهندسی معکوس کد اعمال شوند. برای مشاهده لیستی از خطرات کسب و کار و همچنین تهدیدات فنی مربوطه، پیشنهاد می‌کنیم که به سند OWASP با عنوان "خطرات فنی مهندسی معکوس و مهندسی معکوس تغییر غیر مجاز کد و جلوگیری از تغییر کد" مراجعه شود. (منابع پایین را مشاهده کنید.)

برای اینکه هر یک از کنترل‌های فهرست شده در لیست زیر مؤثر واقع شوند، برنامه‌ی کاربردی باید حداقل تمام سطح یک MASVS (بدین معنی که کنترل‌های مستحکم امنیتی باید در سر جای خود باشند.) و همچنین تمام الزامات شماره‌گذاری شده با عدد پایین‌تر در V8 را برآورده سازد. به‌عنوان مثال، کنترل‌های مبهم‌سازی فهرست شده در زیر قسمت "منع درک کد"، باید همراه با "منع تجزیه و تحلیل پویا و دستکاری" و "اتصال دستگاه" ترکیب شوند.

توجه کنید که محافظت‌های نرم‌افزاری نباید هرگز به عنوان جایگزینی برای کنترل‌های امنیتی استفاده شوند. کنترل‌های فهرست شده در MASVR- به‌منظور اضافه کردن کنترل‌های محافظتی مازاد مرتبط با تهدیدات خاص به برنامه‌هایی که الزامات امنیتی MASVS را برآورده می‌کنند قرار داده شده‌اند.

ملاحظات زیر قابل اجرا هستند:

1. یک مدل تهدید باید تعریف شود که به‌طور روشن طرح کلی تهدیدات سمت کاربر که قرار است تعریف شوند را مشخص نماید. علاوه‌براین، درجه محافظتی که برنامه قرار است ارائه دهد باید مشخص شود. به‌عنوان مثال، اولین هدف می‌تواند این باشد که سازندگان بدافزار هدف که به دنبال سوء استفاده از برنامه‌های کاربردی هستند را مجبور کنیم که برای مهندسی معکوس تلاش زیادی نمایند.
2. مدل تهدید باید معتبر و مناسب باشد. به‌عنوان مثال اگر یک مهاجم بتواند به راحتی کل جعبه سفید را سرقت کند، مخفی کردن یک کلید رمزنگاری در یک پیاده‌سازی جعبه سفید ممکن است کاری زائد باشد.
3. اثربخشی محافظت باید همیشه توسط یک متخصص انسانی دارای که داری تجربه در زمینه راه‌های جلوگیری از دستکاری برنامه و مبهم‌سازی است وارسی و تأیید شود (همچنین به بخش‌های "مهندسی معکوس" و "ارزیابی محافظت‌های نرم‌افزاری" در راهنمای آزمون امنیت موبایل مراجعه کنید).

منع تجزیه و تحلیل پویا و دستکاری برنامه

#	MSTG-ID	شرح	R
8.1	MSTG-RESILIENCE-1	برنامه روت بودن یا جیلبریک بودن گوشی را تشخیص داده و پاسخ مناسبی به آن بدهد. این پاسخ می‌تواند با ارسال هشدار به کاربر یا متوقف کردن برنامه انجام شود.	x
8.2	MSTG-RESILIENCE-2	برنامه‌ی کاربردی از عیب‌یابی (debugging) جلوگیری کرده و یا موقع اتصال یک دیباگر آن را شناسایی کرده و پاسخ مناسب نسبت به آن می‌دهد. تمام پروتکل‌های عیب‌یابی در دسترس باید تحت پوشش قرار گیرند.	x
8.3	MSTG-RESILIENCE-3	برنامه‌ی کاربردی دستکاری فایل‌های اجرایی و داده‌های حساس درون sandbox خود را تشخیص داده و به آن پاسخ می‌دهد.	x
8.4	MSTG-RESILIENCE-4	برنامه‌ی کاربردی، حضور ابزارها و چارچوب‌های پراستفاده مهندسی معکوس را تشخیص داده و به آن پاسخ می‌دهد.	x
8.5	MSTG-RESILIENCE-5	برنامه‌ی کاربردی، اجرا شدن خود داخل شبیه‌ساز را تشخیص داده و به آن پاسخ می‌دهد.	x
8.6	MSTG-RESILIENCE-6	برنامه‌ی کاربردی، تغییر کد و داده در فضای حافظه خودش را تشخیص داده و به آن پاسخ می‌دهد.	x
8.7	MSTG-RESILIENCE-7	برنامه‌ی کاربردی، مکانیزم‌های متعددی را در هر دسته دفاعی 8.1) تا (8.6 به‌کار می‌گیرد. توجه کنید که انعطاف‌پذیری، با مقدار و تنوع اصالت مکانیزم‌های استفاده شده مقیاس می‌یابد.	x
8.8	MSTG-RESILIENCE-8	مکانیزم‌های تشخیص از انواع مختلفی از پاسخ‌ها استفاده می‌نمایند که شامل تاخیر در پاسخ و پاسخ‌های مخفی می‌باشد.	x
8.9	MSTG-RESILIENCE-9	عمل مبهم‌سازی (Obfuscation) به دفاع‌های برنامه‌ای اعمال شده است که باعث جلوگیری از شفاف‌سازی کد (De-obfuscation) توسط تجزیه و تحلیل پویا می‌شود.	x

اتصال دستگاه

#	MSTG-ID	شرح	R
8.10	MSTG-RESILIENCE-10	برنامه‌ی کاربردی، از یک اثر انگشت دستگاه، مشتق شده از ویژگی‌های متعدد یکتا مربوط به دستگاه کمک می‌گیرد و با آن یک عملکرد "اتصال دستگاه" را پیاده‌سازی می‌کند.	x

منع درک کد

#	MSTG-ID	شرح	R
8.11	MSTG-RESILIENCE-11	تمام فایل‌های اجرایی و کتابخانه‌های متعلق به برنامه‌ی کاربردی، یا در سطح فایل رمزنگاری شده‌اند و یا قسمت‌های مهم کد و داده، درون فایل‌های اجرایی، رمزنگاری یا بسته‌بندی شده‌اند. تجزیه و تحلیل جزئی ایستا، کد یا داده مهمی را افشا نمی‌کند.	x
8.12	MSTG-RESILIENCE-12	با توجه به تحقیقات منتشر شده‌ی فعلی، اگر هدف مبهم‌سازی (Obfuscation) محافظت از ارتباطات حساس است، از یک طرح مبهم‌سازی استفاده شود که هم برای وظیفه خاص مناسب باشد و هم در مقابل روش‌های دستی و اتوماتیک شفاف‌سازی کد (De-obfuscation) مقاوم باشد. اثربخشی طرح مبهم‌سازی باید از طریق آزمون دستی وارسی شود. توجه کنید که ویژگی‌های ایزوله‌سازی سخت‌افزاری در مقابل مبهم‌سازی در هر زمان ممکن دارای برتری هستند.	x

منع استراق سمع

#	MSTG-ID	Description	R
8.13	MSTG-RESILIENCE-13	در کنار محکم‌سازی قوی طرف‌های ارتباط، رمزنگاری Payload سطح برنامه‌ی کاربردی، می‌تواند برای جلوگیری از استراق سمع بیشتر به‌عنوان یک دفاع عمیق اعمال شود.	x

منابع

راهنمای وارسی امنیتی موبایل ،OWASP دستورالعمل‌هایی مفصل برای تایید الزامات لیست شده در این بخش، فراهم می‌کند.

- اندروید: تست انعطاف پذیری در برابر مهندسی معکوس - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05j-Testing-Resiliency-Against-Reverse-Engineering.md
- iOS: تست انعطاف پذیری در برابر مهندسی معکوس - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06j-Testing-Resiliency-Against-Reverse-Engineering.md

همچنین برای اطلاعات بیشتر، مشاهده کنید:

- OWASP Mobile Top 10: M8 (دستکاری کد) - https://owasp.org/www-project-mobile-top-10/2016-risks/m8-code-tampering
- OWASP Mobile Top 10: M9 (مهندسی معکوس) - https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering
- تهدیدات مهندسی معکوس (OWASP) - https://wiki.owasp.org/index.php/Technical_Risks_of_Reverse_Engineering_and_Unauthorized_Code_Modification
- مهندسی معکوس و جلوگیری از تغییر کد (OWASP) - https://wiki.owasp.org/index.php/OWASP_Reverse_Engineering_and_Code_Modification_Prevention_Project

پیوست الف: واژه‌نامه

- **(ASLR) Randomization Layout Space Address** تکنیکی برای دشوارسازی بهره‌برداری از باگ‌های خرابی حافظه.
- **Security Application** امنیت سطح برنامه‌ی کاربردی به جای تمرکز بر به‌عنوان مثال سیستم‌عامل پایه یا شبکه‌های متصل شده، بر تجزیه و تحلیل مؤلفه‌هایی که لایه‌ی برنامه‌ی کاربردی مدل اتصال متقابل سامانه‌های باز (OSI) را تشکیل می‌دهند تمرکز دارد.
- **(وارسی امنیت برنامه) Verification Security Application** یک ارزیابی فنی از برنامه‌ی کاربردی در برابر MASVS. OWASP
- **Report Verification Security Application** گزارشی که نتایج نهایی و تجزیه و تحلیل پشتیبان تولید شده توسط تأیید کننده برای یک برنامه کاربردی خاص را مستند سازی می‌کند.
- **Authentication** وارسی هویت ادعا شده توسط کاربر یک برنامه‌ی کاربردی.
- **Verification Automated** استفاده از ابزارهای اتوماتیک (ابزارهای تجزیه و تحلیل پویا و ایستا و یا هر دو) که از امضاهای آسیب‌پذیری جهت یافتن مشکلات استفاده می‌کنند.
- **Testing Box Black** یک روش آزمودن نرم‌افزار است که عملکرد یک برنامه‌ی کاربردی را بدون دانستن ساختار و نحوه‌ی عملکرد داخلی آن بررسی می‌کند.
- **Component** یک واحد کد جامع همراه با رابط‌های دیسک و شبکه مربوطه که با سایر مؤلفه‌ها ارتباط برقرار می‌کند.
- **(XSS) Scripting Cross-Site** یک آسیب‌پذیری امنیتی که معمولاً در برنامه‌های تحت وب یافت می‌شود و تزریق اسکریپت‌های سمت کاربر به محتوا را امکان‌پذیر می‌سازد.
- **Module Cryptographic** نرم‌افزار، سخت افزار و یا میان‌افزار که الگوریتم‌های رمزنگاری را پیاده‌سازی می‌کند و یا کلیدهای رمزنگاری را تولید می‌کند.
- **CWE** یک لیست توسعه یافته شده توسط جامعه‌ی کاربری از ضعف‌های رایج امنیتی نرم‌افزارها است. CWE به‌عنوان یک زبان مشترک، یک معیار اندازه‌گیری برای ابزارهای امنیت نرم‌افزار و به‌عنوان یک خط پایه جهت تلاش برای شناسایی ضعف، کاهش و جلوگیری از آن‌ها است.
- **(DAST) Testing Security Application Dynamic** فناوری‌های آزمودن پویای امنیت برنامه‌ی کاربردی ،(DAST) جهت شناسایی شرایط نشان دهنده‌ی یک آسیب‌پذیری امنیتی در یک برنامه‌ی کاربردی که در حالت اجرایی خود قرار دارد طراحی شده‌اند.
- **Verification Design** ارزیابی فنی معماری امنیت یک برنامه‌ی کاربردی.
- **Verification Dynamic** استفاده از ابزارهای خودکار که از امضاهای آسیب‌پذیری جهت یافتن مشکلات در حین اجرای یک برنامه استفاده می‌کنند.
- **(GUID) Identifier Unique Globally** یک شماره‌ی مرجع یکتا که به‌عنوان یک کد شناسایی در نرم‌افزار مورد استفاده قرار می‌گیرد.
- **(HTTP) Protocol Transfer Text Hyper** یک پروتکل برنامه کاربردی است که برای سیستم‌های توزیع شده، مبتنی بر همکاری و سیستم‌های اطلاعات ابر رسانه مورد استفاده قرار می‌گیرد. HTTP بنیان ارتباط داده برای شبکه‌ی جهانی وب است.
- **Keys Hardcoded** کلیدهای رمزنگاری که بر روی خود دستگاه ذخیره شده‌اند.
- **IPC** ارتباطات بین پروسه‌ای، در IPC پروسه‌ها با یکدیگر و کرنل ارتباط برقرار کرده تا فعالیتهای آن‌ها را هماهنگ سازند.
- **Validation Input** استاندارد سازی و اعتبارسنجی ورودی غیر مطمئن کاربر.
- **Bytecode Java** بایت کد جاوا مجموعه‌ی دستورات ماشین مجازی جاوا (JVM) است. هر بایت کد متشکل از یک یا در برخی موارد دو بایت است که نمایانگر دستورات (کد عملیاتی) هستند و همچنین صفر یا تعداد بیشتری بایت که برای گذر پارامترها هستند.
- **Code Malicious** کد ارائه شده همراه برنامه در طول توسعه بدون اطلاعات صاحب برنامه‌ی کاربردی که سیاست امنیتی مطلوب برنامه را دور می‌زند. این با بدافزار (malware) همانند ویروس یا کرم (worm) تفاوت دارد.
- **Malware** کد اجرایی که در طی زمان اجرای برنامه به آن وارد می‌شود بدون اینکه کاربر برنامه کاربردی یا مدیر از آن خبر داشته باشد.
- **(OWASP) Project Security Application Web Open** پروژه‌ی امنیت برنامه‌ی کاربردی باز (OWASP) یک جامعه‌ی آزاد در سطح جهانی است که بر بهبود امنیت نرم‌افزار تمرکز دارد.مـأموریت ما قابل رویت ساختن امنیت برنامه‌ی کاربردی است، به طوری که مردم و سازمان‌ها بتوانند تصمیمات آگاهانه‌ای درباره‌ی مخاطرات امنیت برنامه‌ی کاربردی بگیرند. مشاهده کنید: https://www.owasp.org/
- **(PII) Information Identifiable Personally** (اطلاعات قابل شناسایی خصوصی) اطلاعاتی است که می‌تواند به خودی خود و یا همراه با سایر اطلاعات جهت شناسایی، برقراری ارتباط یا یافتن مکان یک شخص و یا شناسایی شرایط یک فرد مورد استفاده قرار گیرد.
- **(PIE) Executable Position-Independent** اجرایی مستقل از مکان، یک بدنه کد زبان ماشین است که جایی در حافظه‌ی اصلی قرار می‌گیرد و بدون توجه به آدرس مطلق آن اجرا میشود.
- **(PKI) Infrastructure Key Public** یک PKI آرایشی است که کلیدهای عمومی را با هویت مربوط به موجودیت‌ها تحت انقیاد در می‌آورد. انقیاد از طریق یک فرایند ثبت نام و صدور گواهینامه‌ها در یک مرجع صدور گواهینامه (CA) و توسط آن انجام می‌شود.
- **(SAST) Testing Security Application Static** آزمون امنیت برنامه‌ی ایستا (SAST) مجموعه‌ای از فناوری‌ها است که برای تجزیه و تحلیل کد منبع برنامه‌ی کاربردی، بایت کد و باینری‌ها، برای کد نویسی و طراحی شرایطی که نمایانگر آسیب‌پذیری‌های امنیتی هستند طراحی شده است. راه حل‌های SAST، یک برنامه‌ی کاربردی را از پشت و رو، در حالتی که برنامه در حال اجرا نیست تجزیه و تحلیل می‌کنند.
- **SDLC** چرخه‌ی حیات توسعه‌ی نرم‌افزار.
- **Architecture Security** انتزاعی از طراحی یک برنامه‌ی کاربردی است که شناسایی و توصیف می‌کند که کنترل‌های امنیتی چگونه استفاده شده‌اند و همچنین مکان و حساسیت هر دو کاربر و داده‌ی برنامه را شناسایی و توصیف می‌کند .
- **Configuration Security** پیکربندی زمان اجرای یک برنامه‌ی کاربردی که چگونگی استفاده از کنترل‌های امنیتی را تحت تأثیر قرار می‌دهد.
- **Control Security** تابع یا مؤلفه‌ای که یک ارزیابی امنیتی انجام می‌دهد (به‌عنوان مثال یک چک کردن کنترل دسترسی) و یا موقع فراخوانی موجب یک اثر امنیتی می‌شود. (به‌عنوان مثال تولید یک دنباله‌ی حسابرسی)
- **(SQLi) Injection SQL** یک تکنیک تزریق کد که جهت حمله به برنامه‌های کاربردی مبتنی‌بر داده استفاده می‌شود، در این حمله عبارات SQL مخرب به یک نقطه‌ی ورودی تزریق می‌شوند.
- **Authentication SSO** شناسایی یگانه (SSO) وقتی رخ می‌دهد که یک کاربر وارد یک سیستم می‌شود و سپس به‌طور خودکار وارد سایر سیستم‌ها می‌شود، بدون توجه به پلتفرم، فناوری یا دامنه‌ای که کاربر استفاده می‌کند. به عنوان مثال وقتی که شما به حساب گوگل خود وارد می‌شوید، به طور خودکار

به حساب یوتیوب، docs و سرویس ایمیل خود نیز وارد می‌شوید.

- **Modeling Threat** تکنیکی متشکل از توسعه‌ی معماری‌های تصفیه شده امنیت جهت شناسایی عوامل تهدید، حوزه‌های امنیتی، کنترل‌های امنیتی و دارایی‌های فنی و تجاری مهم.
- **Security Layer Transport** پروتکل‌های رمزنگاری که امنیت ارتباط بر روی اینترنت را تأمین می‌کنند.
- **URL and URI** یک شناسانه منبع یکسان، یک رشته از کاراکترها است که برای شناسایی یک نام یا یک منبع استفاده می‌شود. یک شناسانه منبع یکسان گاهی به‌عنوان یک مرجع به یک منبع استفاده می‌شود.
- **(UAT) Testing Acceptance User** به‌طور سنتی یک محیط آزمون است که همانند محیط تولید عمل می‌کند. یعنی جایی که تمام آزمون‌های نرم‌افزاری قبل از عملیاتی شدن انجام می‌شوند.
- **Verifier** یک فرد یا یک تیم که برنامه‌ی کاربردی را در برابر الزامات MASVS OWASP بازبینی می‌کند.
- **Whitelist** فهرستی از عملیات یا داده‌های مجاز، به‌عنوان مثال فهرستی از کاراکترها که اجازه اعتبار سنجی ورودی دارند.
- **Certificate X.509** یک گواهینامه X.509 یک گواهی دیجیتال است که از استاندارد بین المللی X.509 زیرساخت کلید عمومی (PKI) استفاده می‌کند تا بتواند تأیید کند که یک کلید عمومی متعلق به کاربر، کامپیوتر یا هویت سرویس موجود در داخل گواهینامه است.

منابع ب: پیوست

باشند. مفید استاندارد این پذیرندگان و کاربران برای است ممکن زیر OWASP پروژه‌های

- موبایل امنیت پروژه‌ی (OWASP) - https://owasp.org/www-project-mobile-security/
- موبایل امنیت تست راهنمای (OWASP) - https://owasp.org/www-project-mobile-security-testing-guide/
- 10 موبایل برتر مخاطره‌ی (OWASP) - https://owasp.org/www-project-mobile-top-10/
- کد دستکاری و معکوس مهندسی از جلوگیری (OWASP) - https://wiki.owasp.org/index.php/OWASP_Reverse_Engineering_and_Code_Modification_Prevention_Project

باشند: مفید استاندارد این پذیرندگان و کاربران برای است ممکن زیر وب‌سایت‌های مشابه، به‌طور

- مرسوم ضعف نقاط شمارش (MITRE) - http://cwe.mitre.org/
- امنیتی استانداردهای انجمن (PCI) - https://www.pcisecuritystandards.org
- امنیت ممیزی فرآیند و 3 ورژن (DSS) داده امنیت استاندارد الزامات - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

تغییرات

V1.3 - 13 May 2021

We are proud to announce the introduction of a new document build pipeline, which is a major milestone for our project. The build pipeline is based on Pandocker and Github Actions. This significantly reduces the time spent on creating new releases and will also be the foundation for the OWASP MSTG and will be made available for the OWASP ASVS project.

Changes

- 4 more translations are available, which are Hindi, Farsi, Portuguese and Brazilian Portuguese
- Added requirement MSTG-PLATFORM-11

Special Thanks

- Jeroen Willemsen for kick-starting this initiative last year!
- Damien Clochard and Dalibo for supporting and professionalizing the build pipeline.
- All our Hindi, Farsi, Portuguese and Brazilian Portuguese collaborators for the excellent translation work.

V1.2 - 7 March 2020 - المللی بین انتشار

می‌باشند: 1.2 انتشار از قسمتی رو پیش تغییرات

- می‌باشد. دسترس در MASVS چینی ی ترجمه
- MASVS. کتاب کاور عنوان تغییر
- MASVS. در موجود منابع با آن ادغام و MSTG از CWE و Mobile Top 10 حذف

V1.2-RC - 5 October 2019 - انگلیسی) (فقط انتشار پیش

می‌باشند: 1.2 انتشار از قسمتی رو پیش تغییرات

- پرچمدار. وضعیت به ارتقاء
- دارد. شدن استفاده به نیاز MSTG-STORAGE-1 الزامات: تغییر
- شدند. اضافه داده از حافظت بر تمرکز با MSTG-STORAGE-15 و ,MSTG-STORAGE-13, MSTG-STORAGE-14 الزامات
- گردید. به‌روزرسانی محتوا به وابسته اطلاعات از نگهداری برای MSTG-AUTH-11 الزامات
- گردید. به‌روزرسانی یابی) عیب فقط (نه بیشتر مباحث دادن پوشش برای MSTG-CODE-4 الزامات
- گردید. اضافه WebView از استفاده بیشتر امنیت برای MSTG-PLATFORM-10 الزامات
- . گردید اضافه کاربره چند برنامه‌های برای مخصوصا دسترسی، سطح مجوزهای داشتن برای توسعه‌دهندگان به یادآوری جهت MSTG-AUTH-12 الزامات
- شود. استفاده شده داده مخاطره ممیزی در MASVS از چگونه اینکه درخصوص بیشتر توضیحات شدن اضافه
- پرداخت. محتوای خصوص در بیشتر توضیحات کردن اضافه
- می‌باشد. کاربردی برنامه‌های دوم لایه‌ی برای اطلاعات افشای به پاسخگویی سیاست یک شامل که گردید اضافه MSTG-ARCH-11 الزامات
- دهد. نشان را شوند دنبال باید که المللی بین مشی‌های خط قوانین کاربردی، نرم‌افزار توسعه‌دهندگان به تا شد اضافه MSTG-ARCH-12 الزامات
- انگلیسی. نسخه‌ی در منابع تمامی برای ثابت سبک یک ساخت
- گردید. اضافه شخص سوم صفحه‌کلیدهای با جاسوسی شمارش جهت MSTG-PLATFORM-11 الزامات
- گردید. اضافه کاربردی برنامه‌های در سمع استراق از جلوگیری جهت MSTG-MSTG-RESILIENCE-13 الزامات

V1.1.4 - 4 July 2019 - برتر ویرایش

می‌باشند: 1.1.4 انتشار از قسمتی رو پیش تغییرات

- Markdown. مشکلات تمامی رفع
- فرانسوی. و اسپانیایی ترجم‌های در به‌روزرسانی
- اسپانیایی. و (ZHTW) چینی به تغییرات ترجمه‌ی
- URLها. بودن دسترس در و Markdown سینتکس خودکار وارسی
- شوند. پیدا تر راحت تست‌کیس‌ها و توصیه‌ها تا شد خواهد اضافه MSTG بعدی نسخه‌های به که الزاماتی برای شناسایی کدهای شدن اضافه
- .gitignore. به Generated کردن اضافه و repo حجم کاهش
- راهنما. همکاری و جریان کد یک کردن اضافه
- Pull-Request. تمپلیت کردن اضافه
- Gitbook. وبسایت میزبانان توسط استفاده در repo با سازی همگام به‌روزرسانی
- ترجمه‌ها. تمامی برای XML/JSON/CVS تولید برای اسکریپت‌ها به‌روزرسانی

- چینی(ZHTW). به پیشگفتار ترجمه‌ی

V1.1.3 - 9 January 2019 - کوچک تعمیرات

- اسپانیایی نسخه‌ی در 7.1 الزامات ترجمه‌ی مشکلات رفع
- تصدیق‌ها در ترجمه‌کنندگان جدید آماده‌سازی

V1.1.2 - 3 January 2019 - سازی المللی بین و مالی حمایت

می‌باشند: 1.1.2 انتشار از قسمتی رو پیش تغییرات

- الکترونیکی کتاب خریداران برای تشکر متن کردن اضافه
- 4. نسخه در شده منقضی تصدیق‌های به‌روزشده‌ی لینک‌های و رفته دست از لینک‌های تاییدیه کردن اضافه
- انگلیسی. 4.8 و 4.7 نسخه‌های در swap مشکل رفع
- المللی! بین انتشار اولین
  - (1.1.2). گردیده سازی همگام انگلیسی با حاضر حال در ترجمه اسپانیایی. ترجمه‌ی بهبودسازی
  - (1.1.2). گردیده سازی همگام انگلیسی با حاضر حال در ترجمه روسی. ترجمه‌ی بهبودسازی
  - ژاپنی! و آلمانی فرانسوی، ، (ZHTW) چینی انتشار اولین شدن اضافه
- ترجمه. در سهولت برای مستندات ساده‌سازی
- خودکار. انتشار برای دستورالعمل‌هایی شدن اضافه

V1.1.0 - 14 July 2018

می‌باشند: 1.1.0 انتشار از قسمتی رو پیش تغییرات

- گردید. حذف باشند حساس اطلاعات حاوی است ممکن که متنی زمینه‌های در بورد کلیپ سازی فعال غیر 2.6 الزامات
- گردید. اضافه گردد ذخیره سیستم گواهی‌نامه ذخیره‌سازی امکانات یا برنامه کانتینر خارجی مخازن در نباید حساسی اطلاعات هیچ 2.2 الزامات
- رمزنگاری کلیدهای و کاربر گواهی ،PII مانند حساس اطلاعات ذخیره‌ی برای اختصاصی به‌صورت سیستم گواهی ذخیره‌سازی امکانات به‌شکل 2.1 الزامات کرد. پیدا تغییر می‌گردد استفاده

V1.0 12 - January 2018

می‌باشند: 1.0 انتشار از قسمتی رو پیش تغییرات

- 8.12 همانند 8.9 حذف
- 4.6 سازی عمومی
- (نگارشی) کوچک بهبودهای