Bezpieczeństwo i zgodność

Jak widać, większość łańcuchów bloków jest zdecentralizowana, a tożsamość każdej ze stron jest zwykle chroniona; jednak większość kodu związanego z blockchainem wiąże się z przechowywaniem pewnych poufnych danych, takich jak dane osobowe użytkownika, hasła, kryptowaluta i portfele. Kod związany z blockchainem ma cechy, które sprawiają, że jest magnesem dla hakerów.

- Kod jest zwykle open source dla przejrzystości i promowania współtwórców.

- Znaczna część kodu nie jest wystarczająco dojrzała, aby można go było uznać za stopień zwolnienia.

- W łańcuchach bloków związanych z kryptowalutami utrata danych może oznaczać coś więcej niż zwykłe naruszenie prywatności. Po przeniesieniu środków nie jest łatwo je śledzić, a transfer prawdopodobnie będzie nieodwracalny.

Obawy te zostały spotęgowane, ponieważ technologia blockchain stała się bardziej popularna i coraz więcej osób inwestuje w blockchain. W rzeczywistości pojawia się coraz więcej doniesień o stratach związanych z blockchainem, a nowe ataki są publikowane w serwisach informacyjnych niemal codziennie. Na przykład podczas pisania tej książki z giełdy Binance skradziono 40 milionów dolarów. Ponadto w ciągu ostatnich 12 miesięcy skradziono około 23 miliony dolarów w wyniku ataków z podwójnymi wydatkami. Podobnie z giełd kryptowalut skradziono oszałamiające 1,5 miliarda dolarów. Raporty pośmiertne czasami pokazują wyrafinowaną metodę napadu, której trzeba być geniuszem, aby zapobiec. Jednak większości ataków można łatwo zapobiec i są one niczym innym jak zwykłym przeoczeniem lub wynikiem nieużywania narzędzi zdolnych do ujawnienia luk w zabezpieczeniach.

„Intelektualiści rozwiązują problemy; geniusze im zapobiegają". -Albert Einstein

Jako profesjonaliści, Twoim obowiązkiem wobec klientów, którzy pokładają w Tobie zaufanie, a także Twojej reputacji i odpowiedzialności powierniczej, jest złagodzenie tego ryzyka i zapewnienie ochrony danych. Środki bezpieczeństwa należy rozważyć na wszystkich etapach cyklu rozwoju; w rzeczywistości bezpieczeństwo powinno być najważniejszym aspektem Twojego rozwoju. Jednak nierealistyczne jest założenie, że będę w stanie omówić wszystkie aspekty bezpieczeństwa w jednym rozdziale, ponieważ znanych jest tysiące konkretnych ataków. Oprócz bezpieczeństwa kolejnym aspektem, którym należy się zająć, są regulacje. Organy regulacyjne kształtują technologię ogólnie, a branżę blockchain w szczególności, i istnieje wiele przepisów, których należy przestrzegać w każdej lokalizacji geograficznej. Ponieważ nowe ataki są wymyślane codziennie, przepisy regulacyjne są często weryfikowane. Zrozumienie typowych ataków, zabezpieczeń, prywatności, zgodności i przepisów może być trudnym zadaniem. W tej części przedstawię Ci wgląd w sposób myślenia o bezpieczeństwie i pomogę Ci stać się bardziej świadomym bezpieczeństwa, prywatności i zgodności. Ta część jest podzielona na trzy części.

• Gotowość w zakresie bezpieczeństwa: omówię obszary, które powinieneś wziąć pod uwagę przed iw trakcie rozwijania swojej platformy.

• Typowe ataki typu blockchain: omówię niektóre z najbardziej znanych i powszechnych ataków typu blockchain.

• Cykl rozwoju: Przekażę Ci zalecany cykl rozwoju, dzięki czemu możesz wziąć pod uwagę bezpieczeństwo i zgodność.

W szczególności omówię wymagania dotyczące testowania bezpieczeństwa, prywatności i zgodności, aby upewnić się, że Twój kod uwzględnia jak najwięcej scenariuszy, aby pomóc zabezpieczyć dane użytkowników. Omówię typowe cyberataki związane z blockchainem, które spowodowały duże straty,

a także ataki specyficzne dla sieci blockchain. Omówię, w jaki sposób można było zapobiec tym atakom jako użytkownik i jako programista. Na koniec przedstawię zalecany cykl rozwoju, który możesz zastosować, aby zmniejszyć ryzyko strat i wyłączenia platformy.

Gotowość do bezpieczeństwa i zgodności

W tej sekcji omówię ogólne obszary, które należy wziąć pod uwagę w odniesieniu do testowania bezpieczeństwa i co to oznacza osiągnięcie gotowości bezpieczeństwa. Dodatkowo zrozumiesz, co to znaczy osiągnąć gotowość do zapewnienia zgodności, patrząc na przepisy w Europie i Stanach Zjednoczonych jako przykłady. Na koniec zwrócę uwagę na zalecenia, które powinieneś rozważyć podczas cyklu rozwoju i przed wydaniem kodu.

Gotowość do bezpieczeństwa

W tradycyjnym środowisku kodowania należy wziąć pod uwagę testy bezpieczeństwa, aby znaleźć defekty bezpieczeństwa w kodzie, aby upewnić się, że działa on poprawnie, zgodnie z przeznaczeniem, a dane są chronione.

Uwaga : Testowanie bezpieczeństwa to proces mający na celu znalezienie defektów bezpieczeństwa w kodzie, aby upewnić się, że zarówno kod, jak i dane działają zgodnie z przeznaczeniem.

Testy bezpieczeństwa obejmują następujące środki:

- Poufność: zapewnienie ochrony informacji użytkownika. Przykładem jest implementacja obszaru tylko dla członków za połączeniem Secure Sockets Layer (SSL), które wykorzystuje szyfrowanie danych przesyłanych przez Internet.

- Integralność informacji: ochrona informacji przed zmianą. Przykładem jest szyfrowanie i odszyfrowywanie danych, które przechodzą między różnymi warstwami systemu.

- Uwierzytelnianie: Potwierdzenie tożsamości użytkownika oraz zapewnienie zaufania do systemu. Przykładem jest system logowania.

- Dostępność: zapewnienie, że system jest sprawny i działa. Przykładem jest zainstalowanie zapory, aby zapobiec atakowi.

- Autoryzacja: zapewnienie, że zlecający może otrzymać usługę lub wykonać działanie. Przykładem jest utworzenie łańcucha bloków z uprawnieniami Hyperledger, który ogranicza dostęp do określonej jednostki.

- Niezaprzeczalność: zapewnienie systemu potwierdzania podczas wysyłania i odbierania wiadomości, aby strony nie mogły odmówić otrzymania wiadomości. Przykładem jest powiadomienie e-mail wysyłane w celu potwierdzenia przeniesienia zasobów cyfrowych.

Gotowość do zapewnienia zgodności

Oprócz tych tradycyjnych rozważań dotyczących testowania bezpieczeństwa, należy również wziąć pod uwagę bezpieczeństwo specyficzne dla łańcucha bloków i zgodność lokalną, aby upewnić się, że Twoja platforma jest zgodna z wymogami regulacyjnymi.

Uwaga : Zgodność z zabezpieczeniami jest problemem prawnym dla podmiotów. Jest to norma regulacyjna dotycząca udzielania zaleceń dotyczących prywatności, a także poprawy bezpieczeństwa.

Zgodność nie koncentruje się bezpośrednio na bezpieczeństwie; jednak wiele lokalnych wymagań dotyczących zgodności uwzględnia bezpieczeństwo i zapewnienie ochrony zarówno użytkownika, jak i

danych, więc pośrednio są one ze sobą powiązane. Wiele dużych firm zatrudnia zarówno ekspertów ds. bezpieczeństwa, jak i zgodności, aby zapewnić spełnienie obu. Być może zastanawiasz się, dlaczego w ogóle muszę brać pod uwagę przepisy? Czy blockchain nie miał być zdecentralizowany? To prawda; jednak w ostatnich latach wprowadzono regulacje przeciwko operatorom blockchain z powodu ciągłych oszustw i ataków, co skutkowało znacznymi stratami, a w wielu krajach wprowadzono polityki prywatności i środki bezpieczeństwa. W rezultacie musisz sprawdzić przepisy dotyczące zgodności i bezpieczeństwa, aby upewnić się, że nie naruszasz żadnych przepisów. W rzeczywistości wiele instytucji i organów opublikowało prace badawcze w celu przeanalizowania związku między blockchainem a przepisami dotyczącymi ochrony danych oraz przygotowania do osiągnięcia „gotowości do zapewnienia zgodności".

Uwaga : Gotowość do zapewnienia zgodności zapewnia, że wdrożenie spełnia wymagania dotyczące zarządzania. Blockchain nie jest wyłączony z żadnych obowiązujących praw i przepisów w wielu lokalizacjach na całym świecie.

Na przykład w Europie i Stanach Zjednoczonych istnieje zgodność przepisów i polityki związane z oceną skutków dla ochrony danych (DPIA) i ogólnym rozporządzeniem o ochronie danych (RODO), które szczegółowo opisują, jakie informacje nie mogą być przechowywane w łańcuchu bloków. Nie chodzi jednak tylko o to, jakie dane mogą i nie mogą być przechowywane; wiele krajów wdrożyło przepisy dotyczące prywatności, które ograniczają rodzaj danych, które mogą być przesyłane poza granice geograficzne. W przeciwieństwie do wielu członków społeczności blockchain, którzy uważają, że przepisy dotyczące zgodności są wprowadzane wyłącznie w celu ograniczenia i kontrolowania technologii blockchain przed zastąpieniem tradycyjnych instytucji, wiele zasad ma na celu ochronę inwestorów przed stratami, a także ochronę prywatności użytkownika. Ponadto w niektórych krajach obowiązują przepisy ustawowe i wykonawcze wymagające prowadzenia ewidencji i przechowywania danych użytkowników w celu zapobiegania oszustwom, praniu pieniędzy i terroryzmowi. Na przykład w 2013 r. w Stanach Zjednoczonych ustawa o tajemnicy bankowej z 1970 r. (BSA) i FinCEN wydały wytyczne dla giełd i ICO, klasyfikując je jako firmy świadczące usługi pieniężne (MSB), które wymagają rejestracji, raportowania i przepisów dotyczących prowadzenia dokumentacji. Oznacza to, że w Stanach Zjednoczonych giełdy i ICO muszą zarejestrować się w FinCEN jako MSB. Ignorowanie zgodności może prowadzić do wezwania do sądu, kar finansowych, zamknięcia, a nawet oskarżeń karnych. Na przykład w Europie RODO określiło termin spełnienia określonych wymogów. Firmy, które nie są w stanie tego przestrzegać, ryzykują wysoką grzywną. Dotyczy to urządzeń mobilnych, aplikacji telewizyjnych, portali internetowych, witryn internetowych, interfejsów API i przechowywania w chmurze. W rzeczywistości w 2019 r. CNIL nałożył na Google grzywnę w wysokości 50 milionów euro. Innym przykładem jest uwięź monety stabilnej, która w momencie pisania tego tekstu została zlecona przez Sąd Najwyższy Nowego Jorku w celu zamrożenia transferów swojej monety na giełdzie Bitfinex. Każda lokalizacja geograficzna podlega określonym wymaganiom dotyczącym obsługi technologii blockchain, dlatego ważne jest, aby być świadomym przepisów prawa, zasad bezpieczeństwa i prywatności wprowadzonych przed opracowaniem oprogramowania. W rzeczywistości każdy regulator granic geograficznych może ustalać własne zasady. Jeśli weźmiesz za przykład Stany Zjednoczone i Europę, każde z nich ma inne zasady dotyczące blockchain, a jeśli masz chociaż jednego gościa z tych krajów, powinieneś przestrzegać tych przepisów. W tej części przyjrzysz się jako przykład Stanom Zjednoczonym i Europie; jednak należy sprawdzić każdą konkretną granicę geograficzną pod kątem określonych zasad obowiązujących lokalnie.

Zgodność ze Stanami Zjednoczonymi

W Stanach Zjednoczonych obowiązują przepisy bezpieczeństwa i przepisy dotyczące przelewów pieniężnych, które wymagają przestrzegania określonych przepisów stanowych, a w przypadku

przesyłania kryptowalut może być konieczne złożenie wniosku o licencję stanową. Organami zajmującymi się technologiami związanymi z blockchain w Stanach Zjednoczonych są Komisja Papierów Wartościowych i Giełd (SEC) oraz Alternatywne Systemy Obrotu (ATS). W chwili pisania tego tekstu SEC postrzega zarówno początkowe oferty monet (ICO), jak i oferty tokenów zabezpieczających (STO) jako papiery wartościowe. W związku z tym podlegają przepisom ustawy o giełdzie papierów wartościowych z 1934 r., która określa sposób przenoszenia papierów wartościowych między podmiotami. Na przykład SEC wymaga, aby giełdy rejestrowały się na krajowej giełdzie papierów wartościowych i/lub ATS.

Wskazówka : STO i ICO są uważane za papiery wartościowe w Stanach Zjednoczonych; jednak STO są bardziej modne wśród inwestorów niż ICO, ponieważ wiele ICO zostało zmuszonych do zwrotu inwestorów w 2018 i 2019 roku.

Giełdy wiążą się również z określonymi przepisami; na przykład giełdy, które zajmują się instrumentami pochodnymi, muszą zarejestrować się w Commodity Futures Trading Commission (CFTC) jako giełda CFTC lub wyznaczony rynek towarowy (DCM) ze względu na ustawę o giełdach towarowych z 1936 r. (CEA).

Zgodność z Unią Europejską

Unia Europejska jest w trakcie wdrażania określonych wymagań dla rynków blockchain i kryptowalut; wymagania te będą uwzględniać protokół znany jako Know Your Client (KYC) i przepisy dotyczące przeciwdziałania praniu pieniędzy (AML). W odniesieniu do zasobów cyfrowych rozporządzenie Unii Europejskiej nie sprzeciwia się obecnie giełdom kryptowalutowym i fiat-kryptograficznym. Większość obaw dotyczy upewnienia się, że krypto nie jest wykorzystywane do finansowania nielegalnych działań, takich jak pranie pieniędzy i terroryzm. Aby wziąć pod uwagę te obawy, platformy kryptograficzne muszą dołożyć należytej staranności wobec klientów i zgłaszać wszelkie podejrzane transakcje zgodnie z KYC.

Wskazówka : przepisy często się zmieniają; wypatruj wiadomości i informacji publikowanych przez SEC, EUBOF i inne organizacje, w których publikowana jest Twoja platforma. Jeśli korzystasz z mediów społecznościowych, obserwuj konta tych organizacji lub dodawaj aktualizacje wiadomości do swojej listy czytelniczej.

Zalecenia dotyczące gotowości

Mając świadomość, możesz osiągnąć zarówno zgodność, jak i gotowość do zapewnienia bezpieczeństwa, aby upewnić się, że Twoja platforma jest gotowa do produkcji i zapobiec wyłączeniu przez napastników lub instytucje rządowe. Nie ma dokładnego zestawu reguł, których można użyć globalnie, aby zapewnić gotowość, ponieważ zgodność różni się między granicami geograficznymi; istnieją jednak pewne kluczowe elementy, które stanowią dobrą praktykę i mogą pomóc w przygotowaniu się do zapewnienia bezpieczeństwa i zgodności. W następnych sekcjach omówię konkretne ataki; te ogólne zalecenia to podstawowe zalecenia, które należy wziąć pod uwagę podczas tworzenia aplikacji.

- Lokalizacja geograficzna: jeśli zamierzasz zarejestrować choćby jednego użytkownika na swojej platformie, musisz być gotowy w lokalizacji tego użytkownika i znać obowiązujące tam zasady i przepisy.

- Rozwiąż problem: Upewnij się, że faktycznie rozwiązujesz problem. Zadaj sobie pytanie, jaka jest moja wyjątkowa propozycja sprzedaży (USP)? Nie korzystaj tylko z blockchaina, aby uzyskać dostęp do

szumu. Impreza ICOs 2017 dobiegła końca, ponieważ wiele monet zostało usuniętych z giełdy, a ICO zostały zmuszone do zwrotu pieniędzy inwestorom.

- Blockchain oparty na pozwoleniach: Jeśli budujesz pozwolenie-oparte na blockchain, powinieneś zdefiniować role członków, takich jak administrator, wydawcy, użytkownicy i tak dalej.

- Prywatność: Jeśli chodzi o dostarczanie informacji o użytkowniku, im więcej, tym lepiej. Poinformuj swoich użytkowników jak najwięcej o sprawach związanych z prywatnością. Kiedy zbierasz dane, im mniej tym lepiej; uchwyć tylko to, czego potrzebujesz. Poniżej znajdują się konkretne zalecenia dotyczące prywatności.

Wskazówka : na podstawie raportów z CNIL, NIST i EUBOF zaimplementuj swój kod zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO).

• Polityka prywatności: Ustaw politykę prywatności i poinformuj użytkownika, jakie informacje są przechowywane i jakie informacje są udostępniane stronom trzecim. Na przykład poinformuj użytkowników o logowaniu danych do narzędzia analitycznego w swojej polityce prywatności.

• Anuluj subskrypcję: opublikuj formularz lub adres e-mail w celu uzyskania zgody, wycofania i skarg związanych z polityką prywatności na swojej platformie.

• Zmiany polityki: Poinformuj użytkownika o wszelkich zmianach polityki prywatności.

• Zbieranie danych użytkowników: Przyjmuj minimalistyczne podejście podczas zbierania wszystkich informacji o użytkownikach; przechowuj tylko to, co jest potrzebne.

• Zebrane dane: Podziel dane na dane potrzebne do obsługi platformy i inne zebrane dane.

• Anonimizacja: Rozważ wdrożenie swojej platformy z pełną anonimizacją.

• Lokalizacja geograficzna: Podczas przechowywania danych upewnij się, że są one gromadzone zgodnie z wytycznymi w tej lokalizacji geograficznej.

• Pozwolenie: Poproś użytkownika o pozwolenie na przechowywanie dowolnych danych, takich jak pliki cookie, lokalna baza danych lub chmura.

* Wyczyść wszystko: Wyczyść pliki cookie, sesje i inną pamięć po wylogowaniu się użytkownika. Zezwalaj użytkownikowi na usuwanie danych z wszelkich narzędzi innych firm używanych na Twojej platformie.

• Wyczyść: Zezwalaj użytkownikowi na usuwanie danych i czyszczenie historii.

• Eksportuj: Zezwalaj użytkownikowi na eksportowanie danych.

• Informuj: Poinformuj użytkowników o każdym naruszeniu danych.

- Oto ogólne zalecenia dotyczące bezpieczeństwa:

• Secure Sockets Layer (SSL): HTTPS powinien być używany w aplikacjach internetowych, a zwłaszcza podczas żądania i eksportowania danych.

• Dowód wiedzy o zerowej wiedzy (ZKP): W przypadku łańcuchów bloków należy stosować dowód wiedzy o zerowej wiedzy (ZKP);

Uwaga: ZKP to metoda, w której jedna strona udowadnia weryfikatorowi, że zna wartość, powiedzmy, x. Prawdziwą analogią byłoby zatrzaśnięcie drzwi i podanie tajnego słowa, aby uzyskać dostęp do prywatnego klubu tylko dla członków.

• Szyfrowanie: Użyj szyfrowania homomorficznego lub bezpiecznych obliczeń wielostronnych.

• Bezpieczny system uwierzytelniania: używaj bezpiecznego systemu uwierzytelniania, takiego jak standardy OAuth 2.0.

• Limit czasu usługi i ograniczenia: Ustaw mechanizm limitu czasu dla usług dla opóźnionych odpowiedzi, aby upewnić się, że usługi nie będą się dławić (spowalniać). Implementuj ograniczanie prób logowania. Skonfiguruj bezpieczny uścisk dłoni wszędzie.

• Powszechne luki w zabezpieczeniach: ochrona przed typowymi lukami w zabezpieczeniach, takimi jak rozproszona odmowa usługi (DDoS) i współużytkowanie zasobów między źródłami (CORS).

Uwaga : CORS używa dodatkowych nagłówków HTTP, aby dać aplikacji działającej w jednej domenie dostęp do zasobów na serwerze w innej domenie.

• Informacje poufne: Zapisz hasła i wszelkie inne poufne informacje jako dane zaszyfrowane przy użyciu metody zaszyfrowanej.

• Ograniczenie IP: Ogranicz adresy IP, które mają dostęp do Twoich portów. Na przykład nie masz dostępu do roota i FTP do żadnych adresów IP, tylko do swojego adresu IP.

• Pomiar bezpieczeństwa: Włącz środki bezpieczeństwa do cyklu rozwoju.

Podsumowując, omówiłem, co to znaczy być gotowym na bezpieczeństwo, co to jest testowanie bezpieczeństwa i jak być gotowym na zgodność. Przyjrzałeś się przepisom zgodności w Stanach Zjednoczonych i Unii Europejskiej dotyczących technologii blockchain, a na koniec omówiłem zalecenia dotyczące gotowości bezpieczeństwa, które powinieneś wziąć pod uwagę na wczesnych etapach cyklu rozwoju. W następnej części tego rozdziału przyjrzysz się konkretnym atakom na portfele kryptowalut, które mogą spowodować znaczne straty i sposobom ich zapobiegania.

Typowe ataki Blockchain

W tej sekcji omówię niektóre z najbardziej znanych i powszechnych ataków blockchain. Podzieliłem te ataki na trzy kategorie.

• Cyberataki na portfele: skierowane na portfele kryptograficzne.

• Ataki sieciowe typu blockchain: ukierunkowane na sieć blockchain P2P.

• Ataki platformowe: skierowane na platformy obsługujące blockchain, takie jak giełdy, witryny internetowe i platformy pożyczkowe.

Należy pamiętać, że chociaż podzieliłem ten proces na trzy kategorie, większość z tych ataków wykorzystuje różne techniki i różne cele, ale mają ten sam cel, jakim jest przechwytywanie prywatnych kluczy kryptograficznych.

Cyberataki na portfel

W tej sekcji omówię konkretne cyberataki skierowane na portfele kryptograficzne. Jak podkreśliłem na początku tego rozdziału, po transferze środków kryptograficznych nie jest łatwo je wyśledzić, ponieważ

można je przenieść z jednego portfela do drugiego, a transfer jest nieodwracalny, chyba że większość peerów w sieci wyrazi na to zgodę zmienić blok. Zwykłe ataki na portfel mogą przybierać różne kształty i formy, powodując utratę kluczy prywatnych przez użytkownika. Atakujący często zaczyna od „ataku phishingowego", w wyniku którego poufne informacje użytkownika zostają naruszone, a następnie sprawca jest w stanie przelać środki z konta.

Uwaga : atak typu phishing (pomyśl o poszukiwaniu informacji) to próba nieuczciwego przechwycenia poufnych informacji użytkownika, takich jak nazwy użytkownika, hasła, numery kont itd. Odbywa się to za pomocą komunikacji elektronicznej, takiej jak e-mail, w celu ukrycia atakującego jako podmiot godny zaufania.

W rzeczywistości, poza oszustwami kryptograficznymi, takimi jak Bitconnect i iFan, kradzież portfela spowodowała drugą co do wielkości stratę w aktywach kryptograficznych, wynoszącą blisko 5 miliardów dolarów. Najlepszym rozwiązaniem przeciwko atakom portfelowym jest całkowite usunięcie kryptowaluty z giełd, gdy nie są one używane, i umieszczenie tych kryptowalut we własnym scentralizowanym magazynie „zimnego portfela". Można to osiągnąć za pomocą portfeli sprzętowych, takich jak Nano, Trezor, KeepKey i tak dalej. Przeniesienie krypto do zimnego portfela zapewnia najwyższy poziom ochrony i pozwala uniknąć strat wynikających z wymiany, takich jak incydenty na Mt.Gox, w których hasło administratora zostało złamane, a wielu użytkowników straciło klucze do portfela.

Uwaga: Zimne przechowywanie to metoda przechowywania prywatnych kluczy krypto na dysku USB, papierowym portfelu lub innym nośniku danych w bezpiecznym miejscu. Pomyśl o tym jak o swoim własnym banku.

W następnej sekcji przyjrzysz się powszechnym atakom portfelowym. Dostarczę analizę pośmiertną, aby upewnić się, że nie powtarzasz tych samych błędów, które popełnili inni, zarówno jako programista, jak i użytkownik.

Ataki phishingowe i złośliwe oprogramowanie do portfela online

Portfele online są bardziej podatne na ataki niż portfele offline, ponieważ są połączone z Internetem. Na przykład niedawno przeprowadzono atak phishingowy na portfel Electrum i spowodował straty w wysokości ponad 1 miliona dolarów.

Uwaga: Złośliwe oprogramowanie pochodzi z połączenia słów złośliwy i oprogramowanie. Oprogramowanie ma na celu zakłócanie, uszkadzanie lub uzyskiwanie dostępu do komputera ofiary.

Dokonał tego haker konfigurujący złośliwe serwery; następnie, gdy portfel użytkownika łączył się z jednym z tych serwerów i próbował wysłać transakcję BTC, kod atakującego wyświetlał oficjalnie wyglądającą wiadomość informującą użytkownika, że musi zaktualizować swój portfel Electrum, wraz z fałszywym adresem URL, aby pobrać fałszywą wersję portfela Electrum ze złośliwym oprogramowaniem. Gdy użytkownik użył adresu URL atakującego i pobrał nową fałszywą wersję Electrum, portfel zażądał od użytkownika ponownego wprowadzenia hasła, które zostało następnie wysłane do hakera. Następnie haker został wyposażony w dane logowania użytkownika i mógł zalogować się do prawdziwego portfela Electrum i przenieść klucze prywatne użytkownika do własnego portfela.

Sekcja zwłok

Jako użytkownik, oprócz całkowitego unikania portfeli online i korzystania z chłodni, możesz zmniejszyć ryzyko, wykonując następujące czynności:

• Pobieraj tylko oficjalne oprogramowanie: nie pobieraj portfeli online ani nie aktualizuj z innego źródła niż oficjalna strona internetowa portfela. Sprawdź adresy URL, najeżdżając na linki, ale ich nie klikając. W szczególności sprawdź, czy nie ma małych błędów ortograficznych; sprawdź, czy możesz zauważyć małe błędy ortograficzne tutaj: paypaI.com, Electrom.com.

• Chroń swoje informacje: Uważaj na informacje udostępniane przez e-mail. Wiadomości e-mail z prośbą o potwierdzenie poświadczeń konta muszą być wysyłane od firmy, którą rozpoznajesz, i przez Ciebie, który zainicjował żądanie.

• Zapewnij uwierzytelnianie: Pobierz oprogramowanie portfela i sprawdź podpis GPG. Nigdy nie podawaj kluczy prywatnych swoich aktywów kryptograficznych żadnemu „oficjalnemu" przedstawicielowi.

• Rozpoznaj fałszywy numer telefonu pomocy technicznej: często firmy, które wyłudzają informacje, używają fałszywego numeru pomocy technicznej. Wiele osób szuka w Google numeru telefonu firm i pada ofiarą tego ataku.

Jako programista powinieneś wykonać następujące czynności:

• Użyj weryfikacji podpisu GPG: Implementuj weryfikację podpisu GPG.

Wskazówka: GPG/GNU to pakiet oprogramowania kryptograficznego używanego do szyfrowania w celu zapewnienia autentyczności poprzez porównywanie podpisów z pobranymi plikami. Aby zapobiec atakom na portfel, zaimplementuj GPG lub GNU Privacy Guard. Jako użytkownik nie zapomnij również sprawdzić, czy sam GPG/GNU jest uwierzytelniony i pochodzi od dewelopera.

• Edukuj swoich użytkowników: Ustaw strony, samouczki wideo i wpisy na blogach, aby edukować użytkowników i zapobiegać popełnianiu typowych błędów.

Złośliwe oprogramowanie keyloggera

Większość złośliwego oprogramowania ma na celu uszkodzenie komputera. Popularne złośliwe oprogramowanie, które można wykorzystać do wyodrębnienia kryptowalut, to keylogger lub skrobaczka ekranu. To oprogramowanie rejestruje wszystko, co wpisujesz, a także wykonuje zrzuty ekranu komputera w celu przechwycenia haseł i danych osobowych. Tego typu ataki są mniej prawdopodobne w domu, ponieważ osoba atakująca musi podłączyć do komputera rzeczywisty klucz uniwersalnej magistrali szeregowej (USB), aby zarejestrować dziennik kluczy; może się to jednak zdarzyć, gdy korzystasz z komputera publicznego, na przykład w hotelowym lobby lub bibliotece.

Sekcja zwłok

Jak wspomniano, w domu jest mniej prawdopodobne, że zostaniesz zaatakowany przez keyloggera; jednak logując się do publicznego komputera, zachowaj ostrożność, sprawdź, czy do tego komputera jest podłączony klucz USB i unikaj dostępu do ważnych kont. Na własnym komputerze na komputerze Mac sprawdź Monitor aktywności, aby upewnić się, że rozpoznajesz wszystkie usługi działające w tle. W razie potrzeby przeszukaj sieć, aby znaleźć usługi, których nie rozpoznajesz, a jeśli coś wygląda dziwnie, zatrzymaj i usuń usługę i aplikację. Zainstaluj oprogramowanie antywirusowe i ponownie zainstaluj system operacyjny, jeśli masz wątpliwości.

Atak Pyłu

Atak pyłowy jest przeprowadzany przez atakującego, który wysyła maleńką (pyłową) transakcję, której hakerzy używają albo do spamowania sieci blockchain i zajęcia miejsca na bloki, albo do oznaczenia docelowych adresów w nadziei, że użytkownik dokona transakcji tych kryptowalut, co może pomóc osoba atakująca identyfikuje dane osobowe użytkownika, śledząc historię transakcji.

Sekcja zwłok

Jako użytkownik nie wydawaj nierozpoznanych transakcji. Jako programista zaimplementuj funkcję kontroli monet, aby nierozpoznane transakcje mogły być oznaczone jako „Nie wydawaj" i nie były uwzględniane w transakcjach.

Atak gorącego portfela

W ataku z użyciem gorącego portfela osoba atakująca pobiera klucze prywatne portfela z „gorącego portfela", w którym klucze prywatne są przechowywane online za pomocą phishingu, łamania haseł lub w jakikolwiek inny sposób. Gdy klucze prywatne zostaną wyciągnięte z sieci online, atakujący mogą przenieść te klucze do własnego portfela.

Uwaga : Giełdy przechowują prywatne klucze kryptograficzne użytkownika online w tak zwanych portfelach gorących lub portfelach operacyjnych. Powodem, dla którego te klucze prywatne są przechowywane online, jest umożliwienie wypłat z portfeli w czasie rzeczywistym.

Sekcja zwłok

Jako użytkownik najlepszym sposobem na uniknięcie tych strat jest trzymanie krypto pod własną kontrolą w zimnym portfelu, a nie na scentralizowanych giełdach. Jako programista wykonaj następujące czynności:

• Trzymaj zimny portfel: Przechowuj klucze użytkownika w chłodni i unikaj gorących portfeli, jak to tylko możliwe. Na przykład Coinbase.com twierdzi, że przechowuje 98 procent środków swoich użytkowników na papierowych kopiach zapasowych dystrybuowanych geograficznie do skrytek sejfowych.

• Szyfruj klucze prywatne: Jeśli musisz przechowywać klucze prywatne w magazynie podłączonym do sieci online, zaszyfruj klucze przynajmniej silnym kluczem szyfrowania.

• Uważaj na nietypową aktywność: Na przykład wiele giełd ręcznie zatwierdza duże wypłaty.

Ataki sieciowe Blockchain

W tej sekcji omówię typowe ataki wymierzone w sieć blockchain.

Ataki Sybilli

Imię Sybil jest synonimem osoby, która ma wiele zaburzeń osobowości.

Uwaga: Atak blockchain Sybil to podmiot próbujący wpłynąć na sieć P2P poprzez tworzenie wielu tożsamości i kontrolowanie wielu węzłów.

Atak Sybil tworzy wiele fałszywych kont w celu kontrolowania sieci. Podmiot kontrolujący te liczne konta może następnie wpływać na sieć, ponieważ ma dodatkową siłę głosu w demokratycznej sieci. Łatwym sposobem na zrozumienie tego są wybory w Stanach Zjednoczonych w 2017 r., w których jeden podmiot, Rosja, wpłynął na proces wyborczy, tworząc wiele kont w mediach społecznościowych i kontrolując ich zawartość. Przykładem blockchain mogą być napastnicy próbujący przegłosować uczciwe węzły w sieci P2P, tworząc wiele tożsamości Sybil. Mając większość głosów, atakujący mogą

odmówić otrzymywania bloków lub przesyłania fałszywych bloków. Jeśli ataki Sybil przeprowadzą wystarczająco duży atak, są w stanie kontrolować większość szybkości haszowania sieci P2P i blokować zmiany, co jest wtedy atakiem z podwójnym wydawaniem.

Sekcja zwłok

Jako programista możesz zniechęcić ataki Sybil, czyniąc je niepraktycznymi. Jeśli istnieje koszt związany z uruchomieniem ataku Sybil, taki jak koszty utworzenia konta, uruchomienia serwerów, elektryczności itp., może to zniechęcić lub sprawić, że ataki będą niepraktyczne. Upewnij się jednak, że bierzesz pod uwagę legalnych użytkowników, którzy muszą tworzyć wiele kont. W rzeczywistości popularne blockchainy biorą pod uwagę ataki Sybil. Na przykład algorytm spisu bitcoin PoW wymaga dużej mocy obliczeniowej, więc tworzenie bloku jest proporcjonalne do całkowitej mocy obliczeniowej. To zniechęca napastników, ponieważ górnicy wolą robić prawdziwe wydobycie, niż ryzykować przegraną na nieudanym ataku Sybil. Podobnie algorytm spisu PoS wymaga stakowania monet, więc atakujący będą ryzykować tracąc te monety. Ponadto, jak widzieliście w poprzednich rozdziałach, Ethereum, EOS i NEO zawierają duże koszty związane z wdrażaniem dappów. Ethereum ma minimalną opłatę 32 000 gazu i 200 gazu na te, EOS to około 120 monet, a NEO ma stały koszt od 100 do 1000 gazu. Ponadto wiele łańcuchów bloków, takich jak bitcoin, Ethereum i NEO, pobiera opłatę transakcyjną, co pomaga zniechęcić napastników. Podobnie EOS nie pobiera opłat transakcyjnych, ale wykorzystuje „łańcuch zaufania" do zwalczania napastników.

Uwaga: łańcuch zaufania to sposób na zwalczanie ataków Sybil poprzez wymaganie zaufania przed zezwoleniem nowym tożsamościom na dołączenie do sieci. Wersja łańcucha zaufania może obejmować umożliwienie użytkownikowi utworzenia nowego konta, ale nie nadanie mu pełnych uprawnień przez określony czas.

EOS pobiera od programistów od 1 do 4 USD za nowe konto; oczywiście programiści będą niechętni do tworzenia kont i wprowadzania środków łagodzących, aby uzyskać zatwierdzenie konta. Innym sposobem walki z atakiem Sybilli jest zmiana hierarchii z demokracji na merytokrację (rządzoną przez wybrane osoby). Użytkownicy, którzy zostali stworzeni dawno temu i mają dobrą reputację, mieliby większą wagę niż nowe konta. Pomyśl o systemie reputacji Stackoverflow.com lub Wikipedia.com.

Podwójne wydatki lub atak51 procent

Wcześniej mówiłem o potencjalnych atakach z podwójnymi wydatkami na kryptowaluty, w których złośliwy węzeł przejmuje kontrolę nad ponad 50 procentami współczynnika haszowania sieci blockchain i jest w stanie zmieniać bloki i manipulować nimi. Duże łańcuchy blokowe, takie jak bitcoin i Ethereum, nie są łatwe do pokonania przez atak 51 procent ze względu na konkurencję górników, która wymaga wysokiego poziomu zasobów. Jednak mniejsze łańcuchy bloków były celem 51-procentowego ataku. Tak stało się z blockchainem Verge, który w dwóch atakach stracił prawie 3 miliony dolarów. Złoto Bitcoin poniosło największą stratę 18 milionów dolarów, a Ethereum Classic stracił 1,1 miliona dolarów. W rzeczywistości w ciągu niecałego roku w 2018 i 2019 roku straty poniosły łącznie 23 miliony dolarów.

Sekcja zwłok

Jako inwestor powinieneś sprawdzić koszt ataku na blockchain, w który chcesz zainwestować i czy istnieje mechanizm sieci bezpieczeństwa dla blockchain. Deweloperzy Blockchain powinni stworzyć jakiś mechanizm sieci bezpieczeństwa, na przykład tworząc hash, który przechowuje migawkę wszystkich transakcji i sald każdego z twoich bloków, a następnie przechowując ten hash w większym blockchainie. Na przykład możesz wykorzystać bitcoin OP_RETURN, tak jak w części 4, i przechowywać

skrót jako kopię zapasową na wypadek 51-procentowego ataku. W rzeczywistości, http://komodoplatform.com był w stanie rozwiązać problem podwójnego wydatkowania, tworząc mechanizm zabezpieczenia opóźnionego dowodu pracy (dPoW).

Ransomware Górnika

Jak wspomniałem, te 51 procent ataków jak dotąd nie miało wpływu na bitcoin; jednak hakerzy znaleźli nowy sposób na wpływanie na łańcuchy bloków, atakując górników za pomocą oprogramowania ransomware.

Uwaga: Ransomware to rodzaj złośliwego oprogramowania, którego celem jest blokowanie komputera do czasu wypłaty pieniędzy. Nazwa jest połączeniem słów okup i oprogramowanie.

Hakerzy blokują platformy wydobywcze przy użyciu podobnych technik, które oprogramowanie ransomware wykorzystuje na komputerach osobistych. Na komputerach osobistych złośliwe oprogramowanie, takie jak oprogramowanie ransomware NotPetya, jest pobierane i instalowane, a następnie jest w stanie zablokować komputer użytkownika do momentu wpłacenia okupu na adres portfela. Do tej pory ransomware atakowało tylko komputery osobiste; jednak nowe oprogramowanie ransomware, takie jak hAnt, atakuje górników. Nie wiadomo, w jaki sposób HAnt jest instalowany, ale szacuje się, że jest on prawdopodobnie pobierany z wersją oprogramowania sprzętowego platformy wydobywczej. Następnie oprogramowanie ransomware ma dostęp do oprogramowania układowego górnika i może nim sterować. Atakujący wyświetla komunikat, gdy login administratora grozi przegrzaniem i zniszczeniem górnika. Można to osiągnąć, wyłączając wentylatory, jeśli ofiary nie infekują innych urządzeń ani nie płacą okupu w bitcoinach. Do tej pory ucierpiały tylko koparki bitcoin i litecoin wyprodukowane przez Antminer i Avalon, ale ten atak może potencjalnie zostać wykonany na dowolnym górniku.

Sekcja zwłok

Pozbycie się ransomware nie jest łatwe. Oprogramowanie może być zbudowane ze skryptem „tripwire", który może uszkodzić górnika, jeśli górnik odłączy się od Internetu. Aby rozwiązać ten problem, musisz najpierw chirurgicznie usunąć oprogramowanie ransomware z kart Secure Digital (SD) koparki. Dodatkowo, wyłączenie farmy górniczej na pewien czas jest kosztowne. Najlepszym rozwiązaniem jest całkowite uniknięcie tego ataku poprzez nie pobieranie aktualizacji oprogramowania z jakiegokolwiek źródła niż z oficjalnej strony internetowej dostawcy.

Atak Eclipse na sieć P2P

Atak zaćmienia informacyjnego można przeprowadzić samodzielnie lub jako część innego ataku, na przykład ataku 51 procent. Atakujący uzyskują kontrolę nad dostępem peera do informacji w sieci P2P, manipulując siecią tak, aby węzły komunikowały się tylko ze złośliwymi węzłami. Atakujący może następnie manipulować mechanizmem wydobywania i konsensusu.

Sekcja zwłok

Przeprowadzaj analizy, symulacje i eksperymenty, aby znaleźć środki zaradcze, aby uniknąć ataku zaćmienia. Dobre badania z potencjalnymi środkami zaradczymi w celu zwiększenia zabezpieczeń bitcoinów przed atakiem zaćmienia można znaleźć tutaj (i można je zastosować w wielu innych sieciach blockchain): https://hackernoon.com/eclipse-attacks-on-blockchains-peer-topeer- sieć-26a62f85f11.

Ataki routingu

Ataki routingu internetowego obejmują przejęcia BGP, a złośliwe ataki na dostawców usług internetowych (ISP) mogą być również wykonywane przeciwko łańcuchom bloków.

Uwaga: przejęcie BGP to złośliwie przekierowany atak na ruch internetowy. Odbywa się to poprzez fałszywe ogłaszanie własności grup sukien IP (prefiksów IP).

Duże farmy wydobywcze są scentralizowane w kilku lokalizacjach geograficznych, co czyni je idealnymi do ataku typu ISP. Atakujący mogą popełnić następujące czynności:

- Atak na partycje: dostawca usług internetowych może podzielić sieć P2P na partycje, przejmując kilka prefiksów IP.

Atak opóźniający: dostawca usług internetowych opóźnia ruch do i z węzła łańcucha bloków, co skutkuje opóźnieniem w propagacji bloku, spowalniając transakcje.

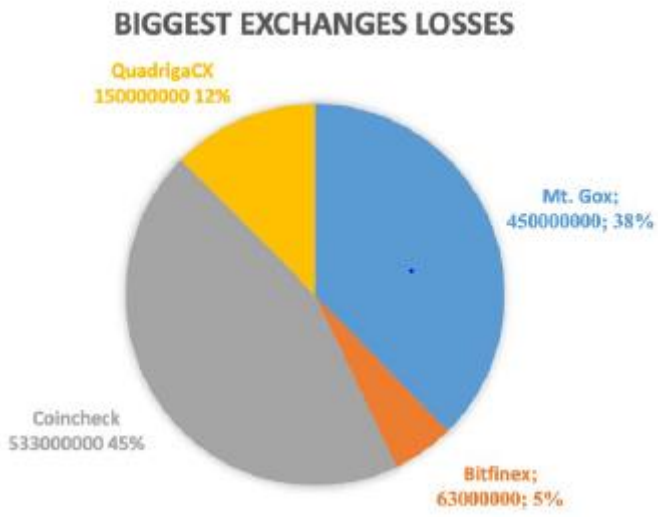
Tego typu ataki mogą zmniejszyć przychody węzła, a także przekształcić się w atak 50%, ponieważ mniej węzłów wpływa na sieć. Dodatkowo ataki te mogą również uniemożliwić wysłanie transakcji przez duże podmioty, takie jak giełdy.

Sekcja zwłok

Utwórz niestandardowy skrypt lub zainstaluj sprzęt do monitorowania sieci. Wielu dostawców usług internetowych zapewnia płatne rozwiązanie do monitorowania sieci i zapobiegania atakom. Zapoznaj się z sekcją „Ataki DoS i DDoS" po śmierci, aby uzyskać więcej rozwiązań, które mogą pomóc w złagodzeniu tego ataku.

Atak na platformę

Sieć blockchain Bitcoina jest z założenia bezpieczną siecią i okazała się niezawodna. Bitcoin został wydany w 2009 roku, a w chwili pisania tego tekstu nie doszło do udanego ataku na sieć blockchain Bitcoina. Powodem, dla którego łańcuch bitcoinów ma wysoki poziom bezpieczeństwa, jest to, że dane są rozproszone między węzłami. Ponadto wydobycie bitcoina jest drogie energetycznie, więc atakowanie sieci bitcoina może kosztować więcej niż samo wydobycie, a atakujący ryzykują utratę pieniędzy po prostu próbując ataku. Jednak to nie jedyny powód; Dużym czynnikiem przyczyniającym się do tego, że bitcoin wytrzymuje próbę czasu, jest to, że jest to open source i umożliwia programistom szybkie wdrażanie zmian w oparciu o badania i zalecenia ekspertów ds. Bezpieczeństwa. Mając to na uwadze, nie zapewnia to bezpieczeństwa innym platformom, które świadczą usługi oparte na bezpiecznych łańcuchach bloków, takich jak giełdy, platformy pożyczkowe, usługi oparte na portfelach i dappy przechowujące klucze prywatne. Na przykład giełdy przechowują miliardy depozytów i są idealnym celem dla hakerów. Jak wspomniano, giełdy przechowują krypto użytkownika w postaci kluczy prywatnych, a niektóre z tych kluczy są przechowywane online w gorącym portfelu, aby umożliwić wypłaty i handel w czasie rzeczywistym. Nieostrożne obchodzenie się z tymi kluczami prywatnymi może spowodować straty. Dobrym przykładem jest naruszenie bezpieczeństwa Mt. Gox w 2011 roku. Atak ten miał miejsce, ponieważ hakerowi udało się złamać hasło audytora z Mount Gox i przenieść do siebie 800 000 bitcoinów. Oprócz Mt. Gox, nieustannie pojawiają się informacje o zamykaniu giełd z powodu utraty kryptowaluty. Jak widać na Rysunku



największą stratę w wysokości blisko 1 miliarda dolarów poniósł Mount Gox w dwóch atakach, a największą kradzieżą w historii kryptowalut był atak na giełdę Coincheck w 2018 roku.

W następnej sekcji omówię niektóre z największych ataków i dam Ci zalecenia dotyczące sposobów zapobiegania tym atakom.

Ataki na poświadczenia

Ataki związane z uwierzytelnianiem, takie jak łamanie haseł, spowodowały milionowe straty.

-Bezpośredni atak na giełdy: Jak wspomniano, 51-procentowy atak Mt.Gox w 2011 r. spowodował dwie oddzielne straty: 2 609 BTC i ponad 750 000 BTC. Hakerzy byli w stanie uzyskać dane uwierzytelniające audytora i przetransferować te bitcoiny na adres hakera.

-Atak na użytkowników: Miliony strat nastąpiły z powodu przejęcia kont użytkowników. Na przykład firmy telekomunikacyjne umożliwiły przejęcie numerów telefonów komórkowych, dostarczając proste informacje rozliczeniowe. Hakerzy mogą przenieść numer do nowego dostawcy, a następnie zatwierdzić resetowanie haseł kont na giełdach za pomocą weryfikacji SMS.

Sekcja zwłok

Jako użytkownik najlepszym sposobem uniknięcia tych strat jest trzymanie swoich kryptowalut w zimnym portfelu, a nie na scentralizowanych giełdach. Na własnym komputerze:

-SSL: Nie rejestruj się w witrynach, które nie mają certyfikatu SSL.

- Silne hasła: używaj unikalnych i silnych haseł o długiej długości i zawierających cyfry, znaki i znaki specjalne.

- Unikalne hasła: nie używaj ponownie tego samego hasła na różnych platformach.

- Warstwy zabezpieczeń: skonfiguruj wszystkie zalecane warstwy zabezpieczeń, takie jak SMS, włączone 2FA, potwierdzenie e-mail i tak dalej.

- Antywirus: Zainstaluj płatne lub bezpłatne oprogramowanie antywirusowe. Na komputerach osobistych Avast Security ma bezpłatną wersję używaną przez 435 milionów osób: https://www.avast.com. Zawiera wtyczkę do Chrome, która ostrzega przed witrynami phishingowymi.

- VPN: używaj połączenia VPN tak często, jak to możliwe, zwłaszcza w sieci, która jest publiczna i nie jest zabezpieczona.

- Unikaj złośliwego oprogramowania i oprogramowania ransomware: pamiętaj o instalowanym oprogramowaniu i upewnij się, że pochodzi ono od renomowanego dostawcy. Przeczytaj wszystkie wiadomości podczas instalacji; nie tylko zgadzaj się na wszystkie wiadomości. Zainstaluj oprogramowanie, które zapobiega ransomware.

Wskazówka: trzymaj swoje aktywa kryptograficzne pod własną kontrolą w zimnym portfelu, a nie na scentralizowanych giełdach. Skonfiguruj więcej warstw niż tylko weryfikacje SMS-owe na ważnych kontach. Warstwy bezpieczeństwa mogą obejmować uwierzytelnianie 2FA, weryfikację poczty e-mail i ograniczenie IP.

Jako programista łamanie haseł jest najczęstszym sposobem uzyskania dostępu do aplikacji internetowej. Zaimplementuj tester bezpieczeństwa, który upewni się, że system wymaga silnego zaszyfrowanego hasła. Dobrym przykładem takiego rozwiązania jest łamacz haseł John the Ripper:

Ponadto zaimplementuj następujące elementy:

- Chroń poświadczenia: Chroń poświadczenia użytkowników za pomocą wielu warstw.

• Silne hasło: Wymuszaj stosowanie silnych haseł podczas tworzenia konta i resetowania haseł.

• Włączono 2FA: skonfiguruj uwierzytelnianie dwuskładnikowe (tzw. włączone 2FA); popularnym przykładem jest Google Authenticator.

• Potwierdzenie: Wymagaj potwierdzenia zarówno SMS-em, jak i e-mailem w przypadku ważnych operacji, takich jak przelewy.

- Przechowywanie: Przechowuj poufne dane użytkowników (takie jak klucze prywatne) zaszyfrowane i na serwerach, które są odłączone od Internetu.

- Szyfrowanie: używaj SSL na wszystkich stronach. Użyj szyfrowania AES-256. Hasła haszujące ze współczynnikiem kosztów 12.

- Zablokuj konto: ogranicz liczbę prób logowania i zablokuj konto po wielu nieudanych próbach.

- Na komputerze osobistym do rozwoju:

• Połączenie zdalne: używaj silnych haseł logowania, zwłaszcza jeśli łączysz się zdalnie z komputerem.

• Szyfruj dane: zaszyfruj dysk twardy, aby włączyć szyfrowanie. Przejdź do Preferencji systemowych i wybierz Prywatność i bezpieczeństwo. Kliknij Włącz FileVault.

• Blokuj przy nieaktywności: Na karcie Ogólne w obszarze Zaawansowane skonfiguruj wylogowanie po pięciu minutach braku aktywności i włącz blokowanie ekranu, wybierając opcję „wymagaj hasła administratora w celu uzyskania dostępu do preferencji systemowych”.

• Zapora: skonfiguruj zaporę na komputerze; na karcie Zapora włącz zaporę.

• VPN: używaj VPN podczas pracy w niezabezpieczonej sieci.

• Oprogramowanie: pamiętaj o instalowanym oprogramowaniu i upewnij się, że pochodzi ono od renomowanego dostawcy.

• Biblioteki: Jeśli to możliwe, unikaj instalowania bibliotek kodu z dostępem administratora.

Wadliwy kod

Wadliwy kod jest jedną z największych przyczyn strat. Stało się tak znaczące, że wiele dużych firm ustala nagrody dla hakerów w białych kapeluszach za wykrycie błędów, co sprawia, że hakerom opłaca się wskazywać błędy zamiast kraść.

Uwaga: haker w białym kapeluszu to osoba moralna, która zdobywa nieautoryzowany dostęp do danych w celu wykrycia wad systemu. Na przykład hakerzy wykorzystali wadliwy kod do wypłaty w Poloniex w 2014 roku. Dokładna liczba skradzionych bitcoinów nie została ujawniona przez firmę.

Sekcja zwłok

Jako programiści:

- Wstrzyknięcia SQL: unikaj wstrzyknięć SQL, testując i implementując filtry wstrzyknięć SQL.

- Atak CSRF: haker wykorzystuje żądania usług do modyfikowania i pobierania danych oraz weryfikacji autentyczności żądań POST, PUT i DELETE. Aby tego uniknąć, postępuj zgodnie z poniższymi zaleceniami:

• Ogranicz adresy IP: ustawienie, aby usługi odpowiadały tylko na określone adresy IP.

• Ustaw narzędzia i biblioteki: Znajdź narzędzia do unikania ataków CSRF tutaj: https://github.com/0xInfection/XSRFProbe.

- Cross-site scripting (XSS): Unikaj XSS, używając narzędzi i bibliotek

Uwaga : wstrzyknięcie SQL to atak polegający na tym, że haker przekazuje niedozwolone instrukcje SQL przez pole wprowadzania tekstu, aby uzyskać dostęp do treści. Hakerzy mogą następnie wykorzystać tę lukę, aby dodać, zmienić, lub usuń dane z bazy danych SQL.

Uwaga : ataki XSS są wykonywane przez wstrzyknięcie złośliwego kodu do zaufanej witryny internetowej.

Sekcja zwłok

Jako użytkownik, zgodnie z zaleceniami w tym rozdziale, umieść krypto w zimnym portfelu. Jako programista zachowaj ostrożność podczas obsługi bibliotek open source. Model open source opiera się na wielu pakietach, ale niewielu programistów obsługuje biblioteki, co może umożliwić złośliwe przejęcie. Aby tego uniknąć, uruchom audyt npm, aby wykryć każdą podatną na zagrożenia zależność.

> npm audit

Sprawdź i przetestuj swój kod pod kątem wszelkich zgłoszonych luk w zabezpieczeniach w bazie danych o lukach, takiej jak strona snyk.io: https://snyk.io/vuln.

Nie ustawiaj pliku package.json tak, aby zawierał automatyczną aktualizację biblioteki.

"dependencies": { "some-library": "latest" }

Zamiast tego sprawdź żądania ściągnięcia w bibliotekach, które chcesz zaktualizować, i ręcznie sprawdź zmiany pod kątem używanych zależności. Użyj wersji specyficznej dla biblioteki.

"dependencies": { "some-library": "1.0.0" }

Tak samo jest z instalacją npm. Zainstaluj określone biblioteki, szczególnie w mniej znanych bibliotekach.

> npm install -g some-library@1.0.0

Ataki DoS i DDoS

Atak typu „odmowa usługi” (DoS) jest powszechnym atakiem mającym na celu uniemożliwienie użytkownikom dostępu do usługi. Atak typu rozproszona odmowa usługi (DDoS) jest podobny do DoS, ale zamiast atakującego wykorzystującego pojedynczą maszynę, atakujący używa wielu maszyn, które atakują jednocześnie. Ze względu na użycie wielu maszyn wzrastają szanse na udany atak i trudniej jest określić dokładną lokalizację atakującego. Giełdy i witryny internetowe są popularnymi celami ataków DoS i DDoS. Na przykład, kiedy oficjalnie pojawił się bitcoin gold, był on celem ataku

Atak DDoS, który zakończył się awarią witryny na wiele godzin. Popularne sieci blockchain mają prosty wbudowany mechanizm zapobiegania DoS; jednak wiele sieci nie jest chronionych przed bardziej wyrafinowanymi atakami. Najczęstsze rodzaje ataków to:

- Przepełnienie bufora: ten atak wysyła do usługi docelowej więcej ruchu, niż jest w stanie obsłużyć. Atak ten może dać atakującemu możliwość awarii, a nawet kontrolowania docelowej usługi.

-Powódź ICMP: znany również jako „ping of death” lub „atak smurf”, ten atak ma na celu przeciążenie sieci poprzez wymuszenie na węźle dystrybucji fałszywych pakietów do wszystkich węzłów, co powoduje przeciążenie sieci.

- SYN flood: wysyłane jest żądanie połączenia, ale nigdy nie zostaje ono w pełni uwierzytelnione. Następnie requester atakuje wszystkie otwarte porty na serwerze, aż serwer ulegnie awarii.

- Wzmocnienie NTP/DNS: Jest to atak na serwery NTP, w którym atakujący wysyła dużą liczbę pakietów UDP i fałszuje źródłowy adres IP, sprawiając, że serwer NTP sądzi, że te pakiety są legalnym ruchem z zamierzonego celu. Przeciążenie powoduje awarię serwera NTP.

Sekcja zwłok

Jako programista musisz wziąć pod uwagę ataki Dos/DDoS i wdrożyć przeciwko nim środki zaradcze. Zobacz następujące przykłady:

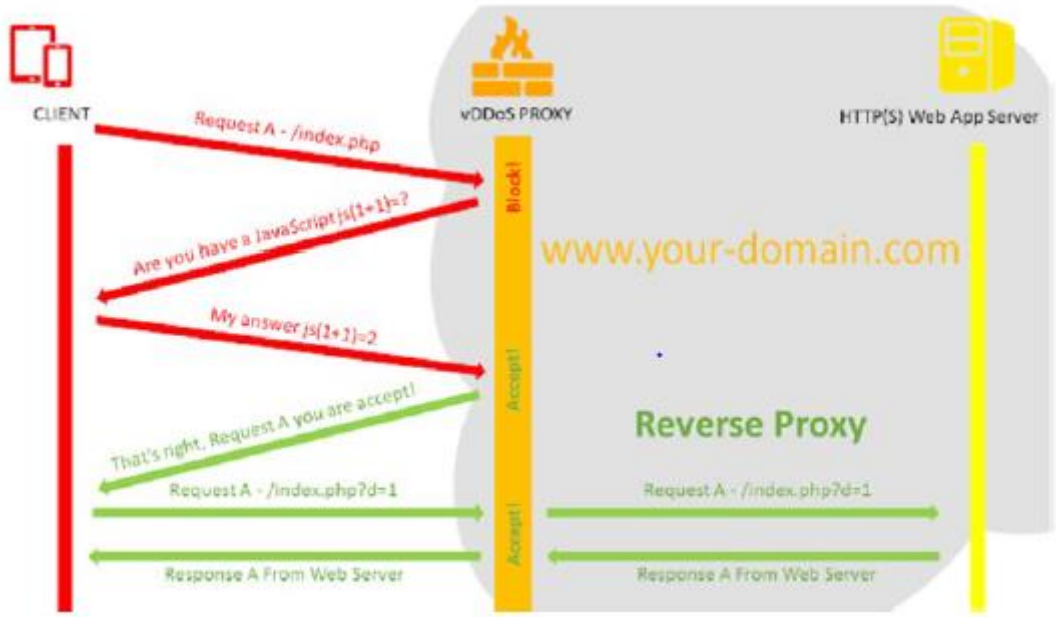
- Filtruj zły ruch:

• Skrypt: Jednym ze sposobów zapobiegania jest zaimplementowanie skryptu sprawdzającego ataki DOS/DDOS. Sprawdź biblioteki ochrony GitHub DDOS:

https://github.com/topics/ddos-protection.

Popularny jest http://vddos.voduy.com/.

• Zapora: użyj zapory do blokowania złego ruchu



- Dedykowany sprzęt: Kup i wdróż dedykowany sprzęt do obsługi łagodzenia ataków DDoS. Sprzęt znajduje się w centrum danych przed serwerami i routerami i może wykrywać i filtrować złośliwy ruch. Przykładem takiego sprzętu jest FortiDDoS firmy www.fortinet.com.

- ISP: dostawcy usług internetowych zapewniają klientom rozwiązania łagodzące ataki DDoS. Na przykład Amazon zapewnia tarczę, w której wszyscy klienci AWS korzystają z automatycznych zabezpieczeń i zapewnia wyższy poziom ochrony przed atakami; zobacz .

- Łagodzenie skutków w chmurze: Niektóre usługi w chmurze zapewniają łagodzenie skutków ataków DoS/DDoS. Usługi te oczyszczają ruch, aby wyeliminować złośliwy ruch. Popularnym dostawcą jest cloudflare.com, który zapewnia bezpłatną wersję standardową i płatne rozwiązanie dla przedsiębiorstw.

Jeśli chodzi o atak DoS/DDoS w sieci blockchain, przeanalizuj istniejące implementacje zapobiegania blockchain, takie jak ochrona klienta bitcoin satoshi, która została zaimplementowana w wersji 0.7.0; zobacz https://en.bitcoin.it/wiki/Słabe strony. Podsumowując, omówiłem typowe ataki na platformy. Przyjrzałeś się atakom na poświadczenia, błędnym kodzie, atakom backdoorem zależności i atakom DoS/DDoS. Dodatkowo przeanalizowałem sposoby, które pomogą Ci zmniejszyć ryzyko i zapobiec tym atakom. W następnej sekcji przedstawię sugerowany cykl rozwoju, który możesz zastosować, aby zmniejszyć ryzyko i zastosować podejście metodologiczne do zapobiegania atakom.

Cykl rozwoju

Jak widzieliśmy w tym rozdziale, Twoja platforma musi być bezpieczna i chroniona przed potencjalnymi atakami. Nie możesz polegać na szczęściu i musisz upewnić się, że korzystasz ze wszystkich dostępnych środków, aby zmniejszyć ryzyko ataku na Twoją platformę, a także upewnić się, że wdrażasz wszystkie najnowsze przepisy dotyczące Twojej lokalizacji. Proces można podzielić na następujące fazy:

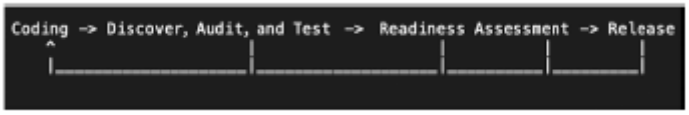
- Projektowanie i kodowanie

- Odkrywaj, audytuj i testuj

- Ocena gotowości

- Wydanie

Jak widać na rysunku 11-7, każda faza może skutkować powrotem do fazy projektowania i kodowania, ponieważ wyniki mogą skutkować zagrożeniem bezpieczeństwa lub przeszkodą.



Wskazówka : ten rozwój jest podstawowym podejściem do cyklu rozwojowego. Zachęcamy do zastosowania własnego lub innego podejścia, które lepiej pasuje do Twojej platformy i potrzeb.

Projektowanie i kodowanie

Przed iw trakcie fazy projektowania i kodowania należy uwzględnić wszystkie elementy bezpieczeństwa, prywatności i zgodności omówione na początku tego rozdziału. Powinny one być brane pod uwagę przy wszystkich elementach Twojej platformy, w tym stronach, systemie logowania, stronie prywatności, integracji z wtyczkami stron trzecich, tworzeniu usług, konfigurowaniu serwerów i tak dalej. Dobrym pomysłem jest stworzenie własnej listy kontrolnej wszystkiego, co należy uwzględnić i wziąć pod uwagę, co dotyczy konkretnie Twojej unikalnej platformy. Nie da się uzyskać jednej listy, która pasuje do wszystkiego. Każda platforma powinna mieć unikalną listę kontrolną. Ponadto po rozpoczęciu nowego cyklu programistycznego może być konieczne zaktualizowanie wymagań. Załóżmy na przykład, że chcesz, aby Twoja platforma była obsługiwana w nowej lokalizacji; będzie to wymagało nowej listy kontrolnej.

Odkrywanie, audyt i testowanie

Ten krok można podzielić na trzy kroki. Kroki są ze sobą powiązane i polegają na sobie, dlatego należy traktować je jako jedną fazę. Te kroki są następujące:

- Odkrywanie: znajdź wersje używane na Twoich platformach, takie jak wersje bibliotek, oprogramowanie układowe, oprogramowanie, zestawy SDK innych firm i tak dalej.

- Audyt: audytuj swój kod i platformę, aby znaleźć typowe problemy, dostępność usług i problemy z wydajnością, które mogą pogorszyć się i sprawić, że Twoja platforma stanie się niedostępna.

- Test: To jest, gdy przeprowadzasz rzeczywiste testy na swojej platformie. Celem jest zidentyfikowanie systemów i usług, z których korzysta Twoja platforma, oraz potencjalnych luk w zabezpieczeniach.

Odkrycie

Odkrycie polega na odkryciu, jakie wersje są używane na Twojej platformie. Na przykład musisz uruchomić fazę wykrywania, aby dowiedzieć się, jakiego oprogramowania używasz. Znajomość wersji dostarcza cennych informacji w przypadku, gdy coś zostało oznaczone jako luka w zabezpieczeniach lub zostało uznane za przestarzałe. Faza wykrywania może być następnie wykorzystana do audytu i testowania oraz wskazania potencjalnych luk w zabezpieczeniach Twojej platformy. Możesz dowiedzieć się podczas sprawdzania wykrywania, że musisz wrócić do fazy kodowania i projektowania z powodu problemów z wersjonowaniem. Na przykład po zmianie wersji biblioteki lub oprogramowania układowego Twój kod może się zepsuć i może być konieczna refaktoryzacja kodu.

Rewizja

W fazie audytu należy przeprowadzać systematyczny przegląd określonych potencjalnych problemów. Podobnie jak księgowy audyt finansowy w firmie, a nawet ta książka została skontrolowana przez zespół, Twoja platforma wymaga audytu i testów, aby upewnić się, że Twój kod jest zgodny z najlepszymi praktykami w celu poprawy wydajności, dostępności i zgodności z wymogami bezpieczeństwa i przepisami. Inspekcję audytową może przeprowadzić Twój własny zespół platformy, ale często przeprowadza ją niezależny podmiot. Należy pamiętać, że nie można oczekiwać, że audyty wykryją wszystkie problemy, które należy rozwiązać. Platforma oparta na blockchain powinna również uwzględniać audyty bezpieczeństwa i zgodności.

Audyt bezpieczeństwa

Audyt bezpieczeństwa może wykorzystywać całkowicie ręczne podejście lub wykorzystywać zautomatyzowane narzędzia do oceny podatności, oceny bezpieczeństwa i testów penetracyjnych w celu określenia, czym należy się zająć. Istnieje ponad 1500 exploitów, więc dobrym pomysłem jest poleganie przynajmniej do pewnego stopnia na automatycznych narzędziach audytowych jako integralnej części cyklu rozwoju i upewnieniu się, że Twoja platforma przechodzi typowe problemy. Nawet zatrudniając zewnętrznego audytora, lepiej najpierw sprawdzić typowe problemy przed rozpoczęciem bardziej energicznego audytu.

Audyt zgodności

W blockchain musisz sprawdzić nie tylko aspekty bezpieczeństwa; musisz również przeprowadzić audyt zgodności, aby zapewnić, że prywatność i przepisy są wdrażane zgodnie z prawem. Podobnie jak audyt bezpieczeństwa, audyt zgodności może być wykonany przez zewnętrznego audytora lub we własnym zakresie. Jak widzieliście wcześniej w tym rozdziale, wiele z problemów, które dotyczą prawodawców w różnych lokalizacjach, dotyczą luk w zabezpieczeniach. Jak już wspomniałem, przepisy dotyczące zgodności mogą się często zmieniać w zależności od lokalizacji, dlatego ocenę zgodności często lepiej przeprowadza się ręcznie niż automatycznie.

Test

Odkrywanie i audyt polegają na testowaniu w celu uzyskania zaleceń dotyczących rozwiązywania problemów na Twojej platformie. Jeśli chodzi o testowanie, istnieją trzy rodzaje.

- Testy dynamiczne: Testuj luki, które atakujący może cel. Osoba atakująca próbująca wykorzystać Twoją platformę nie miałaby dostępu do Twojego kodu i platformy, więc testy są uruchamiane bez dostępu do Twojego kodu źródłowego.

- Testowanie statyczne: jest to podejście od wewnątrz, testujące pod kątem luk w kodzie źródłowym platformy. Te testy oferują bardziej dogłębną migawkę Twojej platformy w czasie rzeczywistym i bibliotek, które tworzą Twoją platformę.

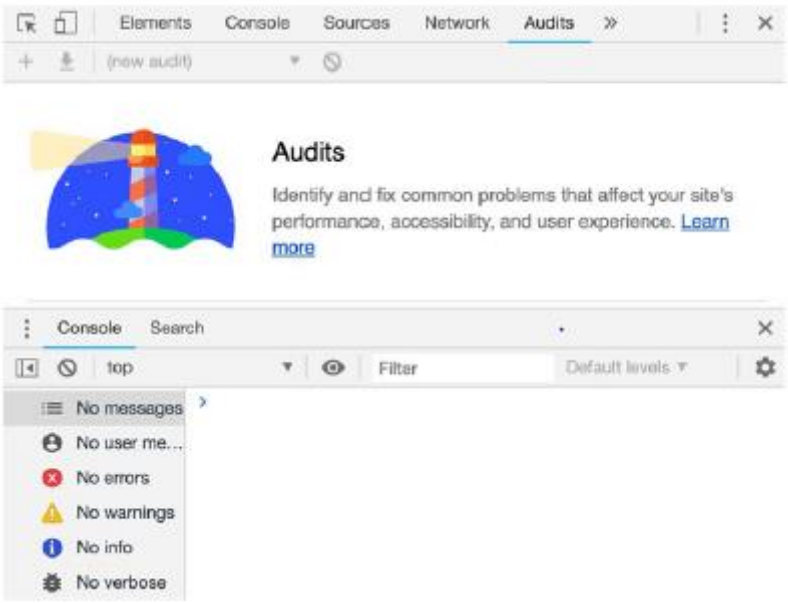
- Test penetracji: symuluje rzeczywisty złośliwy atak. Test penetracyjny może polegać na znalezionych lukach, aby uzyskać dalszy dostęp do Twojej platformy. Może to pomóc w zrozumieniu, jaki dostęp może uzyskać osoba atakująca do informacji poufnych. Testy mogą być przeprowadzane za pomocą zautomatyzowanych narzędzi, ale zaleca się również uwzględnienie testu ręcznego przez rzeczywistego testera, który może polegać na swoim doświadczeniu i wiedzy, aby znaleźć luki, których nie znajdują narzędzia automatyczne.

Zautomatyzowane narzędzia

Istnieje wiele narzędzi testowych, które mogą pomóc w przeprowadzeniu trzech rodzajów testów. Na przykład w przypadku statycznego testowania bibliotek wspomniałem już o audycie npm, który pomaga wykryć wszelkie luki w wersji zależności.

> npm audit

W przypadku aplikacji internetowej narzędzia programistyczne Google Chrome zapewniają wbudowane narzędzia audytu, jak pokazano na rysunku .



Narzędzia programistyczne przeglądarki zapewniają proste narzędzie sieciowe proxy; jednak narzędzia te nie mają wielu funkcji, których możesz potrzebować, takich jak eksportowanie danych, przeprowadzanie symulacji i filtrowanie danych. W fazie audytu przydatne może być skorzystanie z narzędzia internetowego proxy innej firmy. Internetowe narzędzie proxy to głównie analizator protokołów sieciowych, który może dostarczać szczegółowe informacje o protokołach sieciowych, informacjach o pakietach, deszyfrowaniu i tak dalej. Dwa popularne narzędzia to Charlesproxy i Wireshark.

Jeśli chodzi o zautomatyzowane narzędzia penetracyjne, istnieje wiele narzędzi. Oto przykłady kilku popularnych:

1. Narzędzia do automatyzacji bezpieczeństwa

a. OWASP Zed Attack Proxy (ZAP): Obejmuje popularne bezpłatne narzędzia bezpieczeństwa.

b. Burp Suite: To narzędzie do automatyzacji zawiera bezpłatną wersję społecznościową i płatną.

2. Metasploit: To narzędzie jest oparte na exploitie, który próbuje prześcignąć zabezpieczenia Twojej platformy. Możesz go uruchomić z GUI lub wiersza poleceń.

3. CORE Impact: Core Impact Pro testuje penetrację urządzeń mobilnych, identyfikację haseł, łamanie haseł i tak dalej. Ma również GUI i interfejs wiersza poleceń, ale ma wysoką cenę.

4. Netsparker: Obejmuje skaner aplikacji internetowych, który może pomóc zidentyfikować luki w zabezpieczeniach, takie jak dostęp do poufnych danych i sugerowanie rozwiązań. Obejmuje

wstrzykiwanie SQL i indukcję plików lokalnych (LFI). Test penetracyjny fabrykuje wewnętrzny lub zewnętrzny nieautoryzowany atak.

5. Darmowe narzędzie bezpieczeństwa od Google (ratproxy)

6. System operacyjny Kali Linux (OS): To narzędzie jest przeznaczone dla hakerów, a wiele wstępnie zainstalowanych narzędzi hakerskich jest już zainstalowanych. System operacyjny działa jako maszyna wirtualna na komputerze Mac/PC.

7. Wstrzyknięcia SQL:

a. Sqlmap: Jest to zautomatyzowane narzędzie do testowania penetracji typu open source do wykrywania i wykorzystywania wstrzyknięć SQL.

b. SQLNinja: To narzędzie sprawdza pod kątem wstrzyknięć SQL wymierzonych w Microsoft SQL Server.

c. Dodatek do przeglądarki Firefox o nazwie Hackbar: Ten test pomaga przetestować bezpieczeństwo witryny, w tym wstrzyknięcia SQL i dziury XSS.

Uwaga: Włączenie pliku umożliwia atakującemu wstawienie pliku, wykorzystując dynamiczne dołączanie plików (takie jak $.getScript jQuery), które jest zaimplementowane w aplikacji w celu dołączenia innego pliku. Plik jest następnie przesyłany przez dane wejściowe użytkownika i tam, gdzie nie ma odpowiedniej walidacji, aby sprawdzić plik. Rozwiązaniem jest zaimplementowanie walidacji dla dynamicznego włączania plików, aby zapewnić pochodzenie i zawartość.

Podczas faz wykrywania, audytu i testowania najprawdopodobniej znajdziesz małe lub poważne luki, które mogą wymagać powrotu do fazy kodowania, płukania i powtarzania tego procesu, aż Twoja platforma przejdzie wszystkie testy

Ocena gotowości

Gdy Twoja platforma przejdzie fazy wykrywania, audytu i testowania, jesteś gotowy do szczegółowego przyjrzenia się technicznym aspektom aplikacji blockchain, aby zapewnić wdrożenie bezpieczeństwa i zgodności. Odbywa się to poprzez ręczne przeprowadzenie oceny bezpieczeństwa i zgodności.

Ocena bezpieczeństwa i zgodności

Ta ocena opiera się na ocenach podatności wykonanych w poprzednich fazach. Przed wydaniem zaleca się dodanie etapu ręcznej weryfikacji, aby potwierdzić, że na Twojej platformie zastosowano branżowe i/lub wewnętrzne standardy bezpieczeństwa oraz ocenić ryzyko i ekspozycję. Ta faza powinna również obejmować obawy dotyczące gotowości bezpieczeństwa, które omówiłem w pierwszej części tego rozdziału.

Ponadto weryfikacja może obejmować:

- Sprawdzanie autoryzowanego dostępu do Twojej platformy i potwierdzanie ustawień systemowych

- Badanie logów platformy i serwera

- Zapewnienie zgodności z obowiązującymi przepisami

- Sprawdzanie i śledzenie kodów i komunikatów o błędach

- Badanie najnowszych przepisów dotyczących prywatności i przepisów

- Badanie dokumentacji projektowej i architektonicznej w celu upewnienia się, że kod spełnia te wymagania

- Przeprowadzanie przeglądu kodu

Pamiętaj, że ocena bezpieczeństwa i zgodności to szerszy obraz i nie powinieneś patrzeć na konkretne ujawnienie tylko jednej luki w zabezpieczeniach. Zamiast tego spójrz na platformę jako całość. Oceny mogą znaleźć dodatkowe zagrożenia i narażenia, które są nie do przyjęcia, co będzie wymagało powrotu do fazy projektowania i kodowania i ponownego rozpoczęcia tego procesu.

Wydanie

Gdy Twoja platforma przejdzie fazę oceny gotowości, opublikuj swoją platformę. Zaleca się przeprowadzenie tych samych testów i ponowne sprawdzenie rzeczywistego kodu produkcyjnego, aby upewnić się, że platforma nadal przechodzi testy i oceny. Po zakończeniu tego cyklu możesz przepłukać i powtórzyć ten proces dla nowego cyklu rozwoju.

Streszczenie

Podzieliłem bezpieczeństwo i zgodność procesu blockchain na trzy części: gotowość bezpieczeństwa, typowe ataki blockchain i zalecany cykl rozwoju. Pierwsza część służyła jako wprowadzenie, dzięki któremu można lepiej zrozumieć warunki i sposób myślenia o budowaniu bezpiecznej platformy. Omówiłem testowanie bezpieczeństwa i gotowość do zapewnienia zgodności, przyglądając się konkretnie wymaganiom zgodności ze Stanami Zjednoczonymi i Unią Europejską jako przykładami. Omówiłem zalecenia dotyczące gotowości bezpieczeństwa, które należy wziąć pod uwagę na etapie projektowania i kodowania. Następnie omówiłem typowe ataki blockchain, które skutkowały miliardowymi stratami. Ataki te były wymierzone głównie w portfele kryptograficzne, ale także sieci blockchain i platformy oparte na blockchain. Na koniec przedstawiłem zalecany cykl rozwoju, aby zapewnić uwzględnienie wszystkich potrzebnych problemów związanych z bezpieczeństwem i zgodnością. W następnym i ostatnim rozdziale poznasz blockchain nie tylko krypto. Omówię moc blockchain i sposób, w jaki można ją wykorzystać, a także decentralizację konkretnych branż, analizując kilka branż zakłócanych przez blockchain i konkretne studia przypadków.