

السلامة

مهندسی آزمون امنیت، اعتبار سنجی و
تست نرم افزار



انتشارات مهرگان قلم

سرشناسه	مدیری، ناصر، ۱۳۴۱ -
عنوان و نام پدیدآور	مهندسی آزمون امنیت، اعتبار سنجی و تست نرم افزار / ناصر مدیری، طاهره نیری فرد
مشخصات نشر	تهران: مهرگان قلم، ۱۳۹۳.
مشخصات ظاهری	۲۰۴ ص.: مصور، جدول، نمودار.
شابک	978-600-6236-67-4
وضعیت فهرست نویسی	فیا :
موضوع	آزمایش نفوذ (ایمن سازی کامپیوتر) -- آزمون ها
موضوع	کامپیوترها -- ایمنی اطلاعات -- آزمون ها
موضوع	شبکه های کامپیوتری -- تدابیر ایمنی -- آزمون ها
موضوع	نرم افزار -- آزمایش
شناسه افزوده	نیری فرد، طاهره، ۱۳۴۳ -
رده بندی کنگره	QA۷۶۹/۱۳۷۱۳۹۳ ک۹/۹
رده بندی دیویی	۰۰۵/۸ :
شماره کتابشناسی ملی	۳۶۳۰۴۶۷ :

وب سایت: www.mehreganeghalam.com



نام کتاب: مهندسی آزمون امنیت، اعتبار سنجی و تست نرم افزار

مولف: دکتر ناصر مدیری، طاهره نیری فرد

ناشر: مهرگان قلم

نوبت چاپ اول: ۱۳۹۳

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۶۷-۴

تیراژ: ۵۰۰

قیمت: ۱۳۰۰۰ تومان

تکثیر تمام یا قسمتی از اثر بدون
مجوز کتبی ناشر ممنوع است و
متخلفان به موجب قانون حمایت
حقوق مولفان، مصنفان و
هنرمندان تحت پیگرد قانونی قرار
خواهند گرفت.

مرکز پخش

انتشارات مهرگان قلم:

تهران، میدان انقلاب، خیابان کارگر جنوبی، بعد از وحید نظری، کوچه گشتاسب، پلاک ۷، طبقه ۲

تلفن: ۰۹۱۲۳۱۴۶۰۵۸ - ۶۶۴۷۶۲۱۷ - ۶۶۴۷۷۲۲۴-۵

پیشگفتار

شکر و سپاس و منت و عزت خدای را پروردگار خلق و خداوند کبریا

اول، به نام الله آغاز می کنیم که آغاز هر انجام است. شکر و سپاس بر خداوند جهانیان که ما را توفیق انجام وظیفه با قلم خویش داد. هم او که انسان را از «خون بسته» آفرید و به او یاد داد آنچه را که نمی دانست.

مشکل نرم افزار نام امن، شاید مهمترین چالش فنی در زمان ما است. در حال حاضر امنیت، عامل محدود کننده اصلی در مورد آنچه که ما قادر به ایجاد با فن آوری اطلاعات هستیم می باشد. امنیت نرم افزار نظامی است که خصوصیات امنیتی نرم افزار را در مراحل طراحی، آزمایش، پیاده سازی و بکارگیری، مورد خطاب قرار می دهد یعنی در دوره زمانی تولید نرم افزار یا چرخه حیات گسترش نرم افزار، و شامل فعالیت های امنیتی زیادی مانند مدل کردن تهدید، مدیریت خطر و تست های امنیتی است. به سبب پیچیدگی روزافزون برنامه های کاربردی وب، روش سنتی تست امنیتی عملکرد که فقط مکانیزم امنیت نرم افزار را تست و اعتبار سنجی می کند در نمایان کردن نقص های امنیتی پنهان نرم افزار ناکارآمد شده است.

متأسفانه تولید و توسعه نرم افزار امن هنوز تبدیل به دانش نشده است یا قوانین سخت گیرانه ای تبیین نشده است و فرایند توسعه به صورت عمده برای کمینه کردن آسیب پذیری هایی که منجر به حملات می شوند، کنترل نمی شود. سامانه های رایانه ای و شبکه ها به صورت فزاینده ای توسط کیفیت و امنیت نرم افزارشان محدود شده اند. نقایص و آسیب پذیری های امنیتی در نرم افزار متداول شده اند و هنگامی که با حملات مخرب مورد استفاده قرار گیرند می توانند به مخاطرات جدی منجر شوند.

پژوهشی ها نشان می دهد که بر طرف کردن اشکالات امنیتی در مراحل اولیه و با استفاده از روش های نوین، بسیار مؤثرتر و کارآمدتر از برطرف کردن آنها در مراحل پیشرفته تر و با استفاده از روش هایی سنتی می باشد. بدیهی است که نمی توان نرم افزار امن را بدون انجام تست های امنیتی بر روی آن ایجاد کرد. با این حال بسیاری از سازمان های توسعه دهنده نرم افزار، تست امنیت را به عنوان بخشی از فرآیند استاندارد توسعه نرم افزار خود قرار نمی دهند. تست نرم افزار، تنها قدرت معصر به فردی است که میتواند متقاعد کند که مشکل وجود دارد.

در این راستا، کتاب پیش رو در شش فصل تألیف و تدوین شده است:

فصل اول - تست نرم افزار: این بخش به آشنایی کلی با مقوله تست نرم افزار می پردازد. در واقع اولین و مهمترین گام در جهت رسیدن به هدف این کتاب که همان تست امنیت نرم افزار می باشد، آشنایی با مفهوم تست است که بسیار ضروری می نماید. در این فصل چرخه حیات تست نرم افزار بررسی و سپس به معرفی انواع روش ها، استراتژی ها و سطوح مختلف آزمون پرداخته شده است. مطالعه این فصل دید جامعی نسبت به موضوع تست نرم افزار برای خوانندگان فراهم خواهد کرد.

فصل دوم - تست امنیت نرم افزار: می توان گفت مهمترین مسئله در بحث امنیت، درک مفهوم آن و درک مشکلات امنیتی موجود است. در واقع تا نقاط حساس و نقاط ضعف شناسایی نشوند، نمی توان در این حوزه به درستی گام برداشت. این فصل به معرفی عوامل مهم و مؤثر در امنیت نرم افزار می پردازد. همچنین مهمترین خطرات نرم افزاری و راه حل های رفع یا کاهش آن ها بررسی و در ادامه به معرفی انواع روش های تست امنیت پرداخته شده است.

فصل سوم - استاندارد تست نرم افزار OWASP: در این فصل به معرفی و بررسی استاندارد OWASP پرداخته ایم. پروژه آزادی که به منظور بالا بردن سطح امنیت برنامه های کاربردی تحت وب توسعه یافته است. شاید یکی از اصلی ترین سوالات در ذهن خوانندگان کتاب این باشد که چرا OWASP؟ در جواب این پرسش می توان گفت که بیشتر راهنماهای امنیتی موجود، فقط افراد را در مورد مشکل موجود نگران می کنند بدون اینکه اطلاعات کافی برای پیدا کردن، تشخیص و حل مشکلات امنیتی ارائه کنند. پروژه OWASP مهارت و ثبحر در این زمینه را در اختیار افرادی که به آن نیاز دارند، قرار می دهد. پروژه OWASP در تلاش است تا جهان را مکانی بسازد که در آن نرم افزار های نا امن، غیر عادی و نا به هنجار هستند.

فصل چهارم - روش تست نرم افزار ASVS: امنیت برنامه های کاربردی تحت وب از اهمیت زیادی برخوردار است. به این دلیل، تولیدکنندگان و استفاده کنندگان از آن ها نیاز به استنادی دارند تا از آن به عنوان معیاری مشترک برای رسیدن به درجه ای از اطمینان در امنیت یک برنامه کاربردی تحت وب استفاده کنند. در این فصل، استاندارد وارسی امنیت در برنامه های کاربردی معرفی می شود که چهار سطح برای وارسی امنیت برنامه های کاربردی تحت وب تعریف می کند و در هر سطح نیازمندی هایی را تعیین می کند که برای داشتن برنامه کاربردی امن باید آن ها را برآورده کرد.

فصل پنجم - تست برنامه های کاربردی وب بر اساس OWASP: این فصل به چگونگی به کارگیری ASVS در چرخه حیات نرم افزار و معرفی فازهای تست نرم افزار بر اساس چارچوب OWASP می پردازد و کنترل های تست ارائه شده توسط این استاندارد بررسی می شود.

فصل ششم - آزمایشگاه تست امنیت نرم افزار: به منظور انجام تست صحیح، انجام این پروسه در یک روال مشخص شده الزامی است. در این فصل، پس از معرفی چند آزمایشگاه مطرح در این زمینه، فرآیندهای مورد نیاز برای آزمایشگاه تست امنیت نرم افزار معرفی شده اند. همچنین آشنایی با ابزارهای تست نفوذ با قابلیت های مختلف به منظور به کارگیری عملی ارائه گردیده است.

در دنیای نرم افزار های امن، داشتن گام های صحیح در این راستا الزامی است. در نگاهی سطح بالا این گام ها را می توان بدین ترتیب بیان داشت:

گام اول: تست معمول و پایه که در این گام باید کاستی های سیستم شناسایی و کشف شود که چه فرآیندهایی صحیح انجام نشده. بررسی اینکه آیا کیفیت برآورده شده است یا نه در این گام باید مورد توجه قرار گیرد.

گام دوم: تست نفوذ در این مرحله باید ریسک های امنیتی بررسی شده و کاستی ها از منظر امنیتی مورد توجه قرار گرفته و تست نفوذ پذیری در قبال آسیب پذیری ها انجام شود.

گام سوم: رزمایش سایبری پس از گذر از گام های اول و دوم و با شناسایی راه های نفوذ و آسیب پذیری های امنیتی، حال این موضوع حیاتی می شود که آیا آمادگی مقابله با مشکلات شناسایی شده را داریم؟ در واقع با ورود به این حوزه و انجام رزمایش سایبری میزان آمادگی خود در برابر کاستی ها و نقاط مورد سوء استفاده را بررسی کنیم.

با توجه به اهداف این تألیف و معرفی فصول ذکر شده، این کتاب در پیشبرد اهداف امن کردن برنامه های کاربردی، در جایگاه دوم از گام های ذکر شده قرار خواهد گرفت. امیدواریم در تلاش برای نیل به این مقصود موفق بوده و این کتاب مورد استفاده دانشجویان و علاقمندان موضوع قرار گیرد.

از تمامی عزیزانی که در تهیه این کتاب به نحوی یاری رساندند، تشکر و قدرانی می نماییم. با امید به دریافت

فهرست مطالب

۱ تست نرم افزار

۲۴	۱-۱ خلاصه فصل
۲۴	۱-۲ تست نرم افزار چیست
۲۶	۳-۱ وابستگی تست و کیفیت
۲۷	۴-۱ دلایل اهمیت تست نرم افزار و پیامدهای عدم وجود آن
۲۸	۵-۱ چه موقع باید عمل تست انجام شود
۲۸	۶-۱ تست نرم افزار در تئوری و عمل
۲۸	۱-۶-۱ تئوری تست
۲۹	۲-۶-۱ تست در عمل
۲۹	۷-۱ تفاوت تست و اشکالزدایی
۳۰	۸-۱ مفاهیم بنیادی در تست نرم افزار
۳۰	۱-۸-۱ واریسی
۳۰	۱-۸-۲ اعتبارسنجی
۳۱	۱-۸-۳ تفاوت واریسی و اعتبار سنجی
۳۱	۱-۸-۴ ارزیابی
۳۱	۱-۸-۴-۱ قابلیت استفاده
۳۱	۲-۸-۴-۱ قابلیت تحمل
۳۱	۳-۸-۴-۱ قابلیت نگهداری
۳۱	۹-۱ چرخه حیات تست نرم افزار
۳۲	۱-۹-۱ فاز ۱: تحلیل نیازمندی ها
۳۳	۱-۹-۲ فاز ۲: برنامه ریزی تست
۳۳	۱-۹-۳ فاز ۳: توسعه نمونه تست
۳۴	۱-۹-۴ فاز ۴: آماده سازی محیط تست

۳۴	۵-۹-۱ فاز ۵: اجرای تست.....
۳۵	۶-۹-۱ فاز ۶: پایان یافتن چرخه آزمون.....
۳۶	۱-۱۰ زمان شروع تست.....
۳۶	۱-۱۱ زمان پایان تست.....
۳۷	۱-۱۲ اصول تست نرم افزار.....
۳۸	۱-۱۳ روش های تست نرم افزار.....
۳۸	۱-۱۳-۱ تست ایستا.....
۳۸	۲-۱۳-۱ تست پویا.....
۳۸	۱-۱۳-۲-۱ تست تابعی.....
۳۸	۲-۱۳-۲-۲ تست منطقی.....
۳۹	۳-۱۳-۱ مقایسه تست ایستا و پویا.....
۳۹	۱-۱۴ استراتژی های تست.....
۳۹	۱-۱۴-۱ استراتژی تست منطق.....
۳۹	۱-۱۴-۱-۱ تست جعبه سیاه.....
۴۰	۱-۱۴-۱-۱-۱ افراز هم ارزی.....
۴۰	۲-۱۴-۱-۱-۱ تحلیل مقدار مرزی.....
۴۰	۳-۱۴-۱-۱-۱ حدس خطا.....
۴۰	۴-۱۴-۱-۱-۱ نمودار علت و معلول.....
۴۱	۲-۱۴-۱-۱ تست جعبه سفید.....
۴۱	۱-۱۴-۱-۲-۱ تست منطقی.....
۴۱	۲-۱۴-۱-۲-۲ تست های اثبات ریاضی.....
۴۱	۳-۱۴-۱-۲-۲ تست های اتاق تمیز.....
۴۱	۳-۱۴-۱-۲ تست جعبه خاکستری.....
۴۲	۴-۱۴-۱-۲ مقایسه رویکرد تست جعبه سفید، خاکستری و سیاه.....
۴۳	۲-۱۴-۱ استراتژی چگونگی اجرای تست.....

۴۳	 تست بالا به پایین ۱-۱۴-۳-۱
۴۳	 تست پایین به بالا ۱-۱۴-۳-۲
۴۳	 سطوح تست ۱۵-۱
۴۴	 تست واحد ۱-۱۵-۱
۴۴	 تست یکپارچگی ۱-۱۵-۲
۴۴	 تست رابط مؤلفه ۱-۱۵-۳
۴۵	 تست سیستم ۱-۱۵-۴
۴۵	 تست پذیرش ۱-۱۵-۵
۴۶	 انواع تست ۱۶-۱
۴۶	 تست نصب و راه اندازی ۱-۱۶-۱
۴۶	 تست سازگاری ۱-۱۶-۲
۴۶	 تست دود ۱-۱۶-۳
۴۶	 تست رگرسیون ۱-۱۶-۴
۴۶	 تست الفبا ۱-۱۶-۵
۴۷	 تست پنا ۱-۱۶-۶
۴۷	 تست عملکرد ۱-۱۶-۷
۴۷	 تست غیر عملکرد ۱-۱۶-۸
۴۷	 تست مخرب ۱-۱۶-۹
۴۷	 تست کارایی نرم افزار ۱-۱۶-۱۰
۴۸	 تست قابلیت استفاده ۱-۱۶-۱۱
۴۸	 تست امنیت ۱-۱۶-۱۲
۴۸	 متریک های تست ۱۷-۱
۴۸	 متریک های نمونه تست ۱-۱۷-۱
۴۸	 متریک های پوشش ۱-۱۷-۲
۴۸	 متریک های خرابی ۱-۱۷-۳

۴۸..... ۱-۱۷-۳-۱ متوسط زمان برای خطا

۴۹..... ۱-۱۷-۳-۲ قابلیت اطمینان

۴۹..... ۱-۱۷-۳-۳ در دسترس بودن

۴۹..... ۱-۱۷-۴ متریک های قابلیت استفاده

۴۹..... ۱-۱۷-۴-۱ چگالی مشکلات قابلیت استفاده

۴۹..... ۱-۱۷-۴-۲ آسانی استفاده

۵۰..... ۱-۱۷-۴-۳ متریک سرعت کار

۵۰..... ۱-۱۷-۴-۴ بهره وری

۵۰..... ۱۸-۱ گواهینامه تست نرم افزار

۵۰..... ۱-۱۸-۱ انواع گواهینامه های تست نرم افزار

۵۰..... ۱-۱۸-۲ معرفی برخی از گواهینامه های تست

۵۱..... ۱۹-۱ استانداردهای تست نرم افزار

۵۱..... ۱-۱۹-۱ استاندارد ISO/IEC ۹۱۲۶

۵۲..... ۱-۱۹-۲ استاندارد ISO/IEC ۹۲۴۱-۱۱

۵۲..... ۱-۱۹-۳ استاندارد ISO/IEC ۲۵۰۰۰:۲۰۰۵

۵۲..... ۱-۱۹-۴ استاندارد ISO/IEC ۱۲۱۱۹

۵۳..... ۱-۱۹-۵ دیگر استانداردهای تست نرم افزار

۵۳..... ۲۰-۱ نتیجه گیری

۵۴..... ۲۱-۱ سوالات متداول

۵۴..... ۲۲-۱ منابعی برای مطالعات بیشتر

۲ تست امنیت نرم افزار

۵۶..... ۱-۱ خلاصه فصل

۵۶..... ۲-۱ امنیت نرم افزار چیست؟

۵۶..... ۳-۱ مهمترین عوامل برقراری امنیت

۵۷..... ۱-۳-۱ محرمانگی

- ۱-۳-۲ یکپارچگی..... ۵۷
- ۱-۳-۳ دسترس پذیری..... ۵۷
- ۴-۱ معرفی ۲۵ مورد از خطرناک ترین خطاهای نرم افزاری..... ۵۸
- ۱-۴-۱ نگاه طبقه بندی شده به خطاها..... ۶۰
- ۱-۴-۱-۱ تعامل نا امن بین مؤلفه ها..... ۶۱
- ۱-۴-۱-۲ مدیریت پرمخاطره منابع..... ۶۱
- ۱-۴-۱-۳ دفاع نفوذ پذیر..... ۶۲
- ۱-۴-۲ تسکین دهنده و راه حل های عمومی جهت کاهش اثر خطاها..... ۶۲
- ۱-۴-۲-۱ ایجاد و حفظ کنترل بر روی همه ورودی ها - M1..... ۶۲
- ۱-۴-۲-۲ ایجاد و حفظ کنترل بر همه خروجی ها - M2..... ۶۳
- ۱-۴-۲-۳ قفل کردن محیط - M3..... ۶۳
- ۱-۴-۲-۴ فرض اینکه مؤلفه های خارجی می توانند..... ۶۳
- تخریب و کدهای شما توسط هرکسی خوانده شوند - M4..... ۶۴
- ۱-۴-۲-۵ استفاده از ویژگی های امنیتی پذیرفته شده..... ۶۴
- در صنعت به جای نوع آوری - M5..... ۶۴
- ۱-۴-۲-۶ استفاده از کتابخانه ها و چارچوب هایی..... ۶۴
- که اجتناب از ضعف های معرفی شده را آسان می سازند - GP1..... ۶۵
- ۱-۴-۲-۷ یکپارچه کردن امنیت به سرتاسر..... ۶۵
- چرخه حیات توسعه نرم افزار - GP2..... ۶۵
- ۱-۴-۲-۸ استفاده از ترکیب گسترده ای..... ۶۵
- از روش ها برای پیدا کردن و جلوگیری ضعف به طور جامع - GP3..... ۶۵
- ۱-۴-۲-۹ اجازه به کلاینت های قفل شده برای تعامل با نرم افزار - GP4..... ۶۵
- ۱-۴-۳ نگاشت تسکین دهنده ها به ۲۵ خطای مهم نرم افزاری..... ۶۶
- ۱-۴-۴ مقایسه ۲۵ خطای CWE با ده آسیب پذیری مهم OWASP..... ۶۷
- ۵-۱ تست امنیت نرم افزار چیست؟..... ۶۸
- ۶-۱ دلایل تست امنیت نرم افزار..... ۶۸
- ۷-۱ تست امنیت در مقابل تست متعارف نرم افزار..... ۶۹
- ۸-۱ چه زمانی تست امنیت نرم افزار استفاده می شود..... ۶۹
- ۹-۱ برنامه های نیازمند به تست امنیت..... ۶۹

۶۹	۱۰-۱ اصول و قواعد انجام تست امنیت
۷۲	۱۱-۱ تکنیک های تست امنیت
۷۲	۱-۱۱-۱ بازیابی و بازرسی دستی
۷۳	۱-۱۱-۲ مدل سازی تهدید
۷۳	۱-۱۱-۳ بازیابی کد
۷۳	۱-۱۱-۴ تست نفوذ
۷۴	۱-۱۱-۵ مقایسه ۴ تکنیک تست امنیت
۷۵	۱۲-۱ روش های اصلی تست امنیت
۷۵	۱-۱۲-۱ تست امنیت رسمی
۷۵	۱-۱۲-۲ تست امنیت مبتنی بر مدل
۷۶	۱۳-۱ تست امنیت مبتنی بر تزریق خطا
۷۶	۱-۱۳-۱ تست فازی
۷۶	۱-۱۳-۲ تست بررسی آسیب پذیری
۷۷	۱-۱۳-۳ تست مبتنی بر صفت خاص
۷۷	۱-۱۳-۴ تست امنیت مبتنی بر جعبه سفید
۷۷	۱-۱۳-۵ تست امنیت مبتنی بر ریسک
۷۷	۱۴-۱ رویکرد تست امنیت
۷۹	۱۵-۱ تست امنیت در بحث سیستم مدیریت امنیت اطلاعات
۷۹	۱۶-۱ استاندارد ISO/IEC ۲۷۰۳۴ - راهنمای امنیت برنامه کاربردی
۸۰	۱-۱۶-۱ هدف
۸۰	۱-۱۶-۲ فرایندها
۸۱	۱-۱۶-۳ کنترل امنیت برنامه کاربردی
۸۱	۱۷-۱ استاندارد ISO/IEC ۱۵۴۰۸ - معیارهای ارزیابی برای امنیت محصولات IT
۸۱	۱۸-۱ نتیجه گیری
۸۲	۱۹-۱ سوالات متداول

۲۰-۱ منابعی برای مطالعات بیشتر..... ۸۳

۳ استاندارد تست نرم افزار: OWASP

۱-۱ خلاصه فصل..... ۸۶

۲-۱ آشنایی با پروژه امنیت نرم افزار تحت وب باز..... ۸۶

۳-۱ مخاطرات امنیتی برنامه های کاربردی..... ۸۷

۱-۳-۱ رتبه بندی مخاطرات بر اساس روش OWASP..... ۸۷

۱-۳-۲ بررسی ده مخاطره مهم وب سایت ها در سال ۲۰۱۳ و راهکار آن ها از نگاه OWASP..... ۸۷

۱-۳-۲-۱ تزریق (A1)..... ۸۸

۱-۳-۲-۲ احراز هویت و مدیریت نشست نقض شده (A2)..... ۸۹

۱-۳-۲-۳ نفوذ به سایت ها از طریق اسکریپ نویسی (A3)..... ۹۰

۱-۳-۲-۴ ارجاعات شیء مستقیم نا امن (A4)..... ۹۱

۱-۳-۲-۵ پیکربندی نادرست امنیت (A5)..... ۹۲

۱-۳-۲-۶ در معرض قرار گرفتن اطلاعات حساس (A6)..... ۹۴

۱-۳-۲-۷ از دست رفتن کنترل دسترسی سطح عملکرد (A7)..... ۹۵

۱-۳-۲-۸ جعل درخواست خارج از وب سایت (A8)..... ۹۷

۱-۳-۲-۹ استفاده از مؤلفه ها با آسیب پذیری های شناخته شده (A9)..... ۹۸

۱-۳-۲-۱۰ تغییرمسیردهی و انتقال های نامعتبر (A10)..... ۹۹

۴-۱ پروژه فرآیند تضمین امنیت نرم افزار OWASP..... ۱۰۰

۱-۴-۱ تضمین نرم افزار واقعا چیست؟..... ۱۰۰

۱-۴-۲ معرفی فرآیندهای تضمین امنیت نرم افزار..... ۱۰۰

۱-۴-۲-۱ فرآیند های یکپارچه کردن امنیت نرم افزار در SDLC..... ۱۰۱

۱-۴-۲-۲ فرآیند شناسایی نیازمندی های امنیت..... ۱۰۲

۱-۴-۲-۳ فرآیند بازبینی امنیت معماری و طراحی..... ۱۰۲

۱-۴-۲-۴ فرآیند بازبینی کد امن..... ۱۰۳

۱-۴-۲-۵ فرآیند تست امنیت..... ۱۰۳

۱۰۳..... ۱-۴-۲-۶ فرآیند بازیابی امنیت استقرار

۱۰۳..... ۱-۴-۲-۷ فرآیند بازیابی امنیت انتشار

۱۰۳..... ۵-۱ نتیجه گیری

۱۰۴..... ۶-۱ سوالات متداول

۱۰۴..... ۷-۱ منابعی برای مطالعات بیشتر

۴ روش تست نرم افزار: ASVS

۱۰۶..... ۱-۱ خلاصه فصل

۱۰۶..... ۲-۱ نحوه استفاده از استاندارد ASVS

۱۰۸..... ۳-۱ چگونگی رویکرد ASVS

۱۰۹..... ۴-۱ به کارگیری ASVS در چرخه حیات توسعه نرم افزار

۱۰۹..... ۵-۱ بررسی سطوح چهارگانه ASVS

۱۱۰..... ۱-۵-۱ سطح ۱ - واری اتوماتیک

۱۱۰..... ۱-۵-۱-۱ سطح ۱A - اسکن بویا (واری اتوماتیک جزئی)

۱۱۱..... ۱-۵-۱-۲ سطح ۱B - اسکن کد منبع (واری اتوماتیک جزئی)

۱۱۱..... ۱-۵-۲ سطح ۲ - واری دستی

۱۱۲..... ۱-۵-۲-۱ سطح ۲A - تست امنیت (واری دستی جزئی)

۱۱۲..... ۱-۵-۲-۲ سطح ۲B واری کد (واری دستی جزئی)

۱۱۲..... ۱-۵-۳ سطح ۳ - واری طرح

۱۱۲..... ۱-۵-۴ سطح ۴ - واری داخلی

۱۱۳..... ۱-۵-۵ حداقل نیازهای سطح بالا برای سطوح مختلف ASVS

۱۱۴..... ۱-۵-۶ نیازهای تفصیلی واری در ASVS

۱۱۴..... ۱-۵-۶-۱ واری ۱. نیازهای مستندسازی معماری امنیتی

۱۱۵..... ۱-۵-۶-۲ واری ۲. نیازمندی های واری اجزاز هویت

۱۱۷..... ۱-۵-۶-۳ واری ۳. نیازمندی های واری مدیری نشست

۱۱۸..... ۱-۵-۶-۴ واری ۴. نیازمندی های واری مکانیزم دستیابی

- ۱۳۰..... ۵-۵-۶-۵ واری ۵. نیازمندی های واری صحت ورودی.
- ۱۳۱..... ۶-۵-۶-۶ واری ۶. نیازمندی های واری کدگذاری / اسکیپ خروجی.
- ۱۳۲..... ۷-۵-۶-۷ واری ۷. نیازمندی های واری رمزنگاری.
- ۱۳۴..... ۸-۵-۶-۸ واری ۸. نیازمندی های واری مدیریت یا کنترل خطا و گزارش گیری.
- ۱۳۶..... ۹-۵-۶-۹ واری ۹. نیازمندی های واری حفاظت داده.
- ۱۳۶..... ۱۰-۵-۶-۱۰ واری ۱۰. نیازمندی واری امنیت اطلاعات.
- ۱۳۸..... ۱۱-۵-۶-۱۱ واری ۱۱. نیازمندی های واری امنیت HTTP.
- ۱۳۹..... ۱۲-۵-۶-۱۲ واری ۱۲. نیازمندی های واری تنظیم امنیت.
- ۱۳۰..... ۱۳-۵-۶-۱۳ واری ۱۳. نیازمندی های جستجوی کد مخرب.
- ۱۳۰..... ۱۴-۵-۶-۱۴ واری ۱۴. نیازمندی های واری امنیت داخلی.
- ۱۳۱..... ۶-۱ نتیجه گیری.
- ۱۳۱..... ۷-۱ سوالات متداول.
- ۱۳۱..... ۸-۱ منابعی برای مطالعات بیشتر.
- ۵ تست برنامه های کاربردی وب بر اساس OWASP**
- ۱۳۴..... ۱-۱ خلاصه فصل.
- ۱۳۴..... ۲-۱ راه اندازی چرخه حیات توسعه نرم افزار با فعالیت های واری ASVS.
- ۱۳۴..... ۱-۲-۱ گام اول.
- ۱۳۵..... ۱-۲-۲ گام دوم.
- ۱۳۵..... ۱-۲-۳ گام سوم.
- ۱۳۵..... ۱-۲-۴ گام چهارم.
- ۱۳۶..... ۳-۱ چارچوب تست بر اساس OWASP.
- ۱۳۶..... ۱-۳-۱ فاز اول - پیش از شروع توسعه.
- ۱۳۷..... ۱-۳-۱-۱ فاز ۱A: بازبینی سیاست ها و استانداردها.
- ۱۳۷..... ۱-۳-۱-۲ فاز ۱B: توسعه اندازه گیری و معیار متریک ها (تضمین قابلیت ردیابی).
- ۱۳۷..... ۱-۳-۲ فاز دوم - تست در زمان تعریف و طراحی.

- ۱۳۸..... ۱-۳-۳ فاز سوم- تست در طی توسعه.
- ۱۳۸..... ۱-۳-۳-۱ فاز ۳A: جلسه بررسی کند.
- ۱۳۸..... ۱-۳-۳-۲ فاز ۳B: بازیابی های کند.
- ۱۳۸..... ۱-۳-۴ فاز چهارم - تست در طی مستقر کردن.
- ۱۳۸..... ۱-۳-۴-۱ فاز ۴A: تست نفوذ برنامه کاربردی.
- ۱۳۹..... ۱-۳-۴-۲ فاز ۴B: تست مدیریت پیگیر بندی.
- ۱۳۹..... ۱-۳-۵ فاز پنجم- تعمیر و نگهداری و بهره برداری.
- ۱۳۹..... ۱-۳-۵-۱ فاز ۵A: نگهداری و عملیات.
- ۱۳۹..... ۱-۳-۵-۲ فاز ۵B: انجام بررسی های وضعیت سلامت به صورت دوره ای.
- ۱۳۹..... ۱-۳-۵-۳ فاز ۵C: تضمین تأیید تغییر.
- ۱۳۹..... ۱-۳-۵-۴ یک نمونه جریان کاری تست SDLC.
- ۱۴۰..... ۴-۱ تست های نفوذ برنامه های کاربردی تحت وب بر اساس OWASP.
- ۱۴۰..... ۱-۴-۱ تست نفوذ برنامه های کاربردی تحت وب چیست؟
- ۱۴۰..... ۱-۴-۲ آسیب پذیری، تهدید، تست.
- ۱۴۱..... ۱-۴-۳ معرفی متدولوژی تست OWASP.
- ۱۴۱..... ۱-۴-۳-۱ حالت انفعالی.
- ۱۴۱..... ۱-۴-۳-۲ حالت فعال.
- ۱۴۱..... ۱-۴-۴ معرفی کنترل های تست OWASP.
- ۱۴۴..... ۱-۴-۴-۲ جمع آوری اطلاعات.
- ۱۴۴..... ۱-۴-۴-۲-۱ OWASP-IG-001 - روپات ها و خزنده ها.
- ۱۴۵..... ۱-۴-۴-۲-۲ OWASP-IG-002 - کشف/شناسایی موتور جستجو.
- ۱۴۵..... ۱-۴-۴-۲-۳ OWASP-IG-003 - شناسایی نقاط ورود به برنامه کاربردی.
- ۱۴۵..... ۱-۴-۴-۲-۴ OWASP-IG-004 - تست اثرانگشت برنامه کاربردی تحت وب.
- ۱۴۶..... ۱-۴-۴-۲-۵ OWASP-IG-005 - کشف برنامه کاربردی.
- ۱۴۶..... ۱-۴-۴-۲-۶ OWASP-IG-006 - تحلیل کدهای خطا.

۱۴۶.....	۱-۴-۴-۱ تست مدیریت پیکر بندی
۱۴۶.....	۱-۴-۴-۱-۱ OWASP-CM-001 - SSL/TLS تست
۱۴۶.....	۱-۴-۴-۱-۲ OWASP-CM-002 - تست شنود کننده پایگاه داده
۱۴۷.....	۱-۴-۴-۱-۳ OWASP-CM-003 - تست مدیریت پیکربندی زیرساخت
۱۴۷.....	۱-۴-۴-۱-۴ OWASP-CM-004 - تست مدیریت پیکربندی برنامه کاربردی
۱۴۷.....	۱-۴-۴-۱-۵ OWASP-CM-005 - تست مدیریت فرمت های فایل
۱۴۸.....	۱-۴-۴-۱-۶ OWASP-CM-006 - تست فیل های قدیمی، پشتیبان و ارجاع داده نشده
۱۴۸.....	۱-۴-۴-۱-۷ OWASP-CM-007 - رابطه های ادمین برنامه زیرساخت و کاربردی
۱۴۸.....	۱-۴-۴-۱-۸ OWASP-CM-008 - XST و HTTP تست مندهای
۱۴۹.....	۱-۴-۴-۲ تست تصدیق
۱۴۹.....	۱-۴-۴-۲-۱ OWASP-AT-001 - انتقال گواهی نامه ها بر روی یک کانال رمز شده
۱۴۹.....	۱-۴-۴-۲-۲ OWASP-AT-002 - تست جهت شمارش کاربر
۱۴۹.....	۱-۴-۴-۲-۳ OWASP-AT-002 - تست حساب کاربری قابل حدس (دیکشنری)
۱۴۹.....	۱-۴-۴-۲-۴ OWASP-AT-004 - Brute Force تست
۱۵۰.....	۱-۴-۴-۲-۵ OWASP-AT-005 - تست دور زدن طرح های احراز هویت
۱۵۰.....	۱-۴-۴-۲-۶ OWASP-AT-006 - تست آسیب پذیر بودن به یادآوری پسورد و بازیابی آن
۱۵۰.....	۱-۴-۴-۲-۷ OWASP-AT-007 - تست مدیریت خروج و حافظه نهان مرورگر
۱۵۰.....	۱-۴-۴-۲-۸ OWASP-AT-008 - CAPTCHA تست
۱۵۰.....	۱-۴-۴-۲-۹ OWASP-AT-009 - تست احراز هویت عوامل چندگانه
۱۵۱.....	۱-۴-۴-۲-۱۰ OWASP-AT-010 - تست شرایط رقابت
۱۵۱.....	۱-۴-۴-۳ مدیریت نشست
۱۵۱.....	۱-۴-۴-۳-۱ OWASP-SM-001 - تست طرح مدیریت نشست
۱۵۱.....	۱-۴-۴-۳-۲ OWASP-SM-002 - تست ویژگی های کوکی ها
۱۵۲.....	۱-۴-۴-۳-۳ OWASP-SM-003 - تست تثبیت نشست
۱۵۲.....	۱-۴-۴-۳-۴ OWASP-SM-004 - تست متغیرهای افشاء شده نشست

۱۵۳.....	OWASP-SM-005 - CSRF تست ۱-۴-۴-۳-۵
۱۵۳.....	تست مجوز ۱-۴-۴-۴
۱۵۳.....	OWASP-AZ-001 - تست پیمایش مسیر ۱-۴-۴-۴-۱
۱۵۳.....	OWASP-AZ-002 - تست دور زدن طرح مجوز قانونی ۱-۴-۴-۴-۲
۱۵۳.....	OWASP-AZ-003 - تست بالا بردن حق ویژه ۱-۴-۴-۴-۳
۱۵۳.....	OWASP-BL-001 - تست منطق کسب و کار ۱-۴-۴-۵
۱۵۳.....	تست اعتبارسنجی داده ها ۱-۴-۴-۶
۱۵۴.....	OWASP-BL-001 - XSS منعکس شده ۱-۴-۴-۶-۱
۱۵۴.....	OWASP-BL-002 - XSS ذخیره شده ۱-۴-۴-۶-۲
۱۵۴.....	OWASP-BL-003 - XSS بر پایه DOM ۱-۴-۴-۶-۳
۱۵۴.....	OWASP-BL-004 - Cross Site Flashing ۱-۴-۴-۶-۴
۱۵۴.....	OWASP-BL-005 - SQL تزریق ۱-۴-۴-۶-۵
۱۵۵.....	OWASP-BL-006 - LDAP تزریق ۱-۴-۴-۶-۶
۱۵۵.....	OWASP-BL-007 - ORM تزریق ۱-۴-۴-۶-۷
۱۵۵.....	OWASP-BL-008 - XML تزریق ۱-۴-۴-۶-۸
۱۵۵.....	OWASP-BL-009 - SSI تزریق ۱-۴-۴-۶-۹
۱۵۶.....	OWASP-BL-010 - XPath تزریق ۱-۴-۴-۶-۱۰
۱۵۶.....	OWASP-BL-011 - IMAP/SMTP تزریق ۱-۴-۴-۶-۱۱
۱۵۶.....	OWASP-BL-012 - تزریق کد ۱-۴-۴-۶-۱۲
۱۵۶.....	OWASP-BL-013 - فرمان دادن به سیستم عامل ۱-۴-۴-۶-۱۳
۱۵۶.....	OWASP-BL-014 - سر ریز بافر ۱-۴-۴-۶-۱۴
۱۵۶.....	OWASP-BL-015 - تست آسیب پذیری تکوین یافته ۱-۴-۴-۶-۱۵
۱۵۷.....	OWASP-BL-016 - HTTP تکه کردن/قاچاق ۱-۴-۴-۶-۱۶
۱۵۷.....	تست انکار سرویس ۱-۴-۴-۷
۱۵۷.....	OWASP-DS-001 - SQL Wildcard تست حملات ۱-۴-۴-۷-۱

۱۵۷.....	OWASP-DS-002 - OWASP-DS-002	۱-۴-۴-۷-۲
۱۵۷.....	OWASP-DS-003 - OWASP-DS-003	۱-۴-۴-۷-۳
۱۵۷.....	OWASP-DS-004 - OWASP-DS-004	۱-۴-۴-۷-۴
۱۵۷.....	OWASP-DS-005 - OWASP-DS-005	۱-۴-۴-۷-۵
۱۵۸.....	OWASP-DS-006 - OWASP-DS-006	۱-۴-۴-۷-۶
۱۵۸.....	OWASP-DS-007 - OWASP-DS-007	۱-۴-۴-۷-۷
۱۵۸.....	OWASP-DS-008 - OWASP-DS-008	۱-۴-۴-۷-۸
۱۵۸.....	تست سرویس های وب	۱-۴-۴-۸
۱۵۸.....	OWASP-WS-001 - OWASP-WS-001	۱-۴-۴-۸-۱
۱۵۸.....	OWASP-WS-002 - WSDL	۱-۴-۴-۸-۲
۱۵۸.....	OWASP-WS-003 - XML	۱-۴-۴-۸-۳
۱۵۹.....	OWASP-WS-004 - XML	۱-۴-۴-۸-۴
۱۵۹.....	OWASP-WS-005 - HTTP در REST/GET	۱-۴-۴-۸-۵
۱۵۹.....	OWASP-WS-006 - SOAP	۱-۴-۴-۸-۶
۱۵۹.....	OWASP-WS-007 - تست بازپخش	۱-۴-۴-۸-۷
۱۵۹.....	AJAX	۱-۴-۴-۹
۱۵۹.....	OWASP-AJ-001 - AJAX	۱-۴-۴-۹-۱
۱۶۰.....	OWASP-AJ-002 - AJAX	۱-۴-۴-۹-۲
۱۶۰.....	۵- نتیجه گیری	
۱۶۰.....	۶- سوالات متداول	
۱۶۰.....	۷- منابعی برای مطالعات بیشتر	
۶ آزمایشگاه تست امنیت نرم افزار		
۱۶۲.....	۱-۱ خلاصه فصل	
۱۶۲.....	۲-۱ معرفی آزمایشگاه های تست امنیت نرم افزار	
۱۶۲.....	۱-۲-۱ CTL آزمایشگاه	

۱۶۲	Ounce آزمایشگاه
۱۶۳	Bug Huntress آزمایشگاه
۱۶۳	۳-۱ وظایف آزمایشگاه امنیت نرم افزار
۱۶۳	۴-۱ متدولوژی ایجاد آزمایشگاه امنیت نرم افزار
۱۶۳	۱-۴-۱ طراحی آزمایشگاه امنیت نرم افزار
۱۶۳	۱-۴-۱-۱ بخش فنی
۱۶۴	۱-۴-۱-۲ بخش مدیریتی
۱۶۴	۱-۴-۲ پیاده سازی آزمایشگاه امنیت نرم افزار
۱۶۵	۵-۱ فرآیندهای ایجاد آزمایشگاه امنیت نرم افزار
۱۶۵	۱-۵-۱ اندازه گیری و تحلیل امنیت نرم افزار
۱۶۶	۱-۵-۲ شناسایی و تست متداول ترین کنترل های امنیتی
۱۶۶	۱-۵-۳ مدل سازی تهدیدات
۱۶۷	۱-۵-۳-۱ رویکرد مهاجم-محور
۱۶۷	۱-۵-۳-۲ رویکرد نرم افزار-محور
۱۶۷	۱-۵-۳-۳ رویکرد دارایی-محور
۱۶۷	۱-۵-۴ کاهش خطاهای رایج برنامه نویسی
۱۶۷	۱-۵-۵ ارائه خطاها به منظور شناسایی الگوی رفتاری ناشناخته و جلوگیری از ایجاد آن
۱۶۸	۱-۵-۵-۱ CybOX: بیان قابل مشاهده سایبری
۱۶۸	۱-۵-۵-۲ CAPEC: شمارش و دسته بندی الگوهای متداول حمله
۱۶۸	۱-۵-۶ انجام تست های امنیتی عملی با استفاده از ابزارهای موجود
۱۶۸	۱-۶ ابزارهای تست امنیت نرم افزار
۱۶۸	۱-۶-۱ دسته بندی ابزارهای تست امنیت
۱۶۸	۱-۶-۱-۱ ابزارهای منبع باز تست جعبه سیاه
۱۶۹	۱-۶-۱-۲ ابزارهای تجاری تست جعبه سیاه
۱۶۹	۱-۶-۱-۳ ابزارهای منبع باز/رایگان تحلیلگر کد منبع

۱۶۹.....	۱-۶-۱-۴ ابزارهای تجاری تحلیلگر کد منبع.....
۱۷۰.....	۱-۶-۱-۵ ابزارهای منبع باز تست پذیرش.....
۱۷۰.....	۱-۶-۱-۶ ابزارهای تست آسیب پذیری های خاص.....
۱۷۱.....	۱-۶-۲ معرفی برخی از اسکنرهای امنیتی.....
۱۷۱.....	۱-۶-۲-۱ نرم افزار Netsparker.....
۱۷۱.....	۱-۶-۲-۱-۱ امکانات نرم افزار.....
۱۷۲.....	۱-۶-۲-۱-۲ معرفی برخی خروجی های اصلی برنامه.....
۱۷۲.....	۱-۶-۲-۲ نرم افزار Acunetix Web Vulnerability Scanner.....
۱۷۳.....	۱-۶-۲-۲-۱ امکانات نرم افزار.....
۱۷۳.....	۱-۶-۲-۲-۲ معرفی برخی خروجی های اصلی برنامه.....
۱۷۴.....	۱-۶-۲-۳ نرم افزار Subgraph Vega.....
۱۷۴.....	۱-۶-۲-۳-۱ امکانات نرم افزار.....
۱۷۵.....	۱-۶-۲-۳-۲ معرفی برخی خروجی های اصلی برنامه.....
۱۷۵.....	۱-۶-۴ نرم افزار Owasp Zed Attack Proxy.....
۱۷۶.....	۱-۶-۴-۱ امکانات نرم افزار ZAP.....
۱۷۶.....	۱-۶-۴-۵ نرم افزار W3af.....
۱۷۷.....	۱-۶-۴-۶ نرم افزار AppScan - IBM.....
۱۷۷.....	۱-۶-۴-۶-۱ ویرایش ها.....
۱۷۷.....	۱-۶-۴-۷ نرم افزار ParosPro - MileSCAN Technologies.....
۱۷۷.....	۱-۶-۳ توزیع Kali لینوکس، ابزاری برای تست امنیت نرم افزار.....
۱۷۸.....	۱-۶-۳-۱ مجموعه ابزارهای تست نفوذ در توزیع Kali.....
۱۷۹.....	۱-۶-۴ الویت به کارگیری ابزارها.....
۱۸۱.....	۷-۱ پدافند غیر عامل.....
۱۸۱.....	۱-۷-۱ سطوح فعالیت ها.....
۱۸۱.....	۱-۷-۱-۱ سطح حیاتی.....

- ۱۸۱..... ۱-۷-۱-۲ سطح حساس
- ۱۸۱..... ۱-۷-۱-۳ سطح مهم
- ۱۸۱..... ۱-۷-۲ برخی ملاحظات پدافند غیرعامل در ارتباط با آزمایشگاه تست امنیت نرم افزار
- ۱۸۲..... ۸-۱ نتیجه گیری
- ۱۸۲..... ۹-۱ سوالات متداول
- ۱۸۲..... ۱۰-۱ منابعی برای مطالعات بیشتر
- ۱۸۳..... ضمیمه ۱ چک لیست های واری و اعتبار سنجی مرتبط با سیاست های امنیتی در فازهای SDLC
- ۱۹۱..... ضمیمه ۲ راه حل ها و ارائه دهندگان تست ۲۰ کنترل مهم امنیتی
- ۱۹۹..... ضمیمه ۳ واژه نامه انگلیسی به فارسی