خدمات: تســت و نفوذ PENTEST

نوع ســند : مستندات تست و نفوذ

PIHUNTER.NET

INFO@PIHUNTER.NET

مقدمه

در جهان امروز، تهدیدات سایبری به بزرگ‌ترین چالش برای سازمان‌ها تبدیل شده‌اند. با افزایش حملات هکری و پیشرفت روش‌های نفوذ، امنیت اطلاعات به اولویت نخست بسیاری از کسب‌وکارها تبدیل شده است. آیا از قدرتمندی زیرساخت‌های امنیتی خود برای مقابله با این تهدیدات اطمینان دارید؟

ما در پی هانتر با ارائه خدمات تست نفوذ (Penetration Testing) و مشاوره‌های امنیتی، به شما کمک می‌کنیم تا آسیب‌پذیری‌های سیستم‌های خود را شناسایی کرده و از خسارات مالی و اعتبارتان محافظت نمایید. با پیوستن به ما، امنیت دیجیتال خود را با بررسی نقاط ضعف امنیتی کسب‌وکارتان به سطحی بالاتر ارتقا دهید.

تست نفوذ چیست؟

فرآیند تست نفوذ به‌عنوان یک اقدام امنیتی، حملات یک هکر با نیت مخرب را شبیه‌سازی می‌کند تا نقاط ضعف سیستم‌های اطلاعاتی شما شناسایی و ارزیابی شوند. تیم متخصص ما با بررسی دقیق زیرساخت‌ها و نرم‌افزارها، به کشف آسیب‌پذیری‌های موجود می‌پردازد. این فرآیند به شما امکان می‌دهد که سیستم‌های خود را از منظر یک هکر ببینید. پس از انجام تست، گزارشی کامل و دقیق از نقاط ضعف شناسایی‌شده به همراه راهکارهای اصلاحی ارائه می‌دهیم تا بتوانید امنیت کسب‌وکارتان را بهبود بخشید و از حملات و تهدیدات سایبری پیشگیری کنید.

خدمات تست نفوذ ما چگونه کار می‌کند؟

تست نفوذ در مقابل حمله هکری

یک هکر با نیت مخرب به دنبال دسترسی غیرمجاز به سیستم شماست، اما تست کننده نفوذ (pentester) تلاش می‌کند با بررسی نقاط ضعف، امنیت آن را تقویت کند.یکی از اهداف اصلی حملات هکری که شرکت‌های تست نفوذ با آن مقابله می‌کنند، تصاحب غیرقانونی کنترل سیستم‌های اطلاعاتی است. هکرها به دنبال دسترسی به اطلاعات حساس مانند داده‌های شخصی، اعتبارنامه‌های حساب‌های کاری و مالی، مالکیت معنوی و نوآوری‌های شرکت‌ها هستند تا از آن‌ها به سود مالی یا اقتصادی دست یابند. تست نفوذ، ابزاری ضروری در امنیت سایبری است که آسیب‌پذیری‌ها را از زوایای مختلف شناسایی کرده و به کاهش احتمال موفقیت حملات کمک می‌کند.

انجام تست نفوذ به دلایل زیر الزامی است:

ضرورت انجام تست نفوذ

تهدیدات مداوم حملات سایبری : حملات سایبری به سازمان‌ها و شرکت‌ها به طور روزانه در حال افزایش است و صدها مورد در این زمینه گزارش می‌شود. عدم انجام تست نفوذ به معنای دعوت از مهاجمان برای حمله به سیستم‌های شماست. حملات باج‌افزاری که اطلاعات شما را رمزگذاری کرده و برای بازگرداندن آن‌ها درخواست باج می‌کنند، تنها یکی از خطرات موجود است. حتی اگر اطلاعات شما رمزگذاری نشود، مهاجمان می‌توانند تهدید به افشای اطلاعات محرمانه کنند؛ این موضوع می‌تواند برای سازمان‌هایی که با داده‌های حساس کاربران سروکار دارند، فاجعه‌آمیز باشد. بدون تست نفوذ، از میزان آسیب‌پذیری خود در برابر چنین تهدیداتی آگاهی نخواهید داشت و این می‌تواند به خسارات مالی و اعتباری بسیار سنگینی منجر شود.

پیشگیری بهتر از درمان است : هزینه‌های مالی و زمانی ناشی از یک حمله سایبری بسیار بیشتر از هزینه‌های انجام تست نفوذ خواهد بود. یک نقص امنیتی که مورد سوءاستفاده مهاجمان قرار گیرد، ممکن است به توقف کسب‌وکار، از دست دادن مشتریان یا حتی پیگرد قانونی منجر شود. تست نفوذ، همانند یک سرمایه‌گذاری بلندمدت، اطمینان می‌دهد که از آسیب‌های آینده جلوگیری می‌شود.

دسترسی مهاجمان به داده‌های حساس اگر مهاجمی به سامانه‌های شما نفوذ کرده و به داده‌های حساس م شتریان یا اطلاعات مالی دسترسی پیدا کند، این دسترسی می‌تواند منجر به باجگیری، سوءاستفاده از منابع شرکت یا حتی فروش اطلاعات شما به رقبا یا بازارهای سیاه شود. با انجام تست نفوذ، می‌توانید این آسیب‌پذیری‌ها را قبل از سوءاستفاده مهاجمان شناسایی و رفع کنید.

خسارت‌های مالی :سرقت پول، دریافت خدمات بدون پرداخت هزینه و سایر مسائل مالی ممکن است ناشی از نقص‌های امنیتی باشد که می‌تواند به سازمان شما آسیب برساند

حفظ اعتبار سازمان و جلب اعتماد مشتریان: در دنیای کنونی، اعتبار برند و اعتماد مشتریان یکی از بزرگ‌ترین سرمایه‌های هر سازمان محسوب می‌شود. یک نقص امنیتی می‌تواند به سرعت تمام اعتبار شما را به خطر بیندازد و مشتریان را از شما دور کند. مشتریان انتظار دارند اطلاعات آن‌ها به طور کامل امن باشد. انجام تست نفوذ و ن شان دادن این که شما به امنیت اهمیت می‌دهید، موجب افزایش اعتماد م شتریان و تقویت جایگاه شما در بازار خواهد شد.

۱

شروع قرداد وآغاز تست نفوذ

در این مرحله از تست نفوذ، قرارداد عدم افشا (NDA) و سایر توافق‌نامه‌ها امضا می‌شوند. جلسات کاری برگزار می‌گردد تا چارچوب‌های قانونی، اهداف، زمان‌بندی‌ها، برنامه کاری و دامنه تست مشخص شود. همچنین روش تست (سفید، خاکستری یا سیاه) و میزان بهره‌برداری از آسیب‌پذیری‌های شناسایی‌شده تعیین می‌شود. به‌عنوان مثال، ممکن است نیاز به تست نفوذ وب‌سایت داشته باشید که هزینه آن به دامنه و پیچیدگی وب‌سایت بستگی خواهد داشت.

۲

شناسایی و جمع آوری اطلاعات

در این مرحله، ما به جمع‌آوری و تحلیل اطلاعات می‌پردازیم. در مرحله اول، از منابع عمومی و آنلاین مانند موتورهای جستجو، شبکه‌های اجتماعی، وبلاگ‌ها و فروم‌ها استفاده می‌کنیم. هدف ما شناسایی اطلاعات حساسی است که ممکن است در این منابع وجود داشته باشد یا اطلاعات حساسی که به بیرون نشت کرده است، مانند توکن‌های نشت‌شده در گیت‌هاب یا اعتبارنامه‌های مدیریتی و کاربران در IntelX. همچنین، ما به انجام جستجوی معکوس DNS، اسکن پورت‌ها، تحلیل ترافیک، شناسایی زیر دامنه‌ها و شناسایی تکنولوژی‌های مورد استفاده خواهیم پرداخت. سپس، ما تمامی توابع وب‌اپلیکیشن را به‌صورت دقیق مورد بررسی قرار می‌دهیم. این بررسی شامل شناسایی ورودی‌ها، پردازش‌ها و خروجی‌های مرتبط با هر تابع خواهد بود. همچنین، ما به تحلیل منطق تجاری وب‌اپلیکیشن خواهیم پرداخت. این تحلیل شامل درک فرآیندها، قوانین و وابستگی‌هایی است که در پس‌زمینه اپلیکیشن وجود دارد. بسته به نوع توافق تست نفوذ، این اطلاعات می‌تواند در مراحل بعدی کمک قابل‌توجهی به ما کند.

۳

مدل‌سازی تهدیدات

در این مرحله، با توجه به اطلاعات به‌دست‌آمده از مرحله قبل، اهداف و مسیرهای حمله بالقوه شناسایی می‌شوند. این مرحله به دلیل اهمیت بالایی که در امنیت سایبری دارد، نیاز به دقت و تحلیل عمیق دارد. تهدیدات شناسایی‌شده به دو دسته اصلی تقسیم می‌شوند:

- آسیب‌پذیری‌های عمومی: این دسته از آسیب‌پذیری‌ها شامل تهدیداتی مانند SQL وInjection، XSS، CSRF و Misconfigurationو... است که به‌طور گسترده در سیستم‌های مختلف مشاهده می‌شوند.
- آسیب‌پذیری‌های منطقی : این نوع آسیب‌پذیری‌ها به ضعف‌هایی اشاره دارد که به طراحی و منطق تجاری خاص سیستم مربوط می‌شوند.

برای توابع مختلف وب اپلیکیشن، سناریوهای تهدید مدل‌سازی می‌شوند. به‌عنوان مثال، برای تابع آپلود فایل، سناریوهایی با توجه به نقاط ضعف بالقوه طراحی می‌شود. همچنین برای توابع دیگر مانند فراموشی رمز عبور، سناریوهای متفاوتی در نظر گرفته می‌شود که شامل روش‌های ممکن برای بهره‌برداری از آسیب‌پذیری‌ها است. این سناریوها به شناسایی نقاط ضعف کمک کرده .

۴

کشف و بهره برداری از آسیب پذیری ها

در این مرحله، از مدل‌سازی تهدیداتی که در مرحله قبل انجام دادیم، برای کشف آسیب‌پذیری‌ها استفاده می‌کنیم. پس از تأیید آسیب‌پذیری‌ها، امکان بهره‌برداری از آن‌ها را ارزیابی می‌نماییم. بر اساس توافق قبلی درباره درجه بهره‌برداری مجاز، یک حمله واقعی را از سوی یک هکر بالقوه شبیه‌سازی می‌کنیم.

بسته به نیازهای مشتری، این حملات ممکن است شامل حملات به وب‌سایت‌ها، شبکه‌ها، مهندسی اجتماعی و موارد مشابه باشد.
در طول این فرآیند، با بهره‌گیری از دانش فنی، تجربه حرفه‌ای و تکنیک‌های دستی تست نفوذ، بیشترین آسیب‌پذیری‌های بحرانی ممکن را شناسایی کرده و خطرات و پیامدهای احتمالی حملات سایبری را به حداقل می‌رسانیم

۵

تحلیل ریسک، پیشنهادات و پاک‌سازی آثار

بر اساس نتایج تست نفوذ، ما به‌عنوان همکار و مشاور امنیتی شما، تحلیل ریسک انجام می‌دهیم، آسیب‌پذیری‌های شناسایی‌شده را سازمان‌دهی کرده و پیشنهاداتی برای رفع آن‌ها ارائه می‌کنیم.

سپس، فایل‌های موقت، حساب‌های ایجادشده، مجوزهای افزایش‌یافته و سایر آثار مربوط به تست نفوذ زیرساخت یا برنامه را پاک‌سازی کرده و سیستم را به پیکربندی اولیه خود بازمی‌گردانیم. همچنین، اطلاعات مربوط به هرگونه تغییرات مهم را به شما اطلاع می‌دهیم.

۶

ارسال گزارش

در مرحله نهایی، گزارشی دقیق و ساختاریافته ارائه می‌دهیم که شامل روش‌های به‌کاررفته برای شناسایی و بهره‌برداری از آسیب‌پذیری‌ها است. این گزارش شامل شواهدی مانند مراحل بازتولید آسیب‌پذیری‌ها (از جمله کدها، ویدیوها و اسکرین‌شات‌ها) می‌باشد. همچنین، راهکارهای پیشنهادی برای رفع آسیب‌پذیری‌ها و توصیه‌هایی برای بهبود سیستم امنیتی موجود، به‌منظور محافظت از شرکت شما در برابر مجرمان سایبری، ارائه خواهد شد.

روش های مورد استفاده درتست و نفوذ

- تست جعبه سیاه (Black Box Testing) : در این روش، تیم تست نفوذ بدون داشتن اطلاعات داخلی از سیستم ،به شناسایی و بررسی آسیب پذیری ها می پردازد
- تست جعبه سفید (White Box Testing): در این روش، تیم تست نفوذ با داشتن اطلاعات داخلی از سیستم، به شناسایی و بررسی آسیب پذیری ها می پردازد.
- تست جعبه خاکستری(Grey Box Testing): ترکیبی از دو روش بالا است که در آن، تست کنندگان به برخی از اطلاعات داخلی سیستم دسترسی دارند. .(مورد پیشنهادی)

متدولوژی تست نفوذ

تمامی تست‌های نفوذ ما به‌طور انحصاری بر اساس متدولوژی‌های خصوصی خودمان انجام می‌شود که به‌طور کامل به فناوری‌ها و خدمات هدف مشخص‌شده در محدوده وابسته است. با این حال، در صورت نیاز، امکان استفاده از متدولوژی‌های دیگر، مانند OWASP WSTG، نیز وجود دارد

هزینه پروژه

هزینه انجام پروژه پس از توافق و دریافت منابع مورد نیاز اعلام خواهد شد. این مبلغ به صورت دو مرحله‌ای یا در صورت صلاحدید به صورت سه مرحله‌ای قابل پرداخت است:

- ۵۰ درصد هنگام عقد قرارداد
- ۵۰ درصد هنگام دریافت گزارش نهایی

برنامه‌زمانی پروژه

زمان لازم برای انجام تست نفوذ بستگی به دامنه و پیچیدگی سیستم شما دارد و پس از تعیین محدوده تست، پیش از انعقاد قرارداد، به شما اطلاع‌رسانی خواهد شد. ولی بطور معمول این زمان کمتر از ۳۰ روز کاری خواهد بود.

تفاوت باگ بانتی با پروژه تست نفوذ(Pentest)

بررسی جامع و هدفمند :تست نفوذ به‌صورت سیستماتیک و با رویکردی هدفمند انجام می‌شود و قادر است تمامی نقاط ضعف را پیش از ورود عمومی به یک برنامه باگ بانتی شناسایی کند.

کنترل بیشتر بر فرآیند :در تست نفوذ، شرکت کنترل کاملی بر نحوه تست‌ها و بخش‌های بررسی‌شده دارد، در حالی که در برنامه‌های باگ بانتی این کنترل به شرکت‌کنندگان عمومی واگذار می‌شود.

صرفه‌جویی در هزینه‌ها :با انجام تست نفوذ و رفع آسیب‌پذیری‌های اصلی، احتمال شناسایی باگ‌های کمتری در برنامه باگ بانتی وجود دارد که به معنای پاداش‌های کمتر و هزینه‌های پایین‌تر خواهد بود

پیشگیری از آسیب‌های گسترده : تست نفوذ می‌تواند آسیب‌پذیری‌های بزرگ و حیاتی را زودتر شناسایی کرده و پیش از دسترسی عمومی، آن‌ها را برطرف نماید.

صرفه‌جویی در زمان و منابع :با انجام تست نفوذ، شما می‌توانید عمده آسیب‌پذیری‌های سیستم را به‌صورت یکجا شناسایی کرده و زمان و منابع کمتری برای برطرف‌سازی آن‌ها صرف کنید

شناسایی نقاط ضعف توسعه‌دهندگان :پس از دریافت گزارش، می‌توانید متوجه شوید که توسعه‌دهندگان شما در کدام بخش از قوانین امنیتی نقاط ضعفی دارند و پیشگیری از ایجاد آسیب‌پذیری‌ها برای مجموعه‌تان آسان‌تر خواهد بود.

به عبارت دیگر، تست نفوذ به شرکت‌ها اجازه می‌دهد ریسک‌های اصلی را به‌صورت پیشگیرانه مدیریت کنند و سپس از برنامه باگ بانتی به‌عنوان ابزاری تکمیلی برای شناسایی نقص‌های جزئی یا غیرمنتظره بهره‌برداری نمایند.

ابزارهای مورد استفاده در پروژه

Burpsuite ابزاری یکپارچه جهت بررسی و آزمایش امنیت برنامه

Nuclei ابزاری برای اسکن بر اساس الگوهای آسیب‌پذیری‌های کشف شده

Nmap ابزاری برای پویش شبکه و سرویس است

SQLmap ابزای برای شناسایی نقاط ضعف مرتبط با تزریق پایگاه داده

Acunetix. پویش‌گری تخصصی برای ارزیابی آسیب‌پذیری‌های وب

Metasploit نرم‌افزار تخصصی آزمون نفوذ بر روی سکوها، سیستم‌عامل‌ها و

DirSearch/ katana جستجوگر تمام‌خودکار برای خزش در وب‌سایت

Subfinder ابزاری برای بدست آوردن زیر دامنه ها

gf-patterns ابزاری برای کشف URL های آسیب‌پذیر در سامانه است.

dalfox ابزاری برای کشف URL های آسیب‌پذیر در سامانه است.

corsy ابزاری برای کشف آسیب‌پذیری‌های CROS در سامانه است.

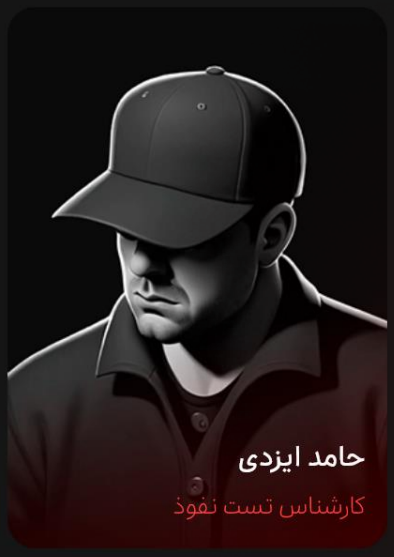
subjs ابزاری برای آنالیز و بررسی حملات بر روی فایل‌ها JavaScript است.

pihunt ابزار اختصاصی تیم پی هانتر برای شناسایی اتوماتیک آسیب پذیری ها

PIHUNTER | پی هانتر

پی هانتر (Pihunter) ترکیبی از دو مفهوم جذاب می‌باشد: پی (π)که یکی از معروف‌ترین اعداد در علم ریاضیات است و هانتر (hunter) که به معنای شکارچی است .در دنیای ریاضیات، عدد پی بی‌پایان و غیرقابل‌پیش‌بینی است، همان‌طور که تهدیدات امنیتی هر روز در حال تغییرند و شناسایی و رفع آن‌ها نیازمند دقت و هوش بالاست .در پی هانتر، ما با دقت و پیچیدگی خاصی که در محاسبات عدد پی وجود دارد، به شکار تهدیدات امنیتی می‌پردازیم. پی نماد بی‌نهایت چالش‌های امنیتی است و ما شکارچیانی هستیم که همواره آماده‌ایم تا این چالش‌ها را کشف و خنثی کنیم.

تیم کارشناسن پروژه



- حامد ایزدی: متخصص تست نفوذ وب اپلیکیشن و شبکه، کارشناس امنیتی در شرکت اسنپ.
- علیرضا کیا: متخصص تست نفوذ وب اپلیکیشن و اندروید، مدیر تیم تست و نفوذ شرکت داتین (وب).
- مهدی مرادلو: محقق امنیتی و متخصص تست نفوذ وب اپلیکیشن، مدیر تیم امنیت سایبری پی هانتر.

افتخارات تیم ما

رتبه دوم مسابقه مهارت

رتبه اول رویدادباگ بانتی

رتبه دوم مسابقه سازمان بورس

رتبه دوم مسابقه CTB 5

افتخارات فردی کارشناسان ما

- حامد ایزدی :کسب مدال نقره در نمایشگاه اختراعات بین‌المللیISIF’21 ، ورود به تالار افتخارات مایکروسافت، گوگل، و پروف‌پوینت، و همچنین تالار افتخارات سازمان ملل.
- علیرضا کیا :کسب رتبه دوم در مسابقه امنیت سایبری مهارت‌های جهانی ایران، رتبه چهارم در CTF مهارت‌های جهانی ایران، و جایگاه برتر در بین ۳۰۰ نفر اول در.TryHackMe
- مهدی مرادلو :رنک اول پلتفرم باگ بانتی راورو و هزاردستان، رنک اول تالار افتخارات برنامه باگ بانتی اسنپ، و رتبه برتر مسابقه برنامه‌نویسی بیان.

چرا تست نفوذ با پی هانتر؟

تجربه و درک عمیق از طراحی و توسعه نرم‌افزار: کارشناسان پی هانتر از توسعه‌دهندگان با تجربه هستند و با چالش‌های مختلف در مسیر توسعه آشنا می‌باشند. این تجربه به ما این امکان را می‌دهد که چالش‌های امنیتی مرتبط با توسعه برنامه را به‌خوبی درک کنیم. ترکیب دانش توسعه و امنیت به ما کمک می‌کند تا آسیب‌پذیری‌های پیچیده را به‌دقت شناسایی کرده و به مشتریان اطمینان دهیم که در برابر تهدیدات سایبری محافظت می‌شوند.

کاهش هزینه‌ها و افزایش کارایی: در پی هانتر، علاوه بر انجام بررسی‌های غیر خودکار، ما برنامه‌هایی را توسعه داده‌ایم که روند تست نفوذ را سریع‌تر و دقیق‌تر می‌سازند. این رویکرد با کاهش هزینه‌ها برای مشتریان و به صرفه‌تر بودن خدمات ما می‌انجامد. با استفاده از این تکنولوژی‌های پیشرفته، قادر هستیم با حفظ کیفیت بالا، به نتایج بهتری دست یابیم.

رویکرد مداوم به یادگیری و به‌روز بودن: در پی هانتر، ما همواره در حال یادگیری و به‌روزرسانی مهارت‌هایمان هستیم. در دنیای امنیت سایبری، اطلاعات جدید هر روز به‌روز می‌شوند و این رویکرد به ما این امکان را می‌دهد که راه‌حل‌های ما همیشه به‌روز و کارآمد باقی بمانند. این تلاش مستمر به ما کمک می‌کند تا بهترین خدمات را به مشتریان خود ارائه دهیم.

تعهد به مشتری‌مداری و ایجاد ارتباطات بلندمدت: در پی هانتر، ما به این باور هستیم که موفقیت ما به موفقیت مشتریان وابسته است. به همین دلیل، با دقت به نیازها و چالش‌های آن‌ها گوش می‌دهیم و خدمات خود را به گونه‌ای تنظیم می‌کنیم که بهترین نتایج ممکن را به‌دست آوریم.

مشتریان ما چه می گویند

خوشحال خواهیم شد که شما نیز به جمع مشتریان راضی ما بپیوندید

مجموعه پی هانتر در همکاری با ما برای تست نفوذ سیستم سی آر ام دیدار، با بررسی همه‌جانبه اپلیکیشن و رفع یا محدود کردن م شکلات مهم، به ما کمک کرد تا با خیالی راحت‌تر به م شتریان سرویس‌دهی کنیم. حرفه‌ای بودن تیم در انجام پروژه، ارائه گزارش نهایی و پیشنهاد راهکارها به قدری واضح بود که مطمئن شدم هر زمان نیاز به مشاوره داشتم، حتما این تیم را معرفی و پیشنهاد خواهم کرد.

علیرضا صفاری دیدار crm

" قبل از دریافت گزارش تست و نفوذ، به هیچ وجه تصور نمی‌کردم برنامه ما تا این حد آسیب‌پذیر باشد. از تیم پی هانتر بابت گزارش شفاف و دقیق‌شان که به تقویت امنیت سامانه ما کمک شایانی کرد، سپاسگزارم."

سعید غفاری رسید ساز

"همکاری با تیم پی هانتر در تست نفوذ ارگانیک ماینند بسیار مؤثر بود. آن‌ها به ما کمک کردند تا به سرعت نقاط ضعف سیستم را شناسایی و رفع کنیم و در نتیجه، امنیت سیستم‌مان را به شکل قابل توجهی افزایش یافت."

دکتر بهزاد چاوشی ارگانیک مایندد

خدمات سفارشی امنیت سایبری

ما به ارائه خدمات سفارشی متناسب با نیازهای خاص شما در حوزه امنیت سایبری متعهد هستیم. علاوه بر انجام تست‌های نفوذ، قادر به اجرای برنامه‌های باگ بانتی برای شرکت‌های درخواست‌کننده هستیم و در داوری و ارزیابی گزارش‌ها نیز به شما کمک خواهیم کرد. این خدمات به شما این امکان را می‌دهد که با حداکثر دقت و امنیت، نقاط قوت و ضعف سیستم‌های خود را شناسایی کنید.

علاوه بر این، بسته به نوع قرارداد، پس از اتمام تست نفوذ می‌توانیم ویژگی‌های جدیدی که به سامانه شما اضافه شده‌اند را دوباره مورد ارزیابی قرار دهیم. این فرایند به شما کمک می‌کند تا از ایمنی و کارایی به‌روز سیستم خود مطمئن شوید.

در صورتی که ایده یا موارد خاصی برای تست دارید، تیم ما آمادگی کامل دارد تا به بررسی و ارزیابی آن‌ها بپردازد. هدف ما این است که خدمات دقیق و متناسبی ارائه کنیم که به بهبود امنیت سامانه‌های شما کمک کند.

سوالات متداول:

آیا نیاز به اعطای دسترسی خاص به پی هانتر است؟ این مورد بستگی به انتخاب روش تست نفوذ توسط خود شرکت دارد.

آیا تست نفوذ باعث اختلال در عملکرد سیستم‌ها می‌شود؟خیر، تمهیدات لازم برای جلوگیری از م شکلات در نظر گرفته شده است. اگر تستی موجب اختلال در سیستم شود، حتماً قبل از انجام آن به اطلاع شرکت رسانده می‌شود.

چگونه می‌توانیم امنیت پس از تست نفوذ را تضمین کنیم؟تست نفوذ به شرکت کمک می‌کند تا بسیاری از آسیب‌پذیری‌ها را شناسایی و برطرف کند. با این حال، باید توجه داشت که امنیت یک موضوع نسبی است و نمی‌توان آن را به‌طور کامل تضمین کرد. اما پس از انجام تست نفوذ، درصد قابل توجهی از آسیب‌پذیری‌ها برطرف شده و امنیت سیستم به‌طور چشمگیری افزایش می‌یابد. همچنین، با اجرای برنامه باگ بانت به‌عنوان مکمل، می‌توانید به‌طور قابل توجهی امنیت خود را تقویت کنید.

آیا اطلاعات ما در طول تست محافظت می‌شود؟ در فرآیند تست، هیچ آسیبی به اطلاعات سایر کاربران نخواهد رسید. در صورت نیاز به انجام تست‌های خاص، حتماً از قبل به شرکت اطلاع‌رسانی خواهد شد و تنها با موافقت شرکت، این تست‌ها انجام می‌پذیرد.

چگونه اطمینان حاصل کنیم که اطلاعات شرکت ما افشا نمی‌شود؟ ما در طول فرآیند تست نفوذ از پروتکل‌های امنیتی سخت‌گیرانه‌ای پیروی می‌کنیم تا اطمینان حاصل شود که هیچ اطلاعات حساسی فاش نمی‌شود. تمام اطلاعات به‌دست‌آمده در طول تست به‌صورت محرمانه نگه‌داری شده و تنها برای اهداف تست و گزارش‌گیری استفاده می‌شود. همچنین، قبل از شروع تست، یک توافق‌نامه عدم افشای اطلاعات (NDA) امضا می‌شود که تعهد به محافظت از اطلاعات شما را تضمین می‌کند.

چگونه از حسن انجام کار اطمینان پیدا کنم؟ تمامی تست‌های انجام‌شده، حتی در صورت عدم وجود آسیب‌پذیری، ثبت و مستند می‌شوند. این مستندات شامل جزئیات فرآیند تست، تکنیک‌های استفاده‌شده و نتایج به‌دست‌آمده هستند. در صورت نیاز، این مستندات به شرکت ارائه می‌شوند تا اطمینان حاصل شود که تمامی مراحل به‌درستی و با دقت انجام شده‌اند.

خروجی ها و نتایج مورد انتظار

پس از انجام تست نفوذ و اجرای توصیه‌های امنیتی، انتظار می‌رود که سیستم بهبودهای زیر را تجربه کند:

- افزایش امنیت: نقاط ضعف و آسیب‌پذیری‌های شناسایی‌شده برطرف خواهند شد.
- رعایت استانداردهای امنیتی: سیستم مطابق با استانداردهای معتبر و قوانین حفاظت از داده‌ها عمل خواهد کرد.
- تقویت اعتماد مشتریان: کاربران و مشتریان با اطمینان بیشتری نسبت به امنیت داده‌های خود احساس آرامش خواهند کرد.

مار در پی هانتر
منتظر تماس شما هستیم

تیم ما متعهد به ارائه بهترین خدمات امنیت سایبری به شماست. پیش از انعقاد قرارداد، می‌توانید از یک جلسه م شاوره رایگان با کارشناسان ما بهره‌مند شوید. این فرصتی مناسب است تا نیازهای امنیتی خود را مطرح کرده و راهکارهای مناسب را مورد بررسی قرار دهید.

شماره تماس: [09120644452]
ایمیل: [info@pihunter.net]
وب‌سایت: [https://pihunter.net]

ما مشتاقانه منتظر گفتگو با شما هستیم و امیدواریم بتوانیم در ارتقاء امنیت کسب‌وکار شما نقش موثری ایفا کنیم!