به نام خدا

دوره تست نفوذ و امنیت وب

مدرس: فرهاد علی‌محمدی

ارائه شده توسط آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران

دانشگاه تهران

آزمایشگاه پژوهشی فضای سایبر

سرفصل های دوره

- معرفی دوره – نقشه راه – راه‌های کسب درآمد – پرسش و پاسخ

فصل ۱ : باگ‌های مهم و رایج در وب

- نصب آزمایشگاه مجازی روی شبیه ساز – Metasploitable 2 – بررسی باگ‌های File Upload و LFI
- بررسی باگ‌های RCE و XSS
- بررسی باگ‌های SQL و Insecure Session Management
- باگ Log4j و سوال GoogleCTF 2022 (امتیازی)

پایان فصل ۱ – تمرین شماره یک

فصل ۲ : تست نفوذ با تئوری Active Directory و Brute Force روی سایت‌ها

- بررسی الگوریتم Brute Force و روش های نوین ترکیب شده با آن روی سایت با امنیت پایین
- حمله با Brute Force به وب سایت های دارای CSRF Tokens و کپچا سطح آسان (تصویر و نوشته)
- حمله با Brute Force به سایت های دارای امنیت بالا (دارای رمزنگاری) + کپچا سطح بالا (Recaptcha , hCaptcha , ...)
- حمله با Brute Force به سایت های دارای امنیت JS Protection با استفاده از Selenium
- بررسی سایت فرادرس در سال ۲۰۱۸-۲۰۱۹ و امنیت آن + سوال Harry Potter در مسابقه XeroCTF

پایان فصل ۲ – تمرین شماره دو

فصل ۳ : تست نفوذ وب با استفاده از برنامه های اندروید و اسنیف API

- نصب برنامه های مورد نیاز، و پیکربندی آن ها + بررسی یک آپ ساده اندروید جهت اسنیف API
- حمله با روش SSL Pinning در اندروید و بررسی و اسنیف API یک آپ با این روش
- ساخت برنامه Brute Force با پایتون با اطلاعات به دست آمده از قسمت های قبلی

پایان فصل ۳ – تمرین شماره سه

نقشه راه Cyber Security

Sans RoadMap

راه های درآمد

۱- ساخت Exploit و فروش آن

0day.today

راه های درآمد

۲- گرفتن سفارش تست نفوذ و ارائه نتیجه آن (Penetration Testing Service)

Upwork.com

Linkedin.com

Indeed.com

Github.com

دانشگاه تهران

۳- فروش اطلاعات حساس (Database Leak)

۴- مسابقات CTF (چالش های Capture The Flag)

ctftime.org

راه های درآمد

۴- پیدا کردن باگ و گزارش آن (Bug Bounty)

ایرانی

bugdasht.ir

ravro.ir

خارجی

hackerone.com

Bugcrowd.com