

۱۹۱۰۹۲۵

امنیت API پیشرفته

Advanced API Security

Securing APIs With OAuth 2.0
Open ID Connect JWS And JWE

نویسنده : بهمان سیرواردنا

مترجم : پژمان حسین



**NAGHOOS
PUBLICATION**

سرشناسه

سیریواردنا، پرابات

Siriwardena, Prabath

عنوان و نام پدیدآور

امنیت API پیشرفته/ نویسنده: پرابات سیریواردنا، مترجم: پژمان حسینی،

مشخصات نشر

تهران: ناخوس، ۱۳۹۷.

مشخصات ظاهری

۲۹۴ص: مصور، جدول، نمودار

شابک

978-600-473-131-7 : ۳۸۵۰۰۰ ریال

وضعیت فهرست نویسی

فیبا

یادداشت

عنوان اصلی: Advanced API security: securing APIs with OAuth2.0

OpenID Connect, JWS, and JWE, [2014]

موضوع

رابط های برنامه سازی کاربردی

موضوع

Application program interfaces (Computer software):

موضوع

رابط های برنامه سازی کاربردی - تدابیر ایمنی

موضوع

Application program interfaces (Computer software) - Security measures:

شناسه افزوده

حسینی، پژمان، ۱۳۶۰-، مترجم

رده بندی کنگره

۱۳۹۷ س ۹ ۷۶/۷۶/۲ QA

رده بندی دیویی

۰۰۵/۳:

شماره کتابخانه ملی

۵۲۳۶۲۵۳:



NAQHOOS
PUBLICATION

برای خرید Online به آدرس زیر مراجعه کنید:

www.naqhoospress.com

انتشارات ناخوس

نام کتاب

امنیت API پیشرفته

نویسنده

سیریواردنا، پرابات

مترجم

پژمان حسینی

ناشر

انتشارات ناخوس

چاپ اول

۱۳۹۷

تیراژ

۱۰۰ جلد

چاپ و صحافی

نارنجستان

قیمت

۳۸۵،۰۰۰ ریال

شابک

۹۷۸-۶۰۰-۴۷۳-۱۳۱-۷

ISBN

978-600-473-131-7

این حق برای سرمایه گذار محفوظ است. این کتاب یا قسمتی از این اثر بصورت حرفه ای یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: انتشارات ناخوس

۱- بلوار کشاورز- خیابان ۱۶ آذر- کوچه پارسی- پلاک ۱۰

تلفاکس: ۶۶۴۷۸۹۵۴-۶۶۴۷۸۹۵۱

فهرست

۱۱	مقدمه
۱۳	پیشگفتار مترجم
۱۵	فصل اول - MANAGED APIS
۱۹	API در مقایسه با API مدیریت شده.....
۲۰	API در برابر Service.....
۲۲	شناسایی و توصیف API ها.....
۲۳	API های مدیریت شده در عمل.....
۲۳	تویینتر API.....
۲۴	مراحل ارتباط با API تویینتر.....
۲۶	Salesforce API.....
۲۶	دسترسی Salesforce API.....
۲۹	خلاصه.....
۳۱	فصل ۲ - SECURITY BY DESIGN
۳۲	چالش های طراحی.....
۳۲	راحتی کاربر.....
۳۲	کارایی.....
۳۳	حمله های خودی.....
۳۴	امنیت توسط ابهام.....
۳۴	اصول طراحی.....
۳۴	کمترین امتیاز.....
۳۴	پیش فرض های شکست خورده.....
۳۵	اقتصاد مکانیسم.....
۳۵	واسطه کامل.....
۳۵	طراحی باز.....
۳۵	جداسازی مجوز.....
۳۵	پذیرش روانشناختی.....
۳۶	محرمانه بودن، یکپارچگی، دسترسی (CIA).....
۳۶	محرمانه بودن.....

۳۸	تمامیت
۳۸	دسترسی
۴۰	کنترل های امنیتی
۴۰	احراز هویت
۴۱	چیزی هایی که می دانید
۴۲	چیزی که شما هستید
۴۲	مجوز
۴۲	کنترل دسترسی اختیاری (DAC) در مقابل کنترل دسترسی اجباری (MAC)
۴۵	تجدید حساب
۴۶	حسابر می
۴۶	الگوهای امنیتی
۴۶	الگوی تایید مستقیم
۴۸	مدیریت مجوزها
۵۰	احراز هویت بیومتریک
۵۱	منطقه الگوی سبز مهر و موم شد
۵۲	مضرترین الگوی مشترک
۵۲	الگو تأییدی کارگذار
۵۳	الگوی کنترل دسترسی مبتنی بر سیاست
۵۶	مدل سازی تهدید
۵۸	خلاصه
۵۹	فصل ۳- HTTP BASIC/DIGEST AUTHENTICATION
۶۰	تایید هویت پایه ای HTTP
۶۰	دسترسی به API GITHUB با استفاده از پروتکل اصلی HTTP
۶۱	تایید هویت مختصر HTTP
۶۴	کارخانه CUTE-CUPCAKE استفاده از دستور العمل API در Apache Tomcat
۶۶	تنظیم پروتکل سرور (LDAP) APACHE
۶۹	اتصال آپاچی تامکت به سرور (LDAP) APA CHE
۶۹	حفاظت از یک API با استفاده از پروتکل HTTP
۷۱	فعال سازی TLS در آپاچی تامکت
۷۳	حفاظت از API Recipe با استفاده از HTTPS DIGEST

۷۴	خلاصه
۷۵	فصل ۴- احراز هویت با TLS
ERROR! BOOKMARK NOT DEFINED.	MUTUAL AUTHENTICATION WITH TLS
۷۶	تکامل TLS
۷۷	TLS، چگونه کار می کند؟
۷۸	TLS Handshake
۸۱	انتقال داده های برنامه
۸۱	کلیدهای کریپتوگرافیک در TLS
۸۵	شناسایی یک API امن با توزیع مجدد TLS و استفاده از cURL
۸۷	مقایسه JKS و PKCS #12
۸۷	قوانین محرمانه
۸۸	مهندسی مجدد TLS
۹۰	خلاصه
۹۱	فصل ۵ - IDENTITY DELEGATION
۹۲	نمایندگی مستقیم در جلسه نمایندگی 'ro'ere
۹۵	Google ClientLogin
۹۶	ورود مشتری گوگل با curl
۹۸	Google AuthSub
۹۹	GOOGLE AUTHSUB WITH CURL
۱۰۱	اعتبار API در Flickr
۱۰۲	اعتبار API در Flickr با Curl
۱۰۴	اعتبار سنجی مبتنی بر مرورگر یاهو (BBAuth)
۱۰۵	یاهو BBAUTH با CURL
۱۰۸	خلاصه
۱۰۹	فصل ۶ - OAUTH 1.0
۱۱۰	ارائه TOKEN
۱۱۱	فاز درخواست اعتبار موقت
۱۱۳	فاز تأیید مالک منابع
۱۱۴	مراحل تقاضای اعتبارنامه
۱۱۵	با استفاده از OAuth 1.0 به یک API تجاری ایمن بروید

۱۱۶.....	Demystifying oauth_signature
۱۲۱.....	OAuth 1.0 با API های توئیتر
۱۲۴.....	OAuth سه پایه در مقابل OAuth دو پایه
۱۲۵.....	WRAP OAuth
۱۲۶.....	خلاصه
۱۲۷.....	فصل ۷ - OAuth 2.0
۱۲۸.....	OAuth WRAP
۱۲۸.....	حساب کاربری و نمایه رمز عبور
۱۳۰.....	نمایه رمز عبور و حساب کاربری
۱۳۱.....	نمایه Web App
۱۳۲.....	نمایه Rich App
۱۳۳.....	دسترسی به API های محافظت شده WRAP
۱۳۳.....	WRAP به OAuth 2.0
۱۳۳.....	انواع OAuth 2.0 Grant
۱۳۶.....	Implicit Grant Type
۱۳۷.....	Resource Owner Password Credentials Grant Type
۱۳۹.....	Client Credentials Grant Type
۱۳۹.....	OAuth 2.0 Token Types
۱۴۰.....	OAuth 2.0 Bearer Token Profile
۱۴۱.....	OAuth 2.0 Client Types
۱۴۲.....	SECURING THE WHITE CUPCAKE FACTORY RECIPE API WITH OAUTH 2.0
۱۴۴.....	دریافت Token دسترسی با احراز هویت کد اعطای OAuth 2.0
۱۴۵.....	دریافت Token دسترسی با نوع کد اعطای مجازی OAuth 2.0
۱۴۶.....	دریافت Token دسترسی با منابع نوع اعطای صاحب اعتبار نامه کلمه عبور OAuth 2.0
۱۴۷.....	دریافت Token دسترسی با نوع اعتبارنامه مشتری OAuth 2.0
۱۴۷.....	Token تازه سازی OAuth 2.0
۱۴۸.....	OAuth 2.0 و فیس بوک
۱۵۰.....	ثبت نام برنامه مشتری با فیس بوک
۱۵۰.....	دریافت Token دسترسی برنامه OAuth از طریق فیس بوک
۱۵۲.....	دریافت Token دسترسی OAuth از طریق فیس بوک

دریافت Token دسترسی به صفحه OAUTH از طریق فیس بوک.....	۱۵۴
OAuth 2.0 و LinkedIn.....	۱۵۶
ثبت نام مشتری با LINKEDIN.....	۱۵۶
دسترسی به LINKEDIN APIS با مشتری OAUTH.....	۱۵۷
OAuth 2.0 و Salesforce.....	۱۵۹
ثبت نام برنامه مشتری با Salesforce.....	۱۵۹
دریافت Token دسترسی از طریق جریان احراز هویت وب سرور SALESFORCE.....	۱۶۰
تهیه توکن دسترسی از طریق فروش مجدد نام کاربری برای رمز عبور و ورود به سیستم.....	۱۶۳
OAuth 2.0 and Google.....	۱۶۴
ثبت نام درخواست مشتری با GOOGLE.....	۱۶۴
تهیه توکن دسترسی رای و سایت های کاربردی گوگل از طریق جریان احراز هویت.....	۱۶۵
تهیه توکن دسترسی از طریق تبادل تصویب درخواست گوگل.....	۱۶۷
تهیه توکن دسترسی از طریق درخواست اعتبارنامه احراز هویت.....	۱۶۹
تهیه توکن دسترسی از طریق جریان احراز هویت.....	۱۷۰
خلاصه ای از اجرای ارائه دهنده OAUTH 2.0.....	۱۷۱
احراز هویت در مقابل مجوز.....	۱۷۲
خلاصه.....	۱۷۳
فصل ۸ - OAUTH 2.0 MAC TOKEN PROFILE.....	۱۷۵
OAuth 2.0 و جاده ای به سمت جهنم.....	۱۷۶
Bearer Token vs. MAC Token.....	۱۷۷
گرفتن یک توکن MAC.....	۱۷۸
OAuth 2.0: اطلاعات مخاطبان.....	۱۷۹
محاسبه MAC.....	۱۸۲
HTTP REQUEST-LINE.....	۱۸۳
اعتبار MAC توسط سرور منبع.....	۱۸۴
انواع اعطای OAuth و نمایه MAC Token.....	۱۸۵
OAuth 1.0 در مقابل OAuth 2.0 MAC Token Profile.....	۱۸۶
خلاصه.....	۱۸۶
فصل ۹ - OAUTH 2.0 PROFILES.....	۱۸۷
نمایه درون گرایی توکن.....	۱۸۸

۱۸۹.....	کنترل دسترسی ACCESS FINE-DRILLED با XACML
۱۹۱.....	XACML و درون گرایی توکن OAuth
۱۹۴.....	نمایه ی اعطای نوع زنجیره ای.....
۱۹۵.....	نمایه ثبت نام مشتری دینامیک.....
۱۹۷.....	نمایه لغو Token.....
۱۹۹.....	از دست دادن Token دسترسی Sasleforce.....
۱۹۹.....	خلاصه.....
۲۰۱	فصل ۱۰- USER MANAGED ACCESS (UMA)
۲۰۲.....	محافظت از خدمات.....
۲۰۷.....	UMA و OAuth.....
۲۰۸.....	معماری UMA.....
۲۰۸.....	فاز های UMA.....
۲۰۹.....	فاز ۱ UMA: حفاظت از منابع.....
۲۱۱.....	فاز ۲ UMA: گرفتن مجوز.....
۲۱۶.....	فاز ۳ UMA: دسترسی به منابع محافظت شده.....
۲۱۶.....	API های UMA.....
۲۱۷.....	محافظت API.....
۲۱۸.....	مجوز API.....
۲۱۸.....	نقش UMA در امنیت API.....
۲۱۹.....	خلاصه.....
۲۲۱	فصل ۱۱- FEDERATION
۲۲۲.....	فعال نمودن Federation.....
۲۲۴.....	زبان نشانه گذاری توافق امنیتی (SAML).....
۲۲۵.....	نمایه SAML 2.0 برای OAuth: احراز هویت مشتری.....
۲۲۷.....	مشخصات SAML 2.0 برای OAuth: نوع اعطا کردن.....
۲۲۹.....	نوع اعطا کردن SAML 2.0 حامل برای OAUTH با سرور IDENTITY WSO2.....
۲۳۰.....	نوع اعطای SAML 2.0 BEARER برای OAUTH با SERVER IDENTITY WSO2.....
۲۳۴.....	مشخصات JWT برای احراز هویت و مجوز مشتری OAuth 2.0.....
۲۳۴.....	خلاصه.....
۲۳۵	فصل ۱۲- OPENID CONNECT

۲۳۶.....	یک تاریخچه مختصر از OpenID Connect
۲۳۶.....	OPENID QUICK START
۲۳۹.....	AMAZON از OPEN ID استفاده می کند!
۲۳۹.....	درک OpenID Connect
۲۳۹.....	تشریح توکن شناسایی
۲۴۱.....	OPENID CONNECT WITH WSO2 IDENTITY SERVER
۲۴۳.....	درخواست اتصال OpenID
۲۴۵.....	درخواست ویژگی های کاربر
۲۴۷.....	نوع اعطا برای اتصال OpenID
۲۴۸.....	درخواست خصوصیات سفارشی کاربر
۲۴۹.....	اتصال OPENID با گزین
۲۵۱.....	کشف OpenID Connect
۲۵۴.....	ابر داده ارائه دهنده شناسه Connect OpenID
۲۵۵.....	ثبت نام پویای مشتری OpenID Connect
۲۵۷.....	OpenID Connect برای امنیت API ها
۲۵۸.....	خلاصه
۲۵۹.....	فصل ۱۳ - JWT, JWS, AND JWE
۲۶۰.....	توکن وب JSON
۲۶۲.....	ایجاد JWT PLAINTEXT
۲۶۴.....	گروه کاری JOSE
۲۶۵.....	JSON Web Signature
۲۶۷.....	الگوریتم های امضا
۲۶۷.....	Serialization
۲۶۹.....	ایجاد JWT با HMAC-SHA256
۲۷۰.....	ایجاد یک JWT امضا شده با RSA-SHA256
۲۷۲.....	رمزگذاری JSON Web
۲۷۴.....	رمزگذاری محتوا در مقابل بسته شدن کلید
۲۷۵.....	Serialization
۲۷۶.....	تولید JWT رمزگذاری شده با AES و RSA-OAEP
۲۸۰.....	خلاصه

۲۸۲.....	Subsystem Trusted	احراز هویت مستقیم با الگوی
۲۸۳.....		تنها ورودی با الگوی کنترل دسترسی
۲۸۴.....	Integrated Windows Authentication	یک ورودی تنها با الگوی
۲۸۵.....		Proxy هویت با الگو کنترل دسترسی مجاز
۲۸۶.....	JSON Web Token	کنترل دسترسی مجاز با الگو
۲۸۷.....		عدم انکار با الگو امضای وب JSON
۲۸۹.....	Chained Access Delegation Pattern	
۲۹۰.....	Trusted Master Access Delegation Pattern	
۲۹۲.....		خدمات امنیتی توکن (STS) با الگوی نمایندگی کنترل دسترسی
۲۹۳.....		نماینده کنترل دسترسی با الگوی اعتبارنامه پنهان
۲۹۴.....		خلاصه

مقدمه

API ها برای به نمایش گذاشتن ویژگی های و خواص Business در نرم افزارها ، به همه جا (REST)، به طور فزاینده ای محبوب شده اند. بر طبق اطلاعات منتشر شده توسط Layer7، ۸۶٫۵ درصد از سازمان ها حداقل یک نرم افزار بر پایه API در پنج سال آینده خواهند داشت. از این تعداد، ۴۳٫۲٪ در حال حاضر یکی از این نرم افزارها را دارند. API ها همچنین پایه و اساس ایجاد کانال های ارتباطی در اینترنت اشیا (IoT) می باشند، از وسایل نقلیه موتوری تا لوازم آشپزخانه، اقلام بی شماری شروع به برقراری ارتباط با یکدیگر از طریق API ها می کنند. سیسکو برآورد می کند که تا سال ۲۰۲۰ تا ۵۰ میلیارد دستگاه بتواند به اینترنت متصل شود.

این کتاب در مورد تأمین امنترین API های شماست. همانطور که در مورد طراحی هر سیستم نرم افزاری وجود دارد ، مردم معمولاً عناصر امنیتی را در مرحله طراحی API نادیده می گیرند. آنها فقط در زمان استقرار با ریسکها، یکپارچه سازی و تکمیل ، توجه به موارد امنیتی را آغاز می کنند. امنیت هرگز نباید بعد از طراحی باشد ، این بخشی جدایی ناپذیر از طراحی هر سیستم نرم افزاری است و باید از ابتدای طراحی به آن توجه شده باشد. یکی از اهداف این کتاب این است که شما را در مورد نیاز به امنیت و گزینه های موجود برای امنیت یک API آموزش دهد. این کتاب شما را از طریق یک فرآیند مشخص هدایت می کند و بهترین شیوه ها را برای طراحی API ها برای امنیت جامع به اشتراک می گذارد.

امنیت API در پنج سال گذشته بسیار پیشرفت کرده است. چند استانداردها نشان داده شده است OAuth 2.0 ، استاندارد ترین استاندارد است. اما این چیزی بیش از یک استاندارد است ، این یک چارچوب است که به مردم اجازه می دهد استانداردها را بر روی آن بسازند. این کتاب به طور عمیق توضیح می دهد چگونه از API های امنیتی، از سنتی HTTP Basic Authentication تا OAuth 2.0 و استانداردهای ساخته شده در کنار آن، از قبیل OpenID Connect، مدیریت دسترسی کاربر (UMA) و بسیاری دیگر چگونه باید استفاده نمود.

JSON نقش مهمی در ارتباطات API ایفا می کند. اکثر API های توسعه یافته امروز تنها از JSON پشتیبانی می کنند، نه XML، این کتاب همچنین بر امنیت JSON تمرکز دارد. JSON Web Encryption (JWE) و JSON Web Signature (JWS) دو عنصر مهم آن هستند. استانداردهای به طور فزاینده ای برای امنیت پیام های JSON استفاده می شوند ، بخش دوم این کتاب جزئیات JWE و JWS را پوشش خواهد داد.

یکی دیگر از اهداف مهم این کتاب این است که نه تنها مفاهیم و نظریه ها را ارائه دهد، بلکه هر یک از آنها را با نمونه های خاص توضیح می دهد. این کتاب نمونه ای جامع از مواردی است که با API ها از گوگل، توییتر، فیس بوک، یاهو، Salesforce، Flickr و GitHub کار می کنند.

تکامل امنیت API موضوع دیگری است که در این کتاب مورد بررسی قرار گرفته است. بسیار مهم است که بدانیم پروتکل های امنیتی در گذشته چگونه طراحی شده اند و چگونه نقاط ضعف در آنها کشف شده است. این کتاب شامل جزئیات، برخی از پروتکل های امنیتی قدیمی مانند Flickr Authentication، Yahoo! BBAuth، Google AuthSub، Google ClientLogin، و ProtectServe نیز می باشد.

امیدوارم این کتاب به طور موثری برای این عنوان پرکاربرد و با اهمیت برای توسعه دهندگان API کاربردی باشد و نیازهای آنان را پوشش دهد و امیدوارم از خواندن آن لذت ببرید. انتشار این فناوری های جدید ممکن می تواند به طور مستقیم سرعت و کارایی بی سابقه ای به تعداد زیادی از مردم عرضه کند. اما هزینه های بالا به این معنی است که کنترل جریان اطلاعات در دست چند نفر انتخاب می شود. کنترل اطلاعات به یک روش متمرکز و یکپارچه تبدیل شده بود که الگوی بخش را تحت تأثیر قرار می داد. اما تهریه های وسیع رسانه ها در اطراف این فناوری رسانه ای وسیع رشد می کنند. که هویت ملی را به وجود آورند و دولت های مستبد را مجبور می کنند تا تبلیغات را به راحتی گسترش دهند.