



راهنمای عملی هک وب با استفاده از کالی لینوکس

تألیف و ترجمه:

دکتر لیلی فرزین وش (استادیار دانشگاه تبریز)

مهندس مهسا علی پور امتنانی - مهندس رویا روشنی ممقانی

سروش‌نامه	فرزین وش، لیلی، ۱۳۶۳.
عنوان و پدیدآور	راهنمای عملی هک وب با استفاده از کالی لینوکس/تالیف و ترجمه: دکتر لیلی
مشخصات نشر	فرزین وش، مهندس مهسا علی پور امتنانی و مهندس رویا روشنی ممقانی
مشخصات ظاهری	نور علم.
شابک	۱۸۵ ص. جدول، نمودار، مصور.
وضعیت فهرست‌نویسی	۱-۱۴۶-۱۶۹-۶۰۰-۹۷۸
یادداشت	براساس اطلاعات فیفا (فهرست‌نویسی پیش از انتشار).
یادداشت	کتابنامه ص ۱۸۵.
یادداشت	فرزین وش، لیلی، ۱۳۶۳، مولف.
یادداشت	علی پور امتنانی، مهسا، ۱۳۶۹، مولف.
یادداشت	روشنی ممقانی، رویا، ۱۳۶۹، مولف.
موضوع	لینوکس (فایل کامپیوتر).
موضوع	شبکه‌های رایانه‌ای.
موضوع	کامپیوترها -- ایمنی اطلاعات.
رده بندی کنگ	TK ۵۱۰۵ ۱۳۹۵ ۲/۴
رده بندی دیو ی	۰۲۵/۰۴

نشر نور علم: تهران، نقاشی، خ ۱۲ فروردین - پلاک ۲۵۹ - ط ۴ - واحد ۸ تلفن: ۶۶۴۰۵۸۹۴ و ۶۶۴۰۵۸۸۰
 ۰۹۱۲۳۳۳۳۲۲۹@reelm@yahoo.com فروشگاه در تهران: دانشکده اقتصاد دانشگاه تهران

راهنمای عملی هک وب با استفاده از کالی لینوکس

تالیف و ترجمه: دکتر لیلی فرزین وش،

مهندس مهسا علی پور امتنانی

مهندس رویا روشنی ممقانی

ناشر: نور علم

شمارگان: ۵۰۰ جلد

شابک: ۱-۱۴۶-۱۶۹-۶۰۰-۹۷۸

نوبت چاپ: اول ۱۳۹۵

چاپ و صحافی: الغدير

قیمت: ۱۵۰۰۰ تومان

موبایل کار: در صورت عدم دسترسی به کتابهای این انتشارات، از طریق تماس با شماره زیر
 ۰۹۱۲۳۳۳۳۲۲۹ کتابها با پست به تمام نقاط ایران ارسال می شود.

۹	مقدمه
۱۱	فصل ۱: مبانی هک وب
۱۲	مقدمه
۱۴	برنامه کاربردی وب چیست؟
۱۵	نکاتی درباره وب سرورها
۱۶	نکات مهم در مورد HTTP
۱۷	چرخه HTTP
۱۷	فیلدهای مهم در سرآیند HTTP
۱۹	حالت وضعیت کدهای HTTP
۲۰	مبانی هک وب
۲۰	اهداف کتاب
۲۱	ابزارهای بررسی شده
۲۲	برنامه‌های کاربردی وب مرتبط با همه بخش‌های فناوری اطلاعات
۲۳	متدولوژی OSSTM
۲۳	رایج‌ترین آسیب پذیری‌های وب
۲۴	تزریق
۲۵	XSS
۲۶	احراز هویت و مدیریت نشست نقض شده
۲۶	CSRF

۲۷	 پیکربندی نادرست
۲۸	 راه اندازی یک محیط آزمایش
۲۹	 برنامه های کاربردی وب هدف
۳۰	 نصب برنامه کاربردی وب هدف
۳۰	 پیکربندی برنامه کاربردی وب هدف
۳۳	 فصل ۲: شناسایی و پویش وب سرور
۳۴	 مقدمه
۳۴	 شناسایی
۳۵	 فایل robots.txt
۳۷	 پویش کردن پورت ها
۳۷	 Nmap
۴۱	 (Nmap Scripting Engine) NSE
۴۵	 پویش آسیب پذیری ها
۴۶	 Nessus
۴۷	 مرور نتایج Nessus
۴۷	 Nikto
۵۰	 اکسپلویت نمودن
۵۱	 اصول Metasploit
۵۲	 جستجو
۵۳	 استفاده
۵۳	 نمایش پیلودها
۵۶	 تنظیم پیلود

۵۷	نمایش گزینه‌ها
۵۸	اکسپلویت
۵۹	ایجاد دسترسی دائمی
۶۰	فصل ۳: شناسایی و پویش برنامه کاربردی وب
۶۱	مقدمه
۶۱	شناسایی برنامه کاربردی وب
۶۲	اصول اولیه پراکسی وب
۶۳	Burp Suite
۶۴	پیکربندی پراکسی Burp
۶۶	اسپایدرینگ با Burp
۶۸	اجرای Burp Spider
۷۳	پویش کردن برنامه کاربردی وب
۷۴	پویشگر چه چیزی را پیدا خواهد کرد؟
۷۵	پویشگر چه چیزی را پیدا نخواهد کرد؟
۷۷	پویش کردن با پراکسی ZAP
۷۸	اجرای ZAP
۸۱	بررسی نتایج ZAP
۸۳	ZAP Brute Force
۸۴	پویش کردن با پویشگر Burp
۸۴	پیکربندی کردن پویشگر Burp
۸۵	اجرای پویشگر Burp
۸۶	بازبینی نتایج پویشگر Burp

فصل ۴: اکسپلویت از برنامه کاربردی وب با استفاده از تزریق..... ۸۹

مقدمه ۹۰

آسیب پذیری‌های تزریق SQL ۹۰

مفسر SQL ۹۱

SQL برای هکرها ۹۲

نمونه به DVWA با استفاده از تزریق SQL ۹۴

پیدا کردن آسیب پذیری‌ها ۹۵

دور زدن احراز هویت ۹۶

استخراج اطلاعات اضافی ۹۹

بدست آوردن چک‌های مرورای عبور ۱۰۳

کرک کردن رمز عبور ۱۰۵

sqlmap ۱۰۶

آسیب پذیری تزریق دستورات سیستم عامل ۱۱۲

تزریق دستورات سیستم عامل برای هکرها ۱۱۲

حملات تزریق دستورات در DVWA ۱۱۴

شل‌های وب ۱۱۷

فصل ۵: اکسپلویت برنامه کاربردی وب با دور زدن مکانیزم‌های احراز هویت

و پیمایش مسیر ۱۲۳

مقدمه ۱۲۴

آسیب پذیری‌های نشست و احراز هویت ۱۲۴

آسیب پذیری‌های پیمایش مسیر ۱۲۶

۱۲۶	حملات جستجوی فراگیر بر روی احراز هویت
۱۲۹	پیکربندی Burp Intruder
۱۳۱	پیلودهای Intruder
۱۳۵	اجرای Intruder
۱۳۶	حمله‌های نشست
۱۳۷	کرک کردن کوکی‌ها
۱۳۷	حمله‌های دزدی کوکی
۱۳۸	حمله پیمایش مسیر
۱۳۹	ساختار فایل سیستم وب سرور
۱۴۱	Forceful Browsing
۱۴۳	فصل ۶: هک کاربران وب
۱۴۴	مقدمه
۱۴۴	آسیب پذیری‌های XSS (cross-site scripting)
۱۴۵	آسیب پذیری‌های جعل درخواست بین سایتی (CSRF)
۱۴۶	XSS در مقابل CSRF
۱۴۷	آسیب پذیری مهندسی اجتماعی
۱۴۸	شناسایی کاربر وب
۱۴۹	پوش کاربران وب
۱۵۰	اجرای حملات XSS (Cross-Site Scripting)
۱۵۱	پیلودهای XSS
۱۵۲	حملات XSS بازتابی

۱۵۴	بررسی پاسخ وب سرور
۱۵۶	کدگذاری پیلودهای XSS
۱۵۸	حمله XSS به URL ها
۱۵۸	حمله های XSS روی شناسه های نشست
۱۵۹	حملات XSS ذخیره شده
۱۶۱	حملات جعل درخواست بین سایتی (CSRF)
۱۶۲	ارار هندسی اجتماعی (SET)
۱۶۴	دیگر چار وب ها: برجسته حمله به کاربر
۱۶۵	فصل ۷: بازسازی و مقوم سازی برنامه های کاربردی وب
۱۶۶	مقدمه
۱۶۶	مقاوم سازی سرور
۱۶۷	پیام های خطای عمومی
۱۶۸	اشکال زدایی برنامه کاربردی وب
۱۶۸	مقابله با حملات تزریق
۱۷۱	اشکال زدایی احراز هویت و مدیریت نشست
۱۷۱	توصیه های امنیتی برای احراز هویت امن
۱۷۳	توصیه های امنیتی برای مدیریت نشست
۱۷۴	اشکال زدایی مسیر پیمایش
۱۷۵	اشکال زدایی کاربر وب
۱۷۵	نکات مهم برای مقابله با حمله XSS
۱۷۶	نکات مهم در اعتبارسنجی ورودی

۱۷۷.....	مقابله با XSS استفاده از کدگذاری
۱۷۷.....	مقابله با XSS از طریق پیکربندی مرورگر
۱۷۸.....	نکات مهم در مقابله با حمله CSRF
۱۷۹.....	دفاع بیشتر در برابر CSRF
۱۸۰.....	مقابله با تکنیک مهندسی اجتماعی
۱۸۱.....	واژه نامه انگلیسی به فارسی
۱۸۵.....	منابع

امروزه استفاده از برنامه‌های کاربردی وب گسترش زیادی یافته است. استفاده از خدمات اینترنتی، انجام امور مختلف، مانند خرید، انجام امور بانکی، پرداخت قبوض، و غیره را بسیار ساده‌تر نموده است. به علاوه، با استفاده از سرویس‌های مختلف مانند ایمیل و شبکه‌های اجتماعی، امکان برقراری ارتباط سریع و ارزان قیمت با سایرین ممکن شده است. یک مسئله مهم در به کارگیری خدمات اینترنتی، امنیت سرویس-های ارائه شده است. متأسفانه مدیران وب سایت‌ها توجه کافی به امن سازی سایت-های خود ندارند. در نتیجه قسمت قابل توجهی از سایت‌ها آسیب پذیر بوده و با استفاده از ابزارهای متداول هک می‌شوند.

هدف از نگارش این کتاب، بررسی آسیب پذیری‌های^۱ برنامه‌های کاربردی وب و آموزش نحوه مقابله با آنها می‌باشد. در مباحث مطرح شده ضمن بیان مفاهیم تئوری، ابزارهای هک را نیز معرفی شده‌اند. خوانندگان تسلط کافی نسبت به موضوع بیابند. ابتدا روش‌های گردآوری اطلاعات راجع به برنامه کاربردی وب توضیح داده شده‌اند. سپس نحوه نفوذ به سیستم با استفاده از آسیب پذیری‌های کشف شده، مطالعه شده است. در اینجا آسیب پذیری‌های متداول، مانند استخراج اطلاعات مهم از پایگاه داده‌ها^۲ و دور زدن مکانیزم‌های احراز هویت، با جزئیات دقیقی بررسی شده است. مباحث این کتاب به صورت پایه‌ای مطرح شده‌اند تا برای خوانندگانی که آشنایی قبلی با هک برنامه کاربردی وب ندارند نیز قابل استفاده باشد.

مباحث مطرح شده در هر فصل به صورت زیر می‌باشد:

1. Vulnerability

۲. Database

- در فصل اول مباحث کلی در مورد هک برنامه‌های کاربردی وب بیان می‌شود. همچنین شمای کلی در مورد حملاتی که ادامه آنها را بررسی خواهیم نمود ارائه می‌گردد.
- مسائل مربوط به شناسایی خصوصیات وب سرور، در فصل دوم مطرح می‌شود. روش‌ها و ابزارهای به کار رفته در این فصل، در حالت کلی برای همه شبکه‌ها قابل استفاده می‌باشد. ابزارهای معرفی شده شامل Nmap، Nessus، و metasploit می‌باشد.
- فصل سوم به روش‌ها و ابزارهای موجود برای شناسایی برنامه کاربردی وب، می‌پردازد. ابزارهای معرفی شده در این فصل، Burp و ZAP می‌باشند. با استفاده از این ابزارهای کارهای به سرعت می‌توان انجام داد. به عنوان مثال می‌توان با استفاده از آنها نقشه وب سایت مورد نظر به دست آورد.
- حملات تزریق^۳ در فصل چهارم مطالعه خواهند شد. این حملات شامل تزریق SQL و دستورات سیستم عامل می‌باشد. ابزارهای استفاده شده برای حمله، Burp، sqlmap و John the Ripper می‌باشند.
- در فصل پنجم نحوه دور زدن مکانیزم‌های حرارت هویت مطالعه خواهند شد. همچنین حملات پیمایش مسیر نیز معرفی می‌شوند.
- یکی از روش‌های موثر در هک برنامه‌های کاربردی وب، حمله به کاربران آن است. بنابراین در فصل ششم، این روش‌ها بررسی خواهند شد. در اینجا دو روش متداول که XSS و CSRF نام دارند، معرفی شده‌اند. همچنین روش‌های مهندسی اجتماعی که مبنای حمله در آنها فریب کاربران است، در ادامه توضیح داده شده‌اند.
- در فصل هفتم روش‌های مقابله با حملات وب معرفی شده‌اند.