Документ: Програма „Възнаграждение за откриване на програмни грешки”

1. Въведение

Предназначението на този документ е да изложи процедурите и да определи правилата за тясно взаимодействие с изследователи-специалисти по компютърна сигурност при провеждане на тестове за проверка на сигурността в работната среда Групата на 4финанс ЕООД и 4финанс ЕООД. Тази програма следва Най-добрите Практики за Информационна Сигурност. Такава процедура се използва в много Финансови институции в Европа. Целите на тази програма са:

- да се определи дали и по какъв начин недобронамерен потребител може да получи неоторизиран достъп до активи, които оказват влияние върху базовата сигурност на системата, файловете, записите и/или чувствителните данни;
- да се потвърди, че приложимите контролни мерки като обхват, управление на уязвимостта, методология и сегментация, са въведени и в сила.

2. Обхват

Обхватът на тази политика включва всички активи на 4финанс ЕООД. Тази Програма обхваща разнообразни работни среди като всички системи, приложения, интернет-услуги, Приложно-Програмни Интерфейси (API), мобилни услуги и всички потенциални обекти на атака, които са част от инфраструктурата на банката.
Докладваните проблемни случаи ще бъдат приемани за действителни, само ако се отнасят до кода, използван в работната среда.

3. Правила за участие

С изпращането на доклади или участвайки по друг начин в тази Програма, Вие потвърждавате, че сте прочели и се съгласявате да следвате Правилата на Програмата и разделите с юридическите условия на тази програмна Политика.

3.1. Правила на Програмата

Нарушаването на което и да е от тези правила може да доведе до неприсъждане на възнаграждение и/или изключване от програмата.

- Никога не използвайте Вашите открития за компрометиране/извличане на данни или пренасочването им към други системи. Използвайте метода за доказване на концепцията единствено с цел демонстрирането на даден проблемен въпрос.
- Ако бъде осъществен достъп до чувствителна информация (например лична информация, идентификационни данни и др.) като част от дадена уязвимост, то тази чувствителна информация не трябва да бъде запомняна, съхранявана, прехвърляна, достъпвана, или обработвана по какъвто и да е друг начин след първоначалното ѝ разкриване. Всички копия на чувствителна информация трябва да бъдат върнати на 4финанс ЕООД и не могат да бъдат запазвани.
- Изследователите не могат и не са оторизирани да извършват каквато и да е дейност, която може да застраши, навреди или нанесе щети на търговските марки на 4финанс ЕООД или на нейните потребители. Това включва: социално инженерство, неправомерно придобиване на чувствителна информация по мрежов път (phishing),

заплахи, свързани с физическата сигурност, и атаки от типа „отказ на услуга” (DDOS) срещу потребители и служители.
- Изследователите не могат да правят откритите уязвимости обществена информация (като споделят каквито и да е подробности с когото и да е, освен с оторизираните служители), или по друг начин да споделят уязвимости с трета страна, без изричното писмено разрешение на 4финанс ЕООД.

3.2. Юридически условия

Във връзка с Вашето участие в тази програма, Вие се съгласявате да спазвате Общите Правила и Условия на 4финанс ЕООД, нейната Политика за Поверителност, както и всички приложими закони и разпоредби, включително всички закони и разпоредби, регулиращи поверителността или законната обработка на данни.

4финанс ЕООД си запазва правото да променя или видоизменя условията на тази програма по всяко време.

4финанс ЕООД не дава разрешение/правомощия (независимо дали по подразбиране или изрични) на никое лице или група лица да извлича лична информация или данни на които и да е потребители или да разгласява тази информация в откритата, обществено достъпна интернет-среда без съгласието на потребителя или да видоизменя или използва за зловредни цели програмни продукти или данни, принадлежащи на 4финанс ЕООД.

Служителите на 4финанс ЕООД (включително бивши служители, които са напуснали в последните 12 месеца), извънредно наети работници, изпълнители по договори и техния персонал, и консултанти, както и техните непосредствени членове на семействата и лица, живеещи в същото домакинство, нямат право да получават награди или възнаграждения от какъвто и да вид по която и да е от програмите за награди за открити програмни грешки (бъгове), независимо дали е организирана от 4финанс ЕООД или която и да е трета страна.

4. Лична неприкосновеност на участниците

4финанс ЕООД няма да завежда дело или друго правораздавателно разследване срещу изследовател в отговор на докладвана от него уязвимост, ако изследователят изпълнява всички изисквания на тази програма.

Важно е да разберете, че ако Вашите проучвателни дейности в областта на сигурността включват мрежи, системи, информация, приложения, продукти или услуги на трета страна (различна от нас), то тази трета страна ще вземе решението дали да предприеме юридически действия. Ние не можем и не предоставяме правомощия за проучвателни дейности по сигурността от името на други организации. Ако бъдат започнати правни действия от трета страна срещу Вас, а Вие сте спазили правилата на тази програма, то ние ще вземем разумни мерки за да оповестим, че Вашите действия са били извършени при спазване на условията на тази програма.

Както винаги, от Вас се очаква да спазвате всички приложими закони и разпоредби.
Моля да изпратите доклад до нас преди да започнете да извършвате действия, които може да не съответстват или да не са описани в тази програма.

Моля да обърнете внимание: в случай, че разгласите публично Вашите открития, преди ние да сме коригирали несъответствията, то това ще Ви отстрани от възможността да получите възнаграждението. Вместо това, моля да говорите с нашите експерти и да им дадете възможност да оценят и разрешат проблема.

5. Отговорно Разгласяване на Уязвимостите

Ние непрекъснато работим за развитието на нашата програма за откриване на програмни грешки. Нашата цел е да отговорим на входящите подадени доклади, колкото е възможно по-бързо и да положим всички усилия за отстраняване на програмните грешки в рамките на **120 дни** след тяхната категоризация.

Проверяващият Защитата на Компютърната Мрежа от Проникване (Penetration Tester) ще отстрани всички данни, отнасящи се до Проверката на Сигурността на Защитата от Проникване за всяка от интернет страниците, от компютър (компютри) на Проверяващия, с използването на метод, одобрен от 4финанс ЕООД.

Всички документи, логове/файлове с данни, тестови резултати, и работни книжа, създадени от Проверяващия Защитата на Компютърната Мрежа от Проникване за Проверката на Сигурността на Защитата от Проникване за всяка интернет страница, не могат да бъдат запазвани от Проверяващия Защитата от Проникване, а трябва да бъдат предадени на 4финанс ЕООД. Всички данни стават собственост на 4финанс ЕООД и ще бъдат съхранявани от Отдела за Сигурност на Информацията.

Докладите трябва да бъдат изготвени в две версии – Резюме и Подробен доклад. Всички файлове, съдържащи чувствителна информация трябва да бъдат изпращани по криптиран канал.

Отделен доклад трябва да бъде представен за Картовите Операции (с обхват Стандарта за Сигурност на Данни в Сектора за Плащане с Карти/PCI DSS) и за работната среда на SWIFT.

6. Проверка/Тестване

Моля да извършите следните действия, когато участвате в програмата „Възнаграждение за откриване на програмни грешки”:

- Трябва да предоставите своя IP-адрес в доклада за програмни грешки. Ние ще запазим тази информация като лична и ще я използваме само за проверката на записи/логове, отнасящи се до Вашата дейност по тестването.
- Включете персонализиран HTTP-хедър в целия Ваш трафик на информация. Програмата Burp и други прокси-програми позволяват автоматичното добавяне на хедъри към всички изходящи запитвания. Уведомете ни за това какъв хедър сте нагласили, за да можем да го идентифицираме по-лесно. Например:
    - Заглавен ред, който включва Вашето потребителско име: *X-Bug-Bounty:HackerOne-<потребителско име>*
    - Заглавен ред, който включва уникален или идентифицируем флаг: *X-Bug-Bounty:ID-<sha256-флаг>*

Когато тествате за програмни грешки, моля също така да имате предвид:

- Използвайте само оторизирани профили, така че да не предизвикате непреднамерено компрометиране на поверителната информация на нашите потребители;
- Когато се опитвате да демонстрирате администраторски права със следните примитиви в даден уязвим процес, моля да използвате следните команди:
    - Прочети (Read): *cat /proc/1/maps*
    - Напиши (Write): *touch /root/<Вашето H1 потребителско име>*
    - Изпълни (Execute): идентификация (id), името на сървъра (hostname), командата pwd (въпреки че технически командите „cat” и „touch” също доказват изпълнение)
- Сведете потенциалните щети до минимум. Следвайте правилата на програмата по всяко време. Не използвайте автоматизирани сканиращи програми/инструменти – тези инструменти включват съдържание, което може да задейства промени в условията или да увреди работните системи и/или данни.
- Преди да нанесете щети или да причините потенциални вреди: Спрете, докладвайте какво сте открили и изискайте разрешение за допълнителни тестове.

7. Изготвяне на доклад

Ако нашият екип по сигурността не може да възпроизведе и провери даден проблемен случай, то възнаграждение не може да бъде дадено. С цел оптимизиране на нашата процедура за приемане на входящи доклади, моля да включвате в тях следното:

- Описание на програмната грешка (бъга)
- Описание на сценария на атаката
- Въздействието на този сценарий
- Стъпки за възпроизвеждане на докладваната уязвимост
- Доказателство за възможността за възползване от уязвимостта (например снимка на екрана, видео)
- Възможно въздействие върху друг потребител или върху организацията
- Списък на интернет адреси (URL) и засегнатите параметри
- Други уязвими интернет адреси (URL), добавено съдържание, Код за Доказване на Концепция
- Браузър, операционна система и/или програмна версия, използвана по време на тестването
- Решение на програмната грешка и нейната корекция.

Внимание: Неспазването на тези минимални изисквания може да доведе до загуба на възнаграждение.

Всички поддържащи доказателствени материали и други приложения трябва да бъдат съхранявани единствено заедно с доклада, който подавате. Не съхранявайте каквито и да е файлове при външни доставчици на услуги.

7.1. Същата Програмна Грешка, но на Друг Хост

За всеки доклад, моля да предоставите достатъчно време на 4финанс ЕООД, за да изготви актуализация (пач) и за случаите с други хостове. Ако откриете същата програмна грешка на различен (уникален) хост, то преди да докладът да бъде обработен, трябва да съобщите за това, в рамките на съществуващия доклад, за да получите допълнителни 10% бонус (на хост, не на домейн). Всички доклади, подадени самостоятелно, докато ние работим активно за решаване на проблема, ще бъдат разглеждани като дубликати на оригиналния доклад.

7.2. Същото Полезно Съдържание, но Различен Параметър

В някои случаи, възнагражденията могат да бъдат обединени в едно плащане. Например, няколко доклада за една и съща уязвимост при различни параметри в рамките на един ресурс, или демонстриране на множество вектори на атака срещу основен системен проблем. Любезно Ви молим да обединявате докладите, вместо да ги разделяте.

8. Възнаграждения

За да поощрим докладването на уязвимости на 4финанс ЕООД, Ви подканяме да ни изпращате каквито и да е уязвимости, които сте открили. Както бе споменато, Вие можете да бъдете възнаграден за това. Размерът на възнаграждението зависи от сериозността на докладваната уязвимост, типа на засегнатата интернет-страница (страници със статична информация срещу страници за онлайн банкиране), както и от качеството на получения от нас доклад. Ако докладът е от голямо значение за непрекъснатостта на процесите и надеждността на банката, то възнаграждението ще бъде значително по-високо.

Вие ще имате право на възнаграждение, само ако сте първия, който съобщи за неизвестен проблем. Класираните програмни грешки ще бъдат възнаграждавани съобразно тяхната сериозност, която ще бъде определена от 4финанс ЕООД по своя преценка. Възнагражденията се отпускат изцяло по преценка на 4финанс ЕООД.

По решение на 4финанс ЕООД, възнаграждението може да бъде увеличено при предоставянето на по-пълно проучване, код за доказване на концепцията и подробно изследване. Обратното също е в сила – 4финанс ЕООД може да заплати по-малко възнаграждение за открити уязвимости, които изискват комплексни или прекалено сложни взаимодействия или чието въздействие или риск за сигурността е пренебрежимо малък. Отпускането на възнаграждение може да бъде отказано, ако съществуват доказателства за нарушения на програмната политика.

Отпускането на възнаграждение ще бъде отказано, ако открием доказателство за злоупотреба.

8.1. Оценяване на уязвимостите

Тази таблица дава обща информация за това как класифицираме уязвимостите, като те са категоризирани според тяхната сериозност от най-висока към най-ниска (в рамките на техния клас на сериозност). Тази таблица служи само за предоставяне на общи насоки, като класа на сериозност на конкретна уязвимост ще бъде определена от 4финанс ЕООД по нейната собствена преценка.

Забележка: Уязвимости, които не са включени в списъка, също могат да участват в програмата. Някои типове уязвимости могат да попаднат под няколко категории на сериозност, в зависимост от обхвата/мащаба на възможната злоупотреба и въздействието й.

Сериозност	Кратко име	Пълно Наименование
Критична	RCE	Дистанционно Изпълнение на Код
Критична	SQLi	Внедряване на SQL-код
Критична	---	Повишаване на Правото за Достъп до Системния Профил
Критична	XXE	XML Външен Субект
Критична	XMLi	Внедряване на XML-код
Висока	VPE	Разширяване на Правото за Достъп във Вертикален Обхват
Висока	IDOR	Несигурна Директна Препратка към Обект
Висока	SSRF	Фалшификация на Заявка от Страна на Сървъра
Висока	---	Заобикаляне на Удостоверяването или Разрешението за Достъп
Висока	LFI	Добавяне на Локални Файлове
Висока	ATO	Поемане на Контрол върху Профил
Висока	SSI	Внедряване на Добавки от Страна на Сървъра
Висока	---	Качване в облачната услуга S3
Висока	---	Масово Извличане на Лична Информация, Позволяваща Идентификация
Средна	SSRF	SSRF на Базата на ‘”Слепи и HTTP Отговори
Средна	XSS	Съхранени Скриптове между Различни Сайтове
Средна	UE	Списък на Потребители и Личната им Информация, Позволяваща Идентификация
Средна	CSRF	Фалшифицирана Заявка за Промяна в Статуса между Различни Сайтове
Средна	---	Получени Идентификационни Данни на Привилегировани Профили
Средна	HPE	Хоризонтално Разширяване на Правото за Достъп
Средна	CRLFi	Внедряване на CRLF-код
Средна	SDTO	Поемане на Контрол над Субдомейн
Средна	---	Излагане на Чувствителни Данни
Ниска	gXSS	GET-базирано Отразено Скриптиране между Различни Сайтове

Ниска	pXSS	POST-базирано Отразено Скриптиране между Различни Сайтове
Ниска	dXSS	DOM -базирано Скриптиране между Различни Сайтове
Ниска	nCSRF	Фалшифицирана Заявка без Промяна в Статуса между Различни Сайтове
Ниска	---	Закачане на DNS Запис
Ниска	---	Получаване на Пароли чрез Cleartext
Ниска	fXSS	Скриптиране Между Различни Сайтове, базирано на Флаш
Ниска	---	Информационна Страница на MySQL с Идентификационни Данни
Ниска	---	Открито Пренасочване
Ниска	---	Сървърна Информационна Страница (с Идентификационни Данни)
Ниска	---	Сървърна Информационна Страница (без Идентификационни Данни)
Ниска	---	Разгласяване на Поверителни Данни
Няма	---	Разгласяване на Данни без Статус на Поверителност

8.2. Програмни грешки на границата на обхвата на програмата, без възнаграждение

Следните проблемни случаи се допускат за подаване на доклад, но не подлежат на възнаграждение или каквото и да е друга награда. Веднъж класифицирани, те ще бъдат закрити със статус „Само за информация”, само ако са действителни, и като „Спам”, ако са недействителни. Когато докладвате за уязвимости, моля да имате предвид сценария на атаката / възможността за злоупотреба, както и въздействието на програмната грешка върху сигурността.

Всяко Медийно Приложение, което не е на 4финанс ЕООД	Списък с профили; "Собствен" (“Self”) XSS
Липсващи Най-Добри Практики в Областта на Сигурността	XSS HTTP-Хедър на Хоста
Изтичане на Поверителна Информация	Кликане в Следствие на Заблуда/Смяна на Потребителския Интерфейс
Използване на библиотека с известни уязвимости (без свидетелства за възможност за злоупотреби)	Умишлени Открити Пренасочвания
Липсващи флагове на „бисквитки”	Отразено сваляне на файл
Най-добри Практики в SSL/TLS	Непълен/Липсващ SPF/DKIM
Физически Атаки	Атаки с цел Социално Инженерство
Резултати от Автоматизирани Скенери	CSRF при Логин/Логаут/Неидентифициран
Функцията за Автоматично Допълване (Autocomplete) в Интернет-формуляри	Използване на недокладвани уязвимости

Използване на Системата за Злоупотреби ("Self" exploitation)	Проблеми, свързани с мрежовите протоколи
XSS във флаш-файловете не е разработен от 4финанс ЕООД или който и да е друг изпълнител по договор	Разгласяване на Софтуерната Версия
Известяване за грешка в страниците (без свидетелства за възможност за злоупотреби)	Атаки от типа „отказ на услуга” (DDOS)
Софтуер на 4финанс ЕООД, който наближава края на срока на поддръжка или вече не се поддържа	Списък с и-мейли
Липсващи HTTP-Хедъри за Сигурност (без свидетелства за възможност за злоупотреби)	Вътрешно пренасочване, сканиране, използване с цел злоупотреба, или извличане на данни

Забележка: Уязвимости „от Ден 0” (от внедряването на даден елемент) могат да бъдат докладвани до 60 дни след първоначалното им обявяване. Наш екип работи специално за проследяването на тези проблеми; хостовете, идентифицирани от този екип, и с назначен вътрешен номер, не могат да се използват за получаване на възнаграждение.

9. Извън обхвата на програмата

Следните проблемни случаи се считат за попадащи извън обхвата на програмата:

- Тези, които се отнасят до услуги, предоставяни от трети страни
- Проблеми, които не засягат последните версии на съвременните браузъри
- Проблеми, за които ние знаем, или които са били вече докладвани в миналото
- Проблеми, които изискват малко вероятно взаимодействие с потребителя
- Разгласяване на информация, която не представлява значителен риск
- Подправяне на Заявка Между Различни Сайтове с минимално влияние върху сигурността
- Внедряване („инжектиране”) на файлове в CSV-формат
- Непълни или липсващи SPF/DKIM
- Съображения относно общоприетите най-добри практики

10. Контакти

Моля да изпращате своите въпроси на:

bugbounty@tbibank.bg