آزمایشگاه امنیت شبکه

حملات مربوط به کاربردهای وب

مقدمه: در این آزمایش قصد بر آن است که دانشجویان با حملات مربوط به کاربردهای وب آشنا شوند.

آزمایش ۱-۶: XSS

- تفاوت حملات XSS Stored و XSS Reflected را بطور عملی نشان دهید. به این صورت که هر دو حمله را به قصد به سرقت بردن کوکی کاربر انجام دهید و علی رغم نتیجه‌ی یکسان تفاوت آن‌ها را بیان کنید. نشان دهید ممکن است هدف به یکی از حملات آسیب پذیر و به دیگری آسیب پذیر نباشد.

آزمایش ۲-۶: دیجی‌کالا

- در سال ۲۰۱۶ یک آسیب‌پذیری در مورد حمله XSS در دیجی‌کالا وجود داشت. تحقیق کنید چه نوع حمله XSS به آن کارگر بود؟
- آیا می‌توانید سودوکدی که منجر به چنین آسیب‌پذیری‌ای شده بود را بنویسید؟

آزمایش ۳-۶: دفاع در مقابل XSS

- یک وب اپلیکیشن بنویسید که دارای آسیب‌پذیری XSS Stored باشد. دلیل آسیب‌پذیری را روی کد خودتان توضیح دهید.
- آسیب‌پذیری موجود را طوری اکسپلویت کنید که اطلاعات(آدرس آی پی، کوکی و...) کاربری که به برنامه شما دسترسی پیدا می‌کند را به ایمیل شما ارسال کند.

*آزمایش ۴-۶: Mutated XSS (mXSS)

- نوع mXSS حملاتی هستند که یک payload عادی تزریق شده اما هنگ ام parse ک ردن توسط مرورگر، payload حالت مخرب پیدا می‌کند. چنین حمله‌ای را روی یک وب اپلیکیش ن انجام دهید. نشان دهید Sanitize کردن معمول نمی‌تواند در مقابل این حمله موثر باشد.

*آزمایش ۵-۶: XSS Fuzzer

- آیا فازینگ برای تشخیص آسیب‌پذیری‌های مربوط به XSS موثر است؟
- اگر پاسخ قسمت قبلی خیر است در مورد mXSS استدلال کنید با فاز ک ردن مرورگ ر نمی‌ت وان تشخیص موثری لحاظ کرد.
- اگر پاسخ قسمت اول بله است آسیب‌پذیری وب اپلیکیشنی که در آزمایش ۳-۶ نوشـتید را بـا یـک فازر تشخیص دهید و آن‌را وصله کنید.