Безопасность WEB

О работе

Структура

Материал:

- О работе
  - Чем занимаюсь
  - Разница в 2ух направлениях AppSec
  - Поиск работы
- О развитии
  - Hard skills
  - Soft skills

О себе

Дмитрий К, 24г (@verouSSS)

Positive Technologies: Анализ защищенности веб приложений, 5 лет

Контур: Инженер AppSec > 1 месяца

Самостоятельно изучил: - Разработку WEB приложений

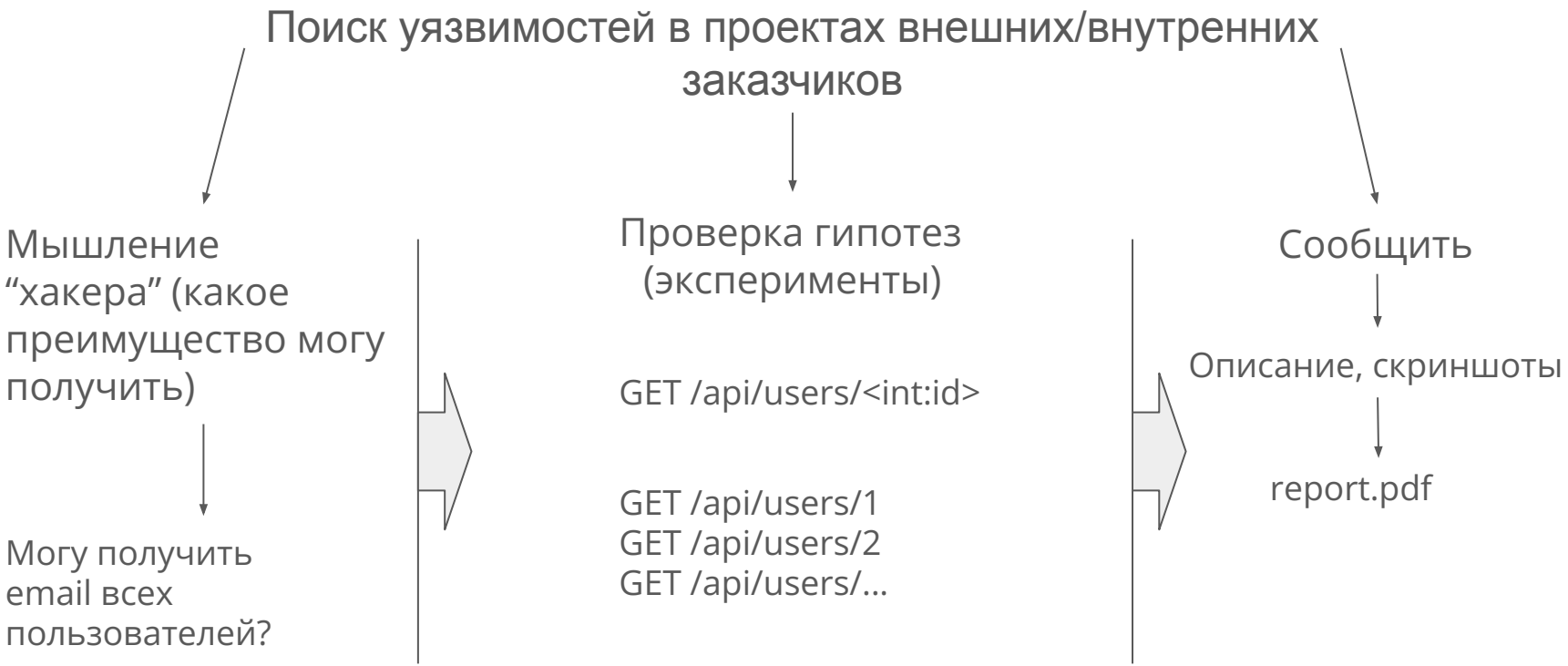
Администрирование Linux

Основы pwn и reverse

Безопасность WEB приложений

Недавно продолжил изучать соц. психологию :| https://t.me/philosophy_code

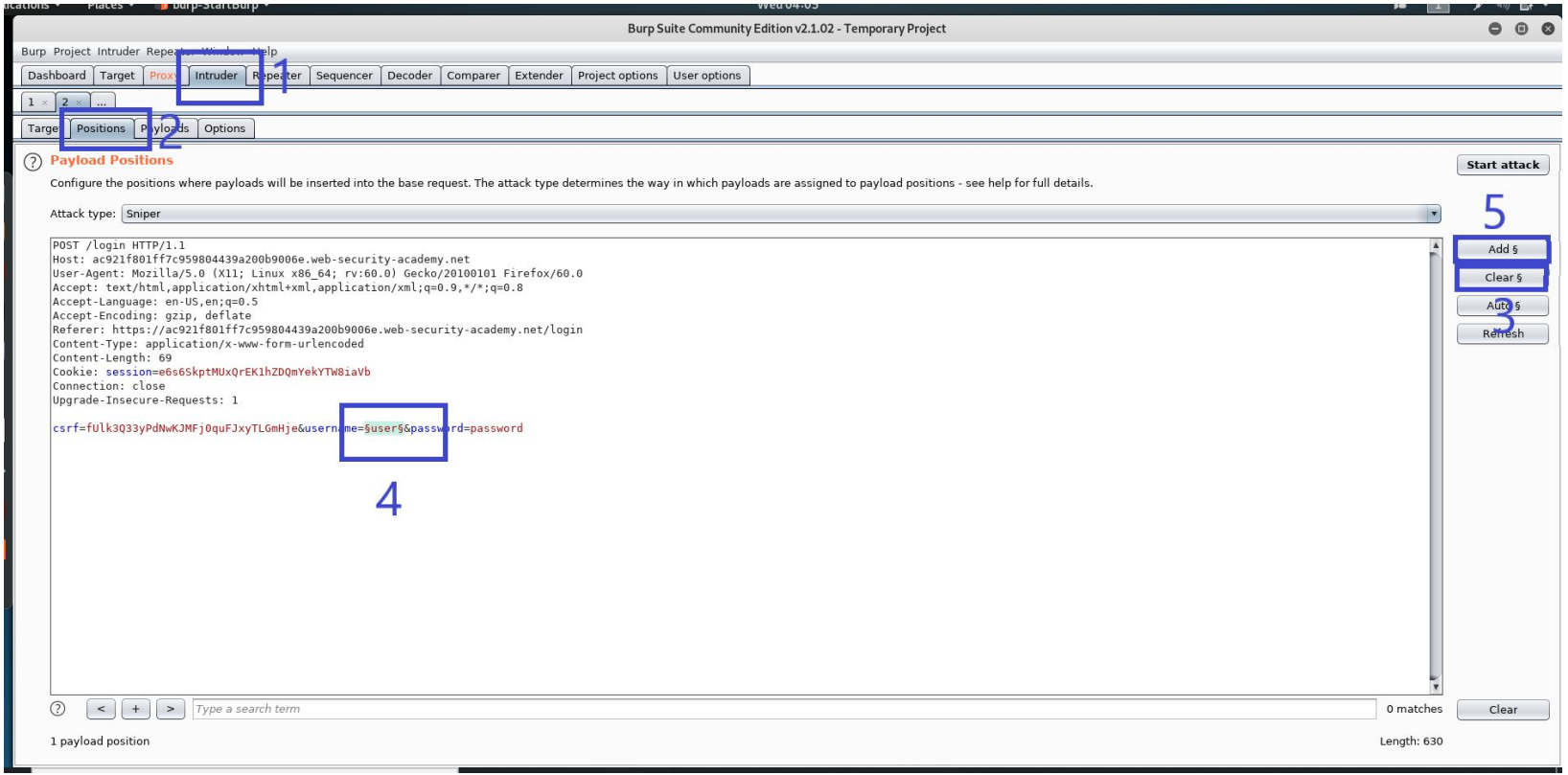
О работе, чем занимаюсь (общее)



О работе, 3 метода тестирования

- Черный ящик (атакуем в слепую веб приложение)
- Серый ящик (предоставляют документацию, учетные записи, добавляют в белый список WAF)
- Белый ящик (заказчик раскрывает исходный код)

О работе, Burp Suite



Разница в работе

Работа при предоставлении услуг

- В основном анализ методом Серого ящика
- Задачи:
  - Найти и описать уязвимость
  - Если есть аналитик, проверить его переформулировку
- Практически нельзя использовать автоматизированные сканеры
- Проекты как правило конвейером по одному

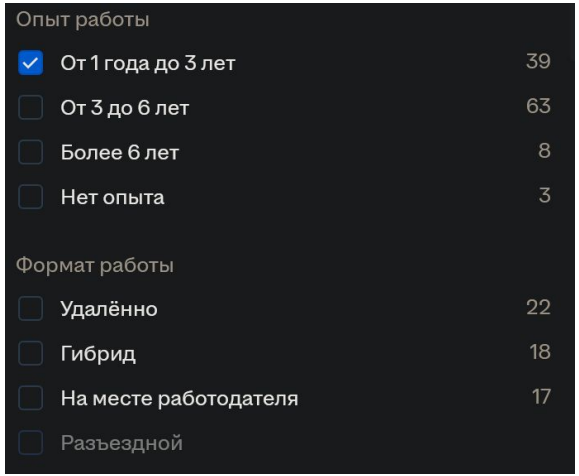
Работа при внутреннем AppSec

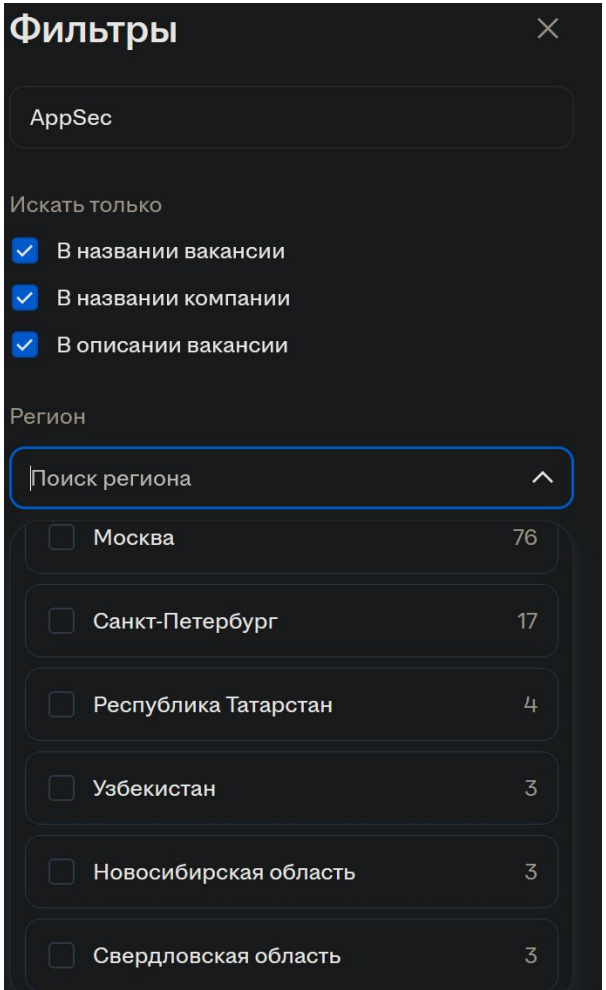
- Есть возможность использовать **Белый ящик**
- Задачи:
  - Найти уязвимости
  - Оценить/доказать критичность (триаж)
  - Проверить исправление
  - Проверять/оценивать репорты из BugBounty
  - Следить чтобы разработчики приходили на аудит
- Пользуйся чем хочешь (не считая пиратского ПО)
- Можешь брать несколько проектов сразу
- Иногда пытаться поймать эксплуатацию уязвимостей других

О поиске работы

Офис или удаленка?

1. В Самаре нет крупных ИТ компаний
    a. Либо удаленно из Самары
    b. Либо релокация в другой город
2. Не все компании готовы брать удаленщиков Junior





Что требуется?

1) Понимание веб уязвимостей + иногда мобилки (поиск, как исправить, последствия)
2) Автоматизация (SAST, DAST…)
3) Триаж уязвимостей
4) Понимание процессов SDLC (безопасный цикл разработки)

Мы ищем человека, у которого:

- Общее понимание базовых принципов информационной безопасности, контроля доступа, криптографии;
- Базовое понимание сетевой модели OSI, основных протоколов;
- Понимание того как должна быть устроена безопасная разработка;
- Знание особенностей веб разработки и меры по обеспечению ее безопасности;
- Знакомство с OWASP Top 10, ASVS, WSTG, MASTG;
- Понимание методов популярных атак на веб-приложения;
- Знакомство с CWE, CVE. Опыт расчёта CVSS (в том числе по версии 4.0);
- Опыт разработки на языках программирования высокого уровня. Умение разбираться в чужом исходном коде;
- Понимание того как устроена современная разработка;
- Знакомство с системами контроля версий. Умение работать с Git. Понимание того как происходит сборка приложений;
- Опыт работы с инструментами статического анализа кода (SAST);
- Опыт работы с инструментами анализа открытого ПО (OSA/SCA);
- Понимание SBOM. Опыт работы с инструментами динамического анализа веб приложений (DAST);
- Умение проходить лабораторные работы на Portswigger;
- Понимание основных принципов обеспечения безопасности REST API;
- Умение работать с Postman, Swagger;
- Умение исключать ложные срабатывания, оценивать критичность обнаруженных недостатков, аргументировать необходимость устранения.

Переход от внешний услуг до внутреннего AppSec

1. Психологический эффект (свой - чужой)
2. Добавляются новые требования к навыкам
3. Как будто основной навык (ручной поиск уязвимостей), мало ценится

О Развитии

Пирамида потребностей Маслоу

Возможность
раскрыть потенциал

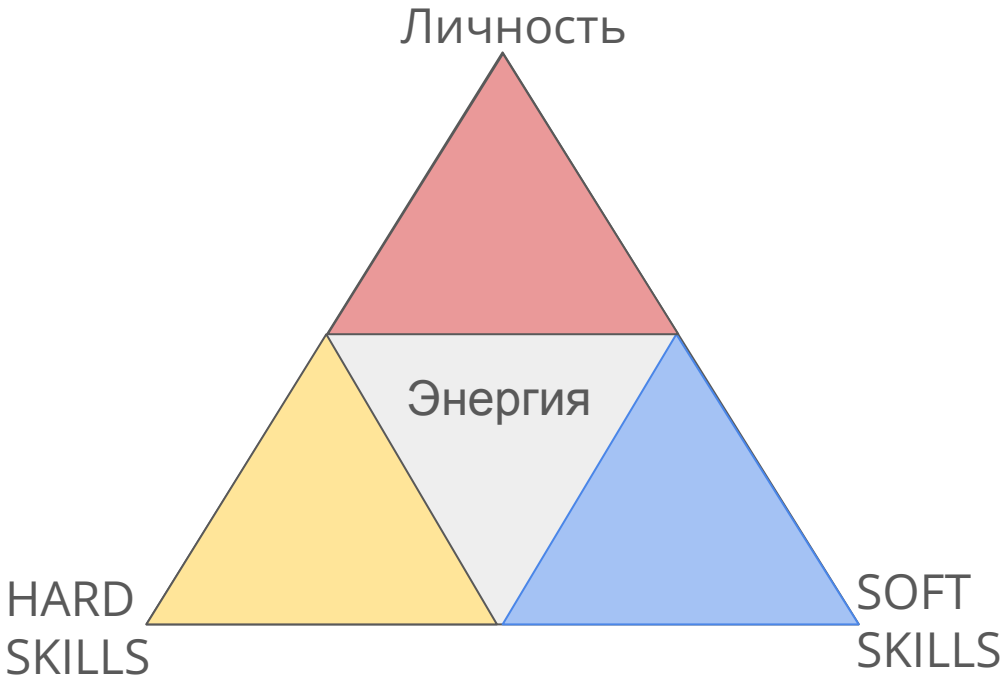
Признание, карьерный рост

Взаимодействие с людьми

Стабильность, замена ИИ

Оплата труда, условия работы

Треугольник развития в ИТ



1) HARD = SOFT
2) Над всем личность
3) Центр всего - энергия

HARD SKILLS

Ответ хорошо даст ChatGPT

Кратко:

1. Основы веб технологий (разработка)
2. OWASP TOP 10
3. Инструменты Burp Suite
4. SAST (CodeQl - написание правил)
5. Практика на вирт стендах: DVWA, Juice Shop
6. Участие в CTF (ctf time), Bug-Bounty (не сильно рекомендую)
7. Чтение документации и статей

Список полезных ресурсов

1) v29.skladchik.org (покупаем в складчину цифровые товары)
2) play.picoctf.org (ctf с доступными заданиями)
3) ctftime.org
4) t.me/critical_bug (раньше были анализы раскрытых уязвимостей)
5) portswigger.net/web-security (Бесплатное онлайн-обучение по веб-безопасности от создателей Burp Suite.)

SOFT SKILLS

1. Самодисциплина - Это навык!
2. Тайм менеджмент

3. Самообучение

Самодисциплина
или
Самообладание

Зефирный тест

- Усадил вокруг стола группу четырехлетних детей
- Положил на стол несколько кусочков зефира и сказал:
  - Что сейчас уйдет и они могут съесть лакомство прямо сейчас.
  - Но если они не съедят зефир до его прихода, то он даст им еще.

Результаты зефирного теста

- Двадцать лет спустя выяснилось, что терпеливые дети окончили университет с более высокими оценками
- Тридцать лет спустя у них был более высокий годовой доход.
- Дети, которые вообще не могли ждать, в течение жизни чаще попадали в тюрьму и чаще страдали от алкогольной или наркотической зависимости.
- Просил детей представить себе, что зефир нарисован на картинке. При таком подходе дети могли ждать в среднем в три раза дольше

Самодисциплина в мелких делах

доктор Филом Куинном:

“В своей практике я постоянно встречался с людьми, которые чувствовали, что жизнь вышла у них из-под контроля. Я обнаружил, что все они без исключения не умели управлять своей жизнью. Им не хватало дисциплины даже для мелочей, а в этом случае любая задача кажется непосильной ”

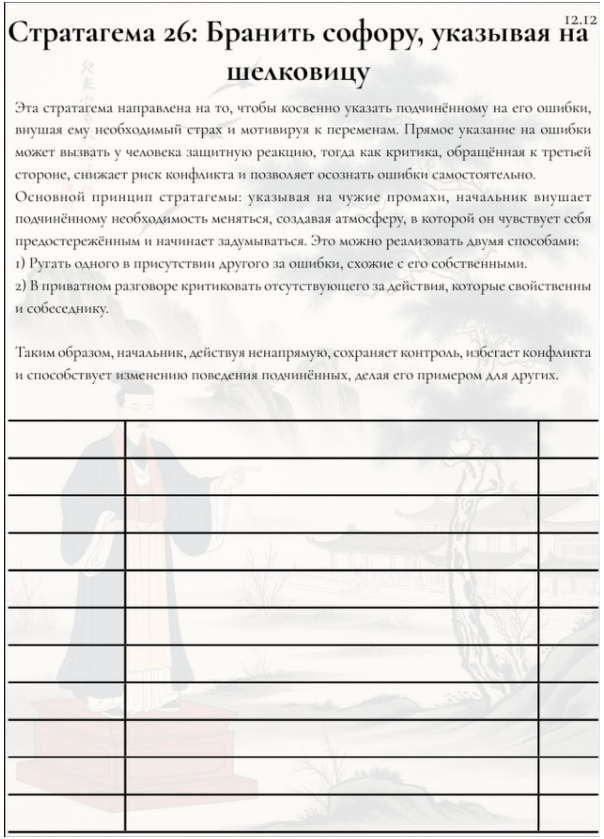
Адмирал Макрейвен говорил:

«Если ты не в состоянии правильно выполнять мелкие дела, то никогда не сможешь сделать что-то великое».

Создание TODO листов

- Перед сном записывает на карточке все дела, которые необходимо выполнить завтра.
- За завтраком он просматривает этот список и вносит необходимые коррективы,
- А затем руководствуется им в течение дня.

- Жизнь слишком сложна, чтобы можно было позволить себе хотя бы день обходиться без плана
- А какое удовольствие взглянуть на карточку в конце дня и увидеть, что все намеченные дела выполнены



12.12

Стратагема 26: Бранить софору, указывая на шелковицу

Эта стратагема направлена на то, чтобы косвенно указать подчинённому на его ошибки, внушая ему необходимый страх и мотивируя к переменам. Прямое указание на ошибки может вызвать у человека защитную реакцию, тогда как критика, обращённая к третьей стороне, снижает риск конфликта и позволяет осознать ошибки самостоятельно.

Основной принцип стратагемы: указывая на чужие промахи, начальник внушает подчинённому необходимость меняться, создавая атмосферу, в которой он чувствует себя предостережённым и начинает задумываться. Это можно реализовать двумя способами:

1) Ругать одного в присутствии другого за ошибки, схожие с его собственными.
2) В приватном разговоре критиковать отсутствующего за действия, которые свойственны и собеседнику.

Таким образом, начальник, действуя ненапрямую, сохраняет контроль, избегает конфликта и способствует изменению поведения подчинённых, делая его примером для других.

Истощение Эго (“я”)

Это идея о том, что самоконтроль или сила воли о*пираются на сознательные психические ресурсы*, *которые могут быть истощены* при постоянном использовании без отсрочки (слово "эго" используется в психоаналитическом смысле)

Самоконтроль улучшается с практикой, а также с возрастом. Неудивительно, что это последнее открытие соответствует созреванию лобных долей, которые связаны с ингибирующим контролем и продолжают развиваться в раннем взрослом возрасте.

Мы обнаружили, что более молодые участники (<25 лет) были восприимчивы к эффектам истощения, но не обнаружили подтверждения таким эффектам в старшей группе (40-65 лет)

(https://pmc.ncbi.nlm.nih.gov/articles/PMC3200324/)

Автор - Roy Baumeister (теория подвергается критике)

Управление временем

Метод помидора

1. Установите таймер на 20-25 минут.
2. Работайте, ни на что не отвлекаясь, до сигнала таймера
3. Сделайте короткий перерыв (5 минут).
4. После каждого 4-го «помидора» делайте длинный перерыв (15-30 минут).

Конец