октябрь / 2024

CHERVETS
PARTNERS

White hat hackers

Наша команда

Синицына
Юлия

Партнер
IP & IT

Мария
Любимова

Партнер
Foreign Desk / IP & IT

I. «Белые хакеры» это легально?

Типизация


Black Hat
хакер-преступник
White Hat
этичный хакер
Grey Hat
и не преступник,
но и не “святой”
Blue Hat
хакер, который мстит
из личных побуждений
Green Hat
хакер-новичок
Red Hat
хакер, который
наказывает
Black Hat

Страны, где пентесты являются законными:

	Правонарушение	Наказание
1	**Германия**	Уголовный кодекс Германии допускает этичный взлом с согласия владельца ИТ системы
2	**Нидерланды**	Уголовный кодекс Нидерландов допускает этичный взлом с согласия владельца
3	**Швейцария**	Уголовный кодекс Швейцарии разрешает этичный взлом, если лицо, осуществляющее взлом, имеет законные полномочия или согласие владельца
4	**Мальта**	Правительство Мальты работает над созданием правовой базы, которая будет поддерживать этичную практику хакерства. Предлагаемые изменения появились после того, как несколько лет назад против трех студентов факультета компьютерных наук Мальтийского университета и их преподавателя были выдвинуты уголовные обвинения. Они обнаружили недостатки в FreeHour, крупнейшем студенческом приложении Мальты.

Страны, с более строгим регулированием:

1. **Великобритания** — В 1990 году был создан Закон о неправомерном использовании компьютеров (CMA) для регулирования законного доступа к компьютерным данным. Этот закон запрещает несанкционированный доступ к данным и изменение хранимой информации без согласия владельца. Согласно CMA, получение несанкционированного доступа к компьютерным системам является незаконным. Национальный центр кибербезопасности Великобритании (NCSC) также руководит тем, как организации могут проводить тестирование на проникновение законно и этично.
2. **Индия** — Перед проведением теста на проникновение в Индии тестировщик должен получить разрешение от руководства. Затем тест должен проводиться в рамках предопределенных ограничений. Различные правовые и нормативные рамки регулируют деятельность по тестированию на проникновение в Индии, включая Закон об ИТ, IPC, руководящие принципы RBI, Национальную политику кибербезопасности и PCI DSS.
3. **Сингапур** — Согласно разделу 3(1) Закона о неправомерном использовании компьютеров 1993 года («CMA»), незаконно, чтобы кто-либо намеренно заставлял компьютер выполнять любую задачу для получения несанкционированного доступа к программе или данным, хранящимся на компьютере. Тестирование на проникновение допускается только с явного разрешения владельца тестируемой системы. Оно должно соответствовать рекомендациям Агентства кибербезопасности Сингапура (CSA).
4. **США** — Закон о компьютерном мошенничестве и злоупотреблении 1986 года (CFAA) запрещает доступ к компьютерным системам без разрешения, что включает в себя тестирование на проникновение. Закон о конфиденциальности электронных коммуникаций (ECPA) также запрещает тестирование на проникновение. NIST публикует различные стандарты и руководства по кибербезопасности, в том числе связанные с тестированием на проникновение.

Страны, с более строгим регулированием:

5. **Япония** — В Японии несколько законов и нормативных актов регулируют деятельность по тестированию на проникновение. Основными законами, регулирующими тестирование на проникновение в Японии, являются Закон о защите личной информации (APPI) и Закон о сетях информации и связи (ICNA).
6. **Канада** — Проведение несанкционированного тестирования на проникновение может считаться нарушением в соответствии с Уголовным кодексом Канады.
7. **Австралия** — Проведение тестирования на проникновение в систему или сеть без получения согласия ее владельца или администратора классифицируется как несанкционированный доступ, нарушение федерального Закона об уголовном кодексе 1995 года, и, следовательно, считается незаконным.
8. **Франция** - Во Франции при проведении тестирования на проникновение необходимо соблюдать требования законодательства, включая Закон о защите данных Франции, Уголовный кодекс Франции, Общий регламент по защите данных (GDPR) и руководящие принципы, установленные ANSSI. Кроме того, тестирование должно быть разрешено владельцем системы и проводиться с согласия лиц, работающих в системе.
9. **Южная Корея** — Основным законом, регулирующим тестирование на проникновение в Южной Корее, является Закон о содействии использованию информационно-коммуникационных сетей и защите информации (далее именуемый «Закон о сетях») и Указ о применении Закона о сетях.

Страны, с более строгим регулированием:

5. **Китай** — Положения о надзоре и инспекции безопасности в Интернете органами общественной безопасности. Эти положения дают полиции и другим органам общественной безопасности полномочия проводить инспекции и расследования в области кибербезопасности, включая пентесты, в отношении компаний, работающих в Китае. Другие организации должны получить необходимые разрешения и одобрения от соответствующих органов перед проведением любых мероприятий по пентестам, чтобы избежать нарушения этих законов и правил.

   Кроме того, Китай передал на аутсорсинг компоненты кибероперации своих военных и разведывательных сообществ, продвигая «патриотический хакеризм» для поддержки усилий страны по подготовке к потенциальному конфликту или во время него.

6. **Россия** - Основной закон регулирующий информационную безопасность - Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ, который определяет стандарты защиты информации. Согласно этому закону, любое испытание на проникновение требует одобрения владельца проверяемой системы.

II. Сертификация «Белых хакеров»

Сертификация оказывает значительное влияние на сферу этичного хакинга, поскольку служит для подтверждения навыков и знаний, которыми обладают этичные хакеры.

Сертификации часто включают в себя инструкции по правовым и этическим аспектам

Основные Сертификации

Certified Ethical Hacker (CEH) от Совета ЕС

одна из самых известных и признанных, охватывает широкий спектр тем, связанных с кибербезопасностью. CEH предназначена для специалистов, которые хотят углубить свои знания в области защиты информации и научиться выявлять уязвимости в системах. (подходит для начинающих)

Offensive Security Certified Professional (OSCP)

предоставляется организацией Offensive Security и ориентирована на практическое применение навыков в области этичного хакинга. Она считается одной из самых сложных и престижных сертификаций в этой области.

Certified Penetration Tester (CPT)

Сертификация предназначена для сотрудников службы безопасности, чьи должностные обязанности включают оценку целевых сетей и систем для поиска уязвимостей безопасности.

Другие популярные сертификации

01

> CISSP (Certified Information Systems Security Professional)

Сертификация CISSP предоставляется организацией (ISC) и охватывает широкий спектр тем в области информационной безопасности. Она предназначена для опытных специалистов и требует не менее 5 лет опыта работы в сфере безопасности. CISSP охватывает такие темы, как управление рисками, разработка и управление программами безопасности, а также правовые и нормативные аспекты информационной безопасности.

02

> GPEN (GIAC Penetration Tester)

предоставляется организацией GIAC и ориентирована на пентестеров. Охватываемые темы: методы взлома, эксплуатация уязвимостей и отчетность. GPEN предназначена для специалистов, которые хотят углубить свои знания в области пентестов и научиться выявлять уязвимости в системах.

03

> CISM (Certified Information Security Manager)

предоставляется организацией ISACA(США) и ориентирована на менеджеров по информационной безопасности. Охватываемые темы: управление рисками, разработка и управление программами безопасности. CISM предназначена для специалистов, которые хотят углубить свои знания в области управления информационной безопасностью и научиться разрабатывать и управлять программами безопасности.

III. Ответственность

Англия:

	Правонарушение	Наказание
1	**Несанкционированное или злонамеренное вмешательство в материалы, хранящиеся на компьютере**	лишение свободы 6 месяцев с возможным штрафом в размере 5000 фунтов
2	**Намерение совершить киберпреступление**	лишение свободы 5 лет или штраф (сумма з-но не ограничена)
3	**Изменение, удаление или кража данных**	лишение свободы 5 лет или штраф (сумма з-но не ограничена)
4	**Помощь в неправомерном использовании компьютеров**	лишение свободы 10 лет или штраф (сумма з-но не ограничена)

США:

	Правонарушение	Наказание
1	**Любой вид ущерба компьютерной системе, вторжение в такие системы или воздействие на них с помощью вредоносных кодов и DDoS**	лишение свободы до 10 лет, за повторное и(или) совершенное умышленно - до 20 лет, в случае причинения вреду человеческой жизни - вплоть до пожизненного. При этом Воздействие на компьютерную систему во время попыток взлома рассчитывается на годовой основе.
2	**Намерение совершить киберпреступление**	лишение свободы 5 лет или штраф (сумма з-но не ограничена)
3	**Изменение, удаление или кража данных**	лишение свободы 5 лет или штраф (сумма з-но не ограничена)
4	**Помощь в неправомерном использовании компьютеров**	лишение свободы 10 лет или штраф (сумма з-но не ограничена)

Германия:

	Правонарушение	Наказание
1	**«шпионаж данных» (ст 202a УК Германии), незаконное получение данных, специально защищеных от несанкционированного доступа** **«фишинг» (ст 202b УК Германии) незаконный перехват данных техническими средствами из непубличного объекта обработки данных**	лишение свободы на срок до 3 лет или штраф. лишение свободы на срок до 2х лет или штраф
2	**«компьютерный саботаж» (DDos атаки) (ст 303b УК Германии). Вмешательство в операции по обработке данных, носителя данных, имеющие существенное значение для другого лица, путем удаления, блокирования, или изменения данных, с намерением причинить ущерб другому лицу**	лишения свободы на срок до 3 лет или штраф, если вмешательство имело существенное значение для бизнеса или предприятия или государственного органа - лишение свободы на срок до 5 лет или штраф
3	**подготовка к совершению преступления путем производства, приобретения для себя или другого лица, продажи, поставки другому лицу, распространения или предоставления иного доступа к программному обеспечению с целью совершения такого преступления (ст. 202c УК)**	лишение свободы на срок до 2 лет или штраф.

В соответствии со статьей 202a УК Германии уголовная ответственность за пентесты исключается только в том случае, если пентест разрешен владельцем ИТ-инфраструктуры, подлежащей тестированию.

Кроме того, даже в случае легальных пентестов правила защиты данных должны быть гарантированы в любое время, как прямо установило Федеральное ведомство по информационной безопасности Германии (Bundesamt für Sicherheit in der Informationstechnik – «BSI»).

В целом, согласно немецкому законодательству, наказание за уголовное или административное правонарушение определяется степенью индивидуальной вины. Судья имеет определенную свободу усмотрения при назначении наказания. Положительное поведение после совершения нарушения, а также возмещение причиненного ущерба влияют на уровень наказания. Поэтому учитываются обстоятельства каждого конкретного случая. В частности, решающее значение имеют также субъективные обстоятельства и установки, а также цели правонарушителя.

Франция:

	Правонарушение	Наказание
1	**Несанкционированный доступ к информационным системам (взлом):** **Несанкционированный доступ или нахождение в автоматизированной информационной системе (ст 323-1 УК)**	лишение свободы на срок до 2 лет или штраф 60 000 евро
2	**Несанкционированный доступ, который приводит к удалению, изменению или мошенническому вводу данных (ст 323-2 УК)**	лишение свободы на срок до 3 лет или штраф 100 000 евро
3	**Несанкционированный доступ, который приводит к серьезному вреду (нарушение в работе систем, компрометация конфиденциальной информации (ст 323-1 УК)**	лишение свободы на срок до 5 лет или штраф 150 000 евро

Казахстан:

в гл. 7 УК РК «Уголовные правонарушения в сфере информатизации и связи» включены 9 составов.

	Правонарушение	Наказание
1	**Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст. 205 УК РК)** **- повлекший существенное нарушение** **- совершенное в отношении критической инфраструктуры**	штраф до 160/200 месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до 160/200 часов, либо арестом на срок до 40/50 суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 2 лет или без такового.
2	**-повлекшие тяжкие последствия**	штраф до 2000 месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до 600 часов, либо ограничением свободы на срок до 2 лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3лет или без такового.

Казахстан:

в гл. 7 УК РК «Уголовные правонарушения в сфере информатизации и связи» включены 9 составов.

	Правонарушение	Наказание
3	**Нарушение работы информационной системы или информационно-коммуникационной сети (ст. 207 УК РК)** **-повлекшие тяжкие последствия, в отношении критической инфраструктуры, преступной группой**	штраф до 2000 месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до 600 часов, либо ограничением свободы на срок до 2 лет, либо лишением свободы до 2 лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 2 лет или без такового лишение свободы от 5 до 10 лет
4	**Создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст.210 УК РК)**	как в ст. 207 УК РК

Китай:

	Правонарушение	Наказание
1	**Удаление, изменение, добавление или вмешательство в работу компьютерных информационных систем в нарушение государственных норм, повлекшее нарушение норм действующего законодательства, а также нарушение их нормальной работы + тяжкие последствия,**	лишение свободы сроком до 5 лет или краткосрочный арест то же деяние, повлекшее особо тяжкие последствия, — наказывается лишением свободы на срок свыше 5 лет.
2	**Нарушение государственных постановлений и удаление, изменение или добавление данных или установка прикладных программ, если это вызвало тяжкие последствия,**	лишение свободы сроком до 5 лет или краткосрочный арест то же деяние, повлекшее особо тяжкие последствия, — наказывается лишением свободы на срок свыше 5 лет.
3	**Преднамеренное создание и распространение компьютерных вирусов и других программ, нарушающих нормальную работу компьютерной системы и вызывающие тяжкие последствия,**	лишение свободы сроком до 5 лет или краткосрочный арест

Пакистан:

	Правонарушение	Наказание
1	**Создание или загрузка вредоносного кода любым лицом с намерением нанести вред любой информационной системе или повлиять на нее каким-либо образом (разделы 2-3 PECA, 2016)**	лишение свободы до 2-х лет или штраф, или и то, и другое.
2	**Несанкционированный доступ к любой информационной системе (разделом 3, PECA, 2016)**	лишение свободы до 3х месяцев или штраф до 50 000 пакистанских рупий (приблизительно 200 долларов США)
3	**Копирование и/или передача или помощь в передаче любых данных, без разрешения и со злым умыслом**	лишение свободы до 6 месяцев или штраф до 100 000 пакистанских рупий (приблизительно 400 долларов США), лили и то, и другое.

Россия:

	Правонарушение	Наказание
1	**Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ)** **при крупном ущербе или с корыстной заинтересованностью**	штраф до 200 тыс руб, или исправительные работы до 1 года, органичение свободы до 2х лет или лишение свободы до 2х лет. штраф до 300 тыс рублей или исправительные работы до двух лет, либо ограничением свободы на срок до 4х лет, либо принудительные работы на срок до 4х лет, либо лишение свободы до 4х лет.
2	**Группой лиц по предварит сговору или с испльзованием должностного положения** **Повлекшие тяжкие последствия**	штраф до 500 тыс рублей либо лишение свободы до 5 лет лишение свободы до 7 лет
3	**Дополнительно используются статьи**	210 УК РФ («Организация преступного сообщества (преступной организации) или участие в нем (ней)») 159 УК РФ («Мошенничество») 187 УК РФ («Неправомерный оборот средств платежей») 183 УК РФ («Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»)

Выводы:

1. В Законах при выборе ответственности необходимо делать различия относительно масштаба и направленности воздействия - тогда эффект “сдерживания” будет работать намного лучше. Наказание создает сдерживание в двух формах: общее (от первого преступления) или специальное (от рецидива).

2. Наказание должно быть соразмерно причиненному эффекту. Чем меньше целевое правонарушение, тем меньше наказание и наоборот

3. Заложить в процесс актуализацию законов в связи с изменением технологий

IV. Регламентация пентестов и bug bounty КИИ. Требования к верификации хакеров

Два метода обнаружения и устранения уязвимостей

01

Пентесты

имитации кибератак, проводимых профессиональными экспертами по безопасности, которые оценивают безопасность системы или сети.

02

BUG BOUNTY (программы вознаграждения за ошибки)

краудсорсинговая инициатива, которая опирается на ИТ специалистов, которые находят и сообщают об уязвимостях или недостатках безопасности в ПО. Вознаграждения только тем, кто успешно находит уязвимости.

Сравнение:

Критерий	Пентест	Bug Bounty
Подход	систематическая запланированная оценка, проводимая профессиональными специалистами по кибербезопасности/белыми хакерами	непрерывная краудсорсинговая модель обнаружения уязвимостей
Временной промежуток	зафиксированный период на тестирование	непрерывное исследование, в течение времени пока доступна программа
Экспертиза	в основном проводится сертифицированными профессионалами	Проводится специалистами разного уровня
Конфиденциальность	высокие требования и уровень конфиденциальности	Зависит от правил платформы, риски выше поскольку доступ имею разные лица
Стоимость	обычно высокая	Оплата только в случае нахождения уязвимости или ошибки
Отчетность	детализированный отчет	Описание уязвимости зависит от уровня экспертизы тестировщика, но обычно содержит подробную информацию, которая должна помочь организации понять и воспроизвести проблему
Взаимодействие с заказчиком	между пентестерами и заказчиком устанавливается личный контакт	нет прямого контакта между пентестером и заказчиком
Какое ПО тестируется	возможно тестирования неопубликованного ПО	только то, что доступно on-line

Тенденции

1. Ожидается, что государственное вмешательство в кибербезопасность усилится в ближайшие годы, поскольку киберзащита станет нормативным обязательством во многих секторах. Например, США стремятся переложить ответственность за кибербезопасность на организации, предоставляющие/производящие продукты и услуги. Аналогичный подход ЕС продвигает в своей Директиве NIS2 и Законе ЕС о киберустойчивости.

2. В последние годы правительства государств создают агентства, призванные защищать КИИ и граждан от киберугроз. Эта задача часто требует разработки новых политик или правил.

V. Как регулируется деятельность Bug Bounty платформ? Требуется ли верификация хакеров на платформах?

Самые крупные Bug Bounty

Крупнейшими платформами Bug Bounty в России являются:

- Bug Bounty RU
- Standoff 365 Bug Bounty
- BI. ZONE Bug Bounty

Platform	Country
Intigriti	Belgium
Vulbox	China
HackenProof	Estonia
YesWeHack	France
Yogosha	France
Hackrate	Hungary
BugBase	India
BugsBounty	India

Platform	Country
Redstorm	Indonesia
Ravro	Iran
BugBounty.jp	Japan
TheBugBounty	Malaysia
Zerocopter	Netherlands
Bugbounty.sa	Saudi Arabia
CyScope	Switzerland
Bugcrowd	U.S.

Platform	Country
Synack	U.S.
Cobalt	U.S.
HackerOne	U.S.
Federacy	U.S.
Huntr	United Kingdom
WhiteHub	Vietnam
BugRank	Vietnam
SafeVuln	Vietnam

Bug Bounty платформы в основном регулируются документами самих платформ

Но в некоторых странах, разработаны рекомендации. Так, выпустили рекомендации Агентство кибербезопасности Сингапура (CSA), Национальный центр кибербезопасности Великобритании (NCSC), в США Министерство юстиции (DOJ) выпустило основу для создания безопасных и надежных программ вознаграждения за обнаружение ошибок (bug bounty) “A Framework for a Vulnerability Disclosure Program for Online Systems”. Программа состоит из 4х шагов.

без четких протоколов, границ и договорных формулировок программы вознаграждения за ошибки могут скомпрометировать конфиденциальную информацию или нарушить работу сервисов.

Программа состоит из 4х шагов:

01 Разработка программы раскрытия уязвимостей

• Определить системы и/или данные, которые подпадают под программу.
• Определить, способ обработки данных, третьих лиц, имеющих доступ, включая получение необходимого разрешения.
• Определить, ограничения на методы и приемы, разрешенные для обнаружения уязвимостей.
• Указать типы уязвимостей для целевого использования и как дифференцировать различные типы.

02 План администрирования программы раскрытия уязвимостей

• Определить процедуры отчетности и протоколы отправки для найденных уязвимостей.

• Определить контактную точку для получения отчетов о найденных уязвимостях.
• Определить персонал, который может помочь с вопросами, касающимися программы bug bounty.
• Прописать, как обрабатывать случайные и добросовестные нарушения, а также те, которые являются преднамеренными и злонамеренными.

Программа состоит из 4х шагов:

03 Составление политики раскрытия уязвимостей

• Определить, какие действия разрешены и неразрешены, используя простые, легко понимаемые термины.

• Определить область действия систем, которые подпадают под действие программы раскрытия уязвимостей, как можно более конкретно.
• Определить протоколы для работы с ограниченными и конфиденциальными данными, требующими особого обращения.
• Указать последствия за нарушения политик программы раскрытия уязвимостей.
• Поощряйте участников получать разъяснения относительно политик программы организации, прежде чем совершать действия, которые могут быть непоследовательными или не охватываться политиками.

04 Внедрение программы раскрытия уязвимостей

• Сделать политику программы широкодоступной
• Поощряйте участников, которые проводят мероприятия по раскрытию уязвимостей, следовать программе и политикам организации по раскрытию уязвимостей.
• Подготовить отдельное соглашение о сотрудничестве
• Установить надлежащие протоколы обучения сотрудников платформы Bug Bounty
• Определить, какие правовые или оперативные меры следует предпринять в случае случайных нарушений, а также преднамеренных и злонамеренных. Определите обязательства платформы в случае, если внешняя организация инициирует судебный иск против третьей стороны, проводящей оценку безопасности систем организации.
• Подготовить отдельную процедуру отчетности в случае обнаружения уязвимости

Правила Bug Bounty (регулирование поведения белых хакеров + действий организации)

01

> Области действия программы bug-bounty.

Организации обычно указывают список системных и продуктовых областей, над которыми должны работать белые хакеры, через a) указание основных веб-сайтов, веб-приложений, API, мобильные приложения физических продуктов с цифровыми компонентами, в качестве цели b) могут предоставлять исходный код

02

> Области, выходящие за рамки действия программы bug-bounty

Заказчик может явно указать все домены и области, в которых они
не хотят, чтобы работали хакеры. Причины a) исключают веб-приложения (например, блог, поддержка, сообщество), размещенные третьими лицами, b) веб-сайты или службы клиентов c). области, принадлежащие деловым партнерам или дочерним компаниям

03

> Допустимые уязвимости

Эта категория предоставляет дополнительные подробные правила, ориентированные на типы уязвимостей, которые организации хотят, чтобы нашли белые хакеры. Обычно это: SQL Injection, Remote Code Execution, подделка межсайтовых запросов, обход каталогов, межсайтовый скриптинг, раскрытие информации и логические проблемы.

Правила Bug Bounty (регулирование поведения белых хакеров + действий организации)

04

> Неприемлемые уязвимости

Определенные типы уязвимостей часто исключаются из вознаграждения за bug bounty из-за очень низкого или нулевого риска безопасности. Например: Self-XSS, Logout CSRF, отсутствие максимальной длины пароля и т. д

05

> Запрещенные или нежелательные действия

дополнительные инструкции для хакеров относительно того,
что они не должны делать, когда они ищут уязвимости для организаций.
Например, a) запрещают или ограничивают использование автоматического сканирования, поскольку оно может привести к большому количеству ложных положительных отчетов и может вызвать значительный объем трафика на сайт b) запрещают взаимодействие с аккаунтами других пользователей, c)запрещают социальная инженерию. Несоблюдение этих правил может лишить белых хакеров возможности получать вознаграждение или участвовать в программе в будущем. Нарушения также могут привести к судебным искам против них или исключению из платформы.

Правила Bug Bounty (регулирование поведения белых хакеров + действий организации)

06

> Правовые положения

Прописываются юридические последствия. Описывается в каких случаях заказчик может/не может подавать судебные иски против хакеров.

07

> Ограничения на участие

Хотя платформы bug bounty известны своей открытостью для приветствия хакеров со всего мира, но некоторые явно исключают определенные типы лиц из участия: a) некоторые запрещают своим сотрудникам участвовать b) ограничения по национальности c) возрастные ограничения

08

> Отчеты об уязвимостях

В этой категории организации описывают, какие сведения об обнаруженных уязвимостях они хотели бы включить в отчеты - определенный формат с достаточным количеством подробностей, таких как снимки экрана, посещенные страницы и т. д

Правила Bug Bounty (регулирование поведения белых хакеров + действий организации)

09

> Правила раскрытия информации

Указывается разрешено или нет публичное раскрытие выявленных проблем, или устанавливают время для устранения проблемы до публичного раскрытия информации.

10

> Ограничения на участие

Хотя платформы bug bounty известны своей открытостью для приветствия хакеров со всего мира, но некоторые явно исключают определенные типы лиц из участия: a) некоторые запрещают своим сотрудникам участвовать b) ограничения по национальности c) возрастные ограничения

11

> Оценка вознаграждения

Правила в этой категории определяют конкретную систему баллов или процесс оценки, который организация использует для определения того, имеют ли найденные уязвимости право на вознаграждение (вопросы дублирующих отчетов).

Верификация

ПЕНТЕСТ

Пентестер известен, заключается договор

BUG BOUNTY

Бывают разные уровни верификации, в зависимости от правил платформы:

1) Частный
Это программа вознаграждения за ошибки, доступная только по приглашению.

2) Публичный
ПО Заказчика, указана на общедоступном сайте, проиндексирована и доступна для поиска в Интернете. Хакеры все равно должны зарегистрироваться на платформе, если они хотят отправить отчет.

3) через Заявку
Хакеры, желающие принять участие в тестировании ПО, должны подать заявку и получить одобрение Заказчика, но все исследователи, зарегистрированные на платформе, могут видеть, что есть это ПО для тестирвания, но подробнотси только после входа в систему и подачи заявки. Если опция «ID-checked» не требуется для исследователей, программа также отображается на общедоступном веб-сайте платформы.

4) через Регистрацию
Все зарегистрированные исследователи на платформе могут видеть полную информацию о ПО и отправлять отчеты. Можно ограничить доступ только для исследователей с проверенным ID.

Выводы

1. Фундаментальным правовым требованием для этичных хакеров является необходимость получения явного письменного разрешения перед проведением любой формы тестирования системы.Это разрешение имеет решающее значение для обеспечения того, чтобы все действия были юридически правомерны.

2. Должны быть четко определены объем и цели тестирования.

3. Соблюдение законов о конфиденциальности

Это не только защищает белого хакера от возможных правовых последствий, но и убеждает владельцев системы в том, что процедуры тестирования безопасны и контролируются.

октябрь /2024

CHERVETS
PARTNERS

Спасибо!

tg: @chervetspartners

chervets.partners

Остались вопросы?

info@chervets.partners

chervets.partners