1. Introducere

Scopul acestui document este să expună procedurile și să definească regulile de interacțiune strânsă cu investigatorii-specialiști în domeniul securității informatice în timpul efectuării testelor de securitate în mediul de lucru al grupului TBI Bank. Acest program urmează Cele mai bune practici de securitate a informațiilor. O astfel de procedură se utilizează în multe Instituții financiare din Europa. Obiectivele acestei politici sunt:

- să stabilească dacă și în ce mod un utilizator neautorizat poate obține acces neautorizat la activele care afectează securitatea de bază a sistemului, fișierele, înregistrările și / sau datele sensibile;
- pentru a confirma că au fost instituite măsuri de control aplicabile, cum ar fi acoperirea, gestionarea vulnerabilităților, metodologia și segmentarea.

2. Domeniu de aplicare

Domeniul de aplicare al acestei politici include toate activele: TBI Bank EAD, TBI Bank EAD Sofia - Sucursala București, TBI Credit IFN SA (România), TBI Leasing IFN SA (România). Acest Program acoperă o varietate de medii de lucru, cum ar fi toate sistemele, aplicațiile, serviciile de internet, Interfețe pentru aplicații (API-urile), serviciile mobile și toate țintele potențiale de atac care fac parte din infrastructura băncii.
Cazurile problematice raportate vor fi luate în considerare, numai dacă acestea se referă la codul utilizat în mediul de lucru.

3. Reguli de participare

Prin trimiterea de rapoarte sau participând altfel la acest Program, dvs. confirmați că ați citit și sunteți de acord să respectați Regulile Programului și secțiunile cu condițiile juridice din această Politică a Programului.

3.1. Regulile Programului

Încălcarea oricăreia dintre aceste reguli poate duce la neatribuirea remunerației și / sau excluderea din program.

- Nu folosiți niciodată descoperirile dvs. pentru a compromite / extrage date sau pentru a le redirecționa către alte sisteme. Folosiți metoda dovedirii conceptului numai pentru a demonstra aspectul problematic concret.
- Dacă informații sensibile (cum ar fi informații personale, date de identitate etc.) sunt accesate ca parte a unei vulnerabilități anume, atunci aceste informațiile sensibile nu ar trebui să fie memorate, stocate, transferate, accesate sau procesate în niciun alt mod după dezvăluirea sa inițială. Toate copiile informațiilor sensibile trebuie returnate lui TBI Bank și nu pot fi păstrate.
- Investigatorii nu pot și nu sunt autorizați să se angajeze în nicio activitate care poate pune în pericol, dăunează sau cauzează pagube mărcilor comerciale ale TBI Bank sau utilizatorilor săi. Inclusiv: inginerie socială, achiziție frauduloasă de informații sensibile pe internet (phishing), amenințări la adresa securității fizice și atacuri de tipul ”refuz de serviciu” (DDOS) împotriva utilizatorilor și angajaților.

- Investigatorii nu pot face vulnerabilitățile descoperite public (prin împărtășirea oricăror detalii cu oricine altcineva decât angajații autorizați) sau în alt mod să împărtășească vulnerabilități cu o terță parte fără permisiunea scrisă expresă a TBI Bank.

3.2. Condiții juridice

În legătură cu participarea dvs. la acest program, dvs. sunteți de acord să respectați Termenii și condițiile generale ale TBI Bank, Politica sa de Confidențialitate, precum și toate legile și reglementările aplicabile, inclusiv orice legi și prevederi care reglementează confidențialitatea sau prelucrarea legală a datelor.

TBI Bank își rezervă dreptul de a schimba sau modifica termenii acestui program în orice moment.

TBI Bank nu acordă permisiunea / autoritatea (implicit sau explicit) nici unei persoane sau grupuri de persoane de a extrage informații personale sau date ale oricăror utilizatori sau de a dezvălui aceste informații într-un mediu de internet deschis, public, fără acordul utilizatorului, sau să modifice sau să utilizeze în scopuri dăunătoare produse software sau date care aparțin lui TBI Bank.

Angajații de la TBI Bank (inclusiv foști angajați care au plecat în ultimele 12 luni), funcționari angajați suplimentar, antreprenorii și personalul acestora, precum și consultanții, dar și membrii de familie pe linie dreaptă și persoanele care locuiesc în aceeași gospodărie nu sunt eligibili pentru a primi recompense sau remunerație de orice fel de la orice programe de răsplătire pentru erori de program descoperite (bugs), indiferent dacă sunt organizate de TBI Bank sau de orice terță parte.

4. Integritatea personală a participanților

TBI Bank nu va da în judecată sau nu va iniția orice altă acțiune legală împotriva unui investigator ca răspuns la o vulnerabilitate raportată de acesta dacă investigatorul îndeplinește toate cerințele acestui program.

Este important să înțelegeți că dacă activitățile dvs. de cercetare în domeniul securității implică rețele, sisteme, informații, aplicații, produse sau servicii ale unei terțe părți (altele decât noi), atunci terța parte va decide dacă va lua măsuri legale. Noi nu putem și nu acordăm autoritate pentru activități de investigare în domeniul securității în numele altor organizații. Dacă va fi inițiată o acțiune juridică împotriva dvs. de către o terță parte, iar dvs. ați respectat regulile acestui program, atunci noi vom lua măsuri rezonabile pentru a anunța că acțiunile dvs. au fost efectuate în conformitate cu termenii acestui program.

Ca întotdeauna, ne așteptăm din partea dvs. să respectați toate legile și reglementările aplicabile.
Vă rugăm să ne trimiteți un raport înainte de a lua măsuri care pot fi în neconcordanță sau care nu se regăsesc în acest program.

Vă rugăm să rețineți următoarele: în cazul în care dezvăluiți public descoperirile dvs. înainte noi de a avea ocazia de a corecta eventualele discrepanțe, acest lucru vă va elimina posibilitatea de

a primi remunerația. În schimb, vorbiți cu experții noștri și permiteți-le să evalueze și să rezolve problema.

5. Dezvăluirea responsabilă a Vulnerabilităților

Lucrăm constant pentru a dezvolta programul nostru de descoperire a erorilor de programare. Scopul nostru este să răspundem cât mai rapid la rapoartele primite și să depunem toate eforturile pentru a îndepărta erorile de programare în termen de **120 de zile** de la clasificarea acestora.

Verificatorul de penetrare a rețelei de calculatoare (Penetration Tester) va elimina toate datele referitoare la Testarea Securității protecției împotriva penetrării pentru fiecare dintre paginile de internet, de pe computerul (calculatoarele) Verificatorului folosind o metodă aprobată de TBI Bank.

Toate documentele, jurnalele / fișierele de date, rezultatele testelor și cărțile de lucru create de Verificatorul Protecției Rețelelor de computere contra Penetrării în legătură cu Verificarea Siguranței Protecției contra Penetrării pentru fiecare pagină de internet nu pot fi păstrate de Verificatorul Protecției contra Penetrării, acestea trebuie să fie predate lui TBI Bank. Toate datele sunt deținute de către TBI Bank și vor fi stocate de Direcția de Securitate Informațională.

Rapoartele trebuie să fie pregătite în două versiuni - Raport sumar și detaliat. Toate fișierele care conțin informații sensibile trebuie trimise prin canal criptat.

Trebuie prezentat un raport separat pentru Operațiunile cu card (cu acoperirea Standardului de Securitate a Datelor din Sectorul de Plată cu Card / PCI DSS) și pentru mediul de lucru SWIFT.

6. Verificare / Testare

Vă rugăm să efectuați următoarele acțiuni atunci când participați la programul "Remunerație pentru detectarea erorilor de programare":

- Trebuie să furnizați adresa dvs. IP în raportul erorilor de programare. Vom păstra această informație ca fiind una personală și o vom folosi doar pentru a verifica înregistrările / jurnalele referitoare la activitatea dvs. de testare.
- Includeți un antet HTTP personalizat în tot traficul dvs. de informații. Programul Burp și alte programe proxy vă permit să adăugați automat anteturi la toate solicitările trimise. Spuneți-ne ce tip de antet ați configurat pentru a-l putea identifica mai ușor. De exemplu:
  - Rândul de antet care include numele dvs. de utilizator: *X-Bug-Bounty: HackerOne- <nume de utilizator>*
  - Rândul de antet care include un flag unic sau identificabil: *X-Bug-Bounty: ID-<sha256-flag>*

Atunci când testați erorile de programare, de asemenea, luați în considerare:

- Folosiți numai conturi autorizate, astfel încât să nu compromiteți din greșeală informațiile confidențiale ale utilizatorilor noștri;
- Când încercați să demonstrați drepturi administrative cu următoarele primitive într-un proces vulnerabil, utilizați următoarele comenzi:

- Citește (Read): cat/proc/1/maps
- Scrieți (Write): *touch/root/<numele dvs. de utilizator H1>*
- Executați (Execute): identificația (id), numele serverului (hostname), comanda pwd (deși comenzile tehnice „cat" și „touch" demonstrează de asemenea executarea)

- Minimizați potențiale daune. Urmați regulile programului în orice moment. Nu folosiți programe / instrumente de scanare automată - aceste instrumente includ conținut care poate declanșa modificări ale condițiilor sau deteriora sistemele și / sau datele de lucru.
- Înainte de a face pagube sau de a provoca daune potențiale: Opriți-vă, raportați ce ați descoperit și solicitați permisiunea pentru teste suplimentare.

7. Pregătirea Raportului

Dacă echipa noastră de securitate nu este în măsură să reproducă și să verifice un aspect problematic, atunci nu se poate acorda remunerație. Pentru a optimiza procedura noastră de primire a rapoartelor trimise, vă rugăm să includeți în acestea următoarele:

- Descrierea erorii de programare (bug-ului)
- Descrierea scenariului de atac
- Impactul acestui scenariu
- Pașii pentru reproducerea vulnerabilității raportate
- Demonstrarea posibilității de folosire a vulnerabilității (ex. Captură de ecran, videoclip)
- Posibilul impact asupra altui utilizator sau asupra organizației
- Lista adreselor de internet (URL) și a parametrilor afectați
- Alte adrese de internet vulnerabile (URL), conținut adăugat, Cod de demonstrare a Concepției
- Browser, sistem de operare și / sau versiune software utilizate în timpul testării
- Soluție pentru eroarea de programare și corecția acesteia.

Atenție: Nerespectarea acestor cerințe minime poate duce la pierderea remunerației.

Toate probele justificative și alte anexe trebuie să fie stocate numai împreună cu raportul pe care îl trimiteți. Nu stocați orice tip de fișiere la furnizori de servicii externi.

7.1. Aceiași eroare de programare, dar la un alt Host

Pentru fiecare raport, vă rugăm să acordați suficient timp lui TBI Bank pentru a pregăti o actualizare (patch) și pentru cazurile cu alte Host-uri. Dacă găsiți același bug la un Host diferit (unic), atunci înainte de procesarea raportului, trebuie să îl raportați în raportul existent pentru a primi bonusul suplimentar de 10% (pentru Host, nu pe Domain). Toate rapoartele trimise separat în timp ce lucrăm activ pentru soluționarea problemei vor fi tratate ca duplicate ale raportului inițial.

7.2. Același Conținut util, dar Parametru Diferit

În unele cazuri, remunerațiile pot fi combinate într-o singură plată. De exemplu, rapoarte multiple despre una și aceiași vulnerabilitate la parametri diferiți în cadrul unei singure resurse sau care

demonstrează mai mulți vectori de atac împotriva unei probleme de sistem majoră. Vă rugăm să uniți rapoartele în loc să le împărțiți.

8. Remunerația

Pentru a încuraja raportarea vulnerabilităților la TBI Bank, vă invităm să ne trimiteți orice fel de vulnerabilități pe care le-ați identificat. După cum am menționat, puteți fi recompensați pentru acest lucru. Suma remunerației depinde de gravitatea vulnerabilității raportate, de tipul paginii de internet afectate (pagini de informații statice versus pagini de tranzacții bancare online), dar și de calitatea raportului pe care îl primim. Dacă raportul are o importanță deosebită pentru continuitatea proceselor și fiabilitatea băncii, atunci remunerația va fi mult mai mare.

Veți avea dreptul la remunerație numai dacă sunteți primul care raportează o problemă necunoscută. Bug-urile clasificate vor fi remunerate în funcție de gravitatea lor, care va fi stabilită de TBI Bank la discreția sa. Remunerația este în totalitate la discreția TBI Bank.

La discreția TBI Bank , remunerația poate fi majorată atunci când se furnizează un studiu mai complet, a codului de probă a concepției și a investigării detaliate. Contrariul este, de asemenea, valabil - TBI Bank poate plăti mai puțin pentru vulnerabilitățile descoperite, care necesită interacțiuni complexe sau prea complexe sau al căror impact sau risc de securitate este neglijabil. Remunerația poate fi refuzată dacă există dovezi privind încălcarea Politicii programului.

Remunerația va fi refuzată dacă găsim dovezi de abuz.

8.1. Evaluarea vulnerabilităților

Acest tabel oferă informații generale despre modul în care clasificăm vulnerabilitățile, clasificându-le în funcție de severitate de la cea mai mare la cea mai mică (în cadrul clasei lor de severitate). Acest tabel este destinat numai orientării generale, având în vedere că severitatea unei anumite vulnerabilități va fi stabilită de TBI Bank, la discreția sa.

Notă: Vulnerabilitățile care nu sunt incluse în listă pot participa la program. Unele tipuri de vulnerabilități se pot încadra în mai multe categorii de severitate, în funcție de sfera / amploarea potențialului abuz și de impactul acestuia.

Severitate	Abreviere	Denumirea în întregime
Critică	RCE	Executarea codului la distanță
Critică	SQLi	Implementarea codului SQL
Critică	---	Creșterea Dreptului de Acces la Profilul de sistem
Critică	XXE	Entitatea externă XML
Critică	XMLi	Implementarea codului XML
Mare	VPE	Extinderea Dreptului de Acces cu Amploare Verticală
Mare	IDOR	Referință directă la Obiect nesigură
Mare	SSRF	Falsificare Cerere din partea Server-

		ului.
Mare	---	Evitarea Autentificației sau Permisiuni de Acces
Mare	LFI	Adăugarea de Fișiere locale
Mare	ATO	Preluarea Controlului Profilului
Mare	SSI	Implementare Componenente din Partea Server-ului
Mare	---	Încărcarea la serviciul cloud S3
Mare	---	Extragerea în masă a informațiilor personale care permit identificarea
Medie	SSRF	SSRF în Baza ”Răspunsuri HTTP și oarbe”
Medie	XSS	Scripturi stocate între diferite site-uri
Medie	UE	Lista utilizatorilor și informațiile lor personale care permit identificarea
Medie	CSRF	Cerere de schimbare a statutului contrafăcută între diferite site-uri
Medie	---	Date primite de identificare a Profilurilor privilegiate
Medie	HPE	Extinderea orizontală a Dreptului de Acces
Medie	CRLFi	Implementarea codului CRLF
Medie	SDTO	Preluarea controlului asupra Subdomeniului
Medie	---	Expunerea de Date sensibile
Scăzută	gXSS	Scripturi reflectate bazate pe GET între Diferite Site-uri
Scăzută	pXSS	Scripturi reflectate bazate pe POST între Diferite Site-uri
Scăzută	dXSS	Scripturi bazate pe DOM între Diferite Site-uri
Scăzută	nCSRF	Cerere contrafăcută fără Schimbare de statut între Diferite Site-uri
Scăzută	---	Atașarea unei înregistrări DNS
Scăzută	---	Primirea de Parole prin Cleartext
Scăzută	fXSS	Scripturi bazate pe Flash între Diferite Site-uri
Scăzută	---	Pagina de informații MySQL cu Date de Identificare
Scăzută	---	Redirecționare deschisă
Scăzută	---	Pagina - server cu informații (cu Date de identificare)
Scăzută	---	Pagina - server cu informații (fără Date de identificare)
Scăzută	---	Dezvăluirea de Date Confidențiale
Nu este	---	Dezvăluirea de Date fără Statut de Confidențialitate

8.2. Erori de programare la granița domeniului de aplicare a programului, fără remunerație

Următoarele cazuri problematice sunt eligibile pentru depunerea unui raport, dar nu sunt remunerative sau nu vor fi răsplătite în niciun alt fel. După ce sunt clasificate, acestea vor fi închise cu status „ Doar informativ", numai dacă sunt valabile, și ca "Spam" dacă sunt invalide. Când raportați vulnerabilități, vă rugăm să luați în considerare scenariul de atac / posibilitatea de abuz, precum și impactul erorilor de programare asupra securității.

Orice Aplicație de tip Media care nu este a lui TBI Bank	Lista profilurilor; "Propriu" ("Self") XSS
Lipsesc Cele mai bune practici de securitate	XSS HTTP - Antetul Host-ului
Scurgerea Informațiilor Confidențiale	Făcând clic pe Consecința Delusion / Schimbarea Interfeței Utilizatorului
Utilizarea bibliotecii cu vulnerabilități cunoscute (fără dovezi de potențiale abuzuri)	Redirecționări intenționate descoperite
Flag-urile cookie-urilor care lipsesc	Descărcarea fișierului reflectată
Cele mai bune practici SSL / TLS	SPF / DKIM incomplet / lipsă
Atacuri fizice	Atacuri cu scop de Inginerie socială
Rezultate de la Scanere Automate	CSRF la Logare / Deconectare / Neidentificat
Funcția Completare automată (Autocomplete) pe formularele web	Utilizarea vulnerabilităților neraportate
Folosirea Sistemului de Abuzuri („Self" exploitation)	Probleme de protocol în rețea
XSS în fișiere flash nu este dezvoltat de TBI Bank sau de orice alt contractant	Publicarea Versiunii Software
Raportarea erorilor din pagină (fără dovezi de potențiale abuzuri)	Atacuri de tip "refuz de serviciu" (DDOS)
Software TBI Bank care se apropie de sfârșitul perioadei sale de întreținere sau nu mai este acceptat	Lista de e-mailuri
Lipsește Antetul HTTP pentru Securitate (fără dovezi de potențiale abuzuri)	Redirecționare internă, scanare, utilizare greșită sau extragere de date

Notă: Vulnerabilitățile "din ziua 0" (din implementarea unui element anume) pot fi raportate până la 60 de zile de la anunțul inițial. Echipa noastră lucrează special pentru a urmări aceste probleme; gazdele identificate de această echipă și atribuite unui număr intern nu pot fi utilizate pentru a primi remunerație.

9. În afara domeniului de aplicare al Programului

Următoarele cazuri problematice sunt considerate că nu intră în sfera de aplicare a programului:

- Cele referitoare la servicii furnizate de terți
- Probleme care nu afectează cele mai recente versiuni ale browser-elor moderne

- Probleme despre care știm sau au fost raportate deja în trecut
- Probleme care necesită interacțiuni improbabile cu utilizatorii
- Dezvăluirea informațiilor care nu prezintă un risc semnificativ
- Refacerea unei Solicitări între diferite site-uri cu impact minim de securitate
- Încorporarea („injectarea”) fișierelor în format CSV
- SPF / DKIM incomplete sau lipsă
- Luarea în considerare a celor mai bune practici general acceptate

10. Contact

Vă rugăm să trimiteți întrebările dvs. la următoarea adresă de e-mail:

bugbounty@tbibank.bg