بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

قوانین و مقررات کلاه سفید

شهریور ۹۸

معرفی سامانه کلاه سفید

از زمان پیدایش سامانه‌های کامپیوتری و پس از آن با افزایش درک اهمیت امنیت اطلاعات، آزمون‌های امنیتی نیز رواج یافته‌اند و ارزیابی امنیتی سامانه‌ها به یکی از اصلی‌ترین نیازهای سازمان‌ها و شرکت‌های تولید و توسعه نرم‌افزار تبدیل شده است.

اما علاوه بر چالش یافتن تیم امنیتی ماهر و متخصص برای ارزیابی امنیتی باکیفیت و همه‌جانبه، سرعت و هزینه آزمون‌های نفوذ و ارزیابی‌های امنیتی، و به عبارتی کارایی مناسب در قبال هزینه‌های پرداختی، از مهم‌ترین دغدغه محسوب می‌شود. به طور سنتی و مرسوم، پس از انعقاد قرارداد آزمون امنیتی، بایستی مستقل از تعداد و کیفیت آسیب‌پذیری‌های کشف‌شده و تنها بر اساس زمان انجام آن، هزینه‌های خدمات ارزیابی امنیتی در قبال آزمون نفوذ پرداخت شود؛ این درحالی است که ممکن است یا به دلیل امنیت بالای سامانه و یا به خاطر فقدان تخصص و دانش در تیم آزمون‌گر هیچ‌گونه آسیب‌پذیری کشف نشود و یا دست‌کم گستره مناسبی از آزمون‌ها صورت نگرفته باشد و تنها بخش کوچکی از حفره‌های سامانه گزارش شود.

مرکز ماهر در راستای ماموریت‌های خود به منظور ارتقای امنیت در سامانه‌های کشور، اقدام به برگزاری مسابقات ارزیابی امنیتی و کشف باگ (Bug bounty) در سطح وب‌سایت‌ها و سامانه‌های دولتی تحت شبکه‌ی اینترنت کرده است. در این راستا سامانه کلاه سفید مرکز ماهر (https://kolahsefid.cert.ir)، آماده ارزیابی امنیتی سامانه‌ها از طریق برگزاری مسابقات عمومی و خصوصی است.

این سامانه با توجه به همین چالش‌ها، راهکار ارائه خدمات برگزاری مسابقه ارزیابی امنیتی را مطرح و بستری فراهم کرده است تا متخصصین مجرب امنیتی و سازمان‌ها و شرکت‌های تولید نرم‌افزار با حداکثر سرعت و حداقل هزینه در کنار یکدیگر قرار بگیرند. با توجه به تعداد بالای متخصصین این سامانه، که تعداد آن‌ها تاکنون به بیش از ۵۰۰ نفر رسیده است، طیف وسیعی از دانش و مهارت مورد نیاز برای ارزیابی امنیتی فراهم شده است. از طرفی، برخلاف رویه سنتی قراردادهای آزمون نفوذ، سازمان و شرکت متقاضی دریافت خدمات ارزیابی امنیتی تنها به ازای آسیب‌پذیری‌های موجود در سامانه خود هزینه پرداخت می‌کند. همچنین، با توجه به ماهیت مسابقه‌بودن، آسیب‌پذیری‌هایی معتبر شناخته شده و مشمول دریافت جایزه به متخصص می‌شوند که علاوه بر تایید نظر داوران سامانه کلاه سفید مبنی بر صحت وجود آن‌ها در سامانه مورد ارزیابی، زودتر از سایر متخصصین گزارش شده باشد. همین امر باعث می‌شود تا افزون بر افزایش کیفیت و کاهش هزینه‌ها، زمان آزمون نفوذ و ارزیابی امنیتی نیز به حداقل برسد.

لازم به ذکر است که داوران سامانه کلاه سفید به عنوان متخصصان بی‌طرف، در اسرع وقت گزارش‌های ارسالی کشف آسیب‌پذیری‌ها را به دقت بررسی می‌کنند. در صورتی که گزارش مطابق با قوانین مسابقه پذیرفته شود، جایزه تعیین‌شده به متخصص گزارش‌دهنده پرداخت خواهد شد. پیش از برگزاری مسابقه و به منظور تعیین شرایط و قوانین آن، تیم فنی و داوران کلاه سفید مشاوره لازم را بر مبنای سامانه مورد آزمون در اختیار سازمان قرار می‌دهد.

مسابقات کلاه سفید به دو صورت عمومی و خصوصی برگزاری می‌گردد. در مسابقات عمومی کلیه متخصصین عضوشده در سامانه امکان مشاهده جزئیات و شرکت در آن را دارند و در مسابقه خصوصی تنها متخصصین شناخته‌شده و منتخب، امکان شرکت دارند.

در انتهای هر مسابقه، تیم فنی و داوران سامانه مستندی از تمامی آسیب‌پذیری‌های موجود در سامانه مورد ارزیابی را در اختیار سازمان یا شرکت مربوطه قرار می‌دهد. این مستند شامل جزئیات هر یک از آسیب‌پذیری‌های گزارش‌شده و شرح مختصری از نحوه برطرف‌کردن آن‌ها است. در صورت تمایل، سازمان می‌تواند درخواست دریافت گواهی و تاییدیه امنیتی سامانه خود را به کلاه سفید ارائه دهد. پس از توافق و اعلام رفع تمامی آسیب‌پذیری‌های قبلی، تیم فنی کلاه سفید به آزمون نفوذ و ارزیابی امنیتی مجدد سامانه می‌پردازد و در صورت گذراندن آزمون‌های مختلف، گواهی و تاییدیه امنیتی به سازمان اعطا خواهد شد.