

OWASP ASVS 2014

استاندارد وارسی امنیت برنامههای کساربردی نسخه ۲۰۱۴

أزمایشگاه تخصصی آپا – دانشگاه فردوسی مشهد

عباس جوان جعفری، سجاد پورعلی ASVS 2014

Abbas Javan Jafari, Sajjad Pourali,

javan@cert.um.ac.ir pourali@cert.um.ac.ir

پیش گفتار

هدف اصلی این نسخه از استاندارد افزایش پذیرش و استفاده ی عمومی است.

یکی از چالشهای اصلی چنین استانداردی، الزام برای برآورده کردن نیازهای دو گروه کاملاً متفاوت است. گروه اول افرادی هستند که با سازماندهی و اجرای یک برنامه ای کاربردی به عهده ی آنها است. اگرچه هر دو گروه به دنبال متخصصین امنیت نرمافزاری که وظیفه وارسی برنامههای کاربردی به عهده ی آنها است. اگرچه هر دو گروه به دنبال یک استاندارد صنعتی برای وارسی برنامههای کاربردی هستند، اما شرایط و محدودیتهای عملیاتی آنها متفاوت است. برای مثال یکی از انتقادهای رایج از استاندارد ASVS 2009 این بود که وارسی خودکار را به عنوان یکی از مراحل (یا زیرمراحل) تأیین کرده بود. خیلی از سازمانهای بزرگ، وارسی خودکار را یک نقطه ی آغاز در ورود به سلسله مراتب وارسی میدانند، و در نتیجه مفهوم یک مرحله ی وارسی خودکار برای آنها مناسب است. از طرف دیگر، متخصصین وارسی میدانند، و در نتیجه مفهوم یک مرحله ی وارسی به فناوری استفاده شده در اجرای پویش بستگی دارد، و در نتیجه امنیت اعتقاد دارند که وسعت و عمق این نوع وارسی به فناوری استفاده شده در اجرای پویش بستگی دارد، و در نتیجه راه را برای تفاسیر متفاوت از این استاندارد باز می گذارد. استاندارد ASVS 2014 یک مرحله ی صفرم را به منظور ایجاد انعطاف پذیری لازم برای غلبه بر این چالش ارائه می دهد.

یکی از اهداف اصلی این استاندارد تمرکز بر روی «چیستیها» به جای «چگونگیها» است. واژگانی مانند پویش پویا، تحلیل ایستا، مدلسازی تحدید، و بازبینی طراحی که در نسخههای پیشین این استاندارد قرار داشتند، در این نسخه دیده نمیشوند. در عوض، رویکرد این نسخه تعیین پیشنیازهای امنیتی است که بایستی پیش از رسیدن برنامهی کاربردی به یک مرحلهی مشخص وارسی شود. نحوهی وارسی این نیازمندیها به عهدهی شخص وارسی کننده است. چالش دیگری که بر آن غلبه کردیم، جداسازی شفاف نیازمندیها از طراحی و از حوزه است. این تنوع جداسازی شفاف در نسخههای پیشین وجود نداشت و منجر به سردرگمی مخاطبین میشد. در این نسخه، ملاحظات طراحی در مرحلهی سوم بیان شده و به وضوح از نیازمندیهای جزئی وارسی تفکیکشده است. علاوه بر این، مفهوم حوزه به کلی جدا شده است – نماد جدید (+) به وارسی کننده اجازه می دهد که در صورت نیاز، مؤلفهها و چارچوبهای جانبی را در بازبینی خود شامل شود.

انتظار نمیرود که این استاندارد به طور ۱۰۰٪ مورد توافق همگان واقع شود. تحلیل ریسک همیشه تا حدودی یک امر نظری و وابسته به دیدگاه شخصی افراد است. در نتیجه هرگونه تلاش برای عمومیت دادن مفاهیم در یک چارچوب و استاندارد واحد با چالشهایی روبهرو است. به هر حال، امیدواریم که جدیدترین بروزرسانیهای انجام شده در این نسخه، گامی در جهت صحیح باشد و مفاهیم مطرح شده در این استاندارد مهم صنعتی را بهبود بخشد.

تقدير و تشكر

نسخه 2014

مديران يروژه:

صحبا کازرونی ۱، دنیل کاسبرت۲

نویسندگان اصلی:

آندرو وندر استاک، صحبا کازرونی، دنیل کاسبرت، کریشنا راجاً

باربینی و همکاری:

جروم آسیاس، بوی باکما، آرکینجل کوسان، سباستیان دیلیرسنیدر، آنتونیو فونتز، اوان گوستاد، سفوات حمدی، آری کسانیمی، اسکات لوک، جیم مانیکو، میت پیکما، یکا سیلانیا، جف سارجنت، اتين استالمانز، كالين واتسون، دكتر ايمن تاتلي. ٥

با تشکر از جامعهی وارسی امنیت برنامههای کاربردی و دیگر علاقهمندان به رایانش اینترنتی مطمئن برای راهنمایی و همکاری آنها در فرآیند آمادهسازی این استاندارد.

نسخه ۲۰۰۹

از آنجایی، ASVS 2014 بسیاری از نیازمندیهای اصلی نسخهی پیشین را شامل می شود، شایسته است از افراد ذیل برای همکاری آنها در فرآیند آمادهسازی نسخهی اولیه سیاسگزاری شود.

مایک بوبرسکی، جف ویلیامز، دیو ویچرز، پیر پرند، آندرو وندر استاک، نم گوین، جان مارتین، گارنگ شا، تیودور وینوگراد، استن ویسمن، بری بوید، استیو کویل، یال دوسیت، کن هانگ، دیو هاسلیدن، مندیپ کرا اسکات متسوموتو، جان استیون، استیون دوریس، دن کورنل، شوویک باردان، دکتر سربری گویتا، ایوین کیری، ریجارد کمبل، مت پرسون،

¹ Sahba Kazerooni (Security Compass, http://www.securitycompass.com)

Daniel Cuthbert (SensePost, http://www.sensepost.com/)

[&]quot;Andrew van der Stock

^{*} Krishna Raja

^a Jerome Athias, Boy Baukema, Archangel Cuison, Sebastien Deleersnyder, Antonio Fontes, Evan Gaustad, Safuat Hamdy, Ari Kesäniemi, Scott Luc, Jim Manico, Mait Peekma, Pekka, Sillanpää, Jeff Sergeant, Etienne Stalmans, Colin Watson, Dr Emin Tatli.

جف لوسیپیو، لیز فانگ، جورج لالس، دیو ون استاین، تری دیاز، کتان دیلیپکومار ویاس، بدریهان اورگن، دکتر توماس بران، کالین واتسون، جرمایا گروسمن.\

تمامی حقوق مادی و معنوی این سند به مؤسسهی OWASP تعلق دارد.

Copyright © 2008 – 2014 The OWASP Foundation. This document is released under the Creative Commons

Attribution ShareAlike 3.0 license. For any reuse or distribution, you must make clear to others the license terms of this work.

٣

¹ Mike Boberski, Jeff Williams, Dave Wichers, Pierre Parrend (OWASP Summer of Code), Andrew van der Stock, Nam Nguyen, John Martin, Gaurang Shah, Theodore Winograd, Stan Wisseman, Barry Boyd, Steve Coyle, Paul Douthit, Ken Huang, Dave Hausladen, Mandeep Khera Scott Matsumoto, John Steven, Stephen de Vries, Dan Cornell, Shouvik Bardhan, Dr. Sarbari Gupta, Eoin Keary, Richard Campbell, Matt Presson, Jeff LoSapio, Liz Fong, George Lawless, Dave van Stein, Terrie Diaz, Ketan Dilipkumar Vyas, Bedirhan Urgun, Dr. Thomas Braun, Colin Watson, Jeremiah Grossman.

مقدمه

پروژه ی آزاد امنیت برنامههای کاربردی (OWASP) یک جامعه ی آزاد است که خودش را وقف کمک به سازمانها برای توسعه، خرید، و نگهداری برنامههای کاربردی قابل اطمینان است. دسترسی به تمامی ابزارها، اسناد، انجمنها، و فصول OWASP برای تمامی علاقه مندان به بهبود امنیت برنامهها آزاد است. رویکرد ما نگاه به امنیت به عنوان یک مسئله ی انسانی، فرآیندی، و مرتبط با فناوری است، زیرا مؤثرترین رویکردها در امنیت شامل بهبود تمامی این موارد است. آدرس ما www.owasp.org است.

سازمان OWASP یک سازمان با ساختار نوین است. استقلال ما از فشارهای تجاری امکان ارائه ی اطلاعات بی طرفانه، عملی، و مقرون به صرفه درباره ی امنیت برنامه های کاربردی را فراهم می کند. اگرچه OWASP از استفاده ی آگاهانه ی فناوری امنیتی تجاری پشتیبانی می کند، ولی هیچ گونه وابستگی حقوقی به سازمان های تجاری ندارد. مؤسسه ی OWASP یک موجودیت کاملاً غیرانتفاعی است.

استاندارد ASVS یک مبنا برای وارسی کنترلهای امنیتی فنی برنامه و هرگونه کنترلهای امنیتی فنی حاضر در محیط ارائه میدهد. با تکیه بر این کنترلهای محیطی میتوان از سیستم در برابر آسیبپذیریهایی مانند SQL Injection و Scripting (XSS) محافظت نمود. با استفاده از این استاندارد میتوان میزانی از اطمینان را برای امنیت برنامههای کاربردی تحت وب، برقرار نمود.

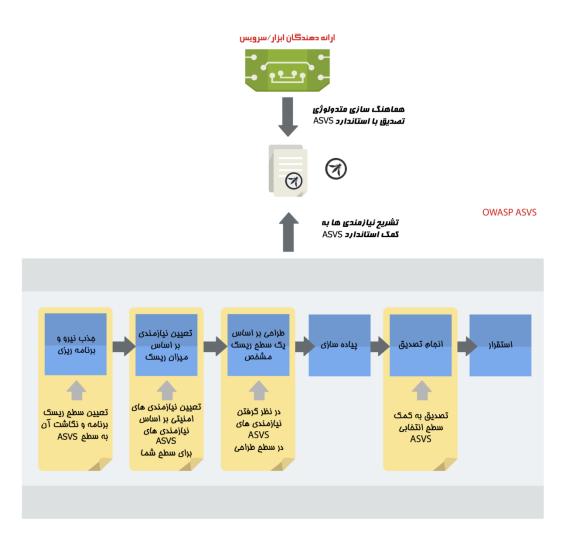
۲

Open Web Application Security Project

نحوهی استفاده از این استاندارد

استاندارد ASVS می تواند توسط هر دو گروه مصرف کننده و تهیه کنندهی سرویسها و ابزارها استفاده شود.

همان طور که در نمودار زیر مشاهده می شود، ASVS دو هدف عمده دارد. هدف اول کمک به سازمانها برای توسعه و نگهداری برنامههای کاربردی امن، و هدف دوم هماهنگی نیازمندیها و خدمات ارائه شده بین مصرف کنندگان و ارائهدهندگان سرویسها و ابزارهای امنیتی است.



شکل ۱ – کاربرد ASVS برای سازمانها و ارائهدهندگان سرویسها و ابزارهای امنیتی

مثالهای زیر برای توضیح موارد کاربرد معمول ASVS توسط یک سازمان ساختگی (ACME Bank) و یک شرکت خدمات امنیتی ساختگی (ACME Bank) و یک شرکت خدمات امنیتی ساختگی (Hack All The Things)، ارائه شدهاند.

مورد کاربرد ۱: وارسی برنامههای کاربردی

بانک ACME یک درگاه بانکداری جدید ایجاد کرده است که قرار است در محیط فرآوری آنها استقرار یابد. این برنامه ی کاربردی از فرآیند SDLC بانک پیروی کرده و انتظار میرود در یک حالت امن قرار داشته باشد. به دلیل استقرار این درگاه بر روی یک بستر اشتراکی، تیم امنیتی داخلی در بانک ACME باید مطمئن شوند که این درگاه پس از استقرار، دیگر برنامههای کاربردی را در معرض خطر قرار نمی دهد. پس از فرآیند مدل سازی تهدید داخلی، توافق شد که ریسک برنامه ی کاربردی و دادههای ذخیره شده در آن در سطح بالایی قرار دارد.

تیم امنیتی از یک برنامه ی شناخته شده ی پویش برنامه های کاربردی تحت وب برای پویش خود کار برنامه استفاده می کند. پس از اتمام تاون پویش خود کار، گزارش تولید شده توسط کارشناس امنیتی بررسی می شود تا مثبت کاذبهای احتمالی (نظیر SQL Injection یا SQS) علامت گذاری شود. تمامی یافته ها، به منظور اصلاح، به مدیران سیستم و تیم توسعه گزارش داده می شود. پس از اصلاح، برنامه ی کاربردی مجدداً بازبینی شده تا از رفع صحیح مسائل پیشین اطمینان حاصل شود.

در این مثال، ASVS به تیم امنیتی داخلی سازمان کمک میکند تا مشکلات رایج برنامه ی کاربردی را پیدا کرده و اطمینان یابد که برنامه بر اساس استانداردهای امنیتی بانک توسعه یافته است.

مورد کاربرد ۲: هماهنگی و تطبیق متدولوژی آزمایش

شرکت (Hack All The Things (HATT) یک شرکت آزمون نفوذ است و تخصص آن اجرای ارزیابی امنیتی برای مشتریان در سطح برنامه ی کاربردی یا در سطح زیرساخت است. برای ایجاد اطمینان خاطر در مشتریان، آنها تصمیم گرفتند تا متدولوژی آزمون نفوذ داخلی خود را با OWASP ASVS منطبق سازند.

برای دستیابی به این هدف، تمامی کارمندان موظفاند برنامهی کاربردی هدف را با کمک نیازمندیهای جزئی وارسی ASVS، و به طور دستی، ارزیابی کنند.

در این مثال، بکارگیری ASVS به HATT این امکان را میدهد که از طرفی یک سری ارزیابیها را بر اساس سطوح چهارگانهی OWASP ارائه دهد و از طرف دیگر بتواند عوامل ارزیابی شده را به طور شفاف به مشتریان گزارش کند.

مورد کاربرد ۳: انتخاب تهیه کننده ی خارجی

بانک ACME توسعه ی درگاه بانکداری خود را به پایان رسانده است. حال تنظیم کنندگان مقررات بانکی الزام کردهاند که یک شرکت خارجی برنامه ی کاربردی این بانک را ارزیابی کرده تا مطمئن شوند که این برنامه تابع مقررات امنیتی بانکداری است.

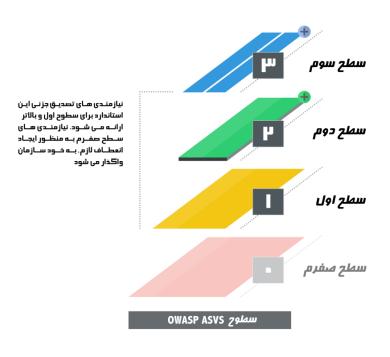
بانک ACME یک تهیه کننده از لیست تهیه کنندگان خود انتخاب کرده است و از شرکت HATT تقاضا کرده که فرایند ارزیابی را انجام دهد. بانک ACME تمام کدهای برنامه و مستندات لازم را در اختیار این شرکت قرار داده و هماهنگیهای لازم برای زمان انجام ارزیابی را نیز انجام داده است. ارزیابی خارجی در چندین فاز انجام شد. ابتدا یک تحلیل ایستا و خودکار بر روی کد برنامه و در کنار آن یک ارزیابی امنیتی از خود برنامه انجام شد. علاوه بر این، منطق کسبوکار برنامه مورد ارزیابی قرار می گیرد تا اطمینان حاصل شود که برنامه مطابق نیازمندیهای کارکردی تعیین شده در مستندات، عمل می کند. پس از اتمام ارزیابی، یک گزارش کار ایجادشده و برای کارمندان بانک ACME ارسال می شود.

در این فرایند، با بکارگیری ASVS توسط هر دو گروه، یک سطح مناسب برای ارزیابی انتخاب، و سپس استفاده شد. در نتیجه هر دو گروه بانک ACME و مشاوران HATT با یکدیگر هماهنگ شده و از نیازهای لازم اَگاه بودند.

سطوح وارسى امنيت برنامهي كاربردي

وارسی امنیت توسط ASVS در چهار سطح انجام می شود و با هر مرحله افزایش در سطح، میزان عمق بررسی افزایش می یابد.

در هر سطح، عمق ارزیابی توسط مجموعهای از نیازمندیهای وارسی امنیتی (که در جداولی در انتهای این سند دستهبندی شدهاند) مشخص می شود. این وظیفه ی وارسی کننده است که تعیین کند که سیستم هدف (TOV)، تمامی نیازمندیهای سطح مورد نظر را برآورده می کند یا خیر. اگر برنامه ی کاربردی تمام نیازمندیهای یک سطح مشخص را برآورده کند، آن را به عنوان برنامهای با سطح N در OWASP ASVS می شناسیم، که N در اینجا تعیین کننده ی سطح وارسی برنامه است. اگر برنامه تمامی نیازمندیهای یک سطح را برآورده نکند ولی تمام نیازمندیهای یک سطح پایین تر را برآورده کند، گواهی وارسی آن سطح پایین تر را دریافت می کند.



شکل ۲ – سطوح OWASP ASVS

گستردگی وارسی، بر اساس اجزای انتخاب شده از برنامه ی کاربردی (بهمنظور بازبینی) تعیین می شود. برای مثال، حوزه ی وارسی ممکن است فراتر از کدهای نوشته شده برای خود برنامه باشد و مؤلفه های بیرونی را نیز شامل شود. این نوع وارسی موشکافانه به وسیله ی نماد "+" در کنار سطح وارسی نشان داده می شود.

[\] Target of Verification

سطح صفر

سطح صفرم، یک گواهی اختیاری است به این معنا که برنامهی کاربردی مدنظر، نوعی وارسی امنیتی را گذرانده است.



شکل ۳ – سطح صفر از OWASP ASVS

هدف از سطح صفرم، ایجاد یک نقطه ی ورود انعطاف پذیر به سلسله مراتب وارسی است. این سطح بیان می کند که نوعی ارزیابی امنیتی برای برنامه ی کاربردی انجام شده است. نیازمندی های جزئی این سطح توسط ASVS ارائه نشده اند. در عوض، سازمان ها می توانند معیارهای حداقلی خود را تعیین کنند (مانند پویش خودکار در زمان اجرا، یا مکانیزم احراز هویت قوی).

این سطح برای سازمانهایی با تعداد زیاد برنامههای کاربردی، که نیازمند یک نقطه ورود مقرون به صرفه هستند، مناسب است. برای مثال، یک سازمان می تواند از سطح صفر برای الزام پویش خودکار برنامههای قابل دسترس از بیرون، به کمک ابزار پویش دلخواه سازمان، استفاده کند؛ و سازمانی دیگر، نیازمندیهای سطح صفر را از دادههای بدست آمده از حملات موفق پیشین استخراج کند.

برعکس سطوح دیگر این استاندارد، سطح صفر پیشنیاز هیچ سطح دیگری نیست. این بدان معنا است که یک برنامه (با فرض عدم تعریف سطح صفر توسط سازمان) می تواند مستقیماً سطح اول را درخواست کند.

توصیه می شود که هنگام تعریف نیازمندی های سطح صفر، تمامی نیازمندی ها مطابق الگوی نیازمندی های وارسی جزئی این استاندارد مستند شوند – واضح، مجزا، واقع بینانه، و قابل تأیید.

کلیات نیازمندیهای وارسی:

استاندارد ASVS نیازمندیهای جزئی وارسی این سطح را تعریف نمی کند. برنامه ی کاربردی بر اساس نیازمندیهای تعیین شده توسط سازمان، ارزیابی می شود.

سطح یک

یک برنامه ی کاربردی در صورتی می تواند گواهی سطح یک را دریافت کند که قادر باشد در برابر آسیبپذیریهایی که به سادگی کشف می شوند، از خود محافظت کند.



شکل ٤ – سطح یک از OWASP ASVS

آسیبپذیریهای مدنظر در سطح یک (که به طور کامل تر در بخش نیازمندیهای جزئی وارسی بررسی می شوند) به گونهای استاند که فرد وارسی کننده می تواند به راحتی و با تلاش اندک آنها را شناسایی کند. در نتیجه، این سطح بیشتر به مثابه یک بازرسی سریع برای برنامه است و نه یک ارزیابی کامل.

سطح یک معمولاً برای برنامههایی مناسب است که میزانی اطمینان از بکارگیری صحیح کنترلهای امنیتی لازم است. علاوه بر این، سطح یک برای پویش سریع انبوه برنامههای یک سازمان مفید بوده، و می تواند راهنمایی برای کمک به ارزیابیهای آتی باشد.

خطراتی که برنامهها را در این سطح تهدید می کند، از جانب مهاجمین ابتدایی است. این نوع مهاجمین با استفاده از روشهای ابتدایی، به دنبال آسیب پذیریهای ساده با روشهای نفوذ آسان میباشند. این دقیقاً نقطه ی مقابل مهاجمین مصمم است که زمان و انرژی متمرکزی برای حمله به یک هدف مشخص صرف می کنند.

كليات نيازمنديهاي وارسى:

یک برنامه ی کاربردی سطح یک، بر اساس نیازمندیهای سطح یک در بخش "نیازمندیهای جزئی وارسی" وارسی می شود.

سطح دو

یک برنامه ی کاربردی در صورتی می تواند گواهی سطح دو را دریافت کند که قادر باشد در برابر آسیب پذیری هایی رایج، که وجود آنها منجر به سطح ریسک متوسط به بالا می شود، از خود محافظت کند.



شکل ه – سطح دو از OWASP ASVS

مجموعهی دقیق آسیبپذیریهای مدنظر در سطح دو در بخش نیازمندیهای جزئی وارسی، بررسی میشود اما به طور کلی ۱۰ آسیبپذیری برتر OWASP و آسیبپذیریهای منطق کسبوکار مشمول این گروه هستند.

سطح دو اطمینان حاصل می کند که کنترلهای امنیتی صحیح در جایگاه صحیح خود مستقر بوده، و در شرایط لازم برای اعمال مقررات بخصوص آن برنامه، به طور مؤثر عمل می کند.

سطح دوم بیانگر یک معیار صنعتی برای ارزیابی اکثر برنامههای حساس یک سازمان است. برنامههای با تعداد معاملات زیاد کسبوکار، به ویژه آنها که اطلاعات بهداشتی و درمانی یا هرگونه فعالیت و دارایی حساس را پردازش میکنند، معمولاً برای وارسی سطح دو مناسب هستند.

خطراتی که برنامهها را در این سطح تهدید می کند، معمولاً مهاجمین ابتدایی و احتمالاً مهاجمین حرفهای و مصمم است.

كليات نيازمنديهاي وارسى:

یک برنامهی کاربردی سطح دو، بر اساس نیازمندیهای سطح دو در بخش "نیازمندیهای جزئی وارسی" وارسی میشود.

سطح سه

یک برنامه ی کاربردی در صورتی می تواند گواهی سطح سه را دریافت کند که قادر باشد در برابر تمام آسیب پذیری هایی پیشرفته محافظت کند و همچنین از اصول صحیح امنیتی در طراحی برنامه استفاده کند.



شکل ه – سطح سه از OWASP ASVS

مجموعهی دقیق آسیبپذیریهای مدنظر در سطح سه در بخش نیازمندیهای جزئی وارسی بررسی می شود. این گونه آسیبپذیریها شامل مواردی است که بهرهبرداری از آنها دشوار بوده و در نتیجه تنها توسط مهاجمین حرفهای و مصمم انجام می پذیرد.

سطح سوم تنها سطح ASVS است که بررسی طراحی برنامه را الزام میکند. علاوه بر این، نیازمندیهای زیر نیز اضافه شدهاند:

- هرگونه کنترل امنیتی اصلی، که بر اجزای متعدد سیستم تأثیرگذار است (مانند اعتبارسنجی ورودی یا احراز هویت)، باید به شکل متمرکز پیادهسازی شود.
- کنترلهای امنیتی که وظیفه ی اعتبارسنجی را به عهده دارند، باید در تصمیم گیریهای خود از رویکرد لیست سفید در نیروی کنند.
- نباید به اعتبارسنجی ورودی به عنوان تنها عامل حفاظت در برابر آسیبپذیریهای injection و july الله اولین اتکا کرد. اعتبارسنجی ورودی دومین خط دفاعی است و پس از پارامتربندی و رمزگذاری خروجی (که اولین اولویت حفاظت هستند) قرار می گیرد.

سطح سوم وارسی معمولاً برای برنامههایی مناسب است که از جان انسانها، زیرساختهای حساس، و امکانات نظامی محافظت می کنند. سطح سه همچنین برای برنامههایی که داراییهای حساس را پردازش می کنند استفاده می شود.

خطرات تهدیدکننده در این سطح، مهاجمین حرفهای و مصمم هستند که از ابزارهای خاصمنظوره و روشهای دستی برای حمله استفاده میکنند.

کلیات نیازمندیهای وارسی:

یک برنامه ی کاربردی سطح سه، بر اساس نیازمندیهای سطح سه در بخش "نیازمندیهای جزئی وارسی" وارسی می شود.

همچنین وارسی میشود که برنامهی کاربردی بر اساس الگوهای موفق زیر پیادهسازی شده است:

- کنترلهای امنیتی در برنامه به طور متمرکز مستقر شدهاند
- کنترلهای امنیتی که وظیفه ی اعتبارسنجی را به عهده دارند، از رویکرد لیست سفید پیروی می کنند
 - فرایندهای رمزگذاری خروجی در کنار کنترلهای اعتبارسنجی داده مستقر شوند
- تمام دادههای نامطمئن که به مفسرهای SQL ارسال میشوند، از واسطهای پارامتری و گزارههای از پیش آماده شده ٔ استفاده می کنند

^{&#}x27; Parameterized interfaces

^r Prepared statements

حوزه وارسي

گستره و حوزه وارسی و نیازمندیهای لازم برای دستیابی به یک سطح، دو بحث جدا از هم است.

پیش فرض ASVS این است که وسعت وارسی تمام کدهای استفاده شده برای توسعه و ایجاد برنامه را شامل می شود. البته، می توان کدهای تمام چارچوبها، کتابخانهها و سرویسهای امنیتی جانبی استفاده شده در برنامه را نیز مشمول وارسی قرار دهد. این نوع وارسی موشکافانه با اضافه کردن کمک نماد "+" به سطح مورد نظر نشان داده می شود. برای مثال یک برنامه می تواند گواهی وارسی +ASVS L3 را دریافت کند.

افزودن مؤلفههای جانبی به فرآیند وارسی اختیاری بوده و برای دستیابی به گواهی هیچ سطحی نیاز نیست. این نوع وارسی موشکافانه معمولاً مناسب برنامههای فوق حساس است، بنابراین در اکثر موارد نماد "+" برای سطح سوم مطرح میشود.

در صورت افزودن مؤلفههای جانبی به حوزه ی بررسی، نیاز نیست که تمامی نیازمندیهای جزئی وارسی به مؤلفههای جانبی اعمال شوند. در حقیقت، بیشتر نیازمندیهای جزئی وارسی به مؤلفههای جانبی قابل اطلاق نیست و تنها بر کد اصلی برنامه اعمال می شود. برای دریافت گواهی یک سطح به همراه (+)، بایستی تمامی نیازمندیهای جزئی وارسی به کد اصلی، و در صورت امکان، به مؤلفههای جانبی برنامه اعمال شود.

نیازمندیهای جزئی وارسی

این بخش از استاندارد وارسی امنیتی برنامه ی کاربردی، نیازمندی جزئی وارسی را تعریف می کند. این نیازمندیها برگرفته از نیازمندیهای سطح بالای هر سطح از سطوح مطرح شده در این استاندارد است.

نیازمندیهای امنیتی ASVS به دستههای زیر تقسیم میشوند. برای کمک به افراد برای فرآیند انتقال به استاندارد جدید، رویهی عددگذاری را با نسخه ی پیشین ASVS سازگار کردهایم.

- ۲ احراز هویت ٔ
- $^{\mathsf{T}}$ مدیریت نشست $^{\mathsf{T}}$
- ۴ کنترل دسترسی^۳
- 4 مدیریت ورودی مخرب -
 - ۷ رمزنگاری
- 8 مدیریت خطا و ثبت گزارش 8
 - ۹ حفاظت از داده ۲
 - ۱۰ ارتباطات^
 - HTTP 11
 - ۱۳ کنترلهای مخرب
 - ۱۵ منطق کسبوکار ۱۰
 - 11 پروندهها و منابع 11
 - ۱۷ موبایل

[\] Authentication

^r Session Management

[&]quot; Access Control

^{*} Malicious Input Handling

^a Cryptography

⁵ Error Handling and Logging

^v Data Protection

[^] Communication

¹ Malicious Controls

^{\.} Business Logic

[&]quot;File and Resource

نیازمندیهای وارسی احراز هویت

		سطو2	نیازمندیهای وارسی احراز هویت	
ш	p	1		
√	✓	√	وارسی کنید که برای تمامی صفحات و منابع احراز هویت انجام شود، بهجز آنهایی که قصد داریم عمومی باشند.	١
√	✓	✓	وارسی کنید که هنگام ورود کلمه ی عبور توسط کاربر، فیلد کلمه ی عبور آن را نشان نمی دهد.	۲
√	✓	✓	وارسی کنید که تمام کنترلهای احراز هویت در سمت سرویسدهنده انجام میشود.	۴
√			وارسی کنید که تمامی کنترلهای احراز هویت بهصورت متمرکز پیادهسازی شدهاند.	۵
√	✓	✓	وارسی کنید که تمام کنترلهای احراز هویت، بهصورت امن با شکست مواجه میشوند.	۶
✓	✓	√	وارسی کنید که کلمات عبور انتخابی به اندازه ی کافی قوی باشند و از انتخاب کلمات عبور متعارف جلوگیری شود. همچنین فیلدهای کلمه ی عبور نباید مانع ورود کلمات عبور پیچیده و طولانی شوند.	Υ
✓	✓		وارسی کنید که تمامی کارکردهای مربوط به احراز هویت (مانند ثبتنام، فراموشی کلمه ی عبور، و غیرفعال سازی حساب کاربری) حداقل به اندازه ی مکانیزم اولیه ی احراز هویت در برابر حملات مقاوم هستند.	٨
	✓		وارسی کنید که کاربران بتوانند به کمک مکانیزمی امن اعتبارنامههای خود را تغییر دهند و این مکانیزم به اندازه ی مکانیزم اولیه احراز هویت در برابر حملات مقاوم باشد.	٩
✓	✓		وارسی کنید که تمام تصمیمات احراز هویت در گزارشها ثبت شوند (درخواستهای ورود ناموفق برای بررسیهای امنیتی لازم است).	17

		سطو2	نیازمندیهای وارسی احراز هویت	
ш	μ	1		
✓	✓		وارسی کنید که کلمههای عبور به همراه یک عدد منحصربهفرد (مثلاً شناسهی کاربری داخلی) ذخیره شوند و قبل از ذخیرهسازی، به کمک روشهایی مانند scrypt ،bcrypt درهمسازی انجام شود.	١٣
√	✓	√	وارسی کنید که تمام اعتبارنامهها و اطلاعات شناسایی که برنامه با آن سروکار دارد، از مسیرهای رمزنگاری نشده (یا رمزنگاری ضعیف) عبور نمی کنند.	18
✓	✓	✓	وارسی کنید که مکانیزمهای بازیابی کلمه ی عبور (در صورت فراموشی کاربر) کلمه ی عبور فعلی را نمایش نمی دهند و کلمه ی عبور جدید به صورت رمزنگاری شده برای کاربر ارسال شود.	۱۷
√	✓	√	وارسی کنید که تشخیص تعداد و نامهای کاربری به کمک مکانیزمهای ورود به سیستم و بازنشانی کلمهی عبور امکانپذیر نباشد.	١٨
√	✓	√	وارسی کنید که چارچوبهای برنامه و مؤلفههای جانبی از کلمات عبور پیشفرض (مانند admin/password) استفاده نمی کنند.	19
	✓		وارسی کنید که فرآیند ورود به سیستم در برابر حملات brute-force عمودی (یک حساب کاربری با تمام کلمههای عبور ممکن آزموده شوند) و یا افقی (تمام حسابهای کاربری با یک کلمه عبور بخصوص آزمایش شوند) محافظت می کند.	۲٠
✓	✓		وارسی کنید که تمام اعتبارنامههای احراز هویت برای دسترسی به سرویسهای خارجی برنامه رمزنگاری شده و در مکانی امن (خارج از کد) نگهداری می شوند.	71
✓			وارسی کنید که مکانیزمهای فراموشی کلمه ی عبور و بازیابی حساب کاربری، به جای ارسال خود کلمه ی عبور به کاربر، یک لینک حاوی نشانه با محدودیت زمانی به کاربر ارسال کنند تا از این طریق حساب خود را بازیابی کند. مکانیزمهای احراز هویت افزونه، مانند نشانههای پیامکی و برنامههای موبایل، پیش از ارسال لینک به کاربر، نیز امکان پذیر است.	77

[\] Hashing

^r Token

		سطوح	نیازمندیهای وارسی احراز هویت	
μ	μ	1		
✓	✓		وارسی کنید که مکانیزمهای فراموشی کلمه ی عبور، تا پس از اتمام موفقیت آمیز تغییر کلمه ی عبور، حساب کاربری را قفل یا غیرفعال نمی کند. هدف این است که دسترسی کاربران معتبر به حسابشان با مانع مواجه نشود.	77
√	✓		وارسی کنید که سؤالات انتخابشده برای بازنشانی کلمه ی عبور با دانش عمومی قابل پاسخ نباشد.	74
√	✓		وارسی کنید که سیستم قابلیت تنظیم برای منع استفاده از کلمههای عبور پیشین (به تعداد قابل تنظیم) را دارد.	۲۵
✓			وارسی کنید که پیش از صدور مجوز انجام عملیات حساس برنامه (با توجه به حساسیت برنامه)، احراز هویت مجدد انجام شود. برای این کار می توان از مکانیزمهای احراز هویت دو مرحلهای، مانند پیامک موبایل، نیز استفاده کرد.	75

جدول ۱ – نیازمندیهای احراز هویت OWASP ASVS

نیازمندیهای وارسی مدیریت نشست

		سطوح	نیازمندیهای وارسی مدیریت نشست	
ш	μ	1		
√	√	√	وارسی کنید برنامه برای کنترل مدیریت نشستها از پیادهسازی پیشفرض چارچوب استفاده می کند.	١
✓	√	✓	وارسی کنید که با خروج ٔ کاربر، تمام نشستهای او باطل میشود.	۲
√	√	√	وارسی کنید که وقتی نشست برای مدتی مشخص غیرفعال باشد، نشست منقضی ^۲ شود.	٣
√			وارسی کنید که نشستها پس از زمانی مشخص (و قابل تنظیم)، صرفنظر از فعال یا غیرفعال بودن، منقضی شوند.	۴
√	√	√	وارسی کنید که تمام صفحاتی که برای دسترسی نیاز به احراز هویت دارند، لینک خروج داشته باشند.	۵
√	√	√	وارسی کنید که شناسههای نشست تنها در کوکیها آشکار شوند و هرگز در URLها، پیامهای خطا، و گزارشات سیستمی آشکار نشوند.	۶
✓	√		وارسی کنید که شناسههای نشست هنگام ورود عوض شود تا از تثبیت نشست ^۴ جلوگیری شود.	٧
√	√		وارسی کنید که شناسهی نشست هنگام احراز هویت مجدد عوض شود.	٨
			وارسی کنید که تنها کوکیهای نشستی که توسط چارچوب برنامه تولید میشوند، توسط برنامه کاربردی معتبر شناخته میشوند.	١٠

[\] Logout

^r Timeout

^τ Session id

^{*} Session fixation

		سطو2	نیازمندیهای وارسی مدیریت نشست	
ш	μ	1		
√	√		وارسی کنید که توکنهای نشست به اندازه ی کافی طولانی و تصادفی هستند تا در برابر حملات حدس توکن مقاوم باشند.	11
✓	✓		وارسی کنید که توکنهای نشستی که از کوکی استفاده میکنند، مسیرشان با یک مقدار محدود مقداردهی میشود. پارامتر کوکی دامنه بایستی تنها به منظور ارضای نیازمندیهای کسبوکار استفاده شود.	١٢
√	✓	√	وارسی کنید که توکنهای نشست احراز هویت شده، که از کوکیهای ارسالشده توسط HttpOnly حفاظت می شوند.	14
✓	✓	✓	وارسی کنید که توکنهای نشستی که بهوسیلهی کوکیها احراز هویت می شوند، به کمک ویژگی secure حفاظت می شوند، و یک سرآیند امنیتی لایهی انتقال (Strict-Transport-Security: max-age=6000; includeSubDomains) وجود دارد.	۱۵
√	✓		وارسی کنید که برنامهی کاربردی اجازهی دو نسخهی همزمان از نشست کاربری را، از سیستمهای متفاوت، نمیدهد.	18

جدول ۲ – نیازمندیهای مدیریت نشست OWASP ASVS

نیازمندیهای وارسی کنترل دسترسی

		<u>سطو2</u>	نیازمندیهای وارسی کنترل دسترسی	
ш	μ	1		
√	√	√	وارسی کنید که تنها کاربرانی که مجوز مخصوص دارند، میتوانند به سرویسها و قابلیتهای حفاظتشده دسترسی یابند.	١
√	√	√	وارسی کنید که تنها کاربرانی که مجوز مخصوص دارند، میتوانند به URLهای حفاظتشده دسترسی یابند.	۲
√	√	√	وارسی کنید که تنها کاربرانی که مجوز مخصوص دارند، میتوانند به پروندهها و دادههای حفاظتشده دسترسی یابند.	٣
	✓	√	وارسی کنید که ارجاعات مستقیم به اشیاء حفاظت شدهاند، به گونهای که کاربر تنها به اشیاء و دادههای دارای مجوز دسترسی داشته باشد.	۴
√	√	✓	وارسی کنید که مرور دایرکتوری ممکن نباشد مگر آنکه تعمداً خواسته باشید.	۵
✓	√	✓	وارسی کنید که کنترلهای دسترسی بهصورت امن با شکست مواجه میشوند.	٨
√	√		وارسی کنید که همان کنترلهای دسترسی که در لایه ی نمایش بیان میشوند، در سمت سرویسدهنده نیز (برای آن نوع کاربر) اعمال میشوند.	٩
✓	✓		وارسی کنید که ویژگیهای کاربری و دادهها، و مقررات کنترل دسترسی از طرف کاربران نهایی قابل دستکاری نباشد، مگر آنکه به طور خاص چنین مجوزی به آنها داده شود.	١٠
√	√	√	وارسی کنید که تمام کنترلهای دسترسی در سمت سرویسدهنده اعمال میشوند.	11
√	√		وارسی کنید که یک مکانیزم مرکزی و متمرکز برای حفاظت از دسترسی به منابع حفاظتشده وجود داشته باشد.	17

[\] Directory browsing

		سطو2	نیازمندیهای وارسی کنترل دسترسی	
ш	μ	1		
√	√		وارسی کنید که تمام تصمیمات کنترل دسترسی در گزارشها ثبت میشوند.	14
✓	✓	✓	وارسی کنید که چارچوب برنامه ی کاربردی برای تمام تراکنشهای مهم و دسترسی به دادههای حساس، توکنهای تصادفی قوی و ضد-CSRF، مختص هر کاربر ایجاد میکند. برنامه ی کاربردی هنگام پردازش این درخواستهای حساس باید از وجود این توکن اطمینان حاصل کند.	18
√	✓		وارسی کنید که سیستم در برابر دسترسیهای پیدرپی و متمرکز به قابلیتها و منابع حفاظتشده مقاوم است. برای مثال تعداد اعمال تغییرات ممکن توسط کاربران به ازای هر ساعت محدود شود تا یک کاربر به تنهایی نتواند تمام پایگاه داده را دگرگون سازد.	١٧

جدول ۳ – نیازمندیهای کنترل دسترسی OWASP ASVS

نیازمندیهای وارسی مدیریت ورودی مخرب

		سطو2	نیازمندیهای وارسی اعتبارسنجی ورودی مخرب	
ш	μ	1		
√	✓	√	وارسی کنید که محیط اجرای برنامه مستعد سرریز بافر نیست یا کنترلهای امنیتی از این آسیبپذیری پیشگیری میکنند.	١
√	✓	√	وارسی کنید که شکست اعتبارسنجی ورودی منجر به عدم پذیرش ورودی میشود.	٣
√	✓		وارسی کنید که مجموعه کاراکتری مانند UTF-8 برای تمام منابع ورودی مشخص شود.	۴
√	✓	√	وارسی کنید که تمام اعتبارسنجیهای ورودی و روشهای رمزگذاری در سمت سرویسدهنده انجام میشود.	۵
✓	✓		وارسی کنید که برنامه از یک کنترل اعتبارسنجی واحد برای تمام دادههای پذیرفته شده استفاده می کند.	۶
√	✓		وارسی کنید که تمام شکستهای اعتبارسنجی ورودی در گزارشهای سیستم ثبت میشوند.	٧
√	✓		وارسی کنید که تمام دادههای ورودی پیش از اعتبارسنجی به قالب استاندارد دیکدرها و مفسرهای پذیرنده تبدیل شود.	٨
√	✓	√	وارسی کنید که محیط اجرای برنامه مستعد SQL Injection نیست یا کنترلهای امنیتی از این آسیبپذیری پیشگیری می کنند.	١٠
√	✓	✓	کنترلهای امنیتی از این آسیبپذیری پیشگیری می کنند. وارسی کنید که محیط اجرای برنامه مستعد LDAP Injection نیست یا کنترلهای امنیتی از این آسیبپذیری پیشگیری می کنند.	11

Buffer overflow

		سطوح	نیازمندیهای وارسی اعتبارسنجی ورودی مخرب	
ш	μ	1		
✓	✓	√	وارسی کنید که محیط اجرای برنامه مستعد OS Command Injection نیست یا کنترلهای امنیتی از این آسیبپذیری پیشگیری میکنند.	١٢
✓	✓	√	وارسی کنید که محیط اجرای برنامه مستعد حملهی XML External Entity نیست یا کنترلهای امنیتی از این حمله پیشگیری میکنند.	١٣
✓	✓	√	وارسی کنید که محیط اجرای برنامه مستعد XML Injection نیست یا کنترلهای امنیتی از این آسیبپذیری پیشگیری می کنند.	14
✓	✓	√	وارسی کنید که تمام دادههای نامطمئن که در قالب خروجی HTML ظاهر می شوند (مانند مقادیر Javascript، بلوکهای CSS، مشخصههای URI)، به قالب استاندارد تبدیل می شوند.	18
✓	✓		اگر چارچوب برنامه اجازه ی تخصیص فراگیر پارامترها (به عبارتی همان انقیاد خودکار متغیرها) را به درخواستهای ورودی میدهد، مطمئن شوید که فیلدهای حساس مانند "Passwrod"، "role"، "accountBalance" در مقابل انقیاد خودکار خرابکارانه حفاظت می شوند.	١٧
√	✓		وارسی کنید که برنامه در برابر حملات آلودهسازی پارامتر HTTP حفاظت می کند، به ویژه اگر چارچوب برنامه بین نوع پارامترهای درخواستی (POST, cookie, header	١٨
✓			وارسی کنید که برای تمام رمزگذاریهای خروجی برنامه، یک کنترل امنیتی واحد برای آن نوع خروجی و مقصد مدنظر وجود دارد.	19

جدول ٤ – نيازمنديهاي ورودي مخرب OWASP ASVS

نیازمندیهای وارسی رمزنگاری

		سطو2	نیازمندیهای وارسی رمزنگاری	
ш	μ	1		
√	√		وارسی کنید که تمام کارکردهای رمزنگاری، که برای حفاظت از اسرار در برابر کاربر استفاده میشوند، در سمت سرویسدهنده پیادهسازی میشوند.	١
√	✓		وارسی کنید که تمام مؤلفههای رمزنگاری بهصورت امن با شکست مواجه میشوند.	۲
✓	✓		وارسی کنید که تمام اسرار اصلی (یک اعتبارنامه ی برنامه ی کاربردی که بر روی دیسک ذخیره شده و برای دسترسی به اطلاعات پیکربندی امنیتی استفاده می شود) در برابر دسترسی غیرمجاز حفاظت شدهاند.	٣
√	✓		وارسی کنید که تمام اعداد تصادفی، نامهای تصادفی فایلها، GUIDهای تصادفی، و رشتههای تصادفی توسط ماژولهای رمزنگاری تأییدشده ایجاد شوند.	۶
√			وارسی کنید که تمام ماژولهای رمزنگاری توسط استاندارد FIPS 140-2 یا مشابه آن اعتبارسنجی شده است.	٧
√			وارسی کنید که تمام ماژولهای رمزنگاری در حالت تأییدشده و بر اساس سیاستهای تصویبشدهی خودشان عمل میکنند.	٨
✓	√		وارسی کنید که برای نحوه ی مدیریت کلیدهای رمزنگاری مقررات صریح وجود دارد. وارسی کنید که این مقررات به درستی اعمال شوند.	٩

جدول ه – نیازمندیهای رمزنگاری OWASP ASVS

نیازمندیهای وارسی مدیریت خطا و ثبت گزارش

		سطو2	نیازمندیهای وارسی مدیریت خطا و ثبت گزارش	
ш	μ	,		
✓	√	√	وارسی کنید که برنامه اطلاعات حساس مانند شناسهی نشست و اطلاعات شخصی را در خروجی پیغامهای خطا نمایش نمیدهد.	١
✓	✓		وارسی کنید که تمام فرآیندهای مدیریت خطا بر روی ابزارهای قابل اعتماد انجام میشود.	۲
✓	✓		وارسی کنید که تمام کنترلهای ثبت گزارش و ثبت وقایع در سمت سرویسدهنده پیادهسازی میشود.	٣
✓	✓		وارسی کنید که منطق مدیریت خطا در کنترلهای دسترسی، به طور پیشفرض از دسترسی جلوگیری می کند.	۴
✓	√		وارسی کنید که کنترلهای ثبت گزارش، توان ثبت حوادث امنیتی در هر دو حالت شکست و موفقیت را دارند.	۵
√	✓		وارسی کنید که هر رویداد ثبتشده شامل موارد زیر باشد: یک برچسب زمانی از منبع قابل اطمینان شدت رویداد رخ داده یک نشانه مبنی بر این که این رویداد امنیتی است (در شرایطی که گزارشها ترکیبی باشند) هویت کاربری که باعث این رویداد شده است (در شرایطی که کاربر در ایجاد رویداد سهیم بوده) آدرس IP مبدأ درخواست که منجر به این رویداد شده است موفقیت یا عدم موفقیت رویداد توضیحاتی در رابطه با رویداد	۶
✓			وارسی کنید که تمام رویدادهایی که شامل دادههای نامطمئن هستند، به عنوان کد در نرمافزار مشاهدهی گزارشها اجرا نشوند.	γ

		سطو2	نیازمندیهای وارسی مدیریت خطا و ثبت گزارش	
ш	ų	1		
√	√		وارسی کنید که گزارشهای امنیتی در برابر دسترسی و دستکاری غیرمجاز محافظت شدهاند.	٨
√			وارسی کنید که نرمافزار از یک پیادهسازی واحد (در سطح برنامه) برای ثبت وقایع استفاده می شود.	٩
✓	✓		وارسی کنید که برنامه اطلاعات حساس مخصوص برنامه از جمله شناسه ی نشست و اطلاعات شخصی، که ممکن است به مهاجم کمک کند را ثبت نمی کند. البته می توان وجود یا عدم وجود این گونه اطلاعات را ثبت کرد.	١٠
√	✓		وارسی کنید که ابزاری برای تحلیل گزارشها وجود دارد که به تحلیلگر اجازه میدهد در بین رویدادها، بر اساس معیارهای مدنظر جستجو کند.	11
√			وارسی کنید که تمام علائم و جداکنندههای غیرقابلنمایش به درستی در گزارشها رمزگذاری شدهاند تا از log injection جلوگیری شود.	۱۳
√			وارسی کنید که ورودیهای ثبتشده در گزارشها از جانب منابع مطمئن و نامطمئن، قابل تمایز باشند.	14
✓			وارسی کنید که ثبت گزارش پیش از اجرای تراکنش انجام شود. در چنین وضعیتی اگر ثبت گزارش با شکست مواجه شود (مثلاً حافظه پر باشد یا مجوز کافی نباشد)، برنامه به صورت امن شکست می خورد.	۱۵

جدول ٦ - نيازمندي هاي مديريت خطا و ثبت گزارش OWASP ASVS

نیازمندیهای وارسی حفاظت از داده

		سطو2	نیازمندیهای وارسی حفاظت از داده	
ш	μ	1		
√	√	✓	وارسی کنید که تمام فرمهایی که حاوی اطلاعات حساس هستند، امکان ثبت در حافظه ی نهان سمت کاربر، و همچنین تکمیل خودکار فرم را غیرفعال کردهاند.	١
✓			وارسی کنید که لیست تمام دادههای حساسی که برنامه پردازش می کند تعریف شده، و یک سیاست صریح برای کنترل دسترسی و رمزنگاری بر این دادهها وجود دارد. وارسی کنید که این سیاستها به درستی اعمال می شوند.	٢
✓	✓	√	وارسی کنید که تمام دادهای حساس درون بدنهی پیام HTTP به سرویسدهنده ارسال میشود (یعنی پارامترهای URL هیچگاه برای ارسال دادههای حساس بکار نمیروند).	٣
✓	✓		وارسی کنید که تمام نسخههای موقت و ذخیرهشده در حافظه ی نهان سمت کاربر در برابر دسترسی غیرمجاز حفاظتشده است، و یا پس از اتمام کار باطل (یا پاکسازی) می شود.	۴
✓	✓		وارسی کنید که تمام نسخههای موقت و ذخیرهشده در حافظهی نهان سمت سرویسدهنده در برابر دسترسی غیرمجاز حفاظتشده است، و یا پس از اتمام کار باطل (یا پاکسازی) میشود.	۵
√			وارسی کنید که راهکاری برای حذف دادههای حساس برنامه پس از اتمام زمان موردنیاز نگهداری آنها وجود دارد.	۶
√			وارسی کنید که برنامه، تعداد پارامترهای ارسالی به سیستمهای نامطمئن، مانند فیلدهای پنهان، متغیرهای Ajax، کوکیها، و مقادیر سرآیندها را به حداقل میرساند.	٧
√			وارسی کنید که برنامه توان شناسایی تعداد غیرطبیعی از درخواستهای اطلاعاتی، و پردازش تراکنشهای مهم را دارد، و در صورت بروز به سیستم اخطار میدهد. برای مثال یک کاربر معمولی نباید به بیش از پنج رکورد در دقیقه دسترسی یابد.	٨

نیازمندیهای وارسی ارتباطات

		سطو2	نیازمندیهای وارسی ارتباطات	
ш	ų	1		
√	√	√	وارسی کنید که می توان یک مسیر از هر $^{\text{CA}}$ معتبر به گواهی نامههای لایه ی انتقال امن $^{\text{TLS}}$) سرور ایجاد کرد، و گواهی نامههای هر سرور معتبر است.	١
✓			وارسی کنید که ارتباطات شکستخوردهی TLS به ارتباطات ناامن HTTP نزول نکنند.	۲
	√		وارسی کنید که برای تمام ارتباطات احراز هویت شده، یا شامل دادههای حساس، از TLS استفاده می شود.	٣
✓	✓		وارسی کنید که شکست ارتباطات TLS پشت خط ثبت میشوند.	۴
√			وارسی کنید که مسیرهای گواهی برای تمام گواهینامههای کاربران ایجاد و وارسی (به کمک علائم اعتماد و اطلاعات ابطال) شود.	۵
√	√		وارسی کنید که تمام ارتباطات به سیستمهای بیرونی، که شامل اطلاعات یا توابع حساس هستند، احراز هویت شوند.	۶
✓	✓		وارسی کنید که تمام ارتباطات به سیستمهای بیرونی، که شامل اطلاعات یا توابع حساس هستند، از یک حساب کاربری با حداقل دسترسی لازم برای اجرای صحیح برنامه استفاده می کنند.	٧
✓			وارسی کنید که یک استاندارد واحد پیادهسازی TLS در برنامه استفاده می شود و به گونه ای تنظیم شده است که در حالت تأییدشده فعالیت کند. (رجوع کنید به: (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140- 2/FIPS1402IG.pdf	٨
✓			وارسی کنید که رمزگذاری مخصوص کاراکترها برای تمام ارتباطات تعریف شده است (برای مثال UTF-8).	٩

[\] Certificate Authority

^r Transport Layer Security

نیازمندیهای وارسی امنیت HTTP

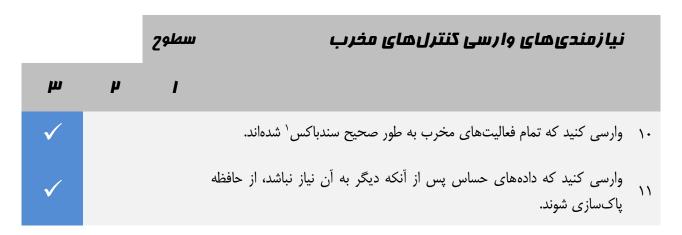
		سطو2	نیازمندیهای وارسی امینت HTTP	
ш	μ	,		
√	√	√	وارسی کنید که برنامه تنها متدهای تعریفشدهی HTTP مانند GET و POST را میپذیرد، و متدهای بلااستفاده را صریحاً منع میکند.	۲
√	✓	√	وارسی کنید که پاسخهای HTTP حاوی یک سرآیند نوع محتوا باشند که یک مجموعه کاراکتر امن (مانند 8-UTF) را تعیین میکنند.	٣
√	√		وارسی کنید که سرآیندهای HTPP در هر دو حالت درخواست و پاسخ تنها شامل کاراکترهای قابل نمایش ASCII هستند.	۶
√	√	✓	وارسی کنید که سرآیندهای HTTP، یا مکانیزم دیگری (برای مرورگرهای قدیمی تر) برای حفاظت در برابر حملات clickjacking وجود دارند.	٨
√	√		وارسی کنید که کاربران نهایی قادر نیستند سرآیندهای HTTP که توسط لایهی بیرونی اضافه شده و توسط برنامه استفاده می شوند را جعل کنند.	٩
√	✓		وارسی کنید که سرآیند X-Frame Options برای سایتهای که محتوای آنها نباید در X-Frame است. یک روش داده شود، استفاده شده است. یک روش میانی ارسال SAMEORIGIN است، به گونهای که تنها سایتهایی با منشأ یکسان بتوانند آن را در frame نمایش دهند.	١٠
✓	√		وارسی کنید که سرآیندهای HTTP اطلاعات حساس مؤلفههای سیستمی را فاش نمی کنند.	١٢

جدول ۹ – نیازمندیهای امنیت HTTP در OWASP ASVS

' Frontend

نیازمندیهای وارسی کنترلهای مخرب

		سطو2	نیازمندیهای وارسی کنترلهای مخرب	
ш	μ	1		
√			وارسی کنید که در کدهایی که به منظور توسعه یا تغییر برنامهی کاربردی استفاده شده، هیچ کد مخربی وجود نداشته باشد.	١
√			وارسی کنید که درستی کدهای تفسیرشده، کتابخانهها، فایلهای اجرایی، و فایلهای پیکربندی با استفاده از checksum یا درهمسازی وارسی شده است.	٢
✓			وارسی کنید که تمام کدهایی که کنترلهای احزار هویت را پیادهسازی کرده یا از آن استفاده میکنند، تحت تأثیر کدهای مخرب قرار نگرفتهاند.	٣
✓			وارسی کنید که تمام کدهایی که کنترلهای مدیریت نشست را پیادهسازی کرده یا از آن استفاده می کنند، تحت تأثیر کدهای مخرب قرار نگرفتهاند.	۴
✓			وارسی کنید که تمام کدهایی که کنترلهای دسترسی را پیادهسازی کرده یا از آن استفاده میکنند، تحت تأثیر کدهای مخرب قرار نگرفتهاند.	۵
✓			وارسی کنید که کنترلهای اعتبارسنجی ورودی تحت تأثیر کدهای مخرب قرار نگرفتهاند.	۶
√			وارسی کنید که تمام کدهایی که کنترلهای اعتبارسنجی خروجی را پیادهسازی کرده یا از آن استفاده می کنند، تحت تأثیر کدهای مخرب قرار نگرفتهاند.	٧
√			وارسی کنید که تمام کدهایی که ماژولهای رمزنگاری را پشتیبانی کرده یا از آن استفاده میکنند، تحت تأثیر کدهای مخرب قرار نگرفتهاند.	٨
√			وارسی کنید که تمام کدهایی که کنترلهای مدیریت خطا و ثبت خطا را پیادهسازی کرده یا از آن استفاده می کنند، تحت تأثیر کدهای مخرب قرار نگرفتهاند.	٩



جدول ۱۰ – نیازمندیهای کنترلهای مخرب OWASP ASVS

نیازمندیهای وارسی منطق کسبوکار

		سطو2	نیازمندیهای وارسی منطق کسبوکار	
ш	ų	ı		
	✓		وارسی کنید که برنامه تمام جریانهای منطق کسبوکار را در یک محیط مطمئن، مانند یک سرویسدهنده ی حفاظتشده و تحت نظارت، پردازش یا وارسی میکند.	
√	√		وارسی کنید که برنامه از تراکنشهای جعلی مهم، مانند آنهایی که به مهاجم اجازه میدهد نشست را دستکاری یا بازاجرا کند، جلوگیری میکند.	٢
√	√		وارسی کنید که برنامه اجازه نمی دهد که پارامترهای کسبوکار باارزش مانند قیمت، موجودی حساب، و شناسه دستکاری شوند.	٣
	✓		وارسی کنید که برنامه به کمک مکانیزمهایی مانند گزارشهای حفاظتشده و قابل تصدیق از تراکنشها، و گزارشهای ثبت سیستمی، در برابر حملات انکاری محافظت می کند.	۴
√	√		وارسی کنید که برنامه در برابر حملات افشای اطلاعات مانند ارجاع مستقیم به شئ، حملات brute-force نشست، و دیگر حملات محافظت می کند.	۵
√	✓		brute- وارسی کنید که برنامه مکانیزمهای شناسایی و حفاظت در برابر حملات force و منع سرویس 7 را دارد.	۶
√	✓		وارسی کنید که کنترلهای دسترسی برنامه در برابر حملات ترفیع مجوز ^۳ ، مانند دسترسی کاربران عادی به دادههای و قابلیتهای حفاظتشده، حفاظت می کند.	٧
✓	✓		وارسی کنید که جریانهای کسبوکار برنامه به ترتیب و مرحلهبهمرحله انجام میشوند، و مراحل خارج از ترتیب و ناقص پردازش نمیشوند.	٨

^{&#}x27;Repudiation attacks

^r Denial of Service

[&]quot; Elevated privilege

		سطو2	نیازمندیهای وارسی منطق کسبوکار	
ш	μ	ı		
✓	√		بر اساس حساسیت برنامه یا سابقه ی رخداد کلاهبرداری، وارسی کنید که برنامه از احراز هویت افزونه (مانند احراز هویت انطباقی) برای سیستمهای کمارزش، یا تفکیک مسئولیتها برای سیستمهای پرارزش، برای اعمال کنترلهای ضد کلاهبرداری استفاده می کند.	٩
✓	✓		وارسی کنید که برنامه دارای محدودیتهای کسبوکار بوده و آنها را در یک محیط امن (مانند یک سرویسدهندهی حفاظتشده)، بر مبنای کاربر و بر مبنای مصرف روزانه، اعمال می کند. برای مثال کاربران جدید سیم کارت نباید روزانه بیش از ۱۰ دلار مصرف کنند، یا پروندههای بیمارانی که یک پزشک می تواند به طور روزانه به آنها دسترسی داشته باشد نباید بیش از تعداد بیماران ممکنی باشد که یک پزشک می تواند در یک روز درمان کند.	١٠

جدول ۱۱ – نیازمندی های منطق کسبوکار OWASP ASVS

37

[`]Segregation of duties

نیازمندیهای وارسی پروندهها و منابع

		سطوح	نیازمندیهای وارسی پروندهها و منابع	
ш	μ	1		
√	√	√	وارسی کنید که باز⊣رسالها و تغییر مسیرهای URL ها شامل دادههای نامعتبر نباشند.	١
✓	✓	√	وارسی کنید که نام پروندهها و دادههای مسیر که از منابع نامطمئن دریافت میشود، به قالب استاندارد و مناسب تبدیل شود تا از حملات پیمایش مسیر جلوگیری شود.	۲
√	✓	✓	وارسی کنید که پروندههای دریافت شده از منابع نامطمئن توسط ابزارهای آنتیویروس پویش شده تا از آپلود محتوای مخرب شناختهشده جلوگیری شود.	٣
✓	✓	✓	وارسی کنید که پارامترهای دریافتشده از منابع نامطمئن برای تغییرات نام فایلها، نام مسیرها، یا اشیاء سیستم بکار نمیروند مگر آنکه ابتدا به قالب استاندارد تبدیل شده و اعتبارسنجی ورودی شوند تا از حملات local file جلوگیری شود.	۴
✓	✓	✓	وارسی کنید که پارامترهای دریافتی از منابع نامطمئن به قالب استاندارد تبدیل شده، اعتبارسنجی ورودی شده، و رمزگذاری خروجی شده تا از حملات remote file inclusion جلوگیری شود. (به ویژه مواردی که ورودی قابل اجرا باشد، مانند سرآیندها)	۵
√	✓	✓	وارسی کنید که IFRAMEها و اشتراکگذاری منابع بین دامنهای در HTML، اجازهی ورود محتوای خارجی غیر قراردادی را نمیدهد.	۶
	√		وارسی کنید که پروندههای دریافت شده از منابع نامطمئن خارج از webroot ذخیره می شوند.	٧
√	✓		وارسی کنید که تنظیمات پیشفرض سرویسدهنده ی وب یا برنامه به گونهای باشد که مانع دسترسی به منابع و سیستمهای خارجی شود.	٨

		سطو2	نیازمندیهای وارسی پروندهها و منابع	
ш	μ	1		
√	√		وارسی کنید که برنامه دادههای آپلود شده از منابع نامطمئن را اجرا نمی کند.	٩
✓	✓		وارسی کنید که آیا Silverlight ،Flash، یا هر نوع پیکربندی دیگری برای اشتراک گذاری منابع بین دامنهای، به گونهای تنظیم شده است که مانع دسترسی خارجی بدون احراز هویت و فاقد مجوز شود.	١٠

جدول ۱۲ – نیازمندیهای پروندهها و منابع OWASP ASVS

نیازمندیهای وارسی موبایل

		سطو2	نیازمندیهای وارسی موبایل	
ш	μ	1		
√	✓	√	وارسی کنید که گواهینامههای SSL در سمت کاربر اعتبارسنجی می شود.	١
√	✓	✓	وارسی کنید که مقادیر شناسهی منحصربهفرد دستگاه (UDID) برای کنترلهای امنیتی استفاده نمیشوند.	٢
✓	✓	✓	وارسی کنید که برنامه ی موبایل دادههای حساس را در منابع اشتراکی موبایل (کارت حافظه، پوشههای اشتراکی) ذخیره نمی کند.	٣
✓	✓	✓	وارسی کنید که دادههای حساس بر روی پایگاه دادهی SQLite در موبایل ذخیره نمی شود.	۴
✓	✓	✓	وارسی کنید که کلیدهای سری و کلمات عبور در کد برنامهی اجرایی ذخیره نشدهاند.	۵
√	✓	✓	وارسی کنید که دادههای حساس برنامه بهوسیلهی ویژگی auto-snapshot در سیستمعامل iOS افشاء نمیشوند.	۶
√	✓		وارسی کنید که برنامه بر روی دستگاههای jailbreak یا root شده قابل اجرا نباشد.	٧
√	✓		وارسی کنید که زمان منقضی شدن نشستها مقداری معقول باشد.	٨
✓ ✓ ✓	√		وارسی کنید که منابع درخواستشده و مجوزهای دسترسی به آن با یکدیگر تطابق داشته باشند (AndroidManifest.xml, iOS Entitlements).	٩
√	✓		وارسی کنید که گزارشهای crash برنامه حاوی دادههای حساس نباشد.	١٠
√	✓		وارسی کنید که کد برنامه مبهمسازی شده باشد ٔ تا عملکرد آن واضح نباشد.	11

		سطو2	نیازمندیهای وارسی موبایل	
ш	μ	1		
✓	✓		وارسی کنید که تمام دادههای آزمایشی از نگهدارندهی برنامه (ipa. یا apk.) حذف شدهاند.	17
√	✓		وارسی کنید که برنامه دادههای حساس را در گزارشات سیستمی یا حافظه ذخیره ثبت نمی کند.	۱۳
√	✓		وارسی کنید که برنامه قابلیت تکمیل خودکار را برای ورودیهای حساس مانند کلمهی عبور و اطلاعات بانکی غیرفعال کرده است.	14
√			وارسی کنید که برنامه قابلیت certificate pinning را پیادهسازی کرده تا از میانجی گری $^{\prime}$ ترافیک برنامه جلوگیری کند.	۱۵
√			وارسی کنید که فایل تنظیمات برنامه حاوی تنظیمات نادرست نبوده (مجوزهای خواند/نوشتن) و حالت پیشفرض تنظیمات حالت امنی است.	18
✓			وارسی کنید که کتابخانههای جانبی بروزرسانی شده و آسیبپذیر نیستند.	۱۷
√			وارسی کنید که دادههای وب، مانند ترافیک HTTPS در حافظه ی نهان ذخیره نمی شود.	١٨
✓			وارسی کنید که برای دادههای حساس از query string استفاده نمی شود. در عوض یک درخواست POST به همراه توکن CSRF از طریق SSL ارسال شود.	19
√			وارسی کنید که، در صورت امکان، شمارهحسابهای شخصی پیش از ذخیره بر روی دستگاه کوتاهسازی ^۲ شوند.	۲٠
√			وارسی کنید که برنامه از تصادفی سازی قالب فضای آدرس 7 استفاده می کند.	۲۱
√			وارسی کنید که دادههای ثبتشده بهوسیلهی صفحه کلید (iOS)، حاوی اعتبارنامهها، و اطلاعات مالی و حساس نیست.	77

[\] Proxying

^r Truncated

^r Address Space Layout Randomization (ASLR)

		سطو2	نیازمندیهای وارسی موبایل	
ш	μ	1		
✓			در سیستم عامل آندروید، وارسی کنید که برنامه فایلهایی با مجوزهای MODE_WORLD_WRITABLE یا MODE_WORLD_READABLE ایجاد نمی کند.	۲۳
✓			وارسی کنید که دادههای حساس به طور امن و رمزنگاریشده ذخیره میشوند (حتی هنگام ذخیرهسازی در iOS keychain)	74
√			وارسی کنید که مکانیزمهای مقابله با debugging و مهندسی معکوس در برنامه پیادهسازی شده است.	۲۵
✓			در سیستمعامل آندروید، وارسی کنید که برنامه فعالیتهای حساس، اهداف، و تهیه کنندگان محتوی را به بیرون درز نمی کند.	78
✓			وارسی کنید که برای رشتههای حساس مانند شماره حساب از ساختارهای تغییرپذیر استفاده شود، و این اطلاعات پس از اتمام نیاز بازنوشته شوند تا خسارات حملات تحلیل حافظه کاهش یابند.	77
√			وارسی کنید که تمام تولیدکنندگان محتوی و دریافتکنندگان اطلاعات که هویت آنها شناختهشده است، ورودیهای دریافتی را اعتبارسنجی کنند.	۲۸

جدول ۱۳ – نیازمندیهای موبایل OWASP ASVS

ضمیمه: لینکهای مفید

- OWASP Top Ten Project http://www.owasp.org/index.php/Top 10
- OWASP Code Review Guide http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- OWASP Testing Guide http://www.owasp.org/index.php/Testing_Guide
- OWASP Enterprise Security API (ESAPI) Project http://www.owasp.org/index.php/ESAPI
- OWASP Legal Project http://www.owasp.org/index.php/Category:OWASP Legal Project
- OWASP Top Ten Project http://www.owasp.org/index.php/Top_10
- OWASP Code Review Guide http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- OWASP Testing Guide http://www.owasp.org/index.php/Testing_Guide
- OWASP Enterprise Security API (ESAPI) Project http://www.owasp.org/index.php/ESAPI
- OWASP Legal Project http://www.owasp.org/index.php/Category:OWASP_Legal_Project