نگاهی گذرا به پلتفرم باگ‌بانتی راورو و شکارچیان آسیب‌پذیری

زمستان ۱۴۰۲

با آگاهی از آسیب‌پذیری‌ها، آینده امن‌تر است...

ما معتقدیم که با به اشتراک‌گذاری، "ما"ی قوی‌تری شکل می‌گیرد.
و این مای قوی‌تر جهان را به جای امن‌تر و بهتری تبدیل می‌کند.

امنیت سایبری قصه‌ها دارد...

در روزگاری نه‌چندان دور، اگر باگ یا آسیب‌پذیری‌ای از وب‌سایتی کشف می‌شد، چه اتفاقی می‌افتاد؟
سه شخصیت هکر، گزارش و کسب‌وکار کجای داستان قرار می‌گرفتند؟

هـــــکر: واژه‌ای که مساوی بود با جرم و جنایت! اکثر جامعه با عینکی سیاه به کسانی که در حوزه‌ی امنیت سایبری تخصص و دانش داشتند، نگاه می‌کردند. یک هکر در نبود سازوکارهای حمایتی و قوانین تخصصی، با استناد به قوانین دزدی، احکامی مانند قطع دست یا زندان نصیبش می‌شد.

گزارش: اگر آسیب‌پذیری‌ای کشف می‌شد، مسیر رایج آن، سرقت و انتشار داده‌ها و کدهای کسب‌وکار در فروم‌های زیرزمینی و بین هکرها بود.

کسب‌وکار: صاحب کسب‌وکار آخرین کسی بود که از آسیب‌پذیری اطلاع پیدا می‌کرد، آن هم از طریق پیغامی که هکر در وبسایت می‌گذاشت یا خبر خبرگزاری‌ها در مورد نشت اطلاعات.

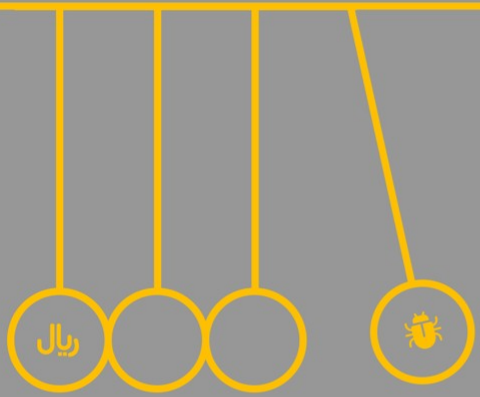
اما امروز...

در این گزارش چه خواهید خواند؟

در این گزارش، با نگاهی **آماری** و به زبان **اعداد**، **ارقام** و **نمودارها** با شما سخن خواهیم گفت و به روایت آن‌چه که تابه‌حال در داستان **پلتفرم باگ‌بانتی راورو** گذشته‌است، می‌پردازیم. با ارائه‌ی **نقل‌وقول**هایی برخاسته از تجربه‌ی زیسته‌ی افرادی که در هوای حوزه‌ی امنیت سایبری زیسته‌اند، نیز آن را تکمیل خواهیم کرد.

اعداد چه می‌گویند؟

اعداد، گفتنی‌هایی راجع به **شکارچیان آسیب‌پذیری**، **گزارش‌های آسیب‌پذیری** و **میدان‌ها** دارند، که با شما درمیان خواهند گذاشت.



این گزارش تقدیم می شود به:

متخصصان امنیت سایبری

که دانش و تخصصشان را در شکارآسیب‌پذیری‌ها به کار می‌گیرند.

کسب‌وکـــارهای پیشـــرو

که میدان کشف آسیب‌پذیری شدند و امن‌تر شدن را این‌گونه یافتند.

فعالان حوزه‌ی امنیت سایبری

که هر کدام به سهمی، نقشی در پررنگ‌شدن حقوق کاربران در زمینه‌ی امنیت سایبری دارند.

و همکاران اجرایی در پلتفرم باگ‌بانتی راورو

که در مسیر این رویا، گام برداشتند.

اولین

گزارش آسیب‌پذیری

در راورو

در تاریخ: ۱۳۹۹/۰۱/۱۰

عنوان گزارش: آسیب‌پذیری Bypass OTP Verification

شکارچی آسیب‌پذیری: @rima

میدان: کانکتیت

بانتی دریافتی: ۱/۵ میلیون تومان

تا به امروز در باگ‌بانتی راورو:

۲۸۷ شکارچی آسیب‌پذیری به‌صورت فعال حضور داشته‌اند.

۴۵ کسب‌وکار امن‌تر شده‌اند.

۳۲۰۰ آسیب‌پذیری گزارش شده‌اند.

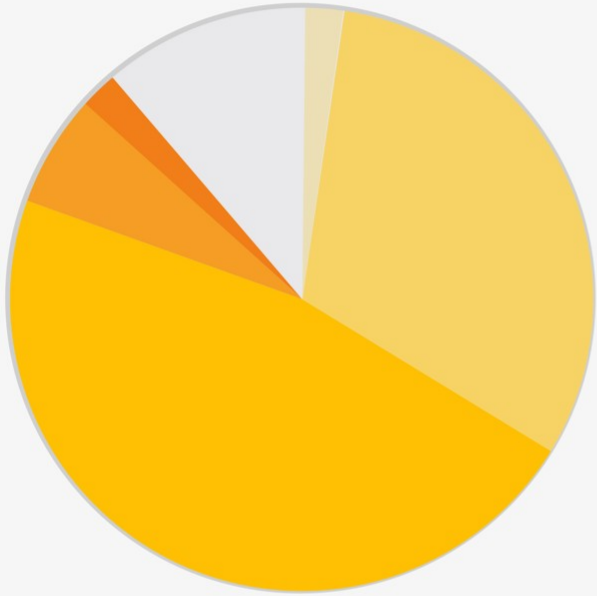
+۲ میلیارد تومان بانتی پرداخت شده‌است.

www.Ravro.ir

داخل پرانتز:

تمامی اعداد و داده‌های ارائه‌شده در صفحه‌های آینده، مربوط به شکـــارچیان آسیب‌پذیری فعال در پلتـفرم باگ‌بانتی راورو است.

سن شکارچیان آسیب‌پذیری



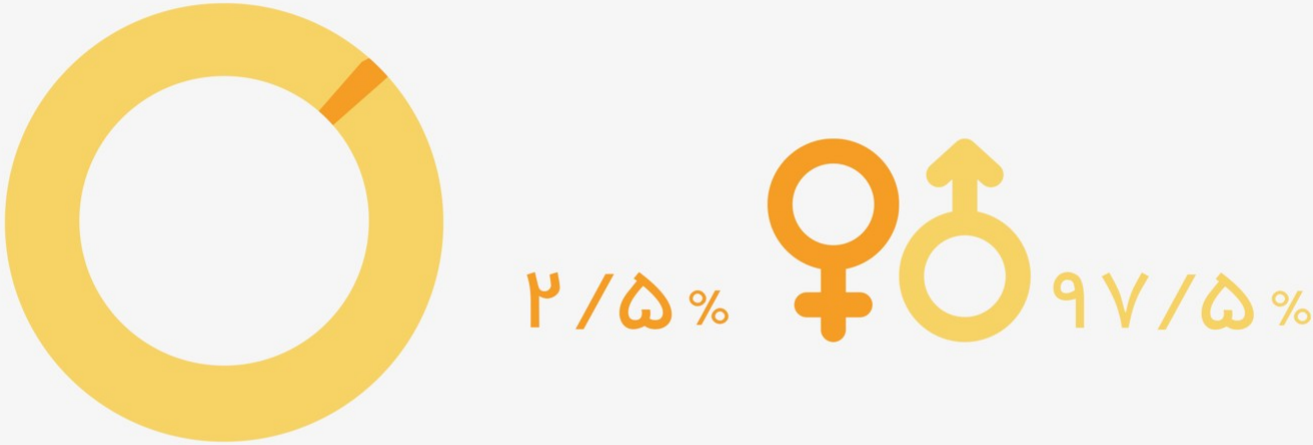
۱ %	۱۳ تا ۱۷ سال
۳۴%	۱۸ تا ۲۴ سال
۴۶%	۲۵ تا ۳۴ سال
۷ %	۳۵ تا ۴۹ سال
۱ %	بیش‌از ۵۰ سال
۱۱%	نامشخص

جوان‌ترین‌ها

۱ **۱۴ سال** از تهران

۲ **۱۷ سال** از زنجان، اهواز، شوشتر و فراهان

جنسیت شکارچیان آسیب‌پذیری



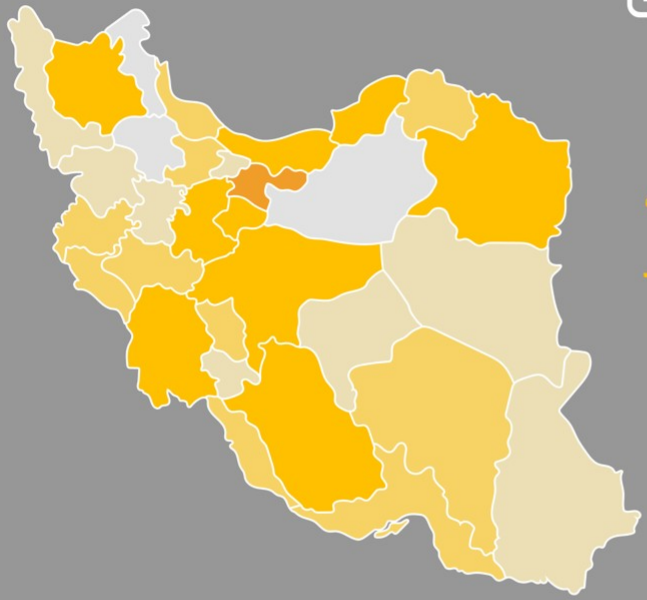
نسبت تعداد شکارچیان آسیب‌پذیری خانم به آقا در جامعه‌ی بین‌المللی امینت سایبری، همواره کم بوده اما این نسبت در ایران **خیلی خیلی کم‌تر** است.

ارغوان کامیار

شکارچی آسیب‌پذیری

یک بار، وقتی که پروژه‌ای را تحویل دادم، شخصی که پروژه را از من تحویل گرفتند، بررسی کردند و به‌قصد تعریف در بازخوردشان گفتند: "خیلی خوب بود. نتیجه‌ی کارتان را خیلی دوست داشتیم. **انتظار نداشتیم که یک خانم بتواند این کار را بکند!**" ایشان می‌خواستند از من تعریف کنند. ظاهرا تعریف بود، ولی پشتش را که می‌بینی، متوجه می‌شوی واقعا چه دیدگاهی وجود دارد... **فکر می‌کنند خانم‌ها نمی‌توانند و چون نمی‌توانند، در این حوزه نیستند!** در صورتی‌که واقعا این‌طور نیست. دلیل این‌که خیلی از خانم‌ها سمت این حوزه نمی‌آیند، این نیست که نمی‌توانند! حتما دلایل مختلفی دارد.

پراکندگی شکارچیان آسیب‌پذیری در سطح ایران



دو **شکارچی آسیب‌پذیری** که برروی یک هدف، **همکاری** داشته‌اند، بیش‌از **۲۵۰۰ کیلومتر** از هم فاصله دارند.

۲۹%

از شکارچیان آسیب‌پذیری ساکن تهران هستند.

استان‌های خراسان رضوی، مازندران، تبریز، اصفهان، فارس، خوزستان، قم، گلستان و مرکزی به‌ترتیب، بیشترین شکارچیان آسیب‌پذیری را دارند.

محمدحسین آشفته‌یزدی

شکارچی آسیب‌پذیری

آرزویم برای حوزه‌ی امنیت برای مناطقی است که مثل تهران شرایط خیلی مهیایی ندارند. **قطعا پتانسیل‌هایی در شهرستان‌ها هم وجود دارند.** مثلا؛ در جایی که من در آن زندگی می‌کنم، افراد کمی هستند و کامیونیتی امنیت قوی‌ای وجود ندارد. همان افراد هم معمولا برای تبادل اطلاعات به تهران می‌روند. خیلی از اساتید خوب، در پایتخت هستند. موسسه‌هایی هستند که فقط آموزش حضوری دارند. البته الان شرایط بهتر شده. **امیدوارم که شرایط مهیا شود و همه چیز منحصر به پایتخت نباشد. امیدوارم کامیونیتی امنیت در شهرهای مختلف رشد کند.** و افراد به‌خاطر فراگیری آموزش، خیلی با چالش جغرافیایی مواجه نشوند.

درآمد شکارچیان آسیب‌پذیری

۱۰٪ از شکارچیان آسیب‌پذیری، **بیش از ۵۰ میلیون تومان** درآمد داشته‌اند.

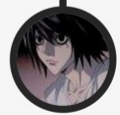
بالاترین درآمد

@moradlooo

۳۳۴ میلیون تومان

@hitman

۱۴۲ میلیون تومان



@mohammadrobot

۹۱ میلیون تومان

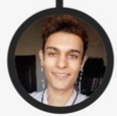
بالاترین بانتی پرداخت‌شده درازای یک گزارش

@hitman

۶۰ میلیون تومان

@moradloo

۴۰ میلیون تومان



@mhnikyar

۲۵ میلیون تومان

بیش از ۸۰٪ از شکـــارچیان راورو کمتر از ۱۰ سال سابقه‌ی کار دارند.

بیش از ۹۰٪ از آن‌ها هم‌زمان مشغول به باگ‌بانتی و تست‌نفوذ هستند.

برخی از کسب‌وکارهایی که در مسیر ارتقای امنیت، به ما اعتماد کردند:

علی جلال‌نژاد

مدیر تضمین امنیت ایرانسل

هرچه‌قدر هم که شرکت ما شرکت بزرگی باشد، امکان ندارد که ما بتوانیم جامعه‌ی خیلی بزرگی از متخصصان امنیت و شکارچیان آسیب‌پذیری، که ذهنیت کنجکاوی دارند، را استخدام کنیم و از نگاهشان بهره بگیریم. هر قدر هم تیم امنیت بزرگی داشته باشیم، بالاخره **افرادی هستند که دیدگاه، خلاقیت و سناریوهای متفاوتی در ذهن دارند که ما به آن‌ها دسترسی نداریم.** به همین ترتیب ما تمایل داریم در سطح کشور و یا فراتر، اگر کسی آسیب‌پذیری‌ای پیدا می کند، بتواند به ما گزارش کند و ما هم در قبالش پاداشی که عنوان شده را پرداخت کنیم.

پرداختی میدان‌ها در باگ‌بانتی

میانگین پرداختی هر میدان:

۴۷ میلیون تومان

۱۵%	کم‌تر از ۱۰ میلیون
۳۰%	۱۰ تا ۲۵ میلیون
۲۰%	۲۵ تا ۵۰ میلیون
۲۰%	۵۰ تا ۱۰۰ میلیون
۱۵%	بیش از ۱۰۰ میلیون

نوید میرحسینی

Namava–Senior DevOps Engineer

در نماوا تیم‌ها در قالب برنامه‌نویسی، دواپس و امنیت مشغول به فعالیت هستند. در عین حال **بدیهی است که به علت حجم کار و میزان تغییرات، مواردی از دیده پنهان شود.** در این‌جاست که حضور تیم‌های امنیتی مانند شکارچیان آسیب پذیری در پلتفرم باگ‌بانتی معنی خاص خود را پیدا می‌کند. ما چندین سال پیش از طریق یکی از همکاران با راورو آشنا شدیم و متوجه شدیم که تعدادی شکارچی در آن حضور دارند که وبسایت‌ها را چک می کنند و باگ‌ها را گزارش می‌دهند. این فرصت را برای ارتقای امنیتمان محترم شمردیم.

گزارش‌های ثبت‌شده برروی میدان‌ها

۶۴% از گزارش‌های ثبت‌شده، **تایید** شده‌اند.

۳۶% از گزارش‌های ثبت‌شده، **رد** شده‌اند.

میانگین تعداد گزارش‌های ثبت‌شده برروی هر میدان: **۳۹**

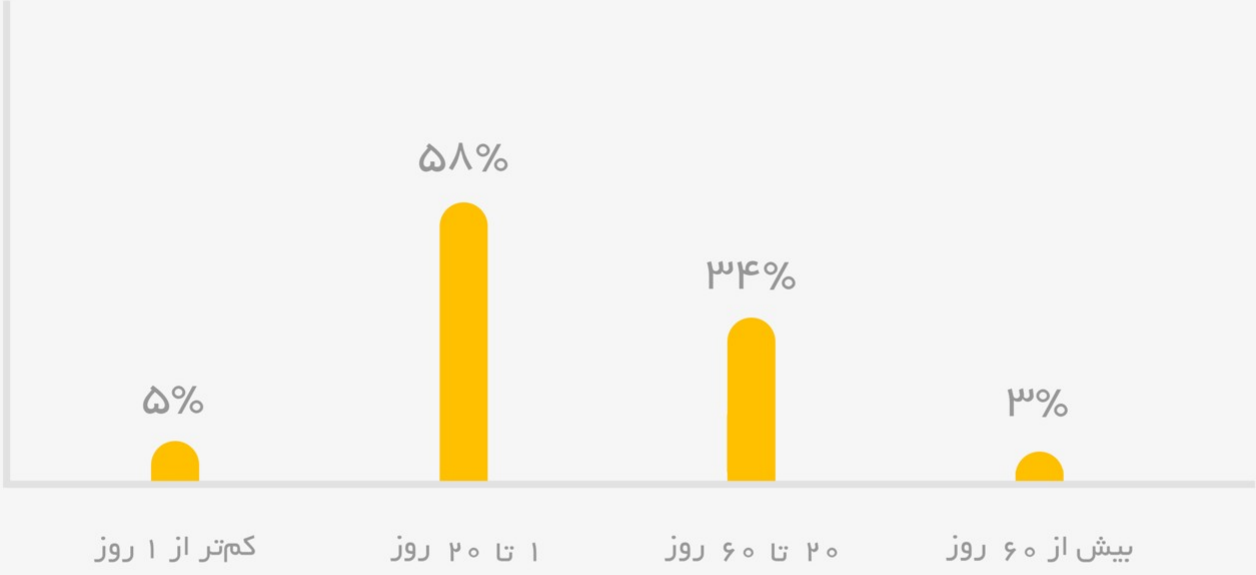
واهاگ گراگوسیان

Flightio Devops Engineer

ما در فلایتیو از باگ بانتی استفاده می‌کنیم، حتی با وجود این‌که گاهی اوقات برایمان گران‌تر هم تمام می‌شود. **به این دلیل از باگ‌بانتی استفاده می‌کنیم که اپلیکیشن از نگاه افراد متفاوتی چک شود و باگ‌هایمان زودتر در بیایند و کشف شوند.** هم‌چنین در طی این فرآیند، در کنار باگ‌های امنیتی، متوجه باگ‌هایی که در فرآیند بیزینسمان دارد اتفاق می‌افتد، هم می‌شویم. این‌طور می توانم تکمیل کنم که از نظر مقداری، حدود ۹۵٪ باگ‌های امنیتی به میان می‌آیند و ۵٪ باگ‌ها بیزینسی هستند.

www.Ravro.ir

مدت زمان ثبت گزارش توسط شکارچی تا پرداخت بانتی توسط میدان

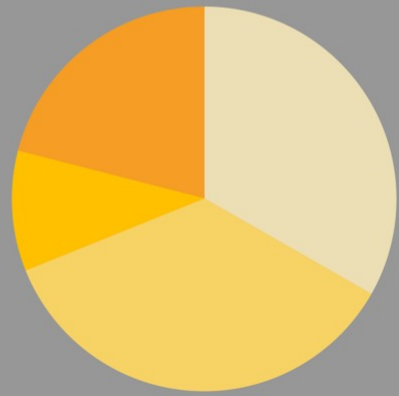


۳٪ از گزارش‌ها زمانی غیرمتعارف و چندماهه برای تعیین‌تکلیف داشته‌اند.

مجموع درآمد شکارچیان آسیب‌پذیری

یک‌سوم از شکارچیان آسیب‌پذیری **بیش از ۱۰ میلیون تومان** درآمد داشته‌اند.

از بین آن‌ها:



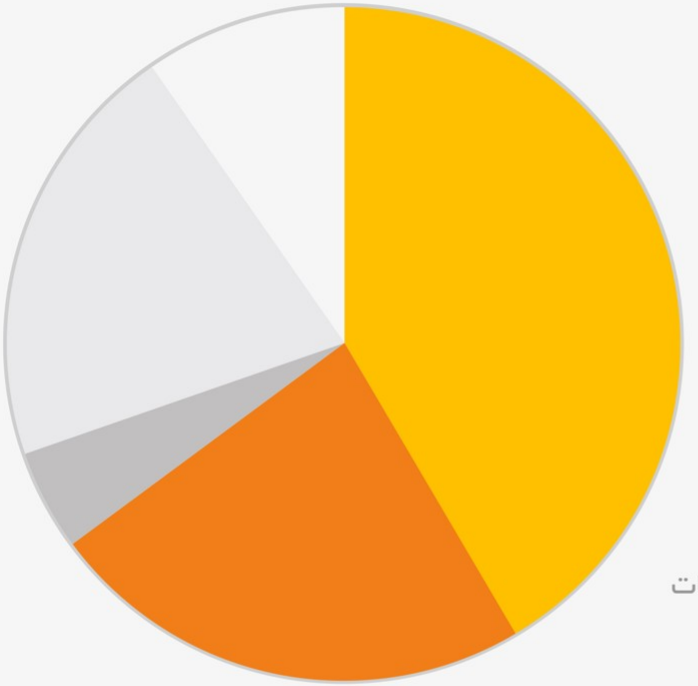
۱۰ تا ۲۰ میلیون	۳۴%
۲۰ تا ۴۰ میلیون	۳۴%
۴۰ تا ۶۰ میلیون	۹ %
بیش‌از ۶۰ میلیون	۲۳%

مهدی مرادلو

شکارچی آسیب‌پذیری

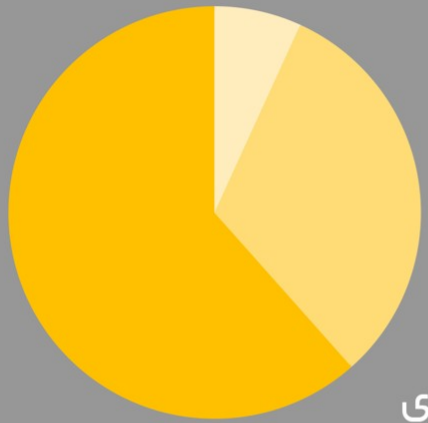
به نظرم **باگ‌بانتی می‌تواند یک شغل تمام‌وقت برای شکارچی باشد.** قطعا به میزان تخصص شکارچی هم بستگی دارد. کسانی که باگ‌بانتی کار می‌کنند، چه در پلتفرم‌های باگ بانتی و چه در خارج از آن‌ها، درآمد خوبی دارند. علاوه‌بر برنامه‌های باگ‌بانتی داخل پلتفرم‌ها، خیلی کسب‌وکارها هم باگ‌بانتی را در زیرساخت خود راه‌اندازی کرده‌اند. حتی بعضی کسب‌وکارها که برنامه‌ی باگ بانتی ندارند هم، وقتی گزارش را بهشان می‌دهی، قبول می‌کنند. **شرایط دریافت گزارش آسیب‌پذیری و نگاه به باگ بانتی در سمت کسب‌وکارها، نسبت به قبل درحال بهبود است و از گزارش‌های آسیب پذیری بیش‌تر استقبال می‌شود.**

سرنوشت گزارش‌های دریافتی



۴۲%	گزارش تاییدشده
۲۲%	گزارش تکراری
۴%	گزارش ردشده – به‌علت نقص اطلاعات
۲۲%	گزارش ردشده – توسط تیم داوری
۱۰%	گزارش ردشده – در مرحله‌ی ارزیابی نهایی

کیفیت گزارش‌های دریافتی



- ۷% گزارش با کیفیت پایین؛ امتیاز کمتر از ۱۰
- ۲۲% گزارش با کیفیت متوسط؛ امتیاز بین ۱۰ تا ۱۵
- ۶۱% گزارش با کیفیت بالا؛ امتیاز بین ۱۵ تا ۲۰

بخش‌های تشکیل‌دهنده‌ی امتیاز گزارش‌آسیب‌پذیری

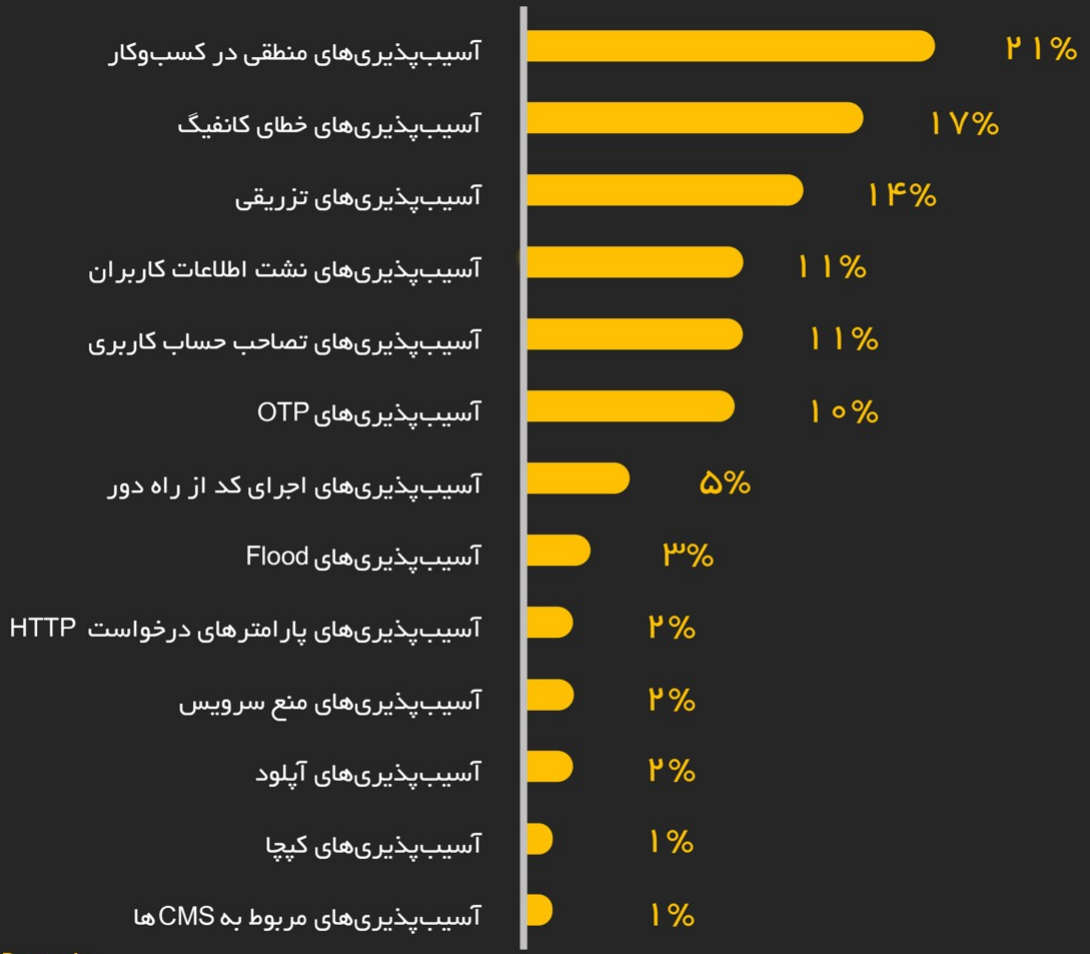
در ۹۰%+ از گزارش‌ها، عنوان، IP و Domain موردتایید است.

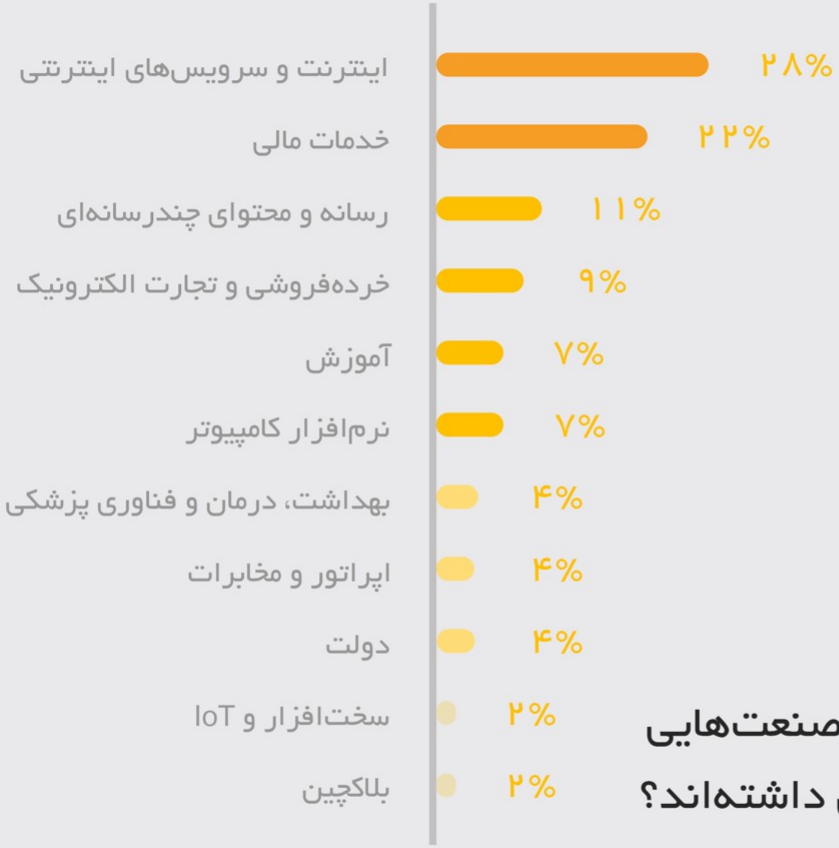
در ۹۰%+ از گزارش‌ها، شدت حساسیت و دسته‌بندی عنوان‌شده با نظر داوری مطابقت دارد.

در ۸۰%+ از گزارش‌ها، به‌ازای ارسال فیلم، سناریو توضیحی ارسال شده‌است.

در ۵۰%+ از گزارش‌ها، راه‌حل با دقت بالا ارائه شده است.

فراوانی آسیب‌پذیری‌ها در گزارش‌های تاییدشده





کسب‌وکارهای مربوط به چه صنعت‌هایی حضور پررنگ‌تری در باگ‌بانتی داشته‌اند؟

پیگیری بررسی گزارش توسط میدان

درخواست دعوت به هدف دعوتنامه‌ای یا خصوصی

اعتراض به مبلغ بانتی

پیگیری پرداخت بانتی

درخواست تایید احراز هویت

مشکل در ثبت گزارش

مشکلات تکرارشونده در گزارش‌های آسیب‌پذیری ارسالی

از دیدگاه تیم داوری راورو

- کیفیت گزارش‌ها
- نقص در فرآیند توضیح آسیب‌پذیری
- نقص اطلاعات موردنیاز
- عدم ارسال ویدئو
- ضعف در توضیح شدت آسیب‌پذیری
- نقص در ارائه‌ی زمان، تاریخ و آدرس IP در زمان ثبت مستندات

چالش‌های تکرارشونده در سمت میدان‌ها

از دیدگاه تیم داوری راورو

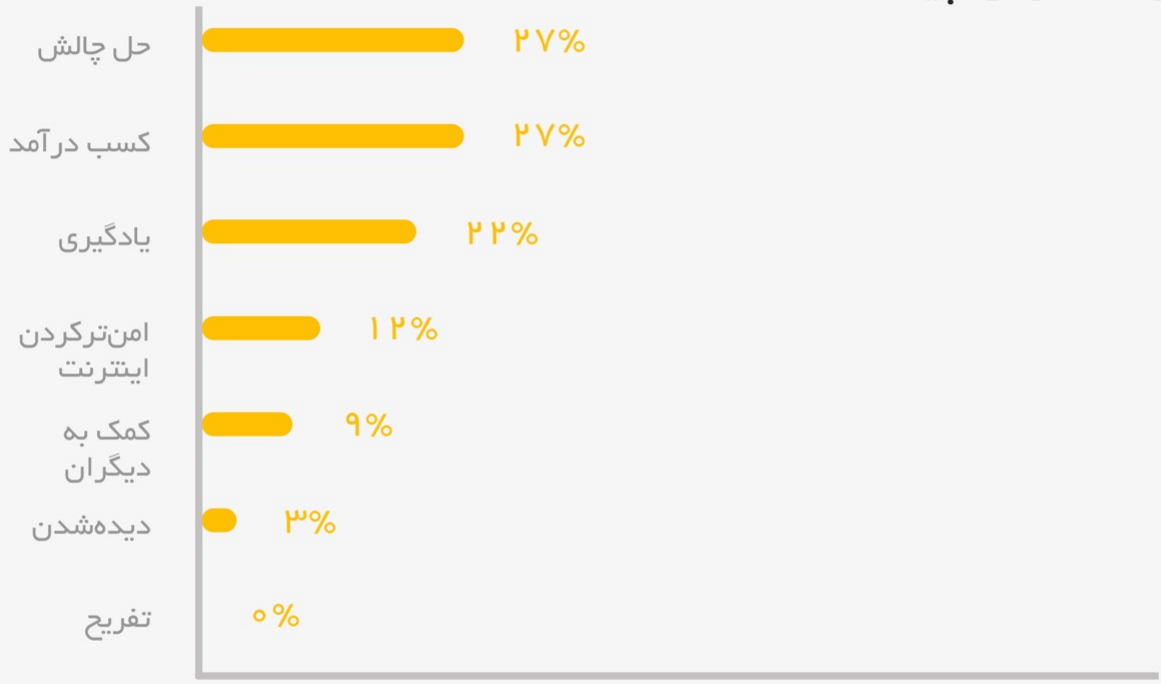
- عدم آشنایی رابط میدان با آسیب‌پذیری‌ها
- عدم ثبت گزارش‌های آسیب‌پذیری قبلی
- عدم وضوح قوانین ثبت‌شده
- تعیین بانتی غیرمتناسب با ابعاد کسب‌وکار
- عدم آشنایی میدان با تاثیر آسیب‌پذیری‌ها
- عدم رفع آسیب‌پذیری‌ها
- عدم تسلط تیم توسعه‌ی محصول به علت تغییر اعضا
- نقص در فرآیند داخلی در جهت تایید و پرداخت

در قالب یک **پرسش‌نامه**

اطلاعاتی از جامعه‌ی شکارچیان آسیب‌پذیری راورو به دست آوردیم.

برخی نتایج آن را در قالب تعدادی آمار و نمودار با شما به اشتراک می‌گذاریم.

انگیزه‌ات از هک‌کردن چیست؟



محمدرضا تیموری

شکارچی آسیب‌پذیری

از نظر من، **هک یک هنر است؛ هنرِ دیدن و پیداکردنِ چیزهایی که از چشم بقیه دور می‌ماند و دیگران نمی‌توانند آن‌ها را ببینند.** نقاشی هم همین است، نقاش نقاشی‌ای می‌کشد که بقیه از آن دید به آن کس یا منظره نگاه نکرده‌اند. فرآیند باگ پیداکردن هم همین است. این‌که از یک منظری به اپلیکیشن نگاه کنی که باعث شود آسیب‌پذیری پیدا شود...

چطور به هک‌کردن علاقه‌مند شدی؟

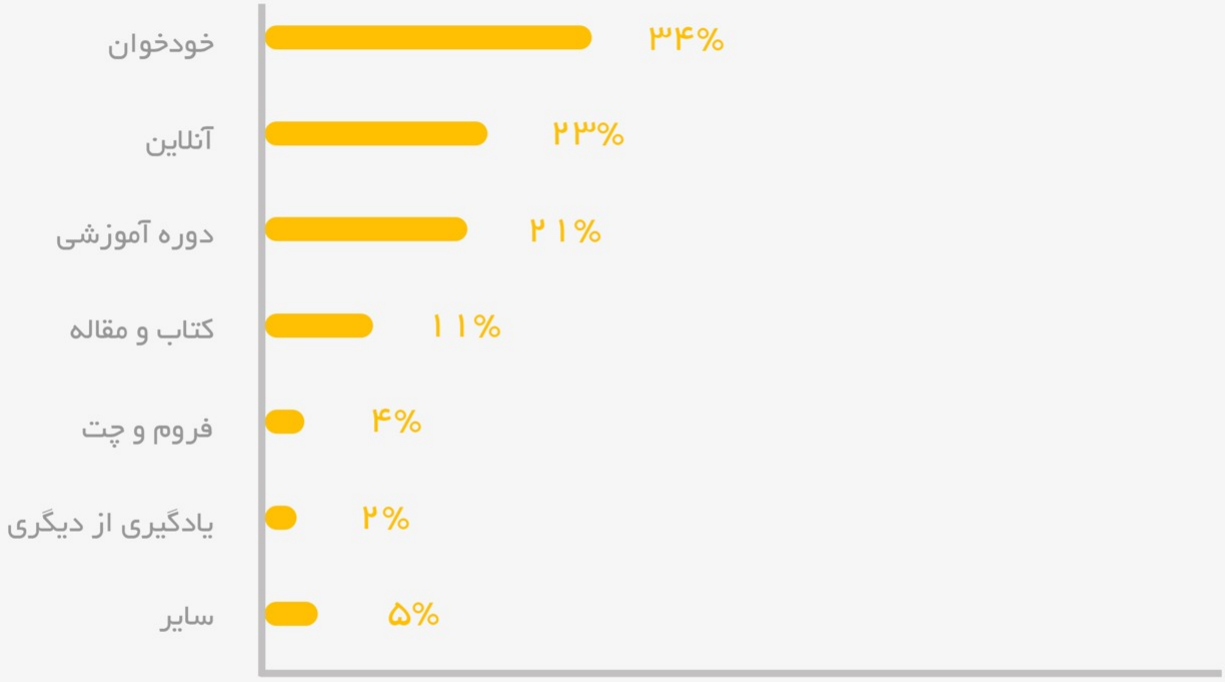
۲۳%
۱۴%
۹%
۷%
۶%
۵%

علی امینی

محقق و شکارچی آسیب‌پذیری باینری

یادم است من که در اتاقم پای کامپیوتر نشسته بودم و بازی می کردم، پدرم در خانه اخبارهایی گوش می‌داد. **یکهو مثلا مجری می گفت: " هکرها حمله کردند به فلان جا و پانصدهزار اکانت را زده اند.**" من می‌دویدم پای تلویزیون، ذوق می‌کردم و با خودم می گفتم: "چه باحال!" بعد می‌رفتم پیش آقا روح‌الله و می‌پرسیدم: " چه‌جوری ویروس می‌سازند؟" بعد او می‌گفت:" **باید برنامه‌نویسی بلد باشی**؛ برنامه‌نویسی زبان C." من آن‌قدری از برنامه‌نویسی نمی‌دانستم که وقتی روح‌الله این را می‌گفت، من فکر می‌کردم ربطی به پارتیشن c که در آن ویندوز نصب می‌کنند، دارد.

چطور هک‌کردن را یاد گرفتی؟



محمد درخشان

شکارچی آسیب‌پذیری

حدود یک سالی با برنامه‌نویسی آشنایی پیدا کردم و بعد از یک سال وارد باگ‌بانتی شدم. بیش‌تر زبان‌های برنامه‌نویسی پایتون و جاوااسکریپت را بلدم. **همه را خودخوان و رایگان یاد گرفتم و کلاسی شرکت نکردم.** زبان انگلیسی را خوب بلد بودم چون برای کنکور می خواندم و این کمکم می‌کرد.

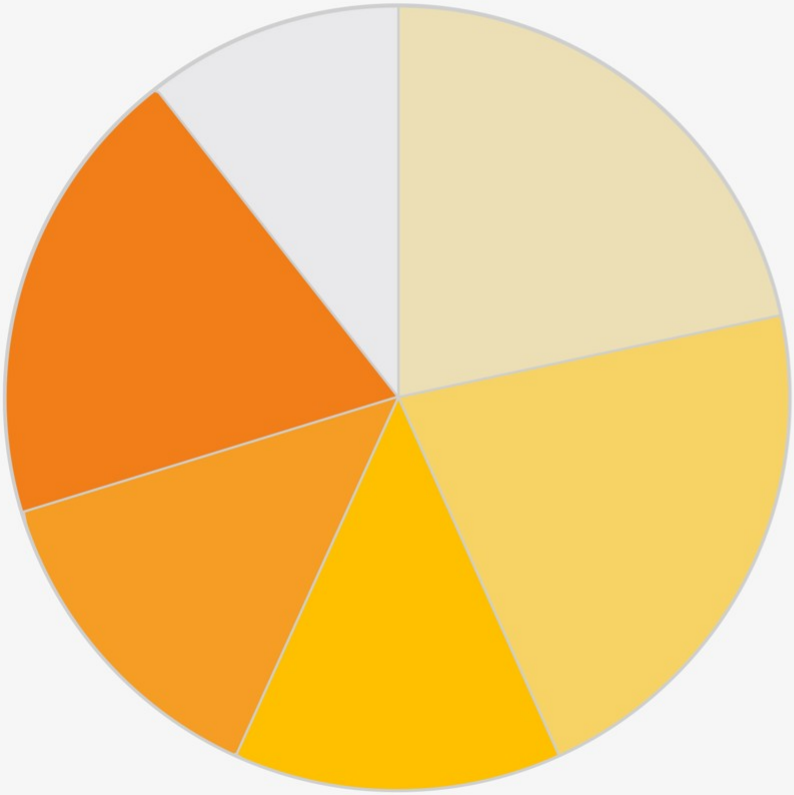
وضعیت شغلی‌ات را در کدام دسته می‌بینی؟

برنا نعمت‌زاده

شکارچی آسیب‌پذیری

درنظرگرفتن باگ‌بانتی به‌عنوان یک شغل تمام‌وقت، یک سری چالش‌ها و مزیت‌ها دارد. یکی از مزیت‌هایش این است که **در باگ بانتی محدودیتی در انتخاب تارگت نداریم**؛ برعکس پن‌تست می‌توانیم هر تارگتی را خودمان انتخاب کنیم. مزیت دیگرش این است که چون یک کار فریلنس است، **محدودیت زمانی برای انجامش نداریم و هر موقعی که بخواهیم می‌توانیم این کار را انجام دهیم.** یکی از چالش‌هایش هم این است که **ممکن است من مدتی وقت بگذارم و نتوانم آسیب پذیری‌ای را پیدا و ثبت کنم.** ممکن هم هست چندروز وقت بگذارم و چند آسیب پذیری خوب را گزارش بدهم. اما احتمال تکراری محسوب‌شدن گزارش ارسالی هم هست.

چند ساعت در هفته، برای هک زمان می‌گذاری؟



۲۳%	کم‌تر از ۱۰ ساعت
۲۳%	۱۰ تا ۲۰ ساعت
۱۱%	۲۰ تا ۳۰ ساعت
۱۱%	۳۰ تا ۴۰ ساعت
۲۰%	بیش‌از ۴۰ ساعت
۱۲%	تمایلی به اعلام ندارم.

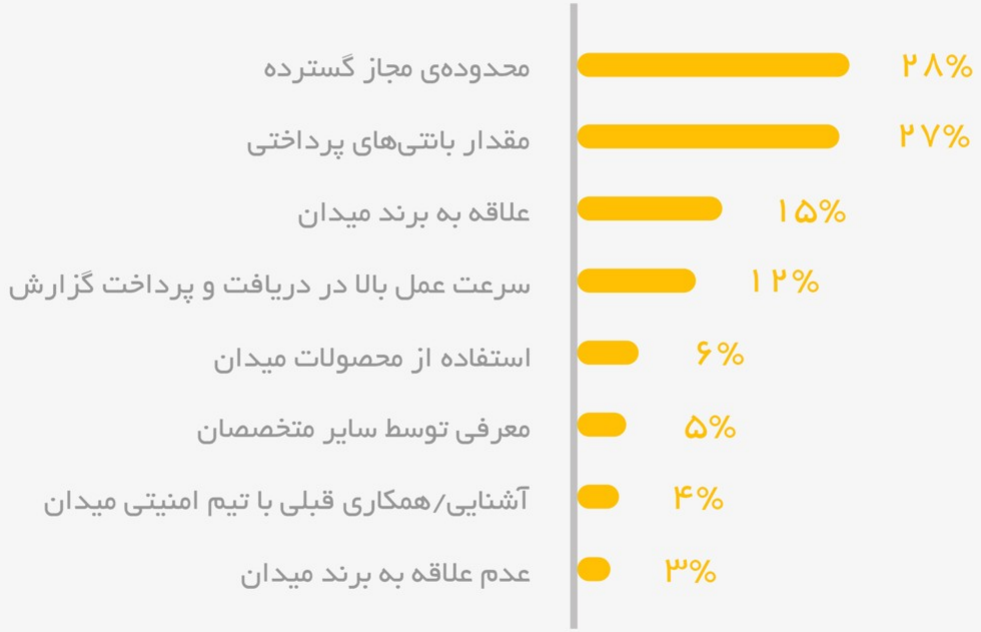
آرمان محمدتاش

شکارچی آسیب‌پذیری

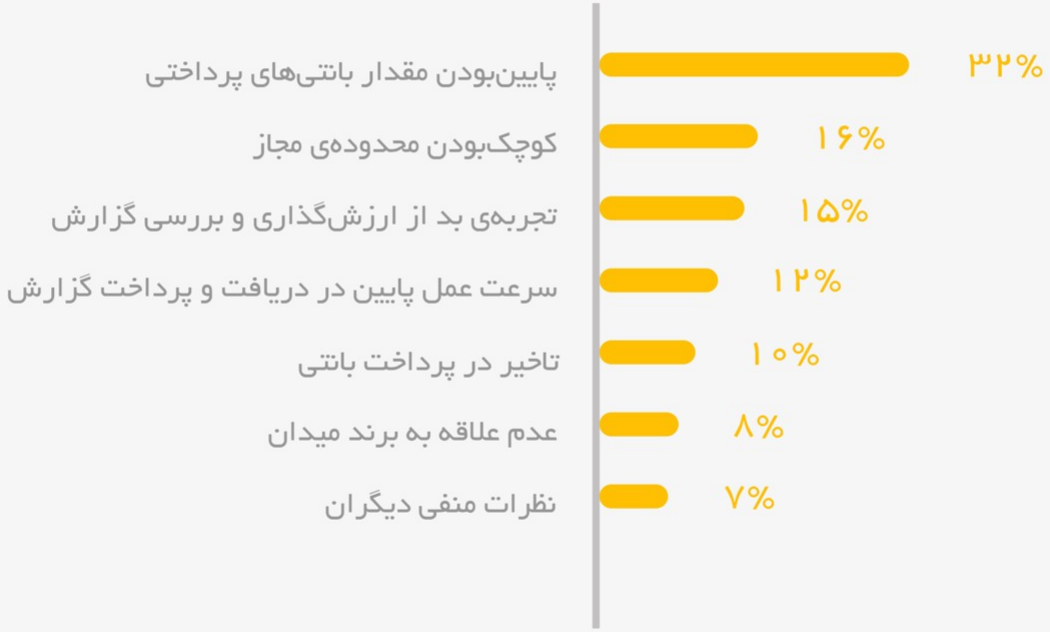
بیش‌ترین تایمی که در ۲۴ ساعت به‌صورت پیوسته برای شکار آسیب‌پذیری گذاشته‌ام، ۱۲ ساعت بوده است.

نمی‌دانم این بازی را بازی کرده‌اید یا نه؛! Prince of Persia من وقتی نصبش کرده بودم، به قدری بازی کردم که وقتی دستم را روی پد موس می گذاشتم، رگم می‌گرفت! خیلی زیاد بازی کرده بودم؛ فکر کنم ۹ ساعت شده بود. بعدش با خودم گفتم: "می‌توانم همچین کاری را برای امنیت انجام دهم؟ می‌توانم ۹ ، ۱۰ ساعت کار امنیت انجام دهم؟" توانستم ؛ موفق شدم و هدفم زدن این تارگت خودم بود. توانستم ۱۲ ساعت پیوسته کار کنم و رکورد بازی را بزنم.

چه مواردی در **انتخاب** یک میدان به‌عنوان **هدف** برای **هک‌کردن** اثر می‌گذارد؟



چه مواردی در **انتخاب‌نکردن** یک میدان به‌عنوان **هدف** برای **هک‌کردن** اثر می‌گذارد؟

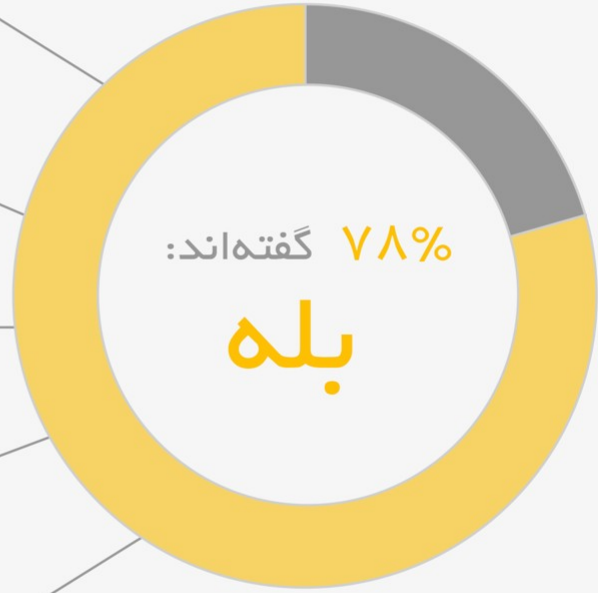


سیدرضا فاطمی

شکارچی آسیب‌پذیری

یک بار یکی از دوستانم اپلیکیشنی آورد و گفت برای یک شرکت استارتاپی ست که گفته‌اند اگر کسی بتواند یک باگ امنیتی واقعی کشف کند، ما حاضریم بانتی هم بدهیم. من تصور خودم را از میزان بانتی داشتم. اتفاقا خیلی سریع یک باگ RCE پیدا کردم. به دوستم گفتم:" مطمئنی بانتی می‌دهند؟" گفت:" آره ، این هم راه ارتباطی‌شان است." من هم ارتباط گرفتم و پرسیدم:" درست است که شما گفته‌اید امن هستید و اگر کسی باگی پیدا کند، بانتی می‌دهید؟" گفتند:" بله، همین طور است." بعد پرسیدم:" جسارتا مبلغ بانتی شما چه‌قدر هست؟" جواب دادند:" بلیط سفر به قم."! پرسیدم:" معادلش را نقدا هم پرداخت می‌کنید؟" گفتند:" بله، **۱۴ هزار تومان**."!

آیا تابه‌حال باگی پیدا کرده‌ای، که گزارش نکنی؟



۲۷%
چون در پلتفرم باگ‌بانتی عضو نبوده‌اند.

۱۴%
چون می‌ترسیدم برایم تبعات قانونی داشته باشد.

۱۳%
چون با تیم فنی‌شان راه ارتباطی پیدا نکردم.

۷%
چون درمورد قیمت به نتیجه نرسیدیم.

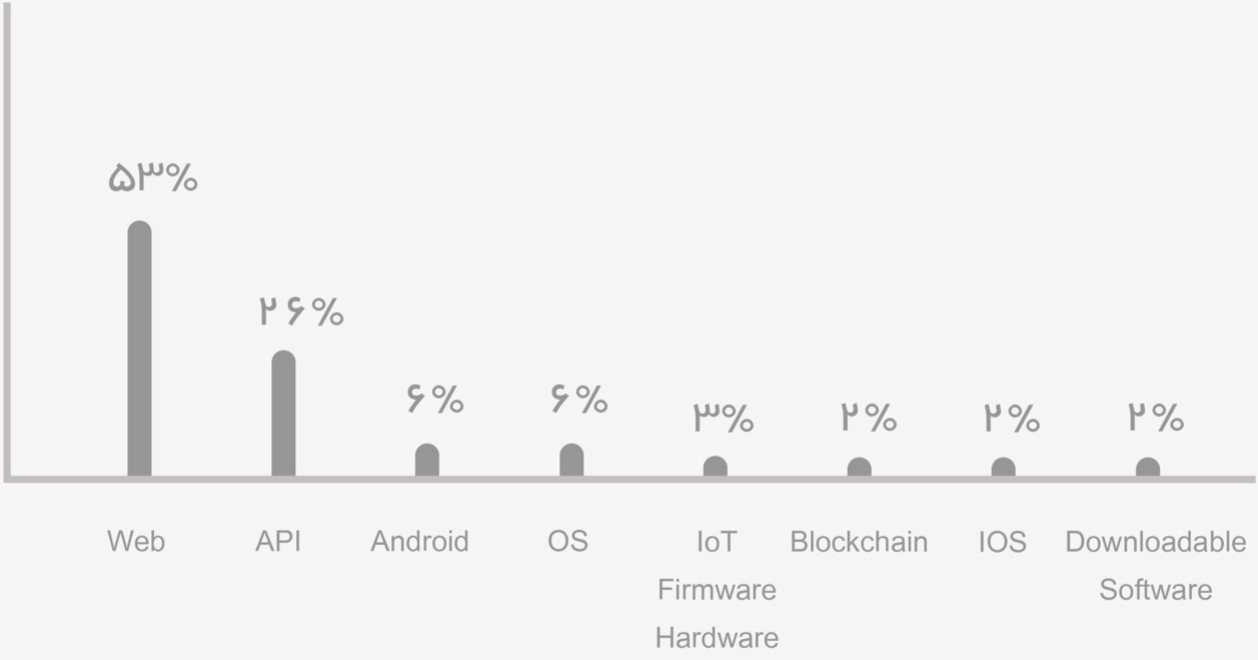
۱۸%
به دلایل دیگر.

علیرضا رضایی

شکارچی آسیب‌پذیری

اکثر بچه‌های حوزه‌ی امنیت، وقتی آسیب‌پذیری‌ای کشف می کنند، **باتوجه به سابقه‌ی رفتاری آن کسب‌وکار عمل می‌کنند.** مثلا شما فرض کنید؛ ۱۰ آسیب‌پذیری را از جایی پیدا کرده‌ایم و به طرف گفته‌ایم و طرف اصلا برایش اهمیتی نداشته است! یا باید دیگر سراغشان نرویم! یا می‌توانیم دیتایشان را بالاخره برداریم! یک کاریش می‌کنیم دیگر! **بستگی به طرف مقابل دارد.** ولی خوب کارهای بد نمی‌کنیم. کارهای بد را برای آدم‌های بد می گذاریم. واقعیت این است که من به‌عنوان یک شکارچی آسیب پذیری، وقت و انرژی برای آن آسیب پذیری صرف می‌کنم. و ترجیح می‌دهم که این قضیه برای من یک عاید یا نتیجه‌ای برای من داشته باشد. پس چه بهتر که بانتی بشود.

بستر موردعلاقه‌ات برای هک کدام است؟



پرکاربردترین ابزار مورداستفاده‌ات در شکار چیست؟

Burp Suite

خودم ابزار می‌نویسم.

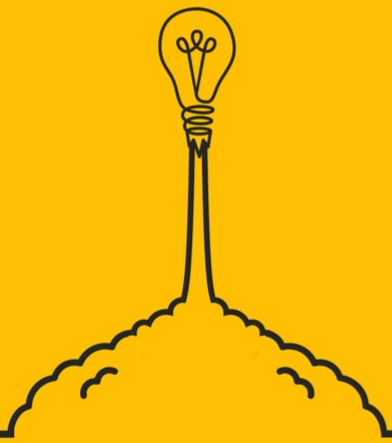
fuzzer

Metasploit

Debugger

پیشنهادهای شکارچیان برای راورو

خبری در راه است...



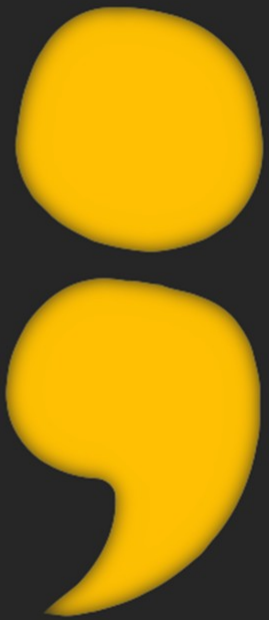
کاژه؛ تست‌نفوذ پلتفرمی مبتنی بر خرد جمعی

کاژه به معنای "پناهگاه امن" است.

www.Ravro.ir

support@Ravro.ir

@Ravro_ir



روز و روزگارتون امن ؛)