

فهرست مطالب

۱	فصل ۱. انتخاب یک برنامه باگ بانتهی
۵-۱-۱	برنامه های دستگاه های تلفن همراه (اندروید، iOS و ویندوز).....
۶-۱-۲	APIها.....
۷-۱-۳	سورس کد و برنامه های اجرایی.....
۷-۱-۴	سخت افزار و اینترنت اشیا.....
۸-۱-۵	پلتفرم های برنامه های باگ بانتهی.....
۹-۱-۵-۱	نکات مثبت.....
۱۰-۱-۵-۲	و همچنین معایب.....
۱۱-۱-۶	محدوده (Scope) برنامه.....
۱۳-۱-۶-۱	مبالغ پرداختی.....
۱۳-۱-۶-۲	زمان پاسخ.....
۱۴-۱-۶-۳	برنامه های خصوصی (Private Programs).....
۱۶-۱-۷	انتخاب برنامه ایده آل.....
۱۹	فصل ۲. تداوم موفقیت شما
۱۹-۲-۱	نوشتن یک گزارش موثر.....
۱۹-۲-۱-۱	ابتدا یک عنوان توصیفی بنویسید.....
۲۰-۲-۱-۲	مرحله ۲: ارائه یک خلاصه مختصر.....
۲۱-۲-۱-۳	مرحله ۳: یک ارزیابی شدت انجام دهید.....
۲۱-۲-۱-۳-۱	شدت کم (Low severity).....
۲۱-۲-۱-۳-۲	شدت متوسط (Medium severity).....

- ۲۱.....(High severity) شدت بالا) ۲-۱-۳-۳
- ۲۲.....(Critical severity) شدت حیاتی) ۲-۱-۳-۴
- ۲۳..... مرحله ۴: دستورالعمل های تولید مجدد واضح را ارائه دهید ۲-۱-۴
- ۲۴..... در مرحله ۵ یک اثبات مفهوم ارائه دهید. ۲-۱-۵
- ۲۵..... مرحله ۶: شرح سناریوهای ضربه و حمله ۲-۱-۶
- ۲۶..... مرحله ۷: اقدامات کاهش بالقوه را توصیه کنید. ۲-۱-۷
- ۲۶..... مرحله ۸: اعتبارسنجی گزارش ۲-۱-۸
- ۲۷..... پیشنهادات بیشتر برای گزارش نویسی بهتر ۲-۱-۹
- ۲۷..... هیچ فرضیه ای نسازید ۲-۱-۹-۱
- ۲۷..... مختصر و شفاف عمل کنید ۲-۱-۹-۲
- ۲۸..... آنچه می خواهید بخوانید را بنویسید ۲-۱-۹-۳
- ۲۸..... با احترام رفتارکن ۲-۱-۹-۴
- ۲۸..... برقراری ارتباط با تیم توسعه ۲-۲
- ۲۹..... درک وضعیت گزارش ۲-۲-۱
- ۲۹..... نیاز به جزئیات بیشتر ۲-۲-۲
- ۳۱..... پرداختن به تعارضات ۲-۲-۳
- ۳۲..... توسعه یک رابطه (Building a Partnership) ۲-۲-۴
- ۳۳..... درک عملکرد ناموفق شما ۲-۳
- ۳۴..... چرا باگ ها را کشف نمی کنید ۲-۳-۱
- ۳۶..... چرا گزارش های شما رد می شوند ۲-۳-۲
- ۳۹..... چگونه در هنگام گیر کردن ادامه دهید ۲-۴
- ۴۰..... اول، استراحت کنید! ۲-۴-۱
- ۴۰..... مرحله ۲: مجموعه مهارت های خود را بسازید ۲-۴-۲
- ۴۱..... مرحله ۳: یک دیدگاه جدید به دست آورید ۲-۴-۳
- ۴۲..... در نهایت، چند کلمه در مورد تجربه ۲-۴-۴

۴۳	فصل ۳. طرز کارکرد شبکه اینترنت
۴۳.....	۳-۱. مدل سرور - کلاینت
۴۵.....	۳-۲. سیستم نام دامنه
۴۶.....	۳-۳. پورت های اینترنت
۴۷.....	۳-۴. ریکوانست ها و ریسپانس های HTTP
۵۱.....	۳-۵. اقدامات ایمنی اینترنت
۵۱.....	۳-۵-۱. کدگذاری محتوا
۵۳.....	۳-۵-۲. مدیریت نشست ها و کوکی های HTTP
۵۵.....	۳-۵-۳. احراز هویت با استفاده از توکن ها
۵۶.....	۳-۵-۴. وب توکن های JSON
۵۸.....	۳-۵-۵. دستکاری میدان alg (Manipulating the alg Field)
۶۰.....	۳-۵-۶. خواندن داده های حساس
۶۰.....	۳-۵-۷. سیاست The Same-Origin Policy
۶۲.....	۳-۶. برنامه نویسی را یاد بگیرید
۶۳	فصل ۴. آماده سازی محیط زیست و بازرسی ترافیک (Traffic Inspection)
۶۳.....	۴-۱. انتخاب یک سیستم عامل
۶۴.....	۴-۲. پیکربندی ضروریات: یک مرورگر وب و یک پروکسی
	۴-۲-۱. راه اندازی مرورگر وب جاسازی شده (Opening the
۶۵.....	Embedded Browser)
۶۶.....	۴-۲-۲. پیکربندی فایرفاکس
۷۰.....	۴-۲-۳. راه اندازی Burp
۷۳.....	۴-۳. استفاده از Burp
۷۷.....	۴-۳-۱. Interuder
۸۰.....	4-3-2. Repeater
۸۱.....	۴-۳-۳. دیکودر (Decoder)
۸۲.....	۴-۳-۴. Comparer

۸۳.....	ذخیره ریکوئست های برپ.....	۴-۳-۵
۸۳.....	نکته پایانی در مورد ..یادداشت برداشتن.....	۴-۴

فصل ۵. ریکان وب هکینگ

۸۶.....	عبور دستی از هدف.....	۵-۱
۸۷.....	Google Dorking.....	5-2.
۹۲.....	کشف دامنه.....	۵-۳
۹۲.....	WHOIS و همچنین Reverse WHOIS.....	۵-۳-۱
۹۳.....	آدرس های پروتکل اینترنت.....	۵-۳-۲
۹۵.....	Certificate Parsing.....	۵-۳-۳
۹۶.....	کاوش ساب دامنه ها.....	۵-۳-۴
۹۸.....	کاوش سرویس.....	۵-۳-۵
۱۰۰.....	بروت فورس کردن دایرکتوری.....	۵-۳-۶
۱۰۱.....	اسپایدرینگ وب سایت (Spidering the Site).....	۵-۳-۷
۱۰۵.....	میزبانی توسط شخص ثالث (Third-Party Hosting).....	۵-۳-۸
۱۰۸.....	ریکان GitHub.....	۵-۳-۹
۱۱۰.....	سایر روش های مخفی OSINT.....	۵-۴
۱۱۳.....	Tech Stack Fingerprinting.....	5-5.
۱۱۵.....	نوشتن اسکریپت ریکان خودتان.....	۵-۶
۱۱۶.....	آشنایی با اصول برنامه نویسی Bash.....	۵-۶-۱
۱۲۰.....	ذخیره خروجی ابزار در فایل.....	۵-۶-۲
۱۲۲.....	افزودن تاریخ اسکن در خروجی.....	۵-۶-۳
۱۲۳.....	افزودن گزینه هایی برای انتخاب ابزارهای اجرایی.....	۵-۶-۴
۱۲۴.....	استفاده از ابزارهای اضافی.....	۵-۶-۵
۱۲۸.....	تجزیه و تحلیل نتایج (Parsing the Results).....	۵-۶-۶
۱۳۱.....	ساخت یک گزارش اصلی.....	۵-۶-۷
۱۳۳.....	اسکن کردن چند دامنه.....	۵-۶-۸

۱۶۱	فصل ۶. آسیب پذیری Cross-Site Scripting
۱۶۲	۶-۱ مکانیسم ها
۱۶۸	۶-۲ انواع XSS
۱۶۸	۶-۲-۱ Stored XSS
۱۷۰	۶-۲-۲ Blind XSS
۱۷۰	۶-۲-۳ Reflected XSS
۱۷۱	۶-۲-۴ XSS مبتنی بر DOM
۱۷۳	6-2-5. Self XSS
۱۷۴	۶-۳ پیشگیری
۱۷۶	۶-۴ هانت کردن XSS
۱۷۷	۶-۴-۱ مرحله ۱: ورودی های بالقوه را جستجو کنید
۱۷۹	۶-۴-۲ مرحله دوم: درج Payloads
۱۷۹	۶-۴-۳ فراتر از تگ <script>
۱۸۵	۶-۴-۴ مرحله ۳: بررسی اثر
۱۸۵	۶-۵ دور زدن حفاظت XSS
۱۸۵	۶-۵-۱ سیستمس متفاوت جاوا اسکریپت
۱۸۶	۶-۵-۲ حروف بزرگ و انکودینگ
۱۸۷	۶-۵-۳ خطاهای منطقی فیلتر
۱۸۸	۶-۶ افزایش سطح حمله
۱۸۹	۶-۷ خودکارسازی شکار XSS
۱۹۰	۶-۸ پیدا کردن اولین XSS شما!
۱۹۱	فصل ۷. آسیب پذیری Open Redirects
۱۹۱	۷-۱ مکانیسم ها
۱۹۳	۷-۲ پیشگیری
۱۹۴	۷-۲-۱ هانت کردن اوپن ریدایرکت ها
۱۹۴	۷-۲-۲ مرحله اول: Redirect Parameters را جستجو کنید

- ۷-۲-۳. مرحله دوم: از Google Dorks برای شناسایی پارامترهای تغییر مسیر اضافی استفاده کنید..... ۱۹۵
- ۷-۲-۴. در مرحله ۳ اوپن ریدایرکت های مبتنی بر پارامتر را آزمایش کنید. ۱۹۷
- ۷-۲-۵. مرحله چهارم: برای اوپن ریدایرکت های Referer-Based آزمایش کنید ۱۹۸
- ۷-۲-۶. دور زدن حفاظت Open Redirect ۱۹۸
- ۷-۲-۷. استفاده از تصحیح خودکار مرورگر وب (Browser Autocorrect)..... ۱۹۹
- ۷-۲-۸. اکسپلویت کردن منطق اعتبار سنجی معیوب..... ۲۰۱
- ۷-۲-۹. استفاده از URL های داده ۲۰۲
- ۷-۲-۱۰. اکسپلویت کردن دیکودینگ URL ۲۰۳
- ۷-۲-۱۱. ترکیب تکنیک های اکسپلویت ۲۰۶
- ۷-۳. افزایش حمله ۲۰۷
- ۷-۴. پیدا کردن اولین Open Redirect شما! ۲۰۹

فصل ۸ آسیب پذیری Clickjacking

- ۲۰۹
- ۸-۱ مکانیسم ها ۲۱۰
- ۸-۲ پیشگیری ۲۱۷
- ۸-۳ هانت کردن برای کلیک جکینگ ۲۱۹
- ۸-۳-۱ مرحله ۱: جستجوی اقدامات تغییر دهنده وضعیت..... ۲۱۹
- ۸-۳-۲ مرحله دوم: هدر ریسپانس را بررسی کنید..... ۲۲۱
- ۸-۳-۳ مرحله سوم: اعتبار سنجی آسیب پذیری ۲۲۲
- ۸-۴ دور زدن اقدامات ایمنی..... ۲۲۲
- ۸-۵ افزایش حمله ۲۲۴
- ۸-۶ نکته ای در مورد تحویل پیلود Clickjacking..... ۲۲۶
- ۸-۷ کشف اولین آسیب پذیری خود در مقابل Clickjacking!..... ۲۲۶

۲۲۷	فصل ۹. آسیب پذیری Cross-Site Request Forgery
۲۲۸.....	۹-۱ مکانیسم ها.....
۲۳۳.....	۹-۲ پیشگیری.....
۲۳۶.....	۹-۳ هانت کردن برای CSRF.....
۲۳۶.....	۹-۳-۱ مرحله اول: اقدامات تغییر دهنده حالت را شناسایی کنید.....
۲۳۸.....	۹-۳-۲ مرحله ۲: عدم وجود حفاظت CSRF را بررسی کنید.....
۲۳۹.....	۹-۳-۳ مرحله سوم: اعتبار سنجی آسیب پذیری.....
۲۴۱.....	۹-۴ دور زدن حفاظت CSRF.....
۲۴۱.....	۹-۴-۱ اکسلویت کلیک جکینگ.....
۲۴۲.....	۹-۴-۲ تغییر روش ریکوئست.....
۲۴۴.....	۹-۴-۳ دور زدن توکن های CSRF ذخیره شده در سرور.....
۲۴۷.....	۹-۴-۴ دور زدن ثبت دوباره توکن های CSRF.....
۲۴۸.....	۹-۴-۵ دور زدن بررسی هدر مرجع CSRF.....
۲۵۱.....	۹-۴-۶ دور زدن حفاظت CSRF با استفاده از XSS.....
۲۵۱.....	۹-۵ افزایش سطح حمله.....
۲۵۲.....	۹-۵-۱ نشت اطلاعات کاربر با استفاده از CSRF.....
۲۵۳.....	۹-۵-۲ با استفاده از CSRF ، Self-XSS ذخیره شده ایجاد کنید.....
۲۵۴.....	۹-۵-۳ با استفاده از CSRF حساب های کاربری را Take Over کنید.....
۲۵۶.....	۹-۶ تحویل پیلود CSRF.....
۲۵۸.....	۹-۷ کشف اولین CSRF شما!.....
۲۶۰	فصل ۱۰. آسیب پذیری Insecure Direct Object References
۲۶۰.....	۱۰-۱ مکانیسم ها.....
۲۶۲.....	۱۰-۲ پیشگیری.....
۲۶۴.....	۱۰-۳ هانت برای IDOR.....
۲۶۴.....	۱۰-۳-۱ مرحله اول. دو اکانت بسازید.....
۲۶۵.....	۱۰-۳-۲ مرحله ۲: شناسایی ویژگی ها.....

۲۶۶.....	مرحله ۳: ریکوئست ها را ضبط کنید	۱۰-۳-۳
۲۶۷.....	مرحله چهارم: شناسه ها را تغییر دهید	۱۰-۳-۴
۲۶۸.....	دور زدن حفاظت IDOR	۱۰-۴
۲۶۹.....	شناسه های رمزگذاری شده و هش شده	۱۰-۴-۱
۲۷۰.....	آیدی های لیک شده	۱۰-۴-۲
	یک شناسه برای برنامه حتی اگر درخواستی نداشته باشد ارائه دهید	۱۰-۴-۳
	۲۷۱	
۲۷۲.....	به دنبال Blind IDOR ها باشید	۱۰-۴-۴
۲۷۲.....	روش درخواست متغیر	۱۰-۴-۵
۲۷۳.....	نوع فایل درخواستی را تغییر دهید	۱۰-۴-۶
۲۷۴.....	افزایش حمله	۱۰-۵

فصل ۱۱. آسیب پذیری Sql Injection

۲۷۷		
۲۷۸.....	مکانیسم ها	۱۱-۱
۲۷۹.....	تزریق کد به کوئری های SQL	۱۱-۱-۱
۲۸۳.....	استفاده از تزریق SQL به صورت Second-Order	۱۱-۱-۲
۲۸۴.....	پیشگیری	۱۱-۲
۲۸۹.....	مرحله ۱: تزریق های سنتی SQL را جستجو کنید	۱۱-۲-۱
۲۹۰.....	در مرحله ۲ به دنبال تزریق SQL بلایند باشید	۱۱-۲-۲
۲۹۳.....	مرحله سوم: استخراج داده ها با استفاده از تزریق SQL	۱۱-۲-۳
۲۹۵.....	مرحله چهارم: به دنبال تزریق NoSQL باشید	۱۱-۲-۴
۲۹۸.....	افزایش حمله	۱۱-۳
۲۹۸.....	یادگیری پیرامون پایگاه داده	۱۱-۳-۱
۳۰۰.....	یک وب شل بگیرید	۱۱-۳-۲
۳۰۰.....	خودکارسازی Sql Injection	۱۱-۳-۳

فصل ۱۲. آسیب پذیری Race Conditions

۳۰۲.....	مکانیسم ها	۱۲-۱
----------	------------	------

۱۲-۲	چه موقع یک Race Condition تبدیل به یک آسیب پذیری می شود.....۳۰۵
۱۲-۳	پیشگیری.....۳۰۹
۱۲-۴	هانت کردن Race Condition.....۳۱۰
۱۲-۴-۱	مرحله ۱: شرایط بالقوه Race Condition را شناسایی کنید.....۳۱۰
۱۲-۴-۲	مرحله ۲: ارسال درخواست های همزمان.....۳۱۱
۱۲-۴-۳	مرحله ۳: نتایج را بررسی کنید.....۳۱۲
۱۲-۴-۴	در مرحله ۴ یک اثبات مفهوم ایجاد کنید.....۳۱۲
۱۲-۵	افزایش سطح شدت Race Condition.....۳۱۳
۱۲-۶	پیدا کردن اولین Race Condition شما!.....۳۱۳

فصل ۱۳. آسیب پذیری Server-Side Request Forgery ۳۱۴

۱۳-۱	مکانیسم ها.....۳۱۴
۱۳-۲	پیشگیری.....۳۱۶
۱۳-۳	هانت کردن برای SSRF.....۳۱۸
۱۳-۳-۱	مرحله اول: شناسایی ویژگی های مستعد SSRF.....۳۱۸
۱۳-۴	مرحله ۲: URL های داخلی را برای اندپوینت ها بالقوه آسیب پذیر ارائه دهید ۳۲۱
۱۳-۴-۱	مرحله ۳: نتایج را بررسی کنید.....۳۲۱
۱۳-۵	دور زدن حفاظت SSRF.....۳۲۵
۱۳-۵-۱	دور زدن لیست های مجاز (Bypass Allowlists).....۳۲۵
۱۳-۵-۲	دور زدن بلاک لیست (Bypass Blocklists).....۳۲۷
۱۳-۵-۳	سوئیچ کردن انکودینگ (Switching Out the Encoding).....۳۲۹
۱۳-۶	افزایش حمله.....۳۳۲
۱۳-۶-۱	انجام اسکن شبکه.....۳۳۲
۱۳-۶-۲	کوئری دادن متادیتا ابر Google Cloud.....۳۳۶
۱۳-۶-۳	اکسپلویت کردن Blind SSRF ها.....۳۳۷
۱۳-۶-۴	شبکه را هدف قرار دهید.....۳۳۹

۳۴۰..... کشف اولين SSRF شما! ۱۳-۷

فصل ۱۴. آسیب پذیری Insecure Deserialization ۳۴۱

۳۴۲..... مکانیسم ها ۱۴-۱

۳۴۴.....PHP 14-1-1

۳۵۶..... جاوا ۱۴-۱-۲

۳۶۰..... پیشگیری ۱۴-۲

۳۶۱..... هانت کردن برای Deserialization ناامن ۱۴-۳

۳۶۲..... افزایش حمله ۱۴-۴

۳۶۳..... پیدا کردن اولين Insecure Deserialization شما! ۱۴-۵

فصل ۱۵. آسیب پذیری XML External Entity ۳۶۴

۳۶۴..... مکانیسم ها ۱۵-۱

۳۶۸..... پیشگیری ۱۵-۲

۳۶۹..... هانت برای XXE ۱۵-۳

۳۶۹..... مرحله اول: نقاط ورودی داده XML را بیابید ۱۵-۴

۳۷۱..... مرحله ۲: تست XXE کلاسیک ۱۵-۴-۱

۳۷۲..... مرحله ۳: Blind XXE را بررسی کنید ۱۵-۴-۲

مرحله چهارم: XXE Payloads را در انواع مختلف فایل جاسازی

۳۷۳ کنید

۳۷۵..... مرحله ۵: XInclude Attacks را بررسی کنید ۱۵-۴-۴

۳۷۵..... افزایش حمله ۱۵-۵

۳۷۶..... خواندن فایل ها ۱۵-۵-۱

۳۷۶..... راه اندازی SSRF ۱۵-۵-۲

۳۷۷..... استفاده از Blind XXE ۱۵-۵-۳

اطلاعات بیشتر درباره از دست دادن اطلاعات با استفاده از XXES ۱۵-۵-۴

۳۸۲

۳۸۴..... پیدا کردن XXE اولیه شما! ۱۵-۶

فصل ۱۶. آسیب پذیری **Template Injection** ۳۸۵

۳۸۶..... ۱۶-۱ مکانیسم ها

۳۸۶..... ۱۶-۱-۱ انجین های تمپلیت (Template Engines)

۳۸۹..... ۱۶-۱-۲ تزریق کد تمپلیت (Injecting Template Code)

۳۹۲..... ۱۶-۲ پیشگیری

۳۹۳..... ۱۶-۳ هانت کردن برای **Template Injection**

۳۹۳..... ۱۶-۳-۱ مرحله ۱: مکان های ورودی کاربر را جستجو کنید

۳۹۳..... ۱۶-۳-۲ مرحله دوم: تشخیص تزریق الگو با ارسال پیلودهای آزمایشی

۱۶-۳-۳ مرحله ۳: تعیین کنید که کدام موتور تمپلیت در حال استفاده است

۳۹۵

۳۹۶..... ۱۶-۴ افزایش حمله

۳۹۷..... ۱۶-۴-۱ در جستجوی دسترسی به سیستم با استفاده از پایتون

۳۹۸..... ۱۶-۴-۲ استفاده از توابع داخلی پایتون برای دور زدن **Sandbox**

۴۰۲..... ۱۶-۴-۳ ثبت پیلود برای آزمایش

۴۰۳..... ۱۶-۵ خودکارسازی **Template Injection**

۴۰۴..... ۱۶-۶ اولین تزریق تمپلیت خود را پیدا کنید!

فصل ۱۷. آسیب پذیری **Application Logic Errors and Broken Access Control** ۴۰۵

۴۰۶..... ۱۷-۱ خطاهای منطق برنامه

۴۰۹..... ۱۷-۲ کنترل دسترسی نامعتبر (**Broken Access Control**)

۴۱۰..... 17-2-1 پنل های ادمین در معرض

۱۷-۲-۲ آسیب پذیری های پیمایش دایرکتوری (**Directory Traversal**)

۴۱۱..... (Vulnerabilities)

۴۱۲..... ۱۷-۳ پیشگیری

۴۱۳..... ۱۷-۳-۱ مرحله ۱: در مورد هدف خود اطلاعات کسب کنید

مرحله ۲: رهگیری (Intercept) درخواست ها در حین مرور سایت ۱۷-۳-۲

۴۱۴

مرحله ۳: تفکر خارج از چارچوب..... ۱۷-۳-۳

کشف خطای لاجیکال برنامه یا نقص کنترل دسترسی!..... ۱۷-۴

فصل ۱۸. آسیب پذیری Remote Code Execution ۴۱۶

۱۸-۱ مکانیسم ها..... ۴۱۷

۱۸-۱-۱ تزریق کد (Code Injection)..... ۴۱۷

۱۸-۱-۲ آسیب پذیری File Inclusion..... ۴۲۱

۱۸-۲ پیشگیری..... ۴۲۴

۱۸-۳ هانت کردن برای RCE..... ۴۲۶

۱۸-۳-۱ گام اول: جمع آوری اطلاعات در مورد هدف..... ۴۲۷

۱۸-۳-۲ گام دوم: مکان های ورودی مشکوک کاربر را شناسایی کنید..... ۴۲۷

۱۸-۳-۳ گام سوم: ثبت پیلودهای آزمایشی..... ۴۲۸

۱۸-۳-۴ گام چهارم: اعتبار سنجی آسیب پذیری..... ۴۳۰

۱۸-۴ افزایش سطح حمله..... ۴۳۰

۱۸-۵ دور زدن حفاظت RCE..... ۴۳۲

۱۸-۶ پیدا کردن RCE اولیه شما!..... ۴۳۵

فصل ۱۹. آسیب پذیری Same-Origin Policy Vulnerabilities ۴۳۶

۱۹-۱ مکانیسم ها..... ۴۳۶

۱۹-۱-۱ اکسپلویت کردن Cross-Origin Resource Sharing..... ۴۳۸

۱۹-۱-۲ اکسپلویت کردن postMessage..... ۴۴۱

۱۹-۱-۳ اکسپلویت کردن JSON با Padding..... ۴۴۵

۱۹-۱-۴ اکسپلویت کردن SOP با استفاده از XSS..... ۴۴۸

۱۹-۲ هانت کردن برای بای پس های SOP..... ۴۴۹

۱۹-۲-۱ مرحله ۲: پیکربندی اشتباه CORS را پیدا کنید..... ۴۵۱

۱۹-۲-۲ مرحله ۳: باگ های postMessage را پیدا کنید..... ۴۵۲

- ۴۵۳.....مرحله ۴: مسائل JSONP را پیدا کنید۱۹-۲-۳
- ۴۵۳.....مرحله ۵: فاکتورهای کاهنده را مدنظر قرار دهید.....۱۹-۲-۴
- ۴۵۳.....افزایش سطح حمله.....۱۹-۳

فصل ۲۰. آسیب پذیری Single-Sign-On Security Issues ۴۵۵

- ۴۵۶.....مکانیسم ها۲۰-۱-۱
- ۴۵۹.....زبان Security Assertion Markup۲۰-۱-۲
- ۴۶۴.....OAuth 20-1-3.....
- ۴۷۰.....هانت کردن برای Subdomain Takeover ها.....۲۰-۲
- ۴۷۰.....مرحله ۱: ساب دامنه های هدف را فهرست کنید.....۲۰-۲-۱
- ۴۷۱.....مرحله ۲: صفحات ثبت نشده را پیدا کنید.....۲۰-۲-۲
- ۴۷۲.....ثبت صفحه۲۰-۲-۳
- ۴۷۳.....نظارت بر Subdomain Takeover ها.....۲۰-۳
- ۴۷۵.....جستجو برای آسیب پذیری SAML.....۲۰-۴
- ۴۷۵.....مرحله ۱: پاسخ SAML را پیدا کنید.....۲۰-۴-۱
- ۴۷۵.....مرحله ۲: فیلدهای پاسخ را تجزیه و تحلیل کنید.....۲۰-۴-۲
- ۴۷۶.....مرحله ۳: دور زدن امضا.....۲۰-۴-۳
- ۴۷۷.....مرحله چهارم: پیام را دوباره رمزگذاری کنید.....۲۰-۴-۴
- ۴۷۷.....بررسی سرقت توکن OAuth.....۲۰-۵
- ۴۷۸.....افزایش سطح حمله.....۲۰-۶
- ۴۷۹.....کشف بای پس SSO اولیه شما!.....۲۰-۷

فصل ۲۱. آسیب پذیری Information Disclosure ۴۷۹

- ۴۸۰.....مکانیسم ها۲۱-۱
- ۴۸۲.....پیشگیری۲۱-۲
- ۴۸۲.....جستجوی افشای اطلاعات.....۲۱-۳
- ۴۸۳.....مرحله اول : یک Path Traversal Attack را امتحان کنید.....۲۱-۳-۱
- ۴۸۴.....مرحله ۲: جستجوی Wayback Machine را انجام دهید.....۲۱-۳-۲

۴۸۷.....	Paste Dump Sites	مرحله ۳: جستجوی	۲۱-۳-۳
	Exposure.git	مرحله چهارم: سورس کد را از دایرکتوری بازسازی کنید	۲۱-۳-۴
			۴۸۸
۴۹۴.....		مرحله ۵: داده ها را در فایل های عمومی پیدا کنید	۲۱-۳-۵
۴۹۵.....		تشدید حمله	۲۱-۳-۶
۴۹۶.....		پیدا کردن اولین افشای اطلاعات خود!	۲۱-۴

۴۹۷

فصل ۲۲. انجام ارزیابی کد

۴۹۸.....		تست بلک باکس در مقابل تست وایت باکس	۲۲-۱
۴۹۹.....		روش سریع: grep بهترین دوست شماست	۲۲-۲
۴۹۹.....		الگوهای خطرناک	۲۲-۲-۱
۵۰۳.....		اسرار فاش شده و رمزگذاری ضعیف	۲۲-۲-۲
۵۰۵.....		تغییرات جدید و dependency های منسوخ شده	۲۲-۲-۳
۵۰۶.....		کامنت های توسعه دهندگان	۲۲-۲-۴
۵۰۷.....		دیبگ کردن عملکردها، فایل های پیکربندی و اندپوینت ها	۲۲-۲-۵
۵۰۸.....		روش تفصیلی	۲۲-۳
۵۰۸.....		توابع مهم	۲۲-۳-۱
۵۰۹.....		ورودی کاربر	۲۲-۳-۲

۵۱۷

فصل ۲۳. هک کردن برنامه ها در اندروید

۵۱۸.....		پیکربندی پروکسی موبایل شما	۲۳-۱
۵۲۰.....		Certificate Pinning دور زدن	۲۳-۲
۵۲۲.....		آناتومی یک apk	۲۳-۳
۵۲۳.....		ابزارهای مفید	۲۳-۴
۵۲۴.....		Android Debug Bridge	۲۳-۴-۱
۵۲۵.....		اندروید استودیو	۲۳-۴-۲
۵۲۶.....		apktool	23-4-3.
۵۲۶.....		Frida	۲۳-۴-۴

- ۵۲۷..... فریمورک امنیت موبایل ۲۳-۴-۵
۵۲۷..... هانت کردن آسیب پذیری ها ۲۳-۵

۵۲۹ فصل 24 هک کردن API

- ۵۳۰..... API چیست؟ ۲۴-۱
۵۳۳..... REST رابط های ۲۴-۱-۱
۵۳۴..... ای پی ای های SOAP ۲۴-۱-۲
۵۳۶..... GraphQL های API ۲۴-۱-۳
۵۴۱..... برنامه های کاربردی مبتنی بر API ۲۴-۱-۴
۵۴۲..... هانت کردن برای آسیب پذیری های API ۲۴-۲
۵۴۳..... پیاده سازی Recon ۲۴-۲-۱
Broken Access Control and Info Leaks تست کردن برای ۲۴-۲-۲
۵۴۶

- ۵۴۹..... Rate-Limiting تست کردن برای مسائل ۲۴-۲-۳
۵۵۰..... تست کردن برای باگ های فنی ۲۴-۳

۵۵۲ فصل ۲۵. کشف آسیب پذیری خودکار با استفاده از فازرها

- ۵۵۳..... Fuzzing چیست؟ ۲۵-۱
۵۵۴..... طرز کارکرد یک وب فازر چگونه است؟ ۲۵-۲
۵۵۵..... فرایند فازینگ ۲۵-۳
۵۵۶..... مرحله اول. نقاط تزریق داده را تعیین کنید. ۲۵-۳-۱
۵۵۷..... ۲. لیست پیلود را تعیین کنید ۲۵-۳-۲
۵۵۸..... مرحله ۳: Fuzz ۲۵-۳-۳
۵۶۰..... مرحله چهارم: نتایج را دنبال کنید ۲۵-۳-۴
۵۶۰..... فاز کردن با Wfuzz ۲۵-۴
۵۶۱..... سرشماری مسیر (Path Enumeration) ۲۵-۴-۱
۵۶۳..... اعتبار سنجی با بروت فورس کردن ۲۵-۴-۲
۵۶۵..... تست آسیب پذیری های رایج وب ۲۵-۴-۳