بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

قوانین و مقررات کلاه سفید

شهریور ۹۸

قوانین و مقررات کلاه سفید

کلاه سفید یک سامانه برخط برای برگزاری مسابقات کشف آسیب‌پذیری و ارزیابی امنیتی با استفاده از خرد جمعی است. این سامانه، نرم‌افزارهای مشتریان را در معرض ارزیابی امنیتی طیف وسیعی از متخصصین امنیت سامانه‌های کامپیوتری قرار می‌دهد. این توافق‌نامه حقوقی شرایط استفاده از سامانه کلاه سفید را برای مشتریان مشخص کرده و کلیه مشتریان حقیقی و حقوقی پیش از استفاده از سامانه موافقت خود را با مفاد آن اعلام می‌کنند.

الف) تعاریف

- آسیب‌پذیری امنیتی (حفره امنیتی): هر نقطه ضعف یا نقیصه‌ای در نرم‌افزارها یا سامانه‌ها که می‌تواند موجب سوءاستفاده نفوذگران واقع شده و خط‌مشی امنیتی را نقض کند.
- مسابقه کشف آسیب‌پذیری: یک مسابقه با هدف کشف آسیب‌پذیری‌های سامانه یا نرم‌افزارهای مشخص‌شده در شرایط مسابقه که با شرکت متخصصین عضو سامانه کلاه سفید برگزار می‌گردد.
- مسابقه عمومی: مسابقاتی که کلیه متخصصین عضوشده در سامانه کلاه سفید امکان مشاهده جزئیات و شرکت در آن را دارند.
- مسابقه خصوصی: مسابقاتی که تنها متخصصین شناخته‌شده و منتخب، امکان شرکت در آن را دارند و امکان شرکت سایر متخصصین وجود ندارد.
- متخصص امنیتی: اشخاص حقیقی یا حقوقی که به عنوان متخصص امنیتی در سامانه کلاه سفید ثبت‌نام کرده و در مسابقات کشف آسیب‌پذیری شرکت می‌نمایند. متخصصینی که اطلاعات هویتی و مهارت آن‌ها مورد تأیید سامانه کلاه سفید باشد، به عنوان متخصص شناخته‌شده در نظر گرفته می‌شوند و از آن‌ها برای شرکت در مسابقات خصوصی دعوت می‌شود.
- برگزارکننده مسابقه: کلیه اشخاص حقیقی یا حقوقی که مایل هستند سامانه یا نرم‌افزار خود را در معرض ارزیابی امنیتی توسط متخصصین امنیتی در سامانه کلاه سفید قرار دهند.
- شرایط و قوانین مسابقه: کلیه ملاحظات و نکات مدنظر برگزارکننده یک مسابقه در شرایط مسابقه ذکر می‌شود. این موارد می‌تواند شامل نحوه کشف آسیب‌پذیری و ثبت گزارش، اهداف و سامانه‌های مورد نظر برای کشف آسیب‌پذیری، آسیب‌پذیری‌های قابل قبول و میزان جوایز آن‌ها، و همچنین آسیب‌پذیری‌های غیر قابل قبول باشد.
- گزارش کشف آسیب‌پذیری: گزارش کشف آسیب‌پذیری شامل کلیه اطلاعاتی است که به داوران سامانه کلاه سفید این امکان را می‌دهد که آسیب‌پذیری کشف‌شده را درستی‌سنجی نمایند. به عنوان مثال، جهت پرداخت جایزه آسیب‌پذیری کشف‌شده، می‌بایست مدارک قابل استناد که آسیب‌پذیری را تأیید کند (مانند فیلم، تصویر، اسکرین‌شات و غیره)، همراه با توضیحات متنی مناسب در گزارش گنجانده شود.

ب) تعهدات و ملاحظات حقوقی متخصصین امنیتی

محرمانگی آسیب‌پذیری‌ها

متخصصین شرکت‌کننده در مسابقات تعهد می‌نمایند که جزئیات آسیب‌پذیری‌های کشف‌شده را جز در سامانه کلاه سفید در هیچ سایت، بلاگ، شبکه اجتماعی یا رسانه دیگری منتشر ننمایند. پس از گزارش آسیب‌پذیری و رفع نقطه ضعف امنیتی، تنها در صورت موافقت کتبی برگزارکننده مسابقه، متخصص می‌تواند جزئیات آسیب‌پذیری را با هماهنگی برگزارکننده منتشر نماید.

گزارش مسئولانه آسیب‌پذیری‌ها

متخصصین شرکت‌کننده در مسابقات تعهد می‌نمایند که در صورت کشف آسیب‌پذیری در سامانه‌های یک مسابقه آن را گزارش نمایند. سامانه‌های مورد ارزیابی در مسابقات تحت نظارت دائمی قرار دارند و در صورت کشف آسیب‌پذیری و عدم گزارش آن، مسئولیت‌های ناشی از سوء استفاده از آسیب‌پذیری مورد نظر بر عهده متخصص مربوطه خواهد بود.

سامانه‌های مجاز برای ارزیابی امنیتی

متخصصین امنیتی تنها مجازند سامانه‌هایی که در بخش سامانه‌های هدف یک مسابقه آورده شده، مورد ارزیابی و نفوذ قرار دهند. در صورتی که سامانه‌ها یا آدرس‌های آی‌پی خارج از این محدوده مورد ارزیابی قرار گیرد، مسئولیت حقوقی آن با متخصص مربوطه خواهد بود.

آسیب‌پذیری‌ها و حملات مجاز

متخصصین تعهد می‌کنند که شرایط برگزاری مسابقه را برای هر یک از مسابقات به دقت مطالعه کرده و تنها اقدام به کشف یا بهره‌برداری از آسیب‌پذیری‌هایی نمایند که در بخش آسیب‌پذیری‌های قابل قبول در شرایط مسابقه آورده شده است. بهره‌برداری یا انجام حملاتی که در شرایط مسابقه ذکر نشده باشد، غیر مجاز بوده و مسئولیت حقوقی آن بر عهده متخصص است.

ج) تعهدات و ملاحظات حقوقی برگزارکنندگان مسابقات

استقلال متخصصین از کلاه سفید

کلاه سفید شرایطی را فراهم می‌کند که سازمان‌ها و متخصصین امنیتی با هم ارتباط برقرار کنند اما کلاه سفید هیچ کنترل یا نظارتی بر روی متخصصین امنیتی ندارد. این متخصصین کارمندان کلاه سفید نیستند. مشتریان تأیید می‌کنند که ارتباط متخصصین امنیتی با کلاه سفید به صورت یک پیمانکار مستقل است.

سامانه‌های مجاز در کلاه سفید

سازمان یا فرد برگزارکننده مسابقه تنها مجاز به برگزاری مسابقه برای محصولات یا سامانه‌هایی است که متعلق به اوست. کلاه سفید پیش از برگزاری مسابقه، اطمینان حاصل می‌کند که فرد یا سازمان، مالک محصول یا سامانه‌ی مورد نظر است. در حال حاضر تنها سامانه‌های مستقر در کشور ایران می‌توانند در مسابقات تعریف شوند.

خط‌مشی حفظ محرمانگی

کلاه‌سفید متعهد می‌شود که اطلاعات برگزارکننده مسابقه و گزارش‌های ارسالی متخصصین را محرمانه تلقی کرده و تنها در اختیار رابط معرفی‌شده برگزارکننده مسابقه قرار می‌دهد.