به نام خدا

درس امنیت داده و شبکه

نیم‌سال اول ۱۴۰۱-۱۴۰۰

دانشکدهٔ مهندسی کامپیوتر

دانشگاه صنعتی شریف

مدرس **مهدی خرازی**

موضوع **بهره‌برداری از آسیب‌پذیری‌های کاربردهای وب**

موعد تحویل **ساعت ۲۳:۵۹ دوشنبه ۱ آذر ۱۴۰۰**

طراحی چالش توسط **سارا عسگری**

با سپاس از **محمد حدادیان**

۱ مقدمه

هدف از این چالش تجربه بیشتر در شناسایی و بهره‌برداری از آسیب‌پذیری‌های کاربردهای وب است. یک ماشین مجازی به شما داده شده‌است که این ماشین روی پورت‌های ۸۰۸۵ و ۸۰۸۰ به ترتیب به درخواست‌های مربوط به بخش اول و بخش دوم این چالش گوش میدهد. نوع شبکه این ماشین مجازی روی NAT تنظیم شده‌است و همچنین پورت‌های ماشین میزبان به پورت‌های ماشین مجازی forward شده‌اند. بنابراین شما میتونید به عنوان مثال با وارد کردن `localhost:8085` در مرورگر ماشین میزبان خود به وب‌سایت بخش اول دسترسی پیدا کنید. این ماشین مجازی را میتوانید از این لینک دانلود کنید. مشاهده ویدیوهای منزل وب پرچم و حل چالش‌های آن توصیه میشود.

۲ بخش اول

در این بخش شما با وب‌سایتی مواجه هستید که بخشی از کد آن در مخزن handouts قرار داده شده‌است. شما باید بتوانید آسیب‌پذیری‌ای را در این وب سرور پیدا کرده و با سوءاستفاده از آن پرچم را به دست بیاورید. قالب پرچم در این بخش یک رشته ۱۸ کاراکتری است که از حروف کوچک و بزرگ انگلیسی، اعداد و _ تشکیل شده است.

۳ بخش دوم

در این بخش کد وب‌سرور به شما داده نشده‌است. در مرحله اول شما باید آسیب‌پذیری این وب سرور را پیدا کنید و سپس با سوءاستفاده از آن به پرچم دست یابید. قالب پرچم در این بخش یک رشته ۳۱ کاراکتری است که از حروف کوچک و بزرگ انگلیسی، اعداد و _ تشکیل شده است.

۴ تحویل‌دادنی‌ها

شما باید یک ویدئو با حجم حداکثر ۴۰ مگابایت و مدت زمان حداکثر ۱۵ دقیقه تهیه کنید و در این ویدئو مراحلی که برای حل هر یک از بخش ها طی نموده‌اید را نشان داده و توضیح دهید. این ویدئو را در یکی از سرویس‌های میزبانی فایل مانند Google Drive آپلود کنید و سپس لینک آن را در یک فایل به نام `links.txt` در پوشه‌ی `chals/chal2` قرار داده و این فایل را به همراه یک فایل به نام `parchams.txt` که پرچم هر یک از بخش‌ها را در آن قرار داده‌اید در مخزن خود در طرشت push کنید. به علاوه اگر برای هر یک از بخش‌ها اسکریپتی نوشته‌اید آن را به همراه یک گزارش که نحوه‌ی اجرای اسکریپت به صورت کامل در آن توضیح داده شده‌است را در همین پوشه از مخزن خود در طرشت push کنید.