

باگ بانتي و باگ هانتينگ

تأليف:

بهرز منصوري

www.ketab.ir

سرنشنامه	: منصورى، بهروز، ۱۳۷۲ -
عنوان و نام پديدآور	: باگ‌بانتى و باگ‌هانتىنگ/ تاليف بهروز منصورى.
مشخصات نشر	: تهران: ميعاد اندیشه، ۱۴۰۰.
مشخصات ظاهرى	: ۱۵۴ ص.: مصور(بخشى رنگى).
شابک	: ۱۰۰۰۰۰۰۰ ر.هال-۸-۷۵۰-۲۳۱-۶۲۲-۹۷۸ :
وضعيت فهرست نويسى	: فبا
موضوع	: وبگاهها -- تدابير امنى
موضوع	: Web sites – Security measures
موضوع	: اشکال‌زدایى (کامپيوتر)
موضوع	: Debugging in computer science
رده بندى کنگره	: TK۵۱۰۵/۵۹
رده بندى ديوبى	: ۰۰۵/۸
شماره کتابشناسى ملي	: ۸۵۲۴۴۵۲
اطلاعات رکورد کتابشناسى	: فبا



Miaadpub.ir

عنوان کتاب : باگ بانتى و باگ هانتىنگ

مؤلف : بهروز منصورى

ناشر : ميعاد اندیشه

طراح جلد : شکوفه احمدى

صفحه آرا : مائده طومار

نوبت چاپ : اول - ۱۴۰۰

شمارگان : ۱۰۰۰ نسخه

قيمت : ۱/۰۰۰/۰۰۰ ريال

شابک : ۸-۷۵۰-۲۳۱-۶۲۲-۹۷۸

تلفن انتشارات: ۰۹۱۲۵۱۲۰۰۶۷ - ۰۲۱۶۶۰۱۷۴۴۸ - ۰۲۱۶۶۰۱۴۷۹۷

تکثیر و انتشار این اثر به هر صورت، از جمله بازنويسى، فتوکپى، ضبط الکترونيكى

و ذخيره در سيستم هاى بازيايى و پخش، بدون دريافت مجوز کتبى و قبلى از مولف

به هر شکلى ممنوع است.

این اثر تحت حمايت «قانون حمايت از حقوق مولفان، مصنفان و هنرمندان ايران» قرار دارد

فهرست مطالب

۱۰	مقدمه.....
۱۱	باگ بانتي چیست (Bug Bounty) ؟.....
۱۲	سناريو ۱ : استخدام يك امنيت كار سايري.....
۱۲	سناريو ۲ : گزارش مردمي (Bug Bounty Platforms).....
۱۳	مقايسه باگ بانتي و تست نفوذ؟.....
۱۴	پلتفرم هاي برتر باگ بانتي.....
۱۵	بانتي هانتر كيست؟.....
۱۵	ارزيابي امنيتي.....
۱۶	۴ مرحله از يك مدل ارزيابي موفقيت آميز خطر.....
۱۶	تست نفوذ چيست؟.....
۱۷	روش هاي تست نفوذ.....
۱۸	دسترسى كامل به حساب از طريق باگ در تنظيم مجله رمز عبور.....
۲۰	دسترسى به سايت از طريق Sql Injection.....
۲۵	آسيب پذيرى xss در artsexperiments.withgoogle.com.....
۲۶	سوءاستفاده از حداكثر محدوديت شخصيت.....
۲۸	آسيب پذيرى IDOR در appsheet.com.....
۳۵	اولين آسيب پذيرى بحراني من.....
۴۰	به دست آوردن اطلاعات کاربران از طريق IDOR.....
۴۳	استفاده از CSRF براي تصاحب كامل حساب.....
۴۶	اما آيا مي توانيم كارهاي بيشتري انجام دهيم؟.....
۴۸	Cache Poisoning از طريق SelfXSS و Path Parameter.....
۴۹	گزارش ۷۵۰ دلاري Paypal.....
۵۰	مسير آسيب پذير.....

۵۱	۴ باگ در یک گزارش
۵۴	آپلود را دور بزنید
۵۷	به دست آوردن آیبی پشت CloudFlare و انجام حمله Sql Injection
۶۳	دست کاری سیستم امتیازدهی
۶۴	سایت واقعی
۶۵	تأثیر باگ
۶۵	افشاگری
۶۶	نتیجه
۶۷	۳ باگ در یک سایت
۶۹	Stored XSS در GameSkinny
۷۱	باگ گوگل
۷۳	دورزدن محدودیت به روزرسانی ایمیل برای تغییر ایمیل اعضای تیم
۷۴	دورزدن اعتبارسنجی از طریق پیامک
۷۹	افشای اطلاعات برای دسترسی حساب
۸۰	آسیب پذیری اولیه چیست؟
۸۲	انجام پروت فورس به واسطه مشکل xmlrpc وردپرس
۸۶	Csrf ابتدایی
۹۰	آسیب پذیری IDOR در قسمت تغییر پسورد
۹۲	آسیب پذیری IDOR در قسمت گالری گوگل
۹۴	آسیب پذیری Sql Injection و جایزه عجیبه ۵۰ دلاری
۹۶	آسیب پذیری Reflected XSS در مایکروسافت
۹۸	افشای مسیر کامل در پرداخت های دیجیتالی
۹۸	مراحل یافتن باگ
۱۰۱	دسترسی به حساب از طریق Open Redirect
۱۰۴	Parameter Tampering و دست کاری قیمت
۱۰۷	دورزدن احراز هویت با استفاده از Javascript Debugger

مقدمه

امنیت، اتفاقی نیست! امنیت به طور کلی یک مقوله نسبی است و کسی نمی‌تواند مدعی ایمنی کامل در برابر خطرات امنیتی باشد. بسیاری از سازمان‌ها و شرکت‌ها تصور می‌کنند که با ایجاد یک دیوار بلند غیرقابل نفوذ در اطراف اطلاعات دیجیتالی خود، توان کافی و قابل اتکا برای مقابله با خطرات امنیتی دارند اما واقعیت آن است که ارتفاع آن دیوار تاثیری ندارد و به هر حال دیر یا زود هکرها نقطه ضعفی بر روی آن دیوار پیدا خواهند کرد و راه نفوذ را خواهند یافت.

از طرفی تکنولوژی به سرعت در حال پیشرفت است و به فراخور آن نیاز است که امنیت و تمهیدات امنیتی نیز با همان سرعت ارتقا یابند. قطعاً دفاع از اطلاعات دیجیتالی نیازمند آن است که آن دیوار دفاعی نیز به طور مستمر و مداوم مورد ارزیابی قرار گیرد و کشف و رفع آسیب‌پذیری‌های آن به موقع انجام شود؛ قبل از آن که هکرها کلاه‌سیاه فرصت سوءاستفاده از آسیب‌پذیری‌های آن را یابند.

www.ketab.ir