По практическому туру максимальная оценка результатов участника возрастной группы (7-8 классы) определяется арифметической суммой всех баллов, полученных за выполнение заданий и не должна превышать 35 баллов.

Задание 1.

Вопрос 1: главная уязвимость кода

Максимальный балл – 7 баллов

Основная уязвимость заключается в хранении пароля в открытом виде внутри кода. Пароль asdfg987 указан непосредственно в условии if, что позволяет легко обнаружить его при просмотре кода, использовать один и тот же пароль во всех системах, где применяется этот скрипт (риск повторного использования).

Обоснование: пароли должны храниться в зашифрованном виде или использовать внешние защищенные хранилища. В противном случае злоумышленник, получивший доступ к коду, немедленно компрометирует систему.

Вопрос 2: как злоумышленник может узнать пароль

Прямой доступ к коду: если злоумышленник может прочитать файл скрипта (например, через уязвимость в веб-приложении, публичный репозиторий или доступ к серверу), пароль будет раскрыт.

Анализ логинов: в некоторых средах пароль может оставаться в текстовом виде в логах ошибок или оперативной памяти.

Социальная инженерия: если код доступен разработчикам или администраторам, злоумышленник может получить пароль через них.

Вопрос 3: принципиальное исправление

Пример улучшенной логики:

python

```
import hashlib
stored_login = "admin"
stored_password_hash = "a1b2c3..."  # Хеш пароля " asdfg987", вычисленный заранее
input_login = input("Введите логин: ")
input_password = input("Введите пароль: ")
input_password_hash = hashlib.sha256(input_password.encode()).hexdigest()
if input_login == stored_login and input_password_hash == stored_password_hash:
    print("Доступ разрешён!")
else:
    print("Неверный логин или пароль!")
```

1. Вынести секретные данные в отдельные конфигурационные файлы или переменные окружения:

Пароль и логин не должны быть «зашиты» в код. Их можно хранить в файле .env или использовать секреты вроде os.getenv("ADMIN_PASSWORD").

Итог: Код станет безопаснее, если пароль не будет храниться в открытом виде, а проверка будет происходить через сравнение хешей.

Задание 2.

Ответ на задание «Анализ фишингового письма»

Максимальный балл – 18 баллов

Вопрос 1: что произойдет, если вы перейдете по ссылке и введете свои данные?

Если перейти по ссылке и ввести свои данные (логин, пароль, подтверждающие сведения и т.д.), произойдет следующее:

Ваши учетные данные будут перехвачены злоумышленниками.

Злоумышленники получат полный доступ к вашей реальной учетной записи на настоящем сайте «ВебЛаб» (или к другой службе, для которой предназначены эти данные).

Последствия могут быть различными: кража личной информации, рассылка спама от вашего имени, финансовые потери (если аккаунт связан с платежными системами), блокировка вашего аккаунта самими злоумышленниками с целью выкупа.

Вопрос 2: перечислите не менее 4 признаков, которые позволяют заподозрить, что это фишинговое письмо.

Подозрительный домен в ссылке. Адрес http://web-lab-security.ru отличается от ожидаемого официального домена компании (например, weblab.ru или weblab.com). Злоумышленники часто регистрируют похожие домены, чтобы обмануть пользователей. Использование HTTP (без S) также является признаком небезопасного соединения.

Требование срочных действий. Фразы «Немедленно перейдите... иначе аккаунт будет заблокирован» создают искусственное ощущение срочности и паники, чтобы пользователь действовал необдуманно и не проверял информацию.

Запрос конфиденциальных данных. Легитимная служба безопасности почти никогда не будет запрашивать у вас пароль или другие полные данные учетной записи по электронной почте. Их задача - защищать эти данные, а не собирать их через почту.

Обобщенное обращение. Письмо начинается с безличного «Уважаемый пользователь!», а не с вашего имени или логина. Это признак массовой рассылки.

(Дополнительные признаки для надежности: Отсутствие официальной подписи с контактными данными компании; Орфографическая ошибка в слове «под-твердите» (дефис посередине слова).)

Вопрос 3: каковы ваши правильные действия после получения такого письма?

Не переходить по ссылке в письме. Это главное правило.

Не вводить и не сообщать какие-либо данные на странице, которая может открыться по этой ссылке.

Самостоятельно перейти на официальный сайт компании. Набрать в браузере известный вам адрес службы (например, weblab.ru) или использовать закладку. Проверить статус своего аккаунта непосредственно в своем личном кабинете на официальном сайте.

Связаться со службой поддержки компании через официальные каналы (телефон, чат на сайте, официальный email), используя контакты, найденные на их настоящем сайте, а не в подозрительном письме, и уточнить информацию.

Удалить фишинговое письмо, если есть сомнения.

Сообщить о фишинге. Если вы работаете в организации, сообщить в ИТ-отдел или службу безопасности. Можно также сообщить о фишинговом письме в саму компанию «ВебЛаб», чтобы они предупредили других пользователей.

Задание 3.

Ответ на задание «Логика разграничения доступа»

Максимальный балл – 10 баллов

Как система должна отреагировать в каждом случае?

При попытке доступа к папке /Ученики/9а/Оценки/:

Система идентифицирует пользователя как "Ваня Петров".

Проверяет его группы: Ученики, Ученики_9а.

Смотрит, каким группам разрешен доступ к папке "Оценки". Это Классный_руководитель_9а и Администрация.

Сравнивает списки. Система не находит пересечений между группами Вани (Ученики, Ученики_9а) и группами с доступом (Классный_руководитель_9а, Администрация).

Реакция системы: ДОСТУП ЗАПРЕЩЁН. Ване будет показано сообщение типа "Отказано в доступе" или "Недостаточно прав".

При попытке доступа к папке /Учителя/Зарплаты/:

Система идентифицирует пользователя как "Ваня Петров".

Проверяет его группы: Ученики, Ученики_9а.

Смотрит, каким группам разрешен доступ к папке "Зарплаты". Это Директор и Бухгалтерия.

Сравнивает списки. Система снова не находит пересечений.

Реакция системы: ДОСТУП ЗАПРЕЩЁН. Ване будет показано аналогичное сообщение об ошибке. В хорошо настроенной системе он даже не должен увидеть, что такая папка существует.