راهنمای عملی
هک وب با استفاده از کالی لینوکس

تالیف و ترجمه:
دکتر لیلی فرزین وش(استادیار دانشگاه تبریز)
مهندس مهسا علی‌پور امتنانی– مهندس رویا روشنی ممقانی

سرشناسه	: فرزین وش، لیلی. ۱۳۶۳.
عنوان و پدیدآور	: راهنمای عملی هک وب با استفاده از کالی لینوکس/تالیف و ترجمه:دکتر لیلی فرزین وش، مهندس مهسا علی پور امتنانی و مهندس رویا روشنی ممقانی
مشخصات نشر	: نور علم.
مشخصات ظاهری	: ۱۸۵ ص. :جدول، نمودار، مصور.
شابک	: ۱-۱۴۶-۱۶۹-۶۰۰-۹۷۸
وضعیت‌فهرست‌نویسی	: براساس اطلاعات فیپا (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 کنگره	۱۳۹۵ ۲ر۴ف/ ۵۱۰۵ TK
رده‌بندی دیویی	: ۰۲۵/۰۴

نشر نورعلم: تهران - انقلاب - خ ۱۲ فروردین-پلاک۲۵۹- ط۴ -واحد ۸ تلفن: ۶۶۴۰۵۸۸۰ و ۶۶۴۰۵۸۹۴

reelm@yahoo.com ۰۹۱۲۳۳۳۴۲۲ 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: ۵۰۰جلد

شابک: ۱-۱۴۶-۱۶۹-۶۰۰-۹۷۸

نوبت چاپ:اول ۱۳۹۵

چاپ و صحافی: الغدیر

قیمت: ۱۵۰۰۰ تومان

فهرست مطالب

مقدمه

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. متاسفانه 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[1] برنامه‌های کاربردی وب و آموزش نحوه مقابله با آنها می‌باشد. در مباحث مطرح شده ضمن بیان مفاهیم تئوری، ابزارهای هک را نیز معرفی شده‌اند تا 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[2] و دور زدن مکانیزم‌های احراز هویت، با جزییات دقیق 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
2. 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 مختلفی می‌توان انجام داد. به عنوان مثال می‌توان با استفاده از آنها نقشه وب سایت مورد نظر را 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 احراز 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.

---

۳. Injection