پروژه 99AP گروه 57

اقدامات مربوط به امنیت

مقدمه

به طور کل در چهار ماه طلایی که این پروژه زده شد چه خودم که در حال ثبت این رکورد به عنوان گزارش اقدامات مربوط به امنیت هستم چه دوستان هم گروهیم، پدرمان در آمد. خیلی از روز ها با عدم موفقیت، شکست های پیاپی، پیدا نکردن راه حل مربوط به ایده های نابمان که برای صفحات مختلف برنامه در نظر داشتیم می گذشتند و ما همچنان مجبور به استفاده از ابزار های منسوخ شده ای مانند جاواافیکس بودیم. ولی در چنین روزی، مورخ 8 مرداد 99، خرسندیم که می توانیم اعلام کنیم پروژه 99AP رسما تمام شده.

امیدواریم توضیحات مزبور درباره داک امنیت اندکی دست شما را در نمره دهی بازتر و بررسی شما را آسانتر کنید.

مورد اول Improper Inputs

به منظور محدود کردن حد ورودی Attacker، میزان ورودی ها را به چیزی حدود 65 هزار کلمه محدود کردیم که این کار با استفاده از توابع writeUTF و readUTF ممکن بود. تمام اعتبارسنجی ها با سیستم Authentication دوگانه ی طراحی شده توسط گروه 57 صورت می پذیرد که معماری Auth-Relic نام دارد. به این شکل احتمال دستکاری اطلاعات توسط فرد مهاجم به حد خوبی پایین می آید.

از طرفی برای ورودی های نامعتبر حد 100 پیام در10 ثانیه DoS جلوگیری از اشغال پهنای باند و اختلال در سرور می شود. همچنین در بخش های مختلف سرور و هندلر که احتمال Down شدن سرور توسط ورودی نامعتبر بود با Try-Catch کردن اکسپشن های مختلف، از خاموش شدن سرور جلوگیری کردیم.

مورد دوم SQL Injection

موقع ارسال Command از سمت کلاینت Validity دستور ارسال شده چک می شود سپس فرایند مربوط به آن صورت می گیرد. این صحت آزمایی با چک شدن بخش های کلیدی محصولات مانند آیدی محصول یا اکنت ها مانند یوزرنیم و... صورت می پذیرد.

همچنین به منظور جلوگیری از حالات پیش بینی نشده دیگر این حمله، از PreparedStatement در یکایک بخش هایی که دیتابیس دستکاری می شد استفاده شد.

مورد سوم Brute Force Attack

برای جلوگیری از این حمله، و اینکه حتی کاربران عادی نتوانند چندین بار ورودی نامعتبر دهند لیست های مختلفی در سرور قرار داده شده، که در صورت کشف یه مورد متخطی با ران کردن ثرد های تایمری مختلف، فرد خطاکار بصورت موقت (60 ثانیه) از ارسال دستور مشابه Ban می شود.

ازین مورد می توان در بخش لوگین کردن مثال زد.

مورد چهارم Denial Of Service/Dos

با قرار دادن لیست آی پی های حمله کننده، افرادی که در 10 ثانیه بیش از 100 دستور به سرور بفرستند و قصد ایجاد اختلال در سرور داشته باشند، بن می شوند و حتی با ریستارت کردن برنامه هم نخواهند توانست دستور جدیدی به سرور بفرستند، مادامی که سرور روشن باشد.