نگاهی گذرا به

# گزارش‌های آسیب‌پذیری در پلتفرم باگ‌بانتی راورو

۱۴۰۳

# 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.

قصه‌ی دیگری از امنیت سایبری برایتان داریم؛

# قصه‌ی گزارش‌های آسیب‌پذیری

# قصه‌ی گزارش‌هایی سرنوشت‌ساز

گزارش آسیب‌پذیری‌هایی که توسط شکارچیان آسیب‌پذیری و هکرهای کلاه‌سفید کشف شدند. برای کسب‌وکارها ارسال شدند، تا قبل از نفوذگران و سوءاستفاده‌گران، ازآن‌ها آگاه شوند. تا از بسیاری از هک‌ها و حمله‌ها جلوگیری شود.

گزارش‌هایی که برخلاف گذشته‌های نه‌چندان دور، دیگر سند جرم و اخاذی انگاشته نمی‌شدند.

گزارش‌هایی که پیامی از جنس صلح‌طلبی و خیرخواهی داشتند و با هر یک از آن‌ها، جهان مجازی قدمی به امن‌ترشدن نزدیک‌تر می‌شد.

این گزارش تقدیم می شود به:

فرستندگان گزارش‌های آسیب‌پذیری؛ **متخصصان امنیت سایبری**

گیرندگان گزارش‌های آسیب‌پذیری؛ **کسب‌وکارهای امنیت‌اندیش**

مروجان فرهنگ ارسال گزارش آسیب‌پذیری؛ **فعالان حوزه‌ی امنیت سایبری**

دست‌اندرکاران اداره‌ی تعیین تکلیف گزارش‌های آسیب‌پذیری؛ **تیم اجرایی پلتفرم راورو**

با حضور فعال ۴۰۰ شکارچی آسیب‌پذیری و ۶۰ میدان

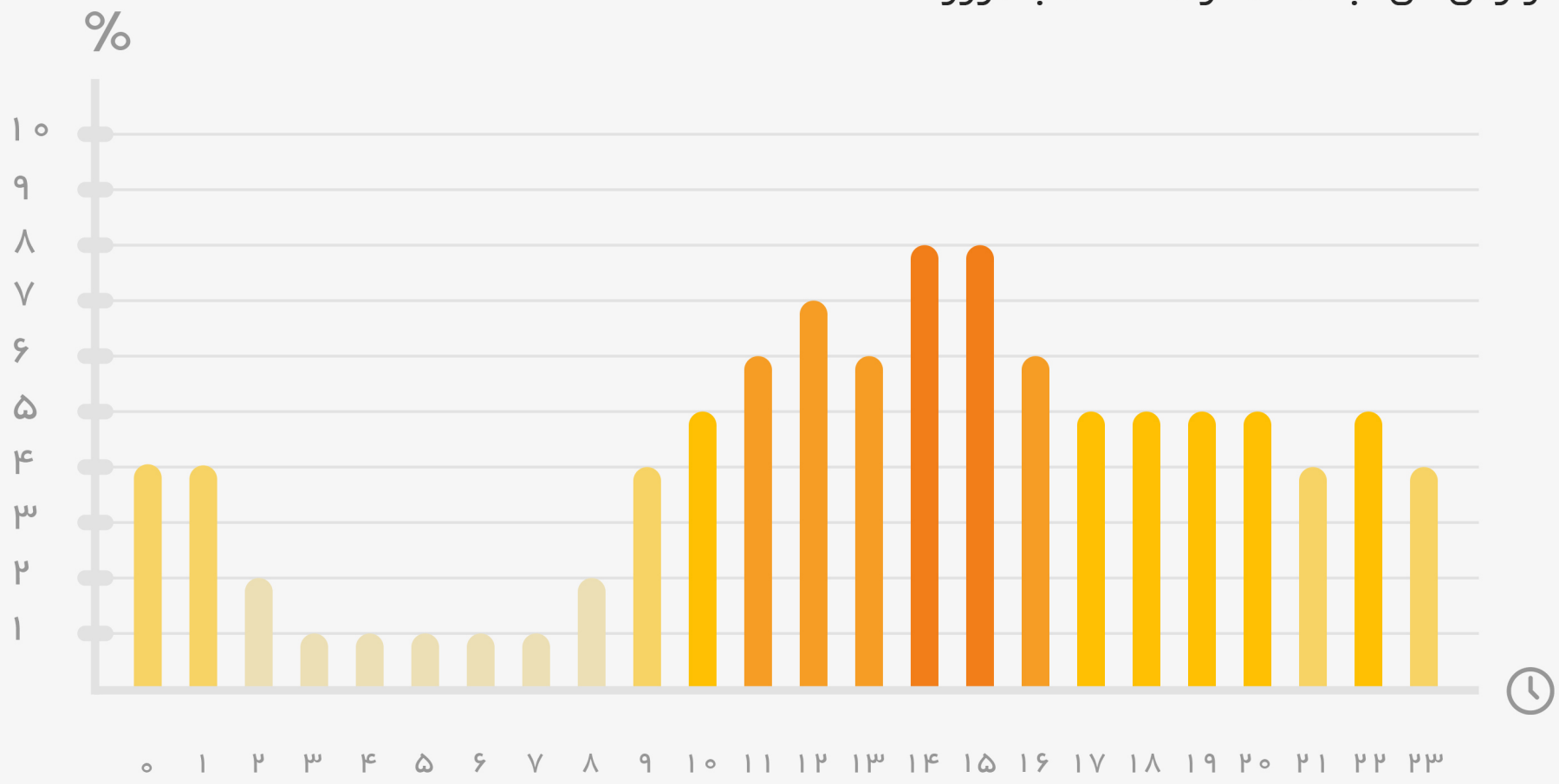
 ۴۰۰۰ گزارش آسیب‌پذیری ثبت شده‌اند.

$ ۴+ میلیارد تومان بانتی پرداخت شده‌است.

# شکارچی‌ها شب‌ها می‌خوابند!

گزارش‌های ثبت‌شده در ساعات شبانه‌روز

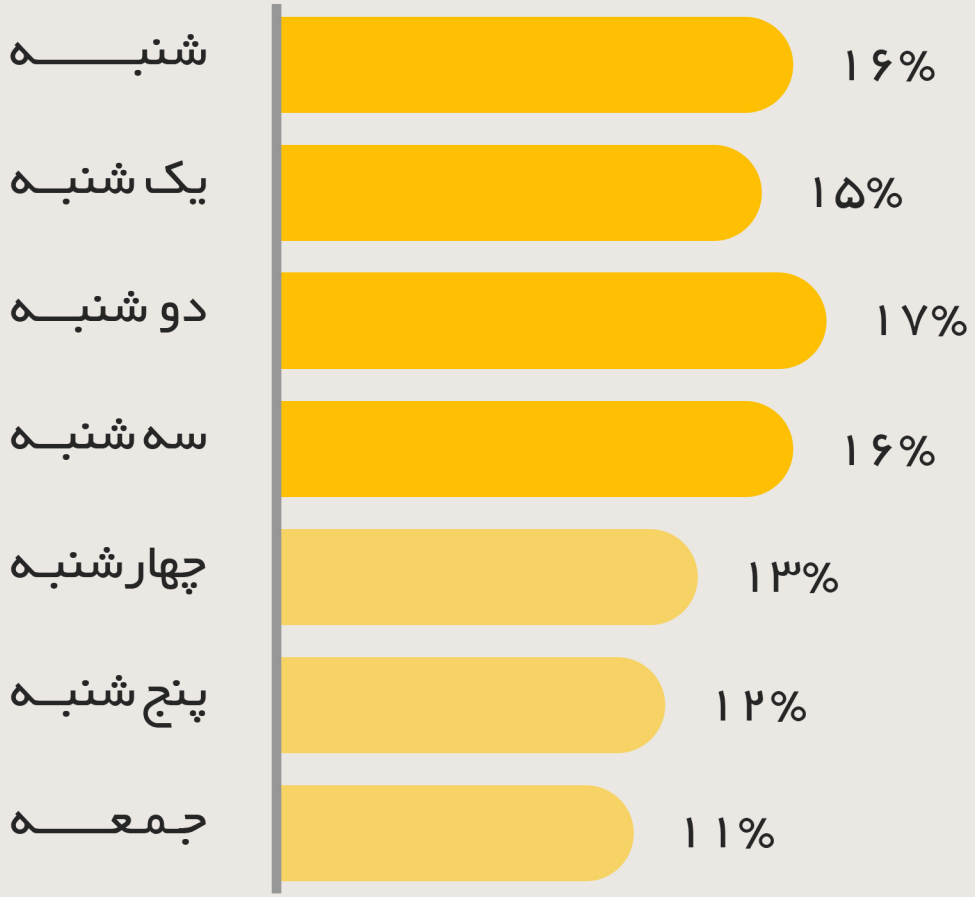
۱۴۰۳



# آخر هفته‌ها هم استراحت می‌کنند...

گزارش‌های ثبت‌شده در روزهای هفته

۱۴۰۳




پرگزارش‌ترین روز :

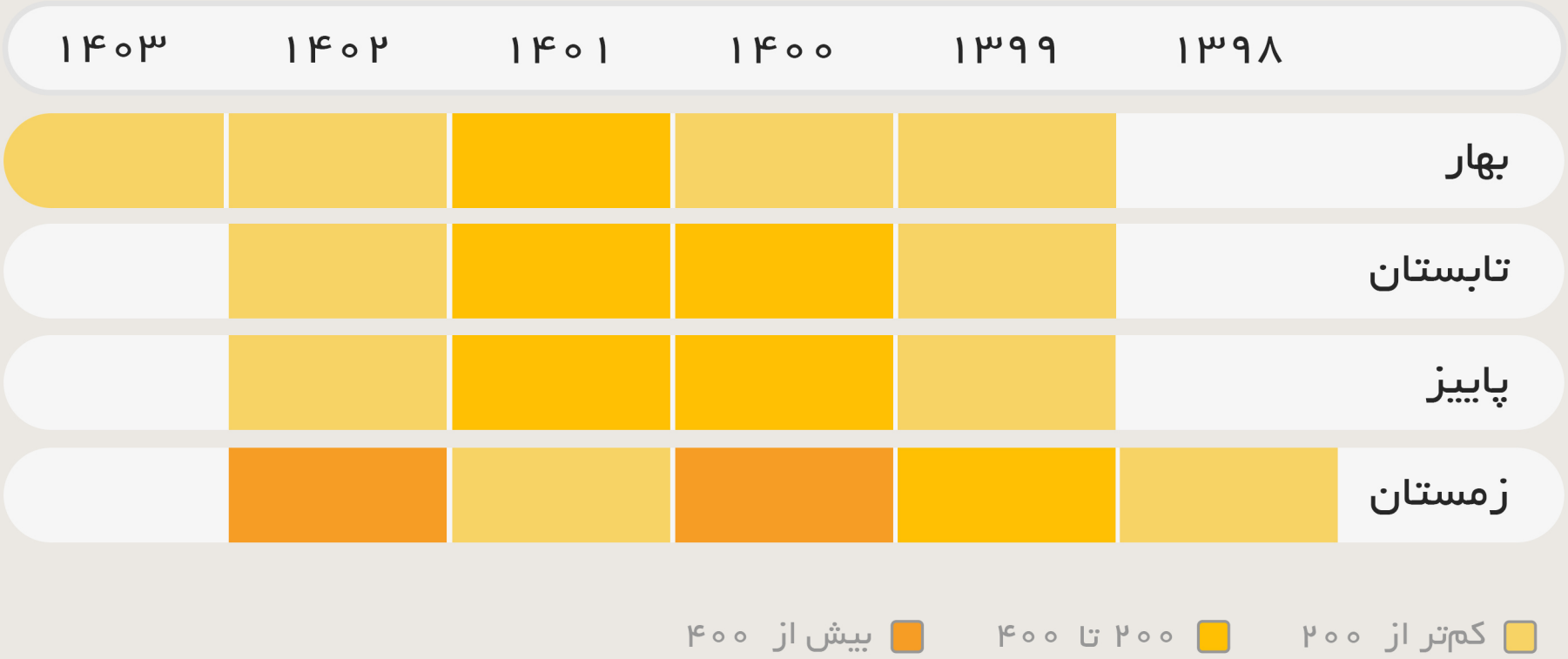
۱۴۰۳/۰۲/۰۳

با ۶۷ گزارش

۱۴۰۳

## اما زمستان فصل کار است...

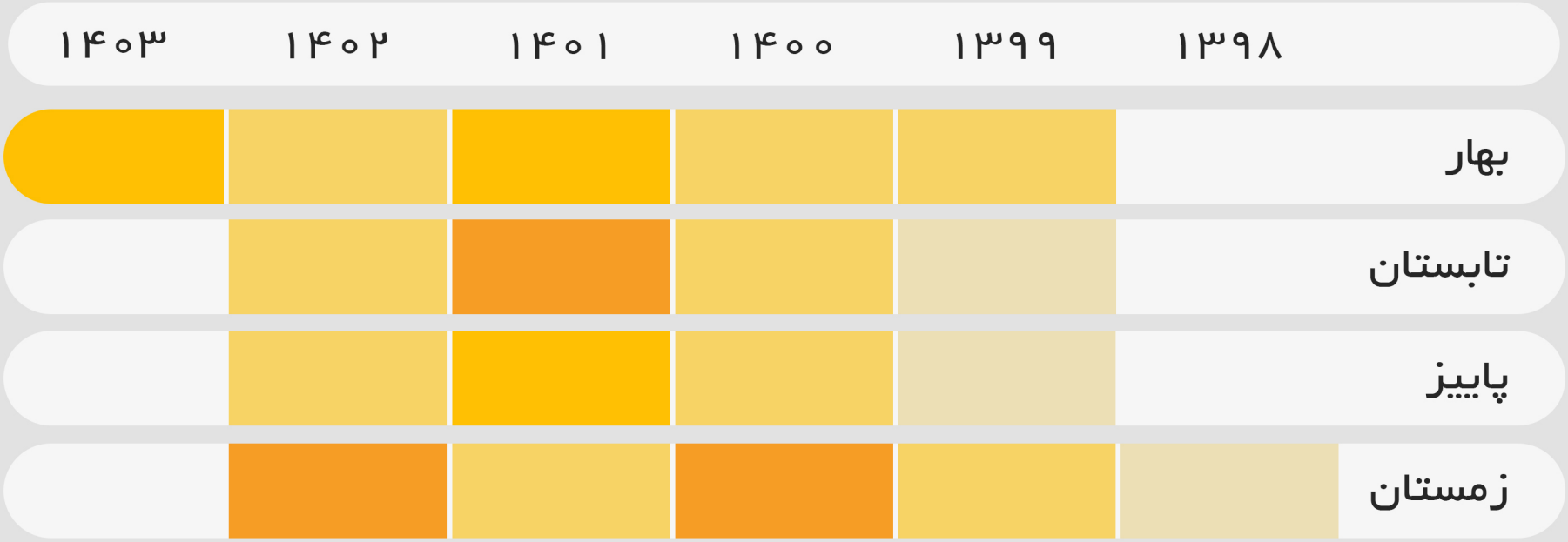
تعداد گزارش ثبت‌شده طی فصل‌ها



# زمستان فصل درآمد هم هست...

۱۴۰۳

مجموع بانتی پرداخت‌شده طی فصل‌ها

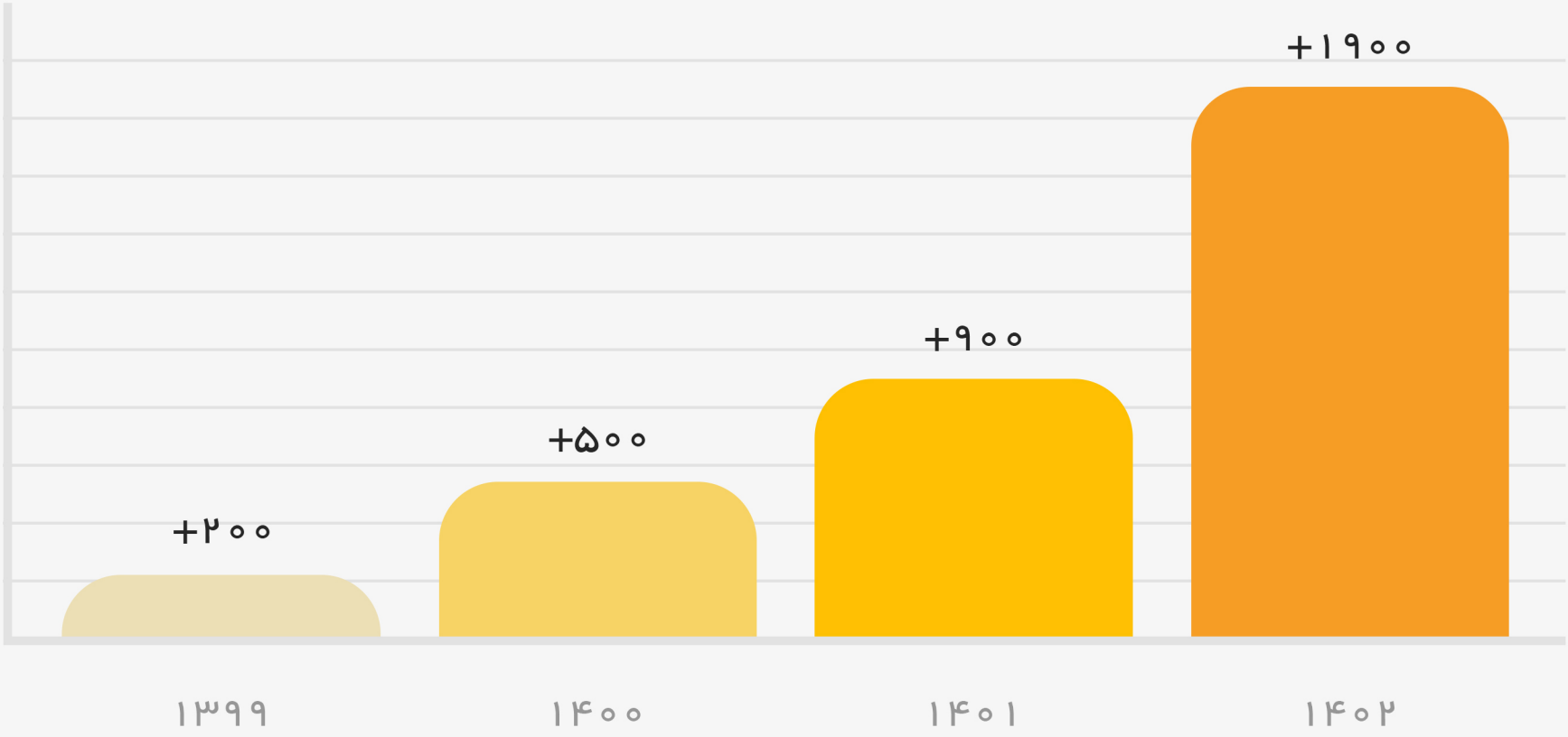



کم‌تر از ۵۰ میلیون تومان
۵۰ تا ۱۵۰ میلیون تومان
۱۵۰ تا ۳۰۰ میلیون تومان
بیش از ۳۰۰ میلیون تومان

# بانتی‌های پرداختی در مسیر رشد

۱۴۰۳

میلیون تومان



# اولین

## بانتی پرداختی بابت

## گزارش آسیب‌پذیری

۱۴۰۳

در تاریخ: ۱۳۹۹/۰۱/۱۰

عنوان گزارش: آسیب‌پذیری Bypass OTP Verification

شکارچی آسیب‌پذیری: @rima

میدان: کانکتیت

بانتی دریافتی: ۱/۵ میلیون تومان

# گران‌ترین

## گزارش آسیب‌پذیری

در تاریخ: ۱۴۰۱/۰۶/۱۹

عنوان گزارش: آسیب‌پذیری Mass Assignment

شکارچی آسیب‌پذیری: @hitman

میدان: راورو

بانتی دریافتی: ۶۰ میلیون تومان

# جای دولتی‌ها خالی

## تفکیک صنعت‌های حاضر

۱۴۰۳

| | |
|---|---|
| خرده‌فروشی و تجارت الکترونیک | ۳۱% |
| خدمات مالی | ۱۳% |
| رسانه و محتوای چندرسانه‌ای | ۱۳% |
| اینترنت و سرویس‌های اینترنتی | ۹% |
| بهداشت و سلامت | ۷% |
| اپراتور و مخابرات | ۷% |
| آموزش | ۷% |
| بلاکچین | ۷% |
| دولت | ۲% |
| نرم‌افزار کامپیوتری | ۲% |
| سخت‌افزار و IoT | ۲% |

رامین اسدیان
شکارچی آسیب‌پذیری

صنایع انرژی مانند نفت و گاز، فولاد، پتروشیمی، صنایع غذایی، سرمایه‌گذاری در بورس و کارگزاران، و همچنین صنعت بیمه، به دلیل ماهیت حساس و پیچیده‌ی فعالیت‌های خود، معمولاً تاکنون کمتر وارد حوزه باگ بانتی شده‌اند. این صنایع به طور عمده بر امنیت فیزیکی و عملیاتی تمرکز داشته‌اند و ممکن است اهمیت و ضرورت امنیت سایبری و شناسایی آسیب‌پذیری‌های نرم‌افزاری را کمتر درک کرده باشند. با این حال، با افزایش وابستگی به فناوری‌های دیجیتال و افزایش تهدیدات سایبری، این صنایع باید در آینده به طور فعال‌تری به حوزه باگ بانتی ورود کنند تا باگ‌ها و ضعف‌های احتمالی سیستم‌های خود را شناسایی و اصلاح کنند، و از آسیب‌های جدی‌تر جلوگیری کنند.

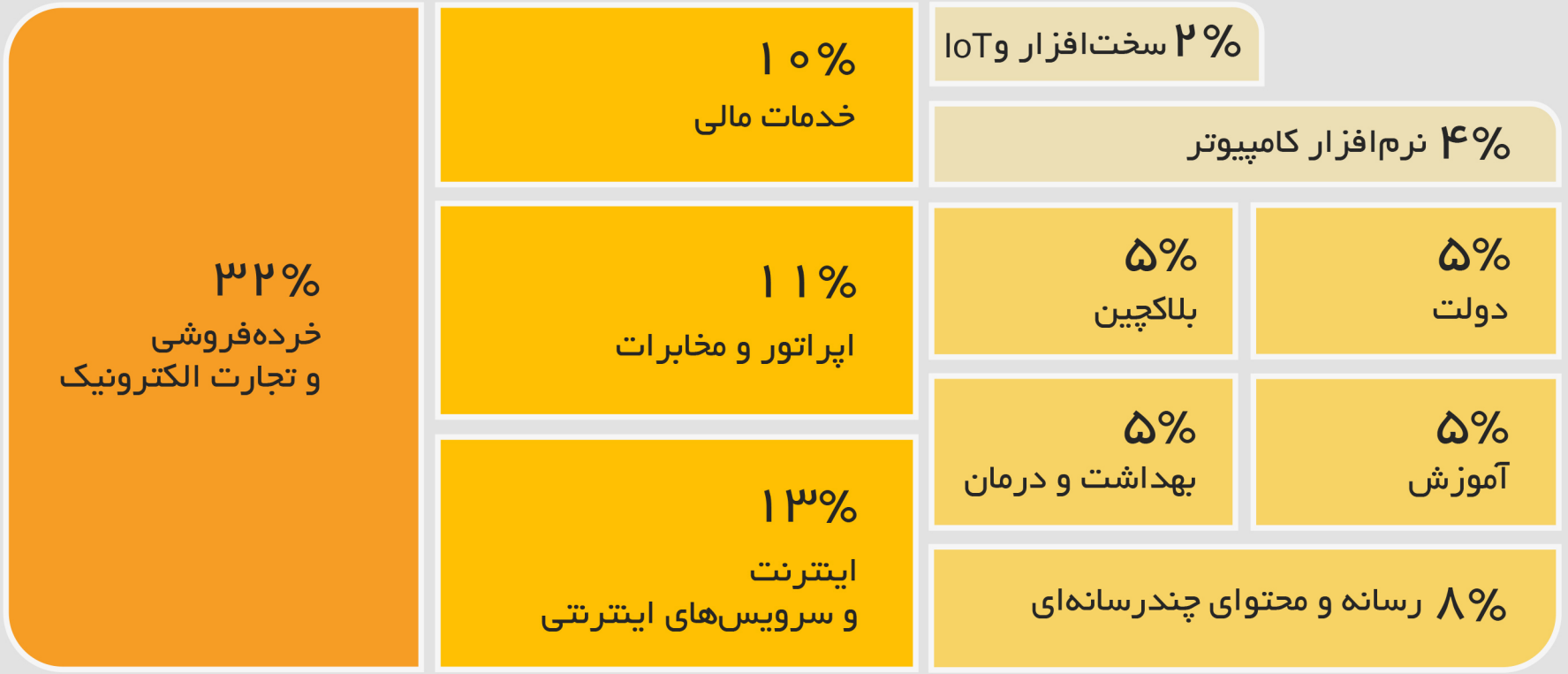
## زهرا ایزدی امیری

شکارچی آسیب‌پذیری

من در کسب‌وکارهایی که تابه‌حال در آن‌ها فعالیت کرده‌ام، شاهد تجربه‌های ناموفق زیادی در رابطه با امنیت سایبری بوده‌ام. به نظرم مهم‌ترین دلیل این ناکامی‌ها، خلأ و نبود استراتژی و مدیریت درست بود. همچنین توجه ناکافی مدیران شرکت‌ها به امنیت سایبری و استفاده‌نکردن مدیران امنیت از افراد توانا و متخصصی که اهلِ شوآف نیستند.

# توازنی که باید به‌هم بخورد...

گزارش‌های ثبت‌شده برای میدان‌های صنایع مختلف



هر آسیب پذیری‌ای که بتواند کسب‌وکار ما را تحت‌تاثیر قرار دهد، برایمان اهمیت دارد. اگر کسی بتواند حتی یک شارژ رایگان هم داشته باشد یا به کوچک‌ترین داده‌های کاربران ما دسترسی پیدا کند، برایمان بسیار مهم خواهد بود.

ایرانسل
MTN

علی جلال‌نژاد
مدیر تضمین امنیت ایرانسل

## انواع هدف در راورو از چه قرار هستند؟

میدان‌ها در فرآیند تعریف هدف در پلتفرم راورو، نوع مشارکت شکارچیان آسیب‌پذیری برروی هدف خود را انتخاب می‌کنند. آن‌ها با این انتخاب تعیین می‌کنند که چه شکارچیانی می‌توانند برروی هدف تعریف‌شده‌ی آن‌ها در پلتفرم، به کشف و گزارش آسیب‌پذیری بپردازند.

اهداف عمومی: همه‌ی شکارچیان آسیب‌پذیری

اهداف خصوصی: سطح انتخاب‌شده از شکارچیان آسیب‌پذیری توسط میدان (شکارچیان آسیب پذیری در راورو براساس امتیاز کسب‌کرده "سطح‌بندی" شده‌اند.)

اهداف دعوت‌نامه‌ای: شکارچیان معدود و انتخابی دعوت‌شده توسط میدان

# هر چه عمومی‌تر، بهتر

گزارش‌های ثبت‌شده برروی اهداف متنوع در طول سال‌ها

| | عمومی | خصوصی | دعوت‌نامه‌ای |
|---|---|---|---|
| ۱۳۹۸ | ۴۸% | ۰% | ۵۲% |
| ۱۳۹۹ | ۴۳% | ۱۴% | ۴۳% |
| ۱۴۰۰ | ۲۸% | ۶% | ۶۶% |
| ۱۴۰۱ | ۳۱% | ۱% | ۶۸% |
| ۱۴۰۲ | ۵۹% | ۱% | ۴۰% |
| ۱۴۰۳ | ۸۹% | ۰% | ۱۱% |

## چه سرنوشتی در انتظار یک گزارش آسیب پذیری پس از ثبت است؟

**بسته‌شده منفی:** گزارشی که از منظر فنی صحیح محسوب نمی‌شود یا مطابق با قوانین میدان نیست. شامل گزارش‌های؛ اسپم، ردشده توسط تیم داوری و ردشده توسط میدان.

**بسته‌شده مثبت:** گزارشی که از نظر فنی صحیح است، اما به بانتی منجر نشده است. شامل گزارش‌های؛ تکراری، آموزنده، ثبت‌شده توسط تیم امنیت.

**منجرشده به بانتی:** گزارشی که از منظر فنی صحیح، مطابق با قوانین میدان و غیرتکراری است و توسط تیم داوری و میدان تایید شده و به آن بانتی تعلق می‌گیرد.

## **وضعیت بسته‌شده منفی** شامل چه دسته گزارش‌هایی است؟

**اسپم:** گزارشی که شامل محتوایی غیرمرتبط به باگ‌بانتی است.

**ردشده توسط تیم داوری:** گزارشی که به دلایل فنی یا مغایرت با قوانین توسط تیم داوری رد شده است.

**ردشده توسط میدان:** گزارشی که به دلایل فنی، مغایرت با قوانین یا سیاست‌های کسب‌وکار، توسط میدان رد شده است.

## وضعیت بسته‌شده مثبت شامل چه دسته گزارش‌هایی است؟

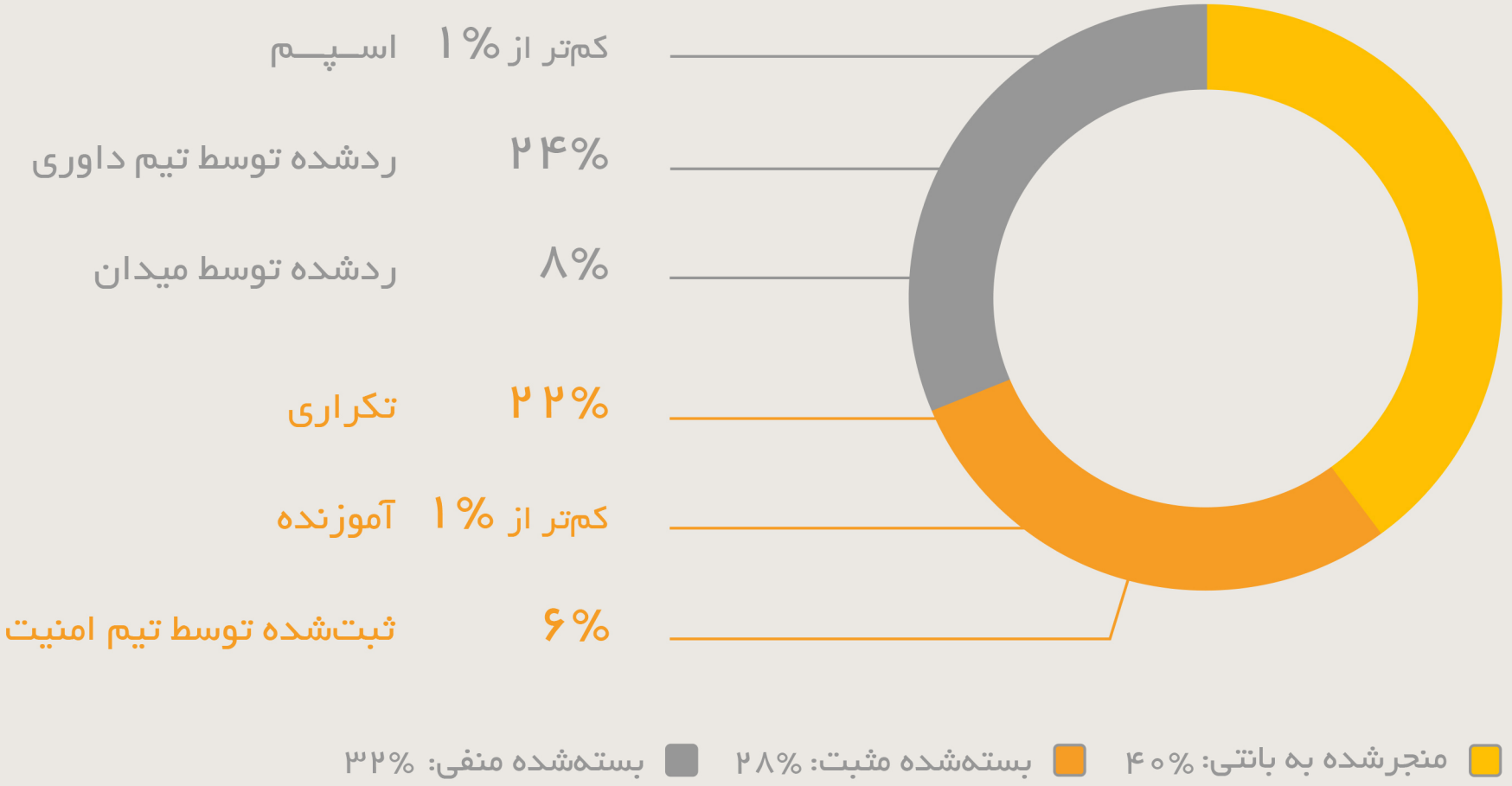
تکراری: گزارشی که قبلا گزارشی همانند آن ثبت شده است.

آموزنده: گزارشی که از نظر فنی صحیح است اما تاثیر امنیتی ندارد و شامل قوانین قابل‌قبول برای پرداخت نمی‌شود.

ثبت‌شده توسط تیم امنیت: گزارشی که توسط تیم امنیت میدان مربوطه، ثبت شده است.

# چه بر سر ۴۰۰۰ گزارش ثبت‌شده آمده؟

۱۴۰۳



شاید فقط ۴۰% از **گزارش‌های ثبت‌شده** به بانتی برسند،

اما یک پلتفرم باگ‌بانتی،

مسئولیت پیگیری ۴۰ % + ۶۰% **گزارش‌ها** را

از لحظه‌ی ثبت تا تعیین تکلیف نهایی به‌عهده دارد.

از **هر ۵ گزارش آسیب‌پذیری ثبت‌شده**،
حداقل **۲ گزارش**،
**تکراری** و یا براساس قوانین و شرایط اعلام‌شده **غیرقابل قبول** هستند.

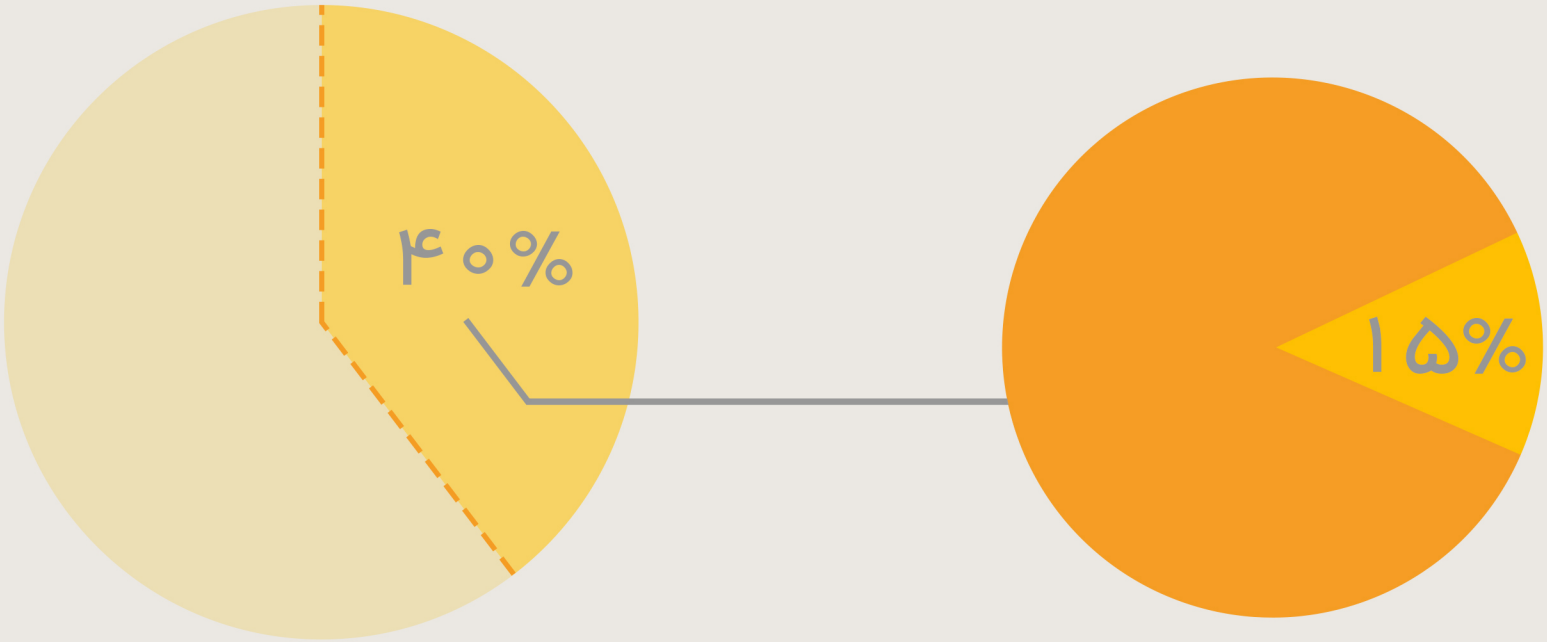
در پلتفرم باگ‌بانتی، این گزارش‌ها قبل از رسیدن به میدان فیلتر می‌شوند.

انتظاراتی که شکارچی آسیب‌پذیری از یک گزارش و رفتار سازمان دارد، با انتظاراتی که میدان از گزارش و رفتار شکارچی دارد، متفاوت است. این تفاوت و فقدان نگاه مشترک، چالش‌زاست. ما به‌عنوان یک پلتفرم سعی می‌کنیم این نگاه‌ها را به‌هم نزدیک‌تر کنیم. این‌گونه، ماجرا برای هر دو طرف قابل‌پذیرش‌تر می‌شود. این روند منجر به رشد و بلوغ امنیتی می‌شود.

نسترن سلیمان
راهبر اجرایی دپارتمان باگ‌بانتی
پلتفرم راورو

# چرا رفعش نمی‌کنید؟

۱۴۰۳




- آسیب‌پذیری‌های رفع‌شده توسط میدان‌ها
- آسیب‌پذیری‌های رفع‌نشده توسط میدان‌ها
- گزارش‌های آسیب‌پذیری تأییدشده
- گزارش‌های آسیب‌پذیری تأییدنشده

## چرا فقط ۱۵% از آسیب‌پذیری‌های تأییدشده، رفع‌شده‌اند؟

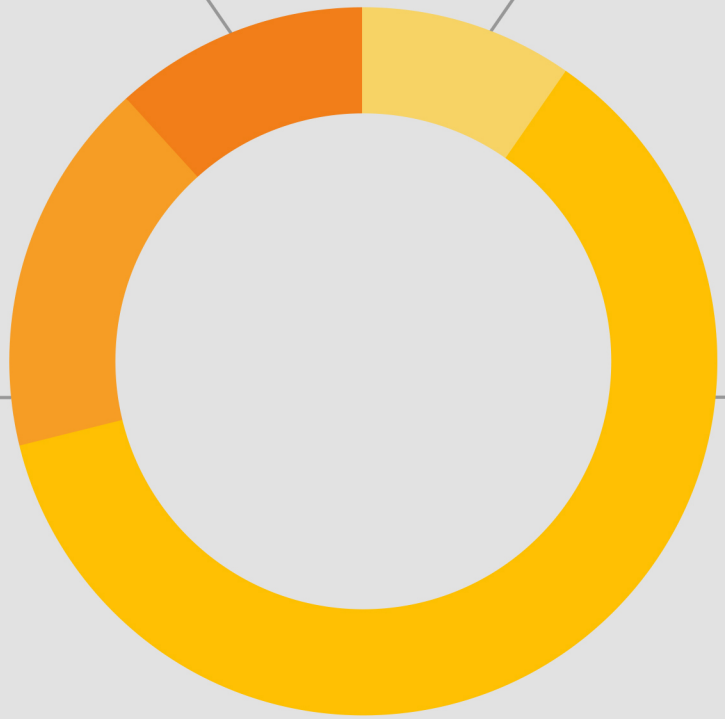
چون کسب‌وکارها

- رفع آسیب‌پذیری‌های حیاتی را در اولویت بالاتری قرار می‌دهند.
- هزینه‌ی مالی و زمانی رفع بعضی آسیب‌پذیری‌ها با سطح خطر متوسط و پایین، را به‌صرفه نمی‌بینند.
- آسیب‌پذیری‌هایی را رفع می‌کنند، اما به پلتفرم باگ‌بانتی اطلاع نمی‌دهند.
- الزام قانونی‌ای برای رفع آسیب‌پذیری‌ها متوجه آن‌ها نیست.
- شاهد اهمیت این موضوع برای مخاطبان نیستند و مطالبه‌ای در این خصوص از سمت آن‌ها نمی‌بینند.

۱۴۰۳

## از هر ۱۰ تا، ۳ تایش جدی است.

تفکیک گزارش‌های تاییدشده براساس رده‌بندی CVSS



**۱۰%**
سطح خطر پایین
شدت بین ۰/۱ تا ۳/۹

**۶۰%**
سطح خطر میانه
شدت بین ۴ تا ۶/۹

**۱۸%**
سطح خطر بالا
شدت بین ۷ تا ۸/۹

**۱۲%**
سطح خطر بحرانی
شدت بین ۹ تا ۱۰

کاظم فلاحی
هم‌بنیان‌گذار پلتفرم راورو

نحوه‌ی گزارش‌نویسی از نکات بسیار موثر در پذیرش و ارزش‌گذاری گزارش توسط میدان است. شفافیت توضیحات در گزارش باید در حدی باشد که فردی از تیم میدان که هیچ دانش امنیتی‌ای ندارد نیز بتواند متوجه آسیب‌پذیری و خطر آن شود. شکارچی باید در گزارش خود به سوال‌هایی پاسخ دهد؛ من به‌عنوان یک مهاجم، به چه چیزی می‌رسم؟ چه کارهایی می‌توانم انجام دهم؟ با آن به کجا می توانم برسم؟

ما گاهی گزارش‌هایی دریافت می‌کنیم که تنها شامل یک لینک هستند! نه خبری از سناریو هست، نه خبری از اکسپلویت‌نویسی و نه عکس و فیلمی به‌عنوان اسناد ارائه شده!

# گزارش‌ها چگونه امتیازبندی می‌شوند؟

۱۴۰۳

برای بعضی از بخش‌های فرم ثبت گزارش آسیب پذیری، متناسب با موضوع و میزان اهمیتشان، بازه‌ای از امتیاز در نظر گرفته شده است.

مجموع امتیازات تعلق‌گرفته به بخش‌ها، امتیاز نهایی گزارش را تشکیل می‌دهد.

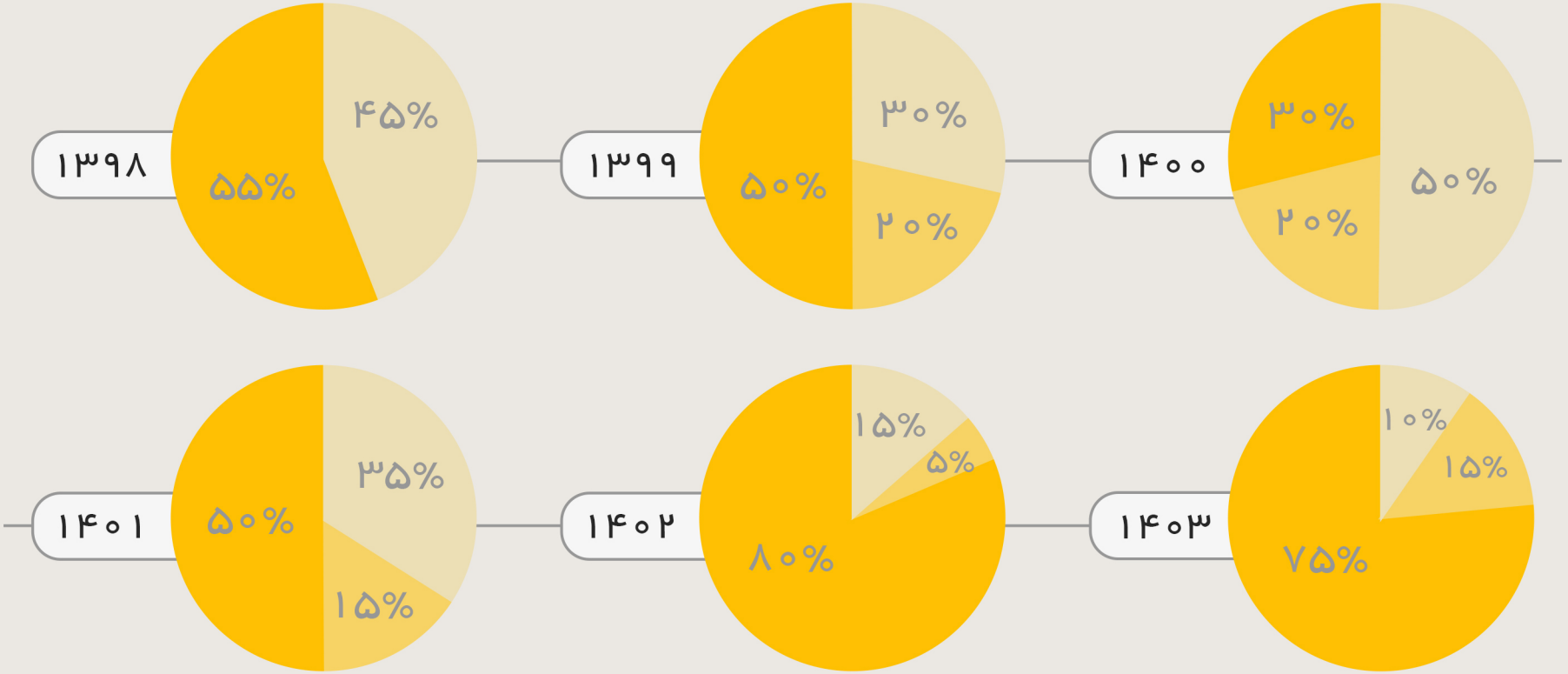
براین اساس در راورو هر گزارش آسیب‌پذیری، امتیازی بین ۰ تا ۲۰ را کسب می‌کند.

من در هنگام نوشتن گزارش، سعی می‌کنم تا جایی که می‌توانم مراحل اثبات آسیب پذیری را کامل بنویسم تا برای داوری، آسیب‌پذیری به‌راحتی قابل بازتولید باشد.
همیشه ویدئوی آسیب‌پذیری را هم به‌عنوان پیوست قرار می‌دهم. اگر در مسیر اثبات آسیب‌پذیری از اسکریپتی استفاده کرده باشم، آن را هم در گزارش قرار می‌دهم.
سعی می‌کنم از آسیب‌پذیری بیشترین ایمپکت را بگیرم و آن ایمپکت را در قسمت‌های مختلف گزارش ذکر کنم. (مثلا؛ در عنوان، خلاصه و همچنین در آخر گزارش)
به دو آسیب پذیری یکسان با ایمپکت متفاوت، بانتی متفاوتی تعلق می‌گیرد. چون چیزی که در آخر برای میدان ها مهم است، تاثیر آسیب‌پذیری ست نه خود آسیب‌پذیری.

محمد درخشان
شکارچی آسیب‌پذیری

# کیفیت گزارش‌ها بالا رفته است...

۱۴۰۳



اجبار ارسال ویدئوی استاندارد در پیوست گزارش آسیب‌پذیری، که از سال ۱۴۰۰ اعمال شده، تاثیر قابل‌توجهی بر ارتقای کیفیت و وضوح گزارش‌ها داشته است.

این آخر قصه‌ی ما از امنیت سایبری ست،
اما آخرین قصه‌ی ما نیست...

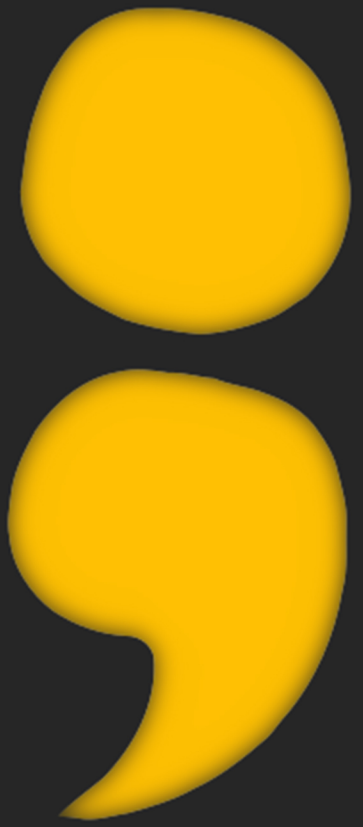
www.Ravro.ir

support@Ravro.ir

@Ravro_ir

۰۲۱۹۱۰۳۵۳۱۵

۱۵۷۸۷۷۵۴۸۸



روز و روزگارتون امن ؛)