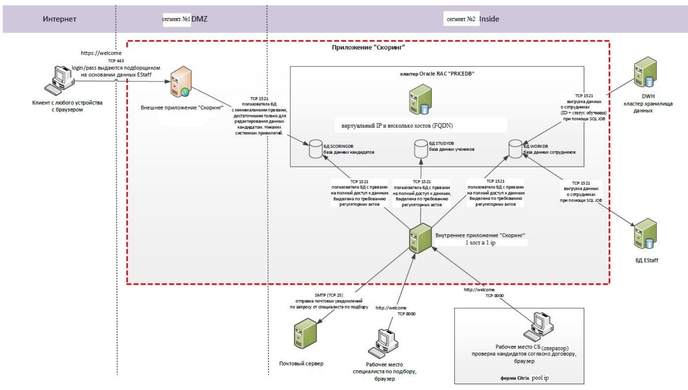
ДЗ № 01 - Денис

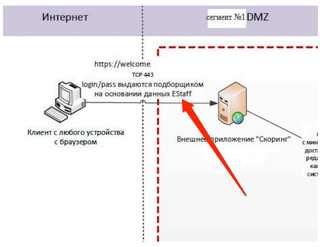
Урок 1. Как встать на путь соискателя в сфере ИБ и что из этого может получиться?.

1. Составить свое экспертное мнение по поводу защищенности планируемой реализации, IT-инфраструктуры и ландшафта, составить предложения по модернизации схемы и внедрению средств защиты (процессы защиты).



Попробую пока без гугления - все мысли как есть, чтобы понять что подтянуть)

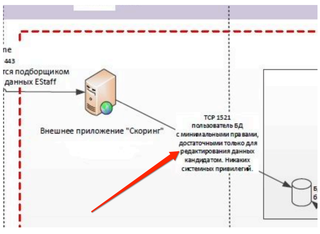
Замечание 1



Риск брутфорса - можно перебором (ФИО, номер/ID/мобильного или как реализовано приложение) получить доступ (одноразовый?) в периметр приложения.
Риск SQL-инъекции + не исключена раскрутка до RCE.

Рекомендация: организовать доступ по ассиметричному ключу, прикрутить 2FA/SMS, настроить антибруфорс, настроить доступ с определенных IP.
Настроить/проверить фильтр запросов на спецсимволы, можно посредством WAF, может быть в приложении есть опция/модуль фильтрации - воспользоваться ими.

Замечание 2

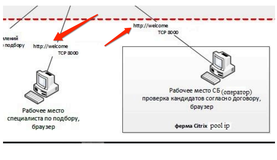


Аналогично - риск SQL-инъекции + не исключен риск RCE при вызове записанных данных в ячеку
Рекомендации - аналогичные по фильтрации вводимых данных + полезно изучить код приложения на слабые места для внедрения полезной нагрузки

Замечание 3

Риск брутфоса или инъекцией, риск перехвата информации, рассылки фишинга от лица компании/администратора, спама
Рекомендации: настройка правил фаервола, фильтра вводимых данных, оптимизация конфига SMTP

Замечание 4



Риск локальной атаки на перехват трафика, утечки данных. Так как задействован браузер - не исключены XSS
Рекомендуется обернуть трафик в HTTPS! Провести анализ кода страницы на риск XSS и настроить фильтрацию или изменить код на более безопасный.

Пока такие мысли.. задание отличное, крайне интересно подробно разобрать.

Задание выполнено!

2020.10.29 20:12