????? ??????????

Начало - договор об оказании услуги. В нем указываются юридические, технические, временнЫе, ... рамки и ограничения, ответственность сторон. Часть вышеуказанной информации попадает в отчет.

Основа хорошего отчета закладывается перед началом тестирования.

Тестирование бывает White box (Организация предоставляет все данные) и Black box (тестирование вслепую).

Оценка уязвимостей и составление отчета

Перед постановкой задачи устранения уязвимости необходимо:

1. Пересчитать критичность уязвимости с учетом "веса" активов и исключений. Добавление исключений должен быть формализован, и включать в себя согласование исключений и регулярный пересмотр. Для пересчета критичности может использоваться фреймворк CVSS.
2. Убедиться, что уязвимость присутствует на самом деле.
3. Определить владельца актива, который будет ответственным за устранение проблемы.

Примечание: Результаты отчета по уязвимостям содержат чувствительные данные, поэтому отчет должен храниться в защищенном месте и иметь строго ограниченный доступ только для тех лиц, которым он предназначен.

Типы отчетов

- Технический отчет — предназначен для инженеров, которые будут работать над устранением уязвимостей. Это наиболее исчерпывающий отчет, включающий в себя множество технических данных. Не предназначен для технически не подкованных людей.
- Отчет об изменениях — показывает изменения с момента предыдущего скана, например, новые сервисы и уязвимости, которые появились в сети, либо же наоборот, устраненные за наблюдаемый период проблемы.
- Отчет о трендах(тенденциях) — показывает изменения уровня рисков и уязвимостей за период времени. Например, отчет может показать, что в этом месяце было обнаружено на 10% больше критичных уязвимостей чем в прошлом.
- Высокоуровневый отчет — предоставляет результаты сканирования в сжатой форме, без технических подробностей. Предназначен для менеджмента и нетехнического персонала, часто включает в себя графики и диаграммы.

Внутренние требования

Шаг 1. Выбор стандарта оценки уязвимостей. Стандарт CVSS v3 используется для оценки технической серьезности уязвимости. Стандарт OWASP Risk Rating Methodology используется для оценки рисков web приложения для бизнеса. Иногда рекомендуют использовать оба стандарта.

Шаг 2. Используемая среда / правила оформления / способ хранения информации о найденных уязвимостях. Упоминаются Dradis, CherryTree, OneNote. В правилах оформления определяется набор данных для каждой уязвимости (например дата и время проведения, скриншоты, формат описания последовательности действий).

Вариант структуры.

1 Вступительная часть
1.1 Классификатор найденных уязвимостей
2. Общее описание проделанной работы
3. Технический отчет
4. Рекомендации по устранению уязвимостей

Вступительная часть
Факты, известные исполнителю и заказчику до начала работ. К ним относятся: дата проведения пентеста, методика, которая применялась (очень кратко), основные этапы тестирования, перечень систем для тестирования и исключения из объема работ, перечень узлов, а также методики, которые исполнитель обязуется не применять (социальную инженерию или атаки на отказ в обслуживании).

Классификатор уязвимостей
Таблица необходима для понимания критериев определения критичности уязвимостей, а также тот ущерб, который они могут нанести в случае успешной реализации.

В заключении вступительной части необходимо описать уточнения договора, актуализированные на этапе тестирования. Например, просьба обратить особое внимание на какой-то новый сервис, который появился за неделю до начала тестирования, или, наоборот, в последний момент попросил исключить из исследования веб-приложение, уязвимости в котором нашли своими силами буквально за день до начала работ и которое собираются капитально доработать прежде, чем вновь показывать пользователям.

Общее описание проделанной работы
Этот раздел должен содержать значимую для руководителей компании-заказчика информацию о проделанной работе и ее результатах. Главные требования, предъявляемые к нему, — понятность и краткость. Сам отчет может растянуться на десятки, если не сотни страниц. Руководитель не всегда готов читать документацию такого объема, и зачастую в этом нет необходимости. Главное — понять критически важные результаты для принятия дальнейших решений. Наша задача в этом разделе — завладеть вниманием читателя с любым

уровнем подготовки, описать общую ситуацию и сообщить о наиболее значимых выводах.

Технический отчет
Предназначен для технических специалистов. В нем мы, как инженеры, объясняем другим техническим специалистам, что мы нашли при тестировании и чем это может грозить.

Вариант - отчет в виде карточек по найденным уязвимостям с разделами:

Краткое описание найденного.	Просто и доступно описываем, что удалось найти, что привлекло наше внимание.
Уровень риска.	Проставляем баллы по той шкале, о которой говорилось ранее.
Указание местонахождения в системе.	Указываем IP-адрес, DNS-имя или что-то, что однозначно идентифицирует систему.
Описание инструментария.	Это необязательный пункт, но он может очень помочь инженерам со стороны заказчика, когда они решат воспроизвести твои действия.
Ссылка на описание уязвимости.	Чтобы чрезмерно не увеличивать размеры отчета, рекомендуем сделать внешние ссылки на описания уязвимостей из открытых баз знаний. Выбрать можно любую, например cve.mitre.org, cvedetails.com, snyk.io или rapid7.com.
Скриншоты и другие подтверждения.	Скриншоты нужно добавлять только при условии, что они наглядно что-то объясняют.
Рекомендации, как исправить уязвимость.	В этом разделе нужно привести рекомендации производителя уязвимого программного обеспечения или свои собственные. В любом случае ответственность за устранение уязвимостей лежит на заказчике и только ему решать, как они будут устранены и будут ли.

CVSS (Common Vulnerability Scoring System)

Открытый стандарт, позволяющий описывать уязвимости. Пример:

```
AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
```

CVSS состоит из трех групп метрик, которые описывают уязвимость:

- Базовая группа. Дает представление об основных характеристиках уязвимости, не меняется со временем (например, уязвимость эксплуатируемая только при локальном доступе).
- Временная группа. Описывает характеристики, которые могу меняться со временем (например, наличие рабочего эксплойта).
- Переменные среды. Характеристики уязвимости, которые связаны с окружением пользователя. Используются для уточнения итоговой оценки уязвимости на стороне компании.

Базовая группа

В версии CVSS 3.0 сюда входят следующие метрики:

Метрика	Описание
AV (Attack Vector)	вектор атаки. Варианты: • N сетевой (Network) • A локальная сеть (Adjacent) • L локальный (Local) • P физический (Physical).
AC (Attack Complexity)	сложность атаки. Варианты: • H высокая. необходимо выполнение доп. условий для эксплуатации уязвимости • M средняя • L низкая
PR (Privileges Required)	привилегии для эксплуатации уязвимости. Варианты: • N (None, привилегии не нужны), • L (Low, нужны низкие привилегии, например права пользователя) • H (High нужны высокие привилегии)
UI (User Interaction)	необходимость пользовательского взаимодействия. Варианты: • N (None, взаимодействие не требуется) • R (Required, требуется)
S (Scope)	граница эксплуатации. Показывает, может ли уязвимость повлиять на безопасность другого компонента системы. Варианты: • U (Unchanged, граница не меняется) • C (Changed, меняется) Например, уязвимость побега из контейнера, позволяющая выполнить код на хосте будет иметь свойство S:C.
C (Confidentiality)	затрагивает ли уязвимость конфиденциальность информации. Варианты: • H высокий • M средний • L низкий
I (Integrity)	затрагивает ли уязвимость целостность информации. Варианты: • H высокий • M средний • L низкий

Метрика	Описание
A (Availability)	затрагивает ли уязвимость доступность информации. Варианты: • H высокий • M средний • L низкий

Временная группа

Метрика	Описание
E (Exploit Code Maturity)	доступность средств эксплуатации. Варианты: • ND/X (Not Defined не определено) • H (High средства доступны или не требуются) • F (Functional средства доступны) • POC/P (Proof-of-Concept есть пример эксплуатации, но он может не работать) • U (Unproven средства недоступны или уязвимость теоретическая)
RL (Remediation Level)	уровень исправления. Очень важная для приоритезации метрика. • ND/X (Not Defined информация отсутствует) • U (Unavailable исправление недоступно) • W (Workaround есть неофициальное исправление) • FT/T (Temporary Fix есть официальное, но временное решение) • OF/O (Official Fix официальное исправление уязвимости)
RC (Report Confidence)	достоверность отчета. • X (Not Defined не определена) • U (Unknown нет информации) • R (Reasonable известны некоторые детали об уязвимости) • C (Confirmed отчет подтвержден)

Переменные среды

Данные параметры проставляются аналитиком для корректировки оценки уязвимости. Например, если для компании важна доступность какого-либо актива, то специалист может выставить параметр Availability Requirement (AR) в значение High(H).

Метрика	Описание

CR (Confidentiality Requirement)	требования к конфиденциальности. Варианты: • H высокий • M средний • L низкий • ND/X не определены
IR (Integrity Requirement)	требования к целостности. Варианты: • H высокий • M средний • L низкий • ND/X не определены
AR (Availability Requirement)	требования к доступности. Варианты: • H высокий • M средний • L низкий • ND/X не определены

Итоговая оценка

После определения метрик по стандарту CVSS рассчитывается итоговая оценка уязвимости, которая считается по шкале от 0 до 10, где 0 — отсутствие уязвимости, а 10 — максимально критичный приоритет. Формула расчета достаточно сложная, проще библиотеками python или калькулятором.

Источники:

Статья на Хакере

CVSS V 3.1 Calculator

Revision #8
Created 29 September 2025 16:24:05 by Admin
Updated 31 October 2025 13:13:52 by Admin