



НАРЪЧНИК ЗА КУПУВАЧА

Наръчник за купувача на тестове за проникване

Пет материала за купувача, обединени в един документ, който можете да прочетете офлайн или да дадете на колега от отдел „Доставки“. Той покрива цялата покупка — решението какво да купите, определянето на обхвата, избора кой да го извърши, прочитането на предложението и договора, и действията по отчета, който получавате. Прилагайте всичко това и към нас, както към всеки друг, когото обмисляте.

PXLSecurity LTD. · София, България · pxlsec.com · Офанзивна сигурност от 2014 г.



СЪДЪРЖАНИЕ

Какво има в този наръчник

Написан за човека, на когото е възложено да купи тест за проникване и който не е купувал такъв досега. Той е умишлено полезен дори ако в крайна сметка наемете някой друг — въпросите са смисълът, не отговорът.

- 1 Как да решите какво ви трябва
- 2 Какво определя обхвата
- 3 Как да изберете доставчик
- 4 Как да прочетете предложението
- 5 Заданието за работа
- 6 Как да прочетете отчета, който получавате
- 7 Контролен списък преди подписване

1. Как да решите какво ви трябва

Почти всеки доставчик обещава едни и същи неща: опитни тестери, задълбочена методология, ясен отчет, повторен тест. Обещанията са евтини и почти идентични, затова решението не може да се вземе чрез четенето им. Това, което можете да уточните, преди да говорите с когото и да е, е какво всъщност искате — а повечето разочароващи ангажменти са били погрешно специфицирани, преди да бъде потърсен и един доставчик.

Купувачът е знаел, че му трябва „тест за проникване“ и нищо по-точно, затова е получил каквото се е случило да бъде продуктът по подразбиране на доставчика — а тези подходи по подразбиране се различават огромно между фирмите. Преди да пишете на някого, запишете въпроса, на който ви трябва отговор. Обикновено е един от четири.

- Имаме ли известни слабости, откриваеми с инструменти? Отговаря се чрез сканиране с човешка проверка. Няма да открие нарушен контрол на достъпа между ролите, нито нещо, което изисква разбиране за какво служи приложението ви.
- Какво би открил компетентен нападател при ограничено усилие? Това, което повечето хора имат предвид под тест за проникване: методология, приложена върху договорен обхват за договорен период, следвайки каквото изглежда интересно и спирайки, когато времето свърши. Методично, но по конструкция ограничено.
- Може ли да бъде постигнато конкретно последствие? Да се достигнат клиентски записи, да се вземе административен контрол над средата, да се извърши плащане с грешен резултат. Определя се чрез цели, а не чрез покритие, затова броят на констатациите може да е малък, а резултатът — сериозен.
- Бихме ли забелязали и бихме ли могли да спрем? Упражнение срещу организацията, а не срещу актива — откриване, ескалация и реакция — което носи разходи по съгласуване, каквито един обхванат тест няма.

Това са различни продукти, не намалени варианти един на друг. Сканирането не е евтин тест за проникване, а симулацията на противник не е скъп такъв. Купувачите най-често остават разочаровани, защото са купили едното и са очаквали отговорите на другото.

Два от тези отговори си заслужава да бъдат изречени направо, защото доставчик със заинтересованост рядко ги предлага сам. Първият е, че оценката на уязвимостите понякога е честната препоръка. Ако обхватът ви е наистина малък — няколко крайни точки зад един шлюз с един модел на авторизация — ръчен ангажмент под определен размер не може да ви каже нищо, което проверено сканиране не би казало. Собственият ни минимум е пет дни тестване, без отчитането; под това бихме ви предали сканиране с титулна страница, затова отказваме работата и казваме защо.

Вторият е симулация на противник, купена твърде рано. Red team измерва дали откривате нападател. Не е преглед на цялата ви среда и ще пропусне неща, които обхванат тест би открил през първата седмица. Ако никой още не е тествал покритието, това е, което трябва да купите първо — и всеки доставчик, който си заслужава да бъде наеман, ще ви каже, когато сте дошли дотук твърде рано.

След това уточнете за кого е предназначен отчетът, защото отчет, който удовлетворява одитор, не е автоматично такъв, по който инженерите ви могат да работят. Решете дали резултатът трябва да издържи пред оценител, пред проверка на сигурността на клиент, пред

застраховател, пред собствените ви разработчици, или пред няколко наведнъж — и го кажете, когато искате предложения. Добавянето на нова публика към вече готов отчет е най-честият източник на преработване.

Формата на ангажимента е различна от неговата дълбочина. Една система, тествана както трябва, е най-честата форма и за повечето екипи правилното начало. Няколко системи и пътищата между тях са друго упражнение, защото констатациите, които имат значение там, рядко са на едно място — те са маршрутът от малка слабост в една система до нещо сериозно в друга. Тестването с определен ритъм подхожда на екипи, чиито системи се променят по-бързо, отколкото един годишен ангажимент може да опише.

2. Какво определя обхвата

Доставчик, който дава оферта само въз основа на броя URL и IP адреси, не е определил никакъв обхват. Усилието следва отделното поведение, не инвентара: четиридесет крайни точки зад един шлюз с един модел на оторизация са малка част от работата по две наистина различни приложения. Вашата задача на първия разговор е да опишете различията и това, което прави една номинално малка система скъпа.

Най-голямата променлива са ролите. Контролът на достъпа не е функция, която проверявате веднъж; той е матрица, която обхождате. За всяка чувствителна операция тестерът трябва да установи кои роли могат да я извършват и да я опита с всяка роля, която не може — след което, за всяка роля, да опита да достигне данни, принадлежащи на друг екземпляр на същата роля: друг потребител, друга клиентска организация. Това са два различни теста и там живеят сериозните констатации в повечето бизнес приложения.

Затова работата расте с ролите, умножени по чувствителните операции, а не събрани с тях — така че предложение, което третира приложение с шест роли като такова с две, е решило да работи с извадка. Донесете матрица на ролите и правата, посочете ролите, които са козметични варианти на едни и същи права, и кажете изрично кои двойки не трябва да могат да се достигат. Точно това съчетаване, а не самият брой роли, е това, срещу което тестерът планира.

Останалото, което наистина мени един обхват:

- Дали API-то се ползва съвместно от мобилен клиент, партньор или публичен потребител, защото споделеното API има извикващи, чиито допускания се различават от тези на уеб интерфейса.
- Наематели — дали съществуват, колко строго трябва да са разделени и дали изолацията се налага на едно място или за всяка заявка, за всяка услуга, за всеки ключ в кеша.
- С удостоверяване, без удостоверяване, или и двете. Отчет без критични констатации означава едно, ако тестерът е разполагал с данни за достъп за всяка роля, и нещо съвсем различно, ако е имал изглед без удостоверяване към страница за вход.
- Облачни акаунти, в които работят продукционни работни натоварвания, и колко са.
- Външни хостове и вътрешни подмрежи и колко адреса в тях са действително живи, а не просто маршрутизируеми.
- Дали Active Directory е в обхвата, колко домейна и дали работата започва от периметъра или от допуснатото вече проникване.
- Къде живее специфичната логика — всичко, което определя цени, движи пари, дава права или налага регулаторно правило. Констатациите, които имат значение, се събират тук, а това трябва да бъде научено, преди да може да бъде атакувано.

- Всичко необичайно в удостоверяването: собствени токени, самостоятелно разработен единен вход, федерация, допълнително потвърждаване, обвързване с устройство, подписано състояние от страна на клиента.
- Работни процеси със състояние. Там, където резултатите зависят от последователността, тестерите трябва да достигнат всяко състояние, преди да го тестват, и да го възстановят след това — време, невидимо в документа за обхват и видимо в графика.
- Интеграции с трети страни и кои от тях могат да бъдат задействани срещу жив контрагент.
- Среда: производствена или тестова, и всяка известна разлика — доставчик на удостоверяване, функционални флагове, инфраструктура, обем на данните.
- Препятствия и ограничения на платформата: ограничаване на честотата, защита от ботове, блокиране по географски признак и дали адресите на източника могат да бъдат добавени в списък с разрешения; плюс времеви прозорци, контрол на промените, периоди на забрана и кой контрол трябва да докаже тестът, ако резултатът е предназначен и за съответствие.

Това, което предавате, променя както цената, така и стойността на работата — и зависимостта е обратна на инстинкта на повечето купувачи. Задържането на информация не намалява работата; то я премества. Тестер, на когото не са дадени данни за достъп, прекарва началния отрязък в извеждане на това, което бихте могли да предоставите първата сутрин: изброяване на роли, обратно инженерство на формата на токен, установяване кой компонент налага авторизацията. Това време излиза от тестването, не от бюджета. Доводът за реализъм също е слаб — истинският нападател не е ограничен във времето, така че симулирането на неговото незнание симулира най-вече първата му седмица.

Затова установете рано кое от следното можете да осигурите и колко време отнема всяко: по един работещ акаунт за всяка роля, проверен от човек, който лично е влязъл с него и с правилното ниво на права; две клиентски организации или по два акаунта за всяка роля, там където изолацията има значение, защото тестване на контрола на достъпа без втори обект, който да бъде достигнат, не е тестване; реалистични въведени данни, тъй като празна среда е почти невъзможна за тестване; документация, включително спецификация на API и матрица на правата; и посочено техническо лице за контакт, което може да действа, а не само да предава.

Две навика си заслужава да се запазят. Групирайте активите по сходство, защото четиридесет крайни точки, описани като един шаблон плюс три изключения, обикновено водят до по-малка оценка от плосък списък от четиридесет и три. И не намалявайте роли или клиентски организации, за да се вметите в бюджет: премахването на роля премахва теста, не пътя на атаката. Намалете обхвата по широчина вместо това и запишете какво сте отложили.

3. Как да изберете доставчик

Тестът за проникване не е продукт със спецификация. Той е количество квалифицирано внимание, насочено към система, която ви е важна, за ограничен период. Инструментите са стандартни, а шаблонът на отчета е решение за форматиране; това, което се различава между доставчици на сходни цени, е преценката на човека, който решава къде да погледне. Скенерът ви казва, че един параметър отразява входните данни. Само тестерът установява, че стойността попада там, където екранирането на вашата рамка не се прилага, че крайната точка е достъпна преди удостоверяване и че откраднатата сесия принадлежи на администратор, който може да изнесе таблицата с клиентите. Две предложения на еднаква цена могат да се различават няколко пъти по стойност, а разликата не се вижда в нито един от двата документа.

PXLSec е доставчик и този наръчник съществува отчасти защото хората, които сравняват доставчици, го намират за полезен. Прилагайте всичко от него и към нас. Ако нашите отговори са по-лоши от тези на някой друг, изберете другия — купувач, който задава трудни въпроси и после избира конкурент, все пак е решил по-добре от онзи, който не е попитал нищо.

Задайте следното писмено, на всички, и сравнявайте отговорите един до друг, а не брошурите. Неяснотата е лесна по телефона и очевиден в имейл.

- Кой извършва теста и какво всъщност е правил? Най-носещият въпрос и този, на който най-често се отговаря с биография на фирмата вместо на човек. Поискайте имена на конкретни хора, опита им със системи като вашата, кой ги замества и на какво ниво, и кой преглежда работата на по-младши колега, като преразглежда системата, а не текста.
- Това ръчно тестване ли е, или проверено сканиране? И двете са законни; проблемът е когато едното се продава като другото. Добрият отговор е конкретен за разделението на труда — автоматизация за изброяване, хора за оторизация и бизнес логика. Поискайте един пример за дефект в логиката, открит в сходна система; неяснотата тук е най-надеждният признак за отчет с формата на скенер.
- Каква част от приложението и колко роли? Покритието е най-тихата променлива в покупката. Попитайте дали се покрива всяка зона с удостоверяване или само извадка, как ще ви бъде съобщено какво е останало извън обхвата и дали се тества хоризонталният контрол на достъпа наред с вертикалния.
- Какво всъщност съдържа отчетът? Не приемайте съдържание. Поискайте да прочетете цял завършен документ, анонимизиран, с изцяло изписани констатации. Само документът показва дали съветите за отстраняване са специфични за вашата технология и дали критичността отразява бизнес въздействие, или само вектор.
- Ще идват ли констатациите със стъпки за възпроизвеждане? Точната заявка, предварителните условия, използваният акаунт, наблюдаемият резултат. Снимка на екрана с заключението на скенер не е доказателство за използваемост; записаните заявка и отговор са — и те са най-добрият показател дали една констатация е била проверена.
- Включен ли е повторен тест и какво покрива? Дали е в цената, в какъв срок можете да го ползвате, дали покрива всички констатации или само сериозните, и какъв документ получавате. Писмо, в което всяка констатация е отбелязана като отстранена, частично отстранена или неразрешена, си заслужава да бъде получено; одиторът го чете буквално.
- Какво се случва, ако по време на теста бъде открито нещо критично? Поискайте механизма, не успокоението: с кого се свързват, по какъв канал, колко бързо и какво прави тестерът след това. И дали ще ви кажат, ако някой друг вече е бил там.
- Ще направят ли хората, които са тествали, разговор по резултатите с вашите инженери? Голяма част от стойността на един ангажимент се реализира тук, а това често е първото, което бива премахнато. Може ли водещият ви разработчик да получи пряк отговор от човека, написал констатацията, без търговски разговор?
- Кой пази данните и можете ли да съотнесете констатациите към нашата рамка? Попитайте къде се съхраняват данните от ангажимента, кой може да ги чете и колко дълго се пазят. А където отчетът има одитна публика — ISO 27001, SOC 2, PCI DSS, DORA, NIS2 — съотнасянето е част от крайния доклад, вместо да бъде възстановявано от вас след това.

- Какво ще ни кажете, че не сте имали време да тествате? Доставчик, който планира да посочи границите на покритието, разграничава „тествахме това и не открихме нищо“ от „не стигнахме до това“ — разликата между увереност и пропуск, за който не знаете.
- Какво би ви накарало да ни кажете, че този ангажимент е грешното нещо за купуване? Най-информативният въпрос в списъка. Всеки честен доставчик има отговор: че преглед на кода би ви послужил по-добре или че първо трябва да отстраните това, което вече знаете.

Разговорът за обхвата преди това е поне толкова показателен: задълбоченият наподобява разпит на вашата архитектура, а не квалифициращо обаждане. Очаквайте известно възмущение. Доставчик, който казва, че обхватът ви е твърде голям за дълбочината, която искате, ви прави услуга; онзи, който приема наполовина описан обхват без нито един уточняващ въпрос, вече е решил какво да ви продаде.

Сертификатите и какво доказват и не доказват

Сертификатите са полезни и на тях рутинно се разчита прекалено. Практическите — OSCP, OSWE, OSEP, наборът OSCE³, регистрираните и сертифицирани изпити за тестери на CREST и техните еквиваленти — се печелят на изпити с ограничено време и практическа работа срещу живи цели, така че издържаният изпит е доказателство, че даден човек би могъл да върши определен клас работа без помощ. Това, което не доказват, е качеството на фирмата. Сертификатът се прикрепя към човек, а хората се разпределят по ангажименти: една фирма може честно да каже, че инженерите ѝ притежават силни сертификати, докато тестерът по вашия проект не притежава нито един от тях.

Акредитацията на ниво фирма е друг вид гаранция: там, където една схема я предлага, тя оценява процесите и работата с данни на организацията, а не само персонала ѝ, и в някои сектори е твърдо изискване. Ако е задължителна за вас, проверете я в собствения регистър на схемата, а не в долния колонтитул на доставчик. За да сме ясни за собствената си позиция: инженерите на PXLSec притежават индивидуални практически сертификати, включително OSCE³, OSWE, OSEP, CRT0 и CREST CRT. Не притежаваме акредитация на ниво фирма по никаква схема и не твърдим, че притежаваме, така че ако правилата ви за доставки изискват акредитиран доставчик, ние не отговаряме на условията. Преценете вместо това по посочените хора и по документ, който можете да прочетете предварително.

Проверявайте независимо. Сертификатите могат да бъдат проверени в регистъра на издателя, членството в схема — в указателя на схемата, публикуваните изследвания — в записите на CVE. Фирма, която публикува изследвания на уязвимости, трябва да публикува и политиката за координирано разкриване, по която работи.

Какво обикновено купува ниската оферта

Ниските оферти рядко са непочтени. Обикновено са различна услуга със същото име, а разликата почти винаги е на едно от шест места, всяко от които оставя следа.

- Автоматизирано сканиране, продадено като тестване. Предложението описва платформа повече, отколкото хора, обещава констатации като брой, а не като изписани описания, и изброява класове уязвимости, а не дейности. Попитайте какво прави тестерът на ръка; фирма, която върши ръчна работа, отговаря веднага.

- Младши тестери без преглед от старши. Цитира се общият опит на фирмата, а конкретни хора — никога, и никъде не се споменава осигуряване на качеството. Наблюдавани младши тестери върху добре подбран обхват е начинът, по който се създават добри тестери; работата на младши тестери без надзор върху вашия модел на оторизация не е.
- Няма повторен тест. Липсва, остойностен е като опция или е описан без обхват — най-честият начин една оферта да изглежда конкурентна, защото пропускът боли само по-късно, когато ви трябва доказателство, че констатациите са затворени.
- Отчети по шаблон. Съвети за отстраняване, общи за уязвимостта, а не специфични за вашата технология, и резюме за ръководството, което би могло да е за всеки. Ако съветът за поправка би подходил на всяко приложение навсякъде, купувате документ.
- Неоповестено изнасяне или подизпълнение. Договарящото лице, обявеното място на изпълнение и местоположението на тестерите явно не са едно и също, а предложението мълчи за това кой извършва работата. Това може да е напълно приемливо; да не ви бъде казано — не е, защото засяга задълженията ви по обработката на данни.
- Обхват, тихо свит, за да се вмести. Най-незабележимото от шестте. Офертата съвпада с бюджета ви, защото работата е била орязана, за да съвпадне с него, а орязването живее в пропуските — по-малко роли, отколкото има приложението ви, API, сгънато в реда за уеб. Доставчик, който свива обхвата умишлено и ви казва, управлява ограничение; онзи, който го свива мълчаливо, ви е продал вида на покритието.

Нищо от това не означава, че най-скъпото предложение е най-доброто. Цената отразява и общи разходи, комисиони и марка, нито едно от които не тества приложението ви. Първо приведете офертите към общ вид: подредете четири колони — обхват, актив по актив, с ролите и средата; дълбочина, изразена чрез това на кой от четирите въпроса отговаря; каква част от усилието е практическо тестване, а не сканиране и отчитане; и предавани документи. След това прочетете изключенията, където най-ниската оферта обикновено се разкрива: непокрити роли, зони с удостоверяване извън обхвата, изключено API, защото е бил назован само уеб интерфейсът. И прочетете цял завършен документ, преди да изберете.

4. Как да прочетете предложението

Предложението е документ, написан, за да спечели работа, което го прави лошо описание на работата и отлична проба за това как мисли доставчикът. Четете го за това, с което се обвързва, а не за това, което твърди. Предложение с определен обхват назовава вашите приложения, преброява вашите роли, споменава механизма за удостоверяване, който сте описали, и посочва какво изключва. Шаблонното описва методология в общи думи и извежда усилието от брой активи.

Следват признаците, които си заслужава да бъдат разгледани. Повечето имат невинно обяснение, затова всеки идва с въпроса, който превръща твърдението в обвързване. Целта не е да дисквалифицирате някого.

Оферта без разговор за обхвата. Остойностена за една нощ по запитване от два реда, без никой да попита колко роли имате. Усилието следва структурата на тестваното, а предположение, което се окаже ниско, се поема чрез намаляване на дълбочината — което вие никога не виждате да се случва. Невинно, бързата оферта показва компетентност, ако сте предоставили документ за обхвата, а индикативен диапазон е приемлив, когато е обозначен като такъв. Попитайте: какво допуснахте и кои допускания биха променили цената, ако са грешни?

Усилие, което не може да покрие заявления обхват. Няколко приложения, API, облачна среда и вътрешна мрежа, с усилие, което би било напрегнато за едно от тях. Подценяването на обхвата е най-честият начин един тест да разочарова, без някой да е излъгал, и това, което пристига, е извадка, представена като оценка. Пестеливата стойност може да е добре преценена там, където активите наистина споделят шлюз и модел на оторизация, така че проверката е дали доставчикът може да обясни групирането. Попитайте: как е разпределено усилието и какво няма да имате време да направите?

„Автоматизирано и ръчно тестване“ — израз, който върши твърде много работа в едно изречение. Използван честно, той описва работен процес: инструменти за известните проблеми, хора за логиката, оторизацията и навързването. Използван нечестно — сканиране с някой, който чете изхода. Автоматизацията е част от всяка добра методология — въпросът е само кои констатации откъде идват. Попитайте: кои класове констатации идват от инструменти и кои от ръчно тестване, и дайте ми един пример от ръчната половина, който никой скенер не би произвел?

Непосочена методология. Предложението трябва да каже какво систематично покрива тестването, с позоваване на призната рамка, подходяща за целта. Методологията е начинът, по който покритието става проверимо, а отчетът от тази година — сравним с миналогодишния. Рамките са под, не таван, а работата, водена от цели, законно се организира около целите вместо това, заявени със същата точност. Попитайте: кои раздели от методологията се прилагат към нашия обхват и кои не? Човек, който работи по дадена рамка, отговаря на нейния език.

Няма примерен отчет. Отчетът е продуктът; всичко останало е логистика. Примерният отчет показва дали констатациите носят стъпки за възпроизвеждане, дали доказателството е действителен материал от заявка и отговор или снимка на екран от панел на скенер, и дали пропуските в покритието са признати. Колебанието относно действителен клиентски отчет е правилно, тъй като те са конфиденциални; но заличен или специално изготвен отчет трябва да съществува, затова ние публикуваме такъв. Попитайте: може ли да видя пълен примерен отчет, включително страниците с подробности? След това прочетете една констатация от начало до край: би ли могъл инженерът ви да действа по нея без помощ?

Няма повторен тест или повторният тест струва допълнително. Констатацията е затворена, когато човек, който разбира атаката, потвърди, че тя вече не работи, а не когато разработчик го каже — и поправките се провалят често: филтърът покрива един параметър, но не и съседния му, проверката достига крайната точка, но не и пакетния ѝ вариант. Изключването на повторния тест може да е честната структура там, където отстраняването ще продължи дълго, така че тревожният признак е мълчанието, а не изключването. Попитайте: включен ли е повторен тест, за кои констатации, колко преминавания и тества ли заобикаляне на поправката или само първоначалния проблем?

Обещани констатации без стъпки за възпроизвеждане. „Подробни описания с оценки на риска и препоръки“ описва документ; „възпроизвеждане стъпка по стъпка, с доказателствата, нужни за независимо повтаряне“ описва завършен продукт. Без стъпки констатацията се превръща в спор, а не в задача. Някои констатации се съпротивляват на свеждане до стъпки — слабост в проектирането, непостоянно състояние на състезание (race condition) — и им е мястото в отчета, с ясно заявена несигурност; тревожен е липсата на стъпки при обикновените механични констатации. Попитайте: ще носи ли всяка използвана констатация стъпки и първични доказателства, договорно?

Обхват, който изброява активи, но не и роли. Назовава приложения и пътища на API и не казва нищо за потребителски роли, клиентски организации или тестови акаунти — най-надеждният признак за предложение, написано от човек, който не е тествал приложение отскоро. Външна оценка без удостоверяване няма роли; за всичко с вход пропускът е съществен. Попитайте: колко акаунта и клиентски организации са ви нужни, с какви роли и какво трябва да има в тях? Доставчик, който казва, че администраторски вход е достатъчен, вече ви е казал плана си.

„Нашият екип от експерти“ — и нищо по-конкретно. Разликата между компетентен старши тестер и младши, работещ по контролен списък, е по-голяма от всеки друг фактор, а в предложението е невидима. Вниманието на продажбите се съсредоточава върху представянето, докато изпълнението се обезпечава с когото се окаже свободен тази седмица. Доставчиците основателно избягват да назовават конкретни хора много напред, а екипите със смесено ниво са добра структура, тъй като младшите вършат отлична работа под преглед; обвържете стандарта, прегледа и отговорния водещ. Попитайте: кой извършва тази работа, на какво ниво и кой отговаря за качеството на отчета?

Твърдения за съответствие, които доставчикът не може да прави. Казва се, че ангажиментът ви прави съответстващи направо. Тестът произвежда доказателство, че даден контрол е бил оценен; дали това удовлетворява една рамка, зависи от обхвата, от оценителя и от вашата контролна среда — а провалът излиза наяве късно, когато дойде одитът и обхватът не покрива това, което стандартът е изисквал. „Този обхват покрива изискването за тестване в клауза X“ е законно; „това ще ви направи съответстващи“ е друго изречение. Попитайте: кое изискване доказва това и какво още изисква рамката?

Няколко по-кратки признака си заслужава да бъдат прегледани наред с горните. Всеки има и невинно четене, затова ги третирайте като въпроси, а не като заключения.

- Шаблонен текст, назоваващ технология, която не използвате, или име на друг клиент в колонтитул или в свойствата на файла. Шаблоните са разумни; шаблонен текст, който противоречи на вашата среда, подсказва, че и разделът за обхвата не е бил написан за вас. Попитайте кои части са написани за вас.
- График без място за преглед от колега — мястото, където критичността се коригира и втори четец пита дали констатацията е доказана или само предполагаема. Кратък срок може да отразява дисциплина, ако екипът пише, докато тества, затова попитайте кой преглежда отчета.
- Имена, които се променят между предложението и началния разговор, без обяснение.
- Гарантирани резултати — обещан брой констатации, обещание, че няма да има такива, или обещание, че ще преминете одит. Нито едно от тях не е във властта на тестера.
- Сертификат за съответствие като основен краен доклад, който твърди повече, отколкото тестването поддържа.
- Оценки на критичността без бизнес обосновка или примерен отчет, в който всичко е високо.
- Брой констатации, използван като търговско предимство — което възнаграждава количеството пред критичността и обикновено означава информационен шум.
- Тактики на натиск: оферта, която изтича тази седмица, или спешност, изкуствено създадена около датата на одита ви.
- Мълчание за работата с данни или нежелание да се подпише споразумение за неразкриване и за обработка на данни преди определянето на обхвата.

- Нежелание тестерите да бъдат поставени в една стая с вашите инженери.

Прилагайте всяко от тези неща и към нас. Ако предложение на PXLSec пристигне без посочена методология, без примерен отчет, без позиция по повторния тест, без споменаване на роли или с технология, която не използвате, задайте въпроса, който го разкрива. Доставчик, който си заслужава да бъде наеман, ще го приветства — и това включва нас.

Два модела си заслужава да се запомнят. Всички полезни въпроси търсят ясна граница: какво не е покрито, за какво няма време, къде спира методологията. Способните доставчици отговарят на тях спокойно; останалите посягат към успокоение. И отговорите принадлежат на заданието за работа, а не на бележките ви от разговора. Предложението е маркетинг; договорът е това, което сте купили.

5. Заданието за работа

Заданието за работа е единствената част от теста за проникване, която съществува преди самия тест. Всичко, което по-късно се обръква — активът, до когото никой не е имал право да се докосне, критичната констатация, изпратена в погрешната пощенска кутия, повторният тест, който се оказва платен — е било решено или оставено нерешено в този документ. Нищо от това не е противопоставяне: добрият доставчик ще повдигне половината от него, без да бъде подсецан, защото неяснотата отнема време и на него.

Обхват, времеви прозорец и правила на ангажимента

Обхватът трябва да се чете като инвентар, не като описание. „Клиентският портал и поддържащите го API“ не означава почти нищо на първата сутрин: две API-та не са били споменати, мобилният клиент говори с трето, а административният интерфейс стои на друго име на хост. Поискайте изключенията с същата точност, защото списъкът на извадените от обхвата е по-полезният от двата — той записва какво един разумен тестер иначе би приел за позволено.

- Изброени активи. Имена на хостове, диапазони от IP адреси, приложения заедно със средата им, базови пътища на API с прикачена спецификация, идентификатори на мобилни пакети, идентификатори на облачни акаунти. Там, където обхватът е диапазон, живите адреси в него се потвърждават, преди да бъде докоснато каквото и да е.
- Изключения, с причина за всяко. Отказ на услуга, социално инженерство, освен ако не е поръчано отделно, физически достъп, споделеният доставчик на идентичност. Установете дали всяко от тях е ваш избор или ограничение от страната на доставчика — това има значение, когато някой чете отчета като доказателство за покритие.
- Процес за промени. Кой може да разреши промяна, в какъв вид и какво се случва с усилието: разменено срещу нещо премахнато, добавено с бележка за промяна, или отложено. Без това тестерът разширява обхвата от добра воля и не му стига време за това, което ви е било важно.
- Активи, открити по време на теста. Правилното поведение е да се спре, да се докладва и да се попита, преди да се разшири обхватът, вместо той тихо да бъде разширен или откритото да бъде подминато. Нещо, достижимо отвътре на обхвата, но стоящо извън него, само по себе си е констатация: достижимостта се докладва, без да се използва това, което никога не е било разрешено.

- Времеви прозорец, не две дати. Начална дата, крайна дата, разрешените часове и часовата зона, като активното тестване се разграничава от периода на ангажимента, който включва отчитането и повторния тест. Датите за предаване и за повторния тест са отделни обвързвания.
- Производствена среда или тестова и разликите ѝ. Ако производствената среда е в обхвата — ограниченията: без разрушителни полезни товари, без промяна на данни отвъд доказването на констатация, без масова автоматизирана дейност срещу крайни точки с ограничена честота. Ако е тестова — съществени разлики, записани, защото именно те се превръщат в по-късния спор дали една констатация се прилага.
- Логистиката, която тихо изразходва време за тестване. Кога пристигат данните за достъп и кой потвърждава, че работят с обявеното ниво на права; кой отговаря за добавянето на адресите на източника в списъка с разрешения, за защитната стена и за защитата от ботове; дали в прозореца попада издание; и дали експлоатационният екип е бил уведомен.
- Посочено лице, което наистина може да даде разрешението. Ентусиазмът на ръководителя на проекта не е разрешение, а където обхватът включва активи, собственост на дружество от групата или на ваш клиент, разрешението трябва да дойде от действителния собственик. Насрещната клауза е също толкова важна: вашето изрично разрешение е това, което предпазва тестера от отговорност за неправилен достъп до компютърни системи, докато върши работата, която сте поискали.
- Разрешения от трети страни, с отговорник и краен срок. Проверете дали действащите условия за тестване на вашата облачна платформа позволяват планираната дейност; ограниченията са конкретни и се променят. Управляваният хостинг, компонентите като услуга в обхвата, доставчикът на плащания или споделената услуга за идентичност може всеки да изисква отделно разрешение. Тестването на платформа, за която само имате абонамент, без нейното съгласие, е неразрешен достъп до чужда система.

Правилата на ангажимента превръщат „тествайте системите ни“ в разрешено поведение. Посочете кои техники са разрешени и кои не. Атаките срещу данните за достъп са обичайният пример: разрешени ли са въобще, срещу кои интерфейси, с каква честота, срещу истински акаунти или само тестови? Блокирането на акаунти е действителен експлоатационен риск и отговорът не трябва да се измисля по време на ангажимента. Решете също дали е разрешено използване на уязвимостите или само демонстрация; дали повишаването на права и хоризонталното придвижване са в границите, след като бъде установена опорна точка; и колко действителни данни могат да бъдат извлечени като доказателство. Техниките, които променят данни, прекъсват услуга или блокират акаунти, заслужават собствено, изрично одобрение.

След това условията за спиране, при които тестването се преустановява незабавно: признаци, че тестването влошава работата на услуга, реални клиентски данни в среда, за която се предполага, че е тестова, признаци за активно проникване, или искане за спиране от посочено лице за контакт. Съчетайте всяко с път за уведомяване и посочен получател, защото условие за спиране без телефонен номер е изречение, не контрол. Поискайте и съгласуване — жив споделен канал, адресите на източника на тестера и познат хедър в трафика на инструментите — така че екипът ви по сигурността да може да попита „това вие ли бяхте?“ и да получи отговор в рамките на минути.

Когато бъде открито нещо сериозно

Сериозните открития са два отделни въпроса, а повечето документи не отговарят на нито един. Първият е ескалирането на критична констатация: ако тестер получи административен контрол или открие път без удостоверяване до нещо сериозно, искате да знаете същия ден. Договорете прага, времето до уведомяване, канала и посочени получатели с резервен вариант, и договорете какво прави тестерът след това — спира и чака указание, продължава другаде, или продължава да доказва въздействието. И трите са обосновани; нито едно не трябва да е изненада.

Вторият е доказателство за предходно проникване — уеб шелове, непознати планирани задачи, данни за достъп, използвани от страни места. Различна ситуация, различно третиране: тестването се спира на засегнатата система, уведомяването отива незабавно до посочено лице за инциденти, тестерът запазва, вместо да разстройва това, което е намерил, и ангажиментът може да бъде прекъснат, докато вие задействате реакцията при инциденти. Посочете кой може да разреши възобновяване и на кого се казва: на хората, които вие сте посочили, и на никой друг — уведомяването на клиентите ви или на регулатора е ваше решение.

Предавани документи, данни и какво значи „готово“

„Отчет“ не е спецификация. Специфицирайте го, както и останалото, което ангажиментът ви дължи.

- Самият отчет. Управленско резюме за нетехнически читател; технически констатации, даващи за всеки проблем засегнатия актив, оценка на критичността с посочен метод на оценяване, основната причина, стъпки за възпроизвеждане, достатъчни инженерът ви да го възпроизведе без помощ, доказателство и конкретен съвет за отстраняване; изявление за покритието, записващо всичко в обхвата, което не е било достигнато; и пътищата на атака, които тестерът е проучил и отхвърлил, защото да знаете, че нещо е било тествано и не е проработило, е увереност, за която сте платили.
- Формати, права за споделяне и хора. Дали се предоставят първичните доказателства или само се споменават, и с кого може да бъде споделен отчетът — повечето купувачи в един момент дават такъв на клиент, одитор или застраховател, затова договорете това сега. След това кой върши работата: нивото на разпределените хора, посочен водещ, отговорен за качеството при представянето на резултатите, и предварително писмено съгласие, преди която и да е част да бъде възложена на подизпълнител.
- Повторен тест, в шест части. Включването и за чия сметка; прозорецът и дали този срок е реалистичен спрямо вашия цикъл на издания; покритието, тъй като повторен тест, ограничен до критичните, оставя средните постоянно непроверени; резултатът — преиздаден отчет или отделно потвърждение; кой го извършва, защото първоначалният тестер разпознава поправка, която само премества проблема; и дали частичното отстраняване се отчита като разрешено, ограничено или отворено, защото тези думи означават различни неща за един оценител.
- Работа с данните. Къде се съхраняват данните от ангажимента, в кои юрисдикции и дали са шифровани в покой; кой вътрешно има достъп до тях и дали достъпът се регистрира; как се предава отчетът, което трябва да означава изтегляне с удостоверяване или шифрована поща, а не незащитен прикачен файл; срокът на съхранение, с разграничение между отчета и първичните доказателства; и какво се унищожава, кога, с писмено потвърждение. Поискайте условия за обработка и посочени подизпълнители по обработката, където в обхвата попадат лични данни.

- Отговорност, с прости думи. Професионална и обща гражданска отговорност на обявено ниво, киберотговорност, ако има такава, таванът и изключенията. Повечето споразумения изключват последващите вреди и прекъсването на дейността, което е нормално, но си заслужава да се знае, тъй като прекъсване, причинено по време на тестване, може да попадне в изключена категория.
- Определение за „готово“. Обхватът е тестван до договорената дълбочина или пропуските са документирани с причини; предаваните документи са получени в указаните формати; проведено е представяне на резултатите с техническия ви екип; повторният тест е извършен или планиран; унищожаването на данните е потвърдено писмено. Плюс срок за приемане, в който могат да се нанасят фактически корекции и да се оспорва критичност, тъй като критичност, която изглежда погрешна, обикновено е пропуск в контекста.

Прилагайте всичко това и към нас. Ако PXLSec ви предаде задание за работа, което оставя някой от тези въпроси открит, попитайте. Нашите правила на ангажимента са публикувани в пълния си вид, вместо да се пазят в договора, именно за да можете да вземете полезното в собствения си документ и да държите всеки тестер отговорен по него — включително нас.

И едно последно нещо преди първия ден. Ангажиментите рядко се провалят, защото тестерът е бил слаб; провалят се, защото първата част е била прекарана в чакане. Тестването е натрупващо се — тестерът държи модел на системата в главата си и губи време да възстановява контекста след всяко прекъсване — така че загубеното време не се връща по-късно. Планирайте и капацитет за отстраняване, преди отчетът да пристигне: отчетите стоят неразгледани не защото никого не го интересува, а защото никой няма заделено време.

6. Как да прочетете отчета, който получавате

Добрият отчет е написан, за да се действа по него, а не за да бъде подреден в папка. Но повечето хора, които получават такъв, никога не са били учени как да го четат — а разделите, които изглеждат най-авторитетни — таблицата с критичността, оценките — са тези, които най-вероятно ще ви накарат да поправяте неща в погрешен ред. Отчетите се различават по стил, но завършеният отчет има едни и същи части.

- Резюме за ръководството. Общият риск и повтарящите се теми, написани за човек, който няма да чете по-надолу и не би трябвало да му се налага.
- Обхват на ангажимента. Цели, вид на оценката, времеви прозорец, стандарти, изключения и допусканията, от които зависи резултатът — частта, която определя колко струва всичко останало.
- Методология. Какво систематично е покрило тестването и разделението на труда между автоматизацията и хората.
- Оценки на критичността. Скалата и как една оценка информира дадена степен, без да я замества.
- Обобщение на констатациите. Една таблица, подредена по това какво да се направи първо, а не по реда, в който нещата са били открити.
- Подробни констатации. Описание, доказателство, възпроизвеждане, въздействие и конкретна препоръка за всяка. Частта, по която си заслужава да съдите една фирма.

- Повторен тест и приключване. Какво е покрил повторният тест и какво заявява писмото за приключване, включително това, което умишлено не заявява.
- Приложения. Използваните инструменти и какво е било извън обхвата и колко струва това на увереността.

Четете ги в неинтуитивен ред: обхват и методология, после резюмето за ръководството, после подредбата за отстраняване, и едва тогава отделните констатации. Извлечете първо три факта от раздела за обхвата: какво е било в обхвата, какъв достъп е имал тестерът и какво според отчета не е било достигнато. Последното е най-ценното изречение в повечето отчети и най-често прескачаното, защото липсата на констатации в област, която никой не е отворил, не е резултат.

„Тествахме това и не открихме нищо“ и „не стигнахме до това“ произвеждат едно и също празно място в таблицата с констатациите и означават противоположни неща. Ако отчетът ви не ги разграничава, попитайте на разговора по резултатите.

От резюмето вземащият решение иска четири неща и нито едно от тях не е число. Темите, защото добрите резюмета назовават модели, вместо да изброяват проблеми — оторизация, налагана непоследователно в различните услуги, валидация, приложена на интерфейса, но не и на API. Най-лошият реалистичен изход, тоест какво наистина би могъл да постигне нападател, а не най-високият етикет за критичност. Дали нещо изисква действие тази седмица. И при повторен ангажимент — дали същите първопричини се появяват отново в нов код, което е констатация за процеса и няма да е в таблицата с констатациите.

Критичността и защо оценката е информативна, а не решаваща

Етикетите за критичност съществуват, за да можете бързо да подредите дълъг списък, и обикновено се извеждат от CVSS — рамка, която оценява присъщите характеристики на една уязвимост: как се достига до нея, колко трудно се използва, какви права изисква и какъв е ефектът ѝ върху конфиденциалността, целостта и наличността. Тази рамка е полезна и умишлено не отчита контекста, затова не е оценка на риска. CVSS не знае, че засегнатият компонент съдържа данни на картодържатели или че един маршрут е достъпен от интернет, докато идентичен дефект стои зад VPN. Затова „средна“ във вашия процес на плащане рутинно има по-голямо значение от „висока“ във вътрешен инструмент.

Това е нашата публикувана скала и реакцията, която всяко ниво очаква. Сравнете я с тази на вашия доставчик, ако той публикува такава.

- **Critical.** Незабавно, тежко бизнес въздействие и лесно за използване — обикновено без удостоверяване и надеждно, водещо директно до загуба на данни, финансова загуба или контрол над средата. Поправете веднага: ескалирайте същия ден и ограничете риска, ако пълната поправка отнема време.
- **High.** Значително въздействие и реалистична възможност за експлоатация, макар да може да изисква позиция, акаунт или предварително условие. Често решаващото звено във верига. Поправете в текущия цикъл; не го допускайте в общия списък със задачи.
- **Medium.** Умерено въздействие или сериозно въздействие, което зависи от условия извън пълния контрол на нападателя. Планирайте отстраняване с договорен срок в следващия цикъл или два.

- Low. Ограничено пряко въздействие — закаляване и защита в дълбочина, полезно за нападател главно в комбинация. Планирайте го наред със свързаната работа.
- Informational. Няма пряко въздействие върху сигурността; наблюдение или отклонение от добрата практика. Действайте по ваша преценка.

Три фактора превръщат етикета в решение: стойността на това, което е изложено, достижимостта и възможността за свързване във верига — защото самостоятелната критичност може да е ниска, докато приносът към една верига е решаващ. Разкриване, което изтича валидни потребителски имена, е незначително само по себе си и съществено за път за подбор на изтекли данни за достъп. Веригите са и мястото, където таблиците с критичност подвеждат най-много: три средни констатации, които се сглобяват в завладяване на акаунт, са критичен проблем, описан на три места — и добрият отчет излага последователността и назовава най-евтиното звено за прекъсване. Затова третирайте колоната с критичността като ред за подреждане, а познанията си за бизнеса — като решаващия вход.

Как да различите истинска констатация от ехо на скенер

Разликата между тест за проникване и сканиране с титулна страница се вижда в самите констатации. Питайте какво е демонстрирал авторът. Истинската констатация има четири свойства.

- Специфична за вашата система. Назовава крайната точка, параметъра, ролята, идентификатора на обекта. Ехото е общо, написано за класа уязвимост, а не за вашия конкретен случай.
- Показва резултата, не задействането. „Отразените входни данни бяха върнати без екраниране“ е задействане; „изпращането на този полезен товар като удостоверен потребител предава сесийния токен към външен хост“ е резултат. Отчетите, произлезли от скенер, спират при задействането, защото инструментът спира там.
- Въздействие на вашия език. Не „може да доведе до разкриване на информация“, а „удостоверен клиент може да изтегли фактурите на друг клиент, включително име, адрес и история на плащанията“. Второто може да бъде отнесено до продуктов отговорник; първото — не.
- Препоръка, която може да бъде приложена — какво да се промени и къде: тази валидация принадлежи от страна на сървъра в този обработчик, тази проверка трябва да се премести в слоя на данните. Ехото казва „въведете подходяща валидация на входните данни“.

Още два признака: констатациите, базирани само на версия, са кандидати, а не заключения — законни като наблюдение за обновяване, но не доказателство за използваемост, освен ако тестерът не го е потвърдил; а записаните опровержения са силен положителен знак, защото „опитахме да заобиколим филтъра за клиентски организации по тези три маршрута, всички наложени правилно“ е увереност и показва, че тестерът е знаел какво да опита.

Доказателството съществува, за да може една констатация да издържи при несъгласие, а проверката е дали някой от вашите инженери, разполагайки само с отчета и нищо друго, би могъл да възпроизведе проблема и след това да потвърди поправката. Достатъчното доказателство е пълно — цялата заявка и отговор, включително хедърите и мястото на токена, които карат заявката да работи, а не изрязана снимка на екрана. То е проследимо: ясно е кой акаунт, роля и клиентска организация е действал, което е целият смисъл при констатация за контрол на достъпа. И е повторяемо, в номерирани стъпки от обявено начално състояние.

Следете и за липсващо отрицателно доказателство: констатацията трябва да показва както че достъпът е успял, така и че системата е трябвало да го предотврати.

Триаж, подреждане и повторният тест

Работете в този ред. Първо, поправете всичко, което води директно до компрометиране на акаунт или данни — заобикаляне на удостоверяването, нарушен контрол на достъпа, излагаш записите на други клиенти, изпълнение на код от разстояние, разкрити данни за достъп. Ако пълната поправка ще отнеме седмици, ограничете риска сега и го запишете като ограничаване, не като разрешаване. Второ, групирайте по първопричина: най-ефективният наличен ход и този, който най-често се прескача. Дванадесет констатации в различни крайни точки често се свеждат до три причини, например оторизация, проверявана в контролера вместо в слоя на данните. Поправянето на причината затваря всеки отделен случай; поправянето на дванадесет поединично гарантира тринадесети. Трето, прекъснете най-евтиното звено във всяка верига. Четвърто, групирайте останалото по отговорник и по внедряване.

Пето, решете изрично какво няма да поправяте. Някои констатации ще бъдат приети, вместо отстранени, защото компонентът предстои да бъде изведен от употреба или поправката струва повече от изложеността. Законно е, но трябва да бъде писмено решение с отговорник и дата за преглед: „никога не стигнахме до това“ и „оценихме го и го приехме“ са много различни отговори за един одитор. През цялото време следете констатациите в системата, която вече ползвате за инженерна работа, с номера от отчета на всяка задача. Отделна таблица за сигурността остарява в рамките на месец.

Повторният тест превръща отчета в промяна на позицията ви по сигурността, а правилно направеният потвърждава три неща за всяка констатация. Че първоначалните стъпки за възпроизвеждане вече не работят. Че е адресирана първопричината, а не отделният случай, защото поправка, приложена към една крайна точка, докато шаблонът остава другаде, не затваря констатацията. И че поправката не може да бъде заобиколена елементарно — валидация, добавена от страна на клиента, докато API-то все още приема заявката, или крайна точка, премахната от интерфейса, но останала жива. Очаквайте ясен статус за всяка констатация: разрешена, частично разрешена, ограничена или отворена.

Използвайте разговора по резултатите за това, което не се вписва в документ. Поставете в стаята разработчиците, които отговарят за засегнатия код, и питайте как е била открита всяка констатация, защото това се пренася по-нататък от самата констатация. Четири въпроса си заслужават мястото: кое е най-важното нещо за поправяне тази седмица; кои констатации са навързани; коя констатация е най-вероятно да поправим погрешно; и какво не сте имали време да тествате. Третият спестява един провален повторен тест.

Пазете комплекта заедно: отчета, потвърждението от повторния тест, решенията за приемане на риск с техните отговорници и дати, и бележката какво не е било тествано. Този комплект отговаря на почти всеки въпрос, който задава одитор или проверяващият сигурността на клиент. Едно нещо, което той не е, е сертификат: отчетът описва какво е било открито, в определен обхват, през определен период — всеки, който го представя като гаранция за сигурност, го представя погрешно, включително ние.

7. Контролен списък преди подписване

Една страница, за срещата. „Не е приложимо“ е добър отговор; празно поле не е. Преминаването през него с готов да съдейства доставчик е най-евтиният час от целия ангажимент.

Преди да се обърнете към когото и да е

- ✓ Въпросът, на който този отчет трябва да отговори, написан в едно изречение, и кой го чете
- ✓ Дълбочина: проверено сканиране, ръчно тестване с ограничено време, водено от цели, или симулация на противник
- ✓ Рамката и контролът, които тестът трябва да докаже, ако има такива
- ✓ Списък на активите, групирани по обща рамка, шлюз и модел на оторизация
- ✓ Матрица на ролите и правата, с назовани двойки, които не трябва да се достигат
- ✓ Модел на обслужване на множество клиентски организации, облачни акаунти, вътрешни подмрежи и дали Active Directory е в обхвата
- ✓ Какво можете да предадете: данни за достъп, документация, спецификация на API, изходен код
- ✓ Ограничения, които не можете да премахнете: времеви прозорци, контрол на промените, периоди на забрана

От всеки доставчик, писмено

- ✓ Кой тества, на какво ниво, с какви практически квалификации и кой преглежда констатациите му
- ✓ Пълен анонимизиран примерен отчет, включително страниците с подробности
- ✓ Как се разделя усилието между практическо тестване и сканиране, триаж и отчитане
- ✓ Един пример за констатация, която никой скенер не би могъл да произведе
- ✓ Колко роли се използват и дали се тества хоризонталният контрол на достъпа наред с вертикалния
- ✓ Дали се покрива цялото приложение или извадка и как научавате какво не е било достигнато
- ✓ Как се съобщават критичните констатации по време на теста, на кого и колко бързо
- ✓ Повторен тест: включен ли е, за кои констатации, колко преминавания, в какъв прозорец и тестват ли се заобикаляния
- ✓ Дали някоя част се възлага на подизпълнител и дали ще подпишат първо вашите споразумения за неразкриване и за обработка на данни

-
- ✓ Какво биха ви казали, ако този ангажимент беше грешното нещо за купуване

В заданието за работа

-
- ✓ Обхват, изброен, а не описан, и всяко изключение с причина
-
- ✓ Процес за промени: кой одобрява, по какъв канал и как се коригира усилено
-
- ✓ Дати на тестване, разрешени часове и часова зона, с отделно посочени отчитане и повторен тест
-
- ✓ Продукционната среда включена или не, и ограниченията; ако е тестова — документираните разлики
-
- ✓ Разрешени и забранени техники, включително атаки срещу данните за достъп и странични ефекти, видими за клиентите
-
- ✓ Условия за спиране, всяко с посочен получател и канал, плюс данни за съгласуване
-
- ✓ Посочено лице с правомощия над активите и разрешения от трети страни, разпределени със срокове
-
- ✓ Праг за критични констатации и получатели, с третирането на предходно проникване като отделна клауза
-
- ✓ Предавани документи, изброени по формат, съдържание за всяка констатация и изявление за покритието
-
- ✓ Работа с данните: местоположение, юрисдикция, шифроване, срок на съхранение, потвърдено унищожаване
-
- ✓ Определение за „готово“ и срок за приемане, в който се нанасят корекции и се оспорва критичност

Преди първия ден

-
- ✓ По един работещ акаунт за всяка роля, в който човек е влязъл с правилното ниво на права
-
- ✓ Две клиентски организации или по два акаунта за всяка роля, с различни въведени данни
-
- ✓ Адресите на източника, добавени в списъка с разрешения през защитната стена, защитата от ботове и ограничителя на честотата
-
- ✓ Стабилна среда, в която не влиза издание по средата на теста, и документация, изпратена, а не обещана
-
- ✓ Посочено техническо лице за контакт, което може да действа, а не само да предава, и уведомен експлоатационен екип за прозореца
-

- ✓ Определени отговорници за отстраняването и предварителна дата за повторния тест в календара

Когато отчетът пристигне

- ✓ Какво е било в обхвата, какъв достъп е имал тестерът и какво според отчета не е било достигнато
- ✓ За всяка констатация: специфична за вашата система, резултат вместо задействане, въздействие на вашия език, приложима поправка
- ✓ Доказателство, което е пълно, проследимо, ограничено и повторяемо от обявено начално състояние
- ✓ Преподреждане според стойността на изложеното, достижимостта и възможността за свързване във верига
- ✓ Първо пътищата до компрометиране, после групиране по първопричина, после веригите, после партидите
- ✓ Приетите рискове, записани, с отговорник и дата за преглед
- ✓ Повторният тест потвърждава, че стъпките се провалят, че първопричината е поправена и че поправката не може да бъде заобиколена елементарно
- ✓ Отчетът, потвърждението от повторния тест, приемането на рискове и бележката за нетестваното, пазени заедно

Клаузите, които изглеждат като бюрокрация — условия за спиране, пътища за ескалация, прозорци за повторен тест, определение за „готово“ — са тези, които решават дали ще стигнете до поправени системи или до подреден в папка документ. Прилагайте всеки въпрос от този наръчник към PXLSec, както и към всеки друг, когото обмисляте. Доставчик, който си заслужава да бъде наеман, ще го приветства.

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331