کاوش تکنیک‌های Google Hacking

گردآورندگان:

محمدجواد عباسی

حسین خدادادی

احمد فلاح بروج

NAGHOOS
PUBLICATION

سرشناسه	: عباسی، محمد جواد،۱۳۶۰
عنوان و نام پدیدآور	: کاوش تکنیک های Google Hacking / گرد آورندگان محمدجواد عباسی، حسین خدادادی احمد فلاح بروج
مشخصات نشر	: تهران : ناقوس، ۱۴۰۰.
مشخصات ظاهری	: ۲۸۰ص. مصور، جدول ، نمودار
شابک	:۸۵۰،۰۰۰ریال : 978-600-473-399-1
وضعیت فهرستنویسی	: فیپا
موضوع	: گوگل Google
موضوع	: جستجوی اینترنتی Internet searching
موضوع	: اینترنت – برنامه نویسی Internet programming
موضوع	: اینترنت – تدابیر ایمنی Internet security measures
موضوع	: شبکه های کامپیوتری – تدابیر ایمنی Computer networks —Security Measures
موضوع	: وب – موتورهای جستجو Web search engines
شناسه افزوده	: خدادادی ، حسین ،۱۳۶۸ . –گرد آورنده
شناسه افزوده	: فلاح بروج ، احمد ، ۱۳۷۳.– گرد اورنده
رده بندی کنگره	: TK۵۱۰۵ /۸۸۵
رده بندی دیویی	: ۰۲۵/۰۴
شمارهٔ کتابشناسی ملی	: ۸۴۲۸۱۵۵

انتشارات ناقوس

نام کتاب	: کاوش تکنیک های Google Hacking
ناشر	: انتشارات ناقوس
گردآورندگان	: محمد جواد عباسی ، حسین خدادادی ، احمد فلاح بروج
چاپ اول	: ۱۴۰۰
تیراژ	: ۵۰۰ جلد
چاپ و صحافی	: حیدری
ناظر چاپ	: یاسمن تجملی محدث
قیمت	: ۸۵۰،۰۰۰ ریال
شابک	: ۹۷۸-۶۰۰-۴۷۳-۳۹۹-۱
ISBN	: 978-600-473-399- 1

انتشارات ناقوس
بلوار کشاورز- خیابان ۱۶آذر- کوچه پارسی – پلاک ۱۰
تلفاکس : ۶۶۴۷۸۹۵۱ - ۶۶۴۷۸۹۵۴

پیشگفتار

به نام خدای حسابگر، حسابساز، حسابرس که ترازش همیشه موزون است.

گوگل محبوب‌ترین موتور جست‌وجو است که تاکنون ایجاد شده است، قابلیت‌های جست‌وجوی گوگل بسیار قدرتمند است، آن‌ها گاهی اوقات محتوایی را کشف می‌کنند که هیچ وقت در دسترس عموم مردم در وب نبوده است، از جمله شماره‌های امنیت اجتماعی، شماره کارت‌های اعتباری، اسرار تجاری و طبقه‌بندی شده، به شما نشان می‌دهد که چگونه متخصصان امنیتی و سرپرست سیستم Google را برای یافتن این اطلاعات حساس و «خودپلیسی» کردن سازمان‌های خود دستکاری می‌کنند. شما خواهید آموخت که چگونه Google Maps و Google Earth دقت نظامی را ارائه می‌دهند، خواهید دید که چگونه افراد بد می‌توانند Google را برای ایجاد کرم‌های فوق‌العاده دستکاری کنند و ببینید که چگونه آن‌ها می‌توانند Google را با استفاده از Facebook، LinkedIn و موارد دیگر برای شناسایی منفعل کنند. این نسخه شامل محتوای کاملاً به‌روز شده در کل و همه هک‌های جدید مانند برنامه‌نویسی Google و استفاده از هک Google با سایر موتورهای جست‌وجو و APIها است. نویسنده مشهور، جانی لانگ، بنیانگذارHackers for Charity، تمام ابزارهایی را که برای انجام آزمایش شناسایی و نفوذ نهایی نیاز دارید، به‌صورت OpenSource در اختیار شما قرار می‌دهد.

اگر شما مسئول منابع IT، یا یک متخصص امنیت هستید، باید این کتاب را داشته باشید. این کتاب نشان می‌دهد که چگونه Google می‌تواند توسط افراد بد برای نمایه‌سازی و برشمردن زیرساخت‌های شبکه شما استفاده شود. جانی لانگ در توضیح چگونگی کار

Google با اپراتورهای پیشرفته و اینکه چگونه می‌تواند نتایج جالبی ارائه دهد بسیار عالی است او نشان می‌دهد که چگونه یک هکر می‌تواند بدون ارسال بسته‌ای به شبکه شما، اطلاعات زیادی درباره شبکه و شرکت شما بیاموزد. شما می‌آموزید که چگونه می‌توانید اطلاعات مربوط به سرورهای اشتباه پیکربندی شده، پرونده‌های «جالب» را که در اطراف سرورها قرار دارند، مکان‌یابی سوءاستفاده‌ها، شبکه‌های نقشه برداری و موارد دیگر را بیابید. اما، شما یاد خواهیدگرفت که چگونه از خود در برابر هکر شیطانی گوگل دفاع‌کنید و از آن محافظت کنید.

هشدار

کتاب GoogleHacking در راستای ارتقا سطح دانش و آشنایی شما دوستان تهیه شده است. هرگونه سوء استفاده و فعالیت غیرقانونی از محتوای کتاب بر عهده خود فرد می‌باشد و تولیدکنندگان این اثر هیچ گونه مسئولیتی در قبال آن ندارد. می‌توان با ایجاد بستر لازم و ایمن برای استفاده از GoogleHacking بهترین استفاده از این دنیای وب را داشت ولی syntax استفاده از محیط بر عهده شماست. در این دنیای پر رمز و راز به‌طور یقین استفاده شر و بد هم دارد. تصور کنید در دنیایی از خلافکاران قدم برمی‌دارید، پس مراتب احتیاط را رعایت کنید.

با آرزوی موفقیت برای خوانندگان عزیز

فهرست مطالب

فصل اول- اصول جست‌وجوی Google ۱۳

۱-۱ مقدمه ۱۳

۱-۲- بررسی رابط مبتنی بر وبGoogle ۱۴

۱-۳- صفحه نتایج وب Google ۱۴

۱-۴- Google Groups ۱۵

۱-۵- جست‌وجوی تصویر Google ۱۶

۱-۶- تنظیمات برگزیده Google ۱۷

۱-۷- ابزار زبان ۱۹

۱-۸- ساخت Google Query ۲۰

۱-۹- قوانین طلایی جست‌وجوی Google ۲۰

۱-۱۰- Google Wildcards ۲۱

۱-۱۱- Google حق نادیده گرفتن شما را برای خود محفوظ می‌دارد ۲۱

۱-۱۲- محدودیت ۳۲ کلمه ۲۲

۱-۱۳- جست‌وجوی ابتدایی ۲۲

۱-۱۴- استفاده از عملگرهای Boolean و کاراکترهای خاص ۲۳

۱-۱۵- کاهش جست‌وجو ۲۶

۱-۱۶- کار باURLهای Google ۲۹

۱-۱۷- ساختار URL ۳۰

۱-۱۸- کاراکترهای خاص ۳۰
۱-۱۹- قرار دادن قطعات با هم ۳۱
۱-۲۰- خلاصه فصل ۳۳
فصل دوم- اپراتورهای پیشرفته ۳۹
۲-۱- مقدمه ۳۹
۲-۲- ساختار اپراتور ۳۹
۲-۳- عیب‌یابی برای Syntax خود ۴۱
۲-۴- معرفی اپراتورهای پیشرفته Google ۴۲
۲-۴-۱- "INTITLE" و "ALLINTITLE" جست‌وجو در داخل عنوان یک صفحه ۴۳
۲-۴-۲- ALLINTEXT: یک رشته را در داخل متن یک صفحه قرار دهید ۴۵
۲-۴-۳- INURL و ALLINURL: یافتن متن در یک URL ۴۶
۲-۴-۴- SITE: جست‌وجوی محدود شده برای سایت‌های خاص ۴۷
۲-۴-۵- FILETYPE: جست‌وجو برای فایل‌های یک نوع خاص ۴۹
۲-۴-۶- LINK: جست‌وجو برای پیوندها به یک صفحه ۵۱
۲-۴-۷- INANCHOR: جست‌وجو متن درون متن لینک ۵۳
۲-۴-۸- CACHE: نسخه ذخیره شده یک صفحه را نشان دهید ۵۴
۲-۴-۹- NUMRANGE: براساس اعداد جست‌وجو کنید ۵۵
۲-۴-۱۰- DATERANGE: جست‌وجو برای صفحه‌های منتشر شده در محدوده
تاریخ مشخص ۵۵
۲-۴-۱۱- INFO: اطلاعات خلاصه‌ای از Google را نمایش می‌دهد ۵۷
۲-۴-۱۲- RELATED: سایت‌های مرتبط را نشان دهید ۵۸
۲-۴-۱۳- STOCKS: جست‌وجوی اطلاعات سهام ۵۸
۲-۴-۱۴- DEFINE: تعریف یک اصطلاح را نشان دهید ۵۹
۲-۵- تداخل عملکردها و جست‌وجوهای بد شما ۶۰
۲-۶- خلاصه فصل ۶۲
فصل سوم- اصول Google Hacking ۶۵
۳-۱- مقدمه ۶۵

۳-۲- گمنامی با Caches ۶۶
۳-۳- Directory Listing ۷۰
۳-۴- جست‌وجوی Directory Listing ۷۱
۳-۵- یافتن دایرکتوری‌های خاص ۷۲
۳-۶- پیداکردن فایل‌های خاص ۷۳
۳-۷- ورود به یک چالش: تکنیک‌های TRAVERSAL ۷۶
۳-۸- خلاصه فصل ۸۰
فصل چهارم- Document Grinding and Database Digging ۸۵
۴-۱- مقدمه ۸۵
۴-۲- فایل‌های پیکربندی ۸۶
۴-۳- جست‌وجوی فایل‌ها ۹۱
۴-۴- فایل‌های لاگ ۹۱
۴-۵- اسناد Office ۹۲
۴-۶- DATABASE DIGGING ۹۳
۴-۷- بخش ورود به سیستم ۹۴
۴-۸- فایل‌های پشتیبانی ۹۴
۴-۹- پیغام خطا ۹۶
۴-۱۰- Dumpهای پایگاه داده ۹۶
۴-۱۱- فایل‌های پایگاه داده واقعی ۹۸
۴-۱۱-۱- GRINDING اتوماتیک ۹۸
۴-۱۲- خلاصه فصل ۱۰۳
فصل پنجم- چهارچوب جمع‌آوری اطلاعات ۱۰۷
۵-۱- مقدمه ۱۰۷
۵-۲- اصول جست‌وجوی خودکار ۱۰۸
۵-۳- اصطلاح اصلی جست‌وجو ۱۱۰
۵-۳-۱- گسترش شرایط جست‌وجو ۱۱۱
۵-۴- آدرس ایمیل ۱۱۲

۵-۴-۱-تایید آدرس ایمیل ۱۱۳
۵-۵- شماره تلفن ۱۱۴
۵-۶- اشخاص ۱۱۵
۵-۷- گرفتن نتایج زیاد ۱۱۶
۵-۸- استفاده از اپراتورهای "XSPECIAL" ۱۱۸
۵-۹- دریافت داده‌ها از منابع ۱۱۹
۵-۱۰- SCRAPING خودتان: فروشگاه قصاب ۱۲۵
۵-۱۰- استفاده از موتور جست‌وجوهای دیگر ۱۳۱
۵-۱۲- دامنه‌ها و زیر دامنه‌ها ۱۳۶
۵-۱۳- شماره‌های تلفن ۱۳۷
۵-۱۴- مرتب سازی نتایج براساس ارتباط ۱۴۰
۵-۱۵- فراتر از قطعه‌ها ۱۴۲
۵-۱۶- جمع‌آوری شرایط جست‌وجو ۱۴۴
۵-۱۷- جاسوسی در مورد خود شما ۱۴۴
۵-۱۸- syntax تشخیص Transparent Proxy ۱۴۸
۵-۱۹- ارجاعات ۱۴۹
۵-۱۹- خلاصه فصل ۱۵۰
فصل ششم- Locating Exploits and Finding Target ۱۵۱
۶-۱- مقدمه ۱۵۱
۶-۲- Locating Exploit Code ۱۵۱
۶-۳- جست‌وجوی سایت‌های Public Exploit ۱۵۲
۶-۴- جست‌وجوی اکسپلویت‌ها از طریق رشته‌های کد مشترک ۱۵۳
۶-۵- جست‌وجوی اهداف آسیب‌پذیر ۱۵۴
۶-۵-۱- جست‌وجوی اهداف از طریق افشای آسیب‌پذیری ۱۵۴
۶-۵-۲- جست‌وجوی اهداف از طریق سورس کد ۱۵۵
۶-۶- خلاصه فصل ۱۵۵
فصل هفتم- ده جستجوی امنیتی ساده و کارساز ۱۵۷

۷-۱- مقدمه ۱۵۷
۷-۲- ده عملگر پایه ۱۵۷
۷-۲-۱- Site ۱۵۷
۷-۲-۲- Intitle:Index.OF ۱۵۹
۷-۲-۳- Error | Warning ۱۵۹
۷-۲-۴- Loggin | Logon ۱۶۱
۷-۲-۵- "USERNAME IS"\USERID|EMPLOYEE. ID|USERNAME ۱۶۲
۷-۲-۶- "YOUR PASSWORD IS" | PASSCODE | PASSWORD ۱۶۳
۷-۲-۷- Admin | Administrator ۱۶۴
۷-۲-۸- -EXT:HTML -EXT:HTM-EXT:ASP -EXT:PHP ۱۶۶
۷-۲-۹- INURL:TEMP | INURL:TMP | INURL:BACKUP ۱۶۹
۷-۲-۱۰- INTRANET | HELP.DESK ۱۶۹
۷-۳- خلاصه فصل ۱۷۱
فصل هشتم- ردیابی کردن وب سرورها، پورتال های ورود به سیستم و سخت‌افزار شبکه ۱۷۳
۸-۱- مقدمه ۱۷۳
۸-۲- مکان‌یابی و ایجاد پروفایل سرورهای وب ۱۷۴
۸-۳- Directory Listing ۱۷۵
۸-۴- پیام‌های خطای نرم‌افزار وب سرور ۱۷۶
۸-۵- Microsoft IIS ۱۷۶
۸-۶- پیام‌های خطای نرم‌افزاری کاربردی ۱۸۵
۸-۷- Default Page ۱۸۶
۸-۸- Default Documentation ۱۸۸
۸-۹- جست‌وجوی ورودی پرتال ۱۸۸
۸-۱۰- استفاده و مکان‌یابی خدمات مختلف وب ۱۹۰
۸-۱۱- هدف‌گذاری دستگاه‌های شبکه تحت وب ۱۹۵
۸-۱۲- جست‌وجو گزارش‌های شبکه ۱۹۶

۸-۱۳- جست‌وجو سخت‌افزار شبکه ۱۹۶
۸-۱۴- خلاصه فصل ۱۹۹
فصل نهم- نام‌های کاربری، گذرواژه‌ها و موارد مخفی ۲۰۱
۹-۱- مقدمه ۲۰۱
۹-۲- جست‌وجو برای نام‌های کاربری ۲۰۲
۹-۳- جست‌وجو رمزهای عبور ۲۰۴
۹-۴- جست‌وجوی شماره‌های کارت اعتباری، شماره‌های امنیت اجتماعی و موارد دیگر ۲۰۷
۹-۵- شماره‌های امنیت اجتماعی ۲۰۹
۹-۶- جست‌وجو برای سایر اطلاعات سلیقه‌ای ۲۱۰
۹-۷- خلاصه فصل ۲۱۱
فصل دهم- هک کردن سرویس‌های Google ۲۱۳
۱۰-۱- مقدمه ۲۱۳
۱۰-۲- Signaling Alert ۲۱۵
۱۰-۲- Google CO-OP ۲۱۶
۱۰-۳- موتور جست‌وجوهای سفارشی Google ۲۱۷
فصل یازدهم- هک کردن Google ShowCase ۲۱۹
۱۱-۱- مقدمه ۲۱۹
۱۱-۲- Geek Stuff ۲۲۰
۱۱-۳- دستگاه‌های شبکه‌ساز ۲۲۴
۱۱-۴- برنامه‌های باز ۲۳۱
۱۱-۵- دوربین‌های عکاسی ۲۳۷
۱۱-۶- Telco Gear ۲۴۵
۱۱-۷- Power ۲۵۰
۱۱-۸- اطلاعات حساس ۲۵۴
۱۱-۹- خلاصه فصل ۲۵۵
فصل دوازدهم- از خود در برابر Google Hacker مراقبت کنید ۲۵۷
۱۲-۱- مقدمه ۲۵۷