SECURITYWORLD

Business Logic Write-ups 01

Exploiting Max. Character Limitation

Sunil Yedla به عنوان یک تست نفوذگر و شکارچی باگ، علاقه زیادی به شکستن عملکردها (Functionality) و پیدا کردن برخی باگ‌های جالب دارد. وی تاکید زیادی بر اهمیت درک عملکردها دارد و اشاره می‌کند که باید هر روش ممکن را برای شکستن عملکردها در جهت پیدا کردن راه‌های فرار از ویژگی‌های امنیتی معتبر جستجو کنیم.

تست نفوذگر ۶ ماه پیش، یک دعوتنامه خصوصی از سایت هکروان دریافت می‌کند، وی به سرعت دعوت را باز نموده و مشاهده می‌کند که دعوت نامه مربوط به یک برنامه رمزنگاری می‌باشد. از آنجا که تست نفوذگر طرفدار پروپا قرص جمع آوری اطلاعات یا همان Recon نمی‌باشد، شروع به تست همه عملکردهای برنامه به صورت یک به یک می‌نماید.

وی در فرآیند تست مشاهده می‌کند که هیچ محدودیت کاراکتری، برای فیلد نام وجود ندارد. در این حالت وی دو گزینه را پیش رو دارد:

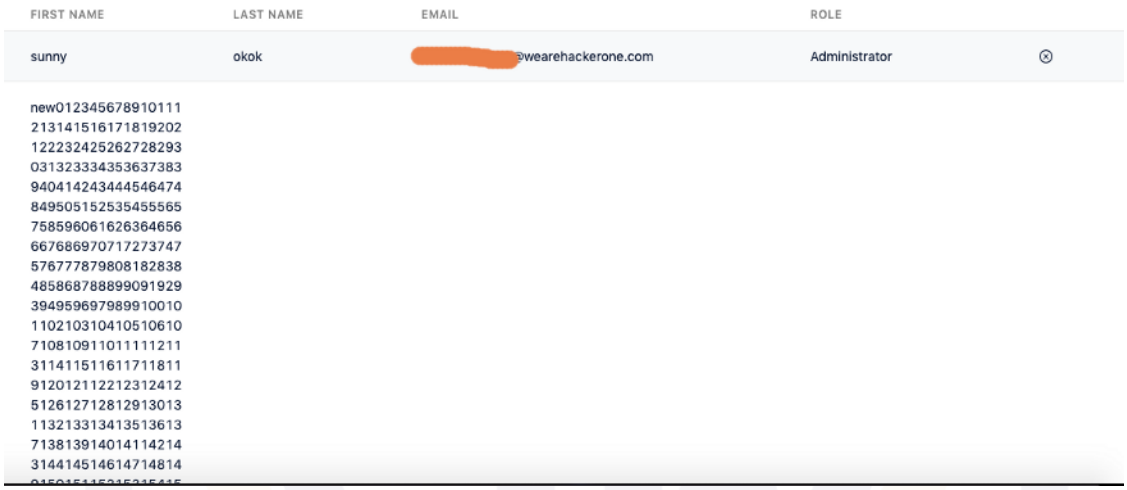
می‌تواند این موضوع را نادیده بگیرد زیرا به هر حال در صورت گزارش این موضوع، گزارش وی به عنوان اطلاع‌رسانی(Informative) و یا گاهی اوقات Not Applicable در نظر گرفته خواهد شد.

همچنین می‌تواند بررسی بیشتری انجام دهد و ببیند که این نام طولانی کجا می‌تواند به یک تهدید بالقوه برای یک شرکت یا کاربران یا عملکرد تبدیل شود.

تست نفوذگر روش دوم را انتخاب می‌کند و به کار خود ادامه می‌دهد.

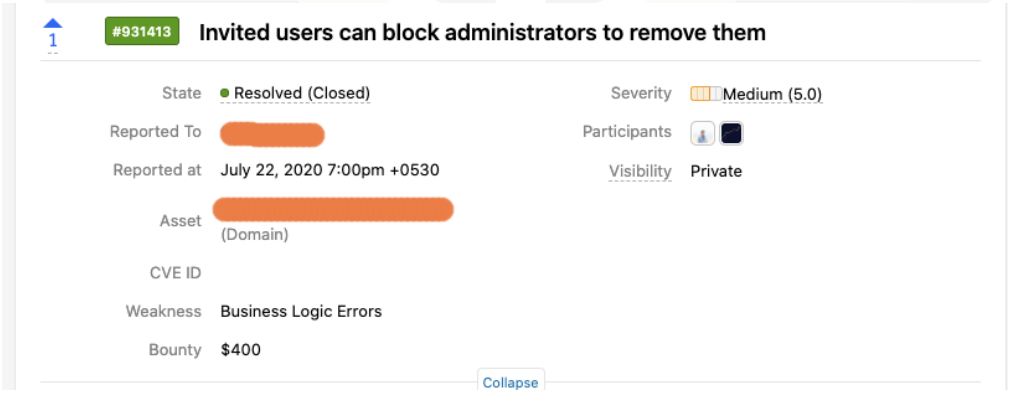
بنابراین شروع به بررسی تمام ویژگی‌ها نموده و در ابتدا متوجه می‌شود که این کار باعث حمله DoS می‌گردد. اما از آنجا که این امر تنها در مرورگر کروم اتفاق می‌افتد، تیم Triage سایت هکروان، این موضوع را قبول نکرده و گزارش تست نفوذگر را به عنوانInformative می بندد.

تست نفوذگر به کاوش ادامه می‌دهد و متوجه می‌شود که کاربران مدیر می‌توانند کاربران دیگر را دعوت کنند و تنها کاربر مدیر می‌تواند کاربر دعوت‌شده را در هر زمانی که بخواهد حذف نماید. امکان حذف کاربران دعوت‌شده تنها در یک صفحه وجود دارد که در آن لیست تمام جزئیات کاربران مانند: نام، نام خانوادگی، ایمیل و نقش کاربران در آن نمایش داده می‌شود. اما زمانی که فرد دعوت‌شده نام خود را به نامی طولانی با کاراکترهای زیاد تغییر می‌دهد، آنگاه کاربر ادمین قادر به مشاهده گزینه حذف نخواهد بود.



تاثیر این موضوع در اینجاست که کاربران دعوت‌شده می‌توانند برای همیشه در تیم باقی بمانند.

تیم Triage پس از بررسی این گزارش، آن را با شدت ۵ پذیرفته و مبلغ ۴۰۰ دلار جایزه برای آن در نظر می‌گیرد.



منبع:

https://sunilyedla.medium.com/exploiting-max-character-limitation-cde982545019