Калинин Александр Романович

Junior Penetration Tester / Специалист по тестированию на проникновение

Город: Коломна
Телефон: +7 936 333 01 58
Email: a67664159@gmail.com
Telegram: @mult1993
GitHub: https://github.com/Miksander1
CTFtime / профили на платформах: https://tryhackme.com/p/jurniedeqf302

Цель

Получить позицию **Junior Penetration Tester** в компании, где смогу применять навыки тестирования на проникновение, анализа защищенности веб-приложений и Linux-систем, а также развиваться в направлении offensive security в составе профессиональной команды.

Кратко обо мне:

Начинающий специалист по информационной безопасности с практическим опытом в области **web application security**, **CTF**, анализа сетевого трафика и работы с уязвимыми Linux-машинами.

Имею опыт проведения **согласованного аудита безопасности веб-приложения** с документальным подтверждением полномочий и согласованной областью работ. По результатам аудита выявил уязвимости уровней **Critical, High, Medium, Info**, подготовил отчет и рекомендации по устранению.

Знаком с методологией **OWASP Top 10**, использую инструменты: **Burp Suite, Nmap, Wireshark, SQLMap, ffuf, Gobuster, Metasploit, enum4linux, curl, GTFOBins**. Понимаю основы работы с **Linux**, **Kali Linux**, **Active Directory**, сетевыми сервисами и перечислением уязвимых конфигураций.

Умею понятно объяснять найденные уязвимости заказчику и готовить техническое описание с рекомендациями для разработчиков.

Ключевые навыки

Web Application Security

- Понимание методологии **OWASP Top 10**

- Практический поиск типовых веб-уязвимостей в согласованных средах и CTF
- Работа с HTTP-запросами, анализ параметров, форм, cookie, заголовков
- Поиск и эксплуатация **XSS** в рамках соревнований / согласованных сред
- Использование **Burp Suite**, **ffuf**, **Gobuster**, **SQLMap**, **curl**
- Перебор директорий и эндпоинтов
- Базовый анализ исходного кода на **PHP** и **Java**

Network Security

- Анализ сетевого трафика в **Wireshark**
- Извлечение данных из захватов трафика для CTF-задач
- Сканирование и перечисление сервисов с помощью **Nmap**
- Базовое перечисление Windows/SMB-окружений с помощью **enum4linux**
- Понимание основ **Active Directory**

Linux Security

- Уверенная работа в **Linux**
- Использование **Kali Linux**
- Практика на уязвимых Linux-машинах
- Разведка, эксплуатация и повышение привилегий в учебных средах
- Использование **GTFOBins** для анализа возможностей повышения привилегий

Инструменты

- Burp Suite
- Nmap
- Wireshark
- SQLMap
- ffuf
- Gobuster
- enum4linux
- Metasploit
- curl
- GTFOBins

Программирование и скриптинг

- **Python** — изучаю, пишу простые скрипты и автоматизацию
- **PHP** — читаю код
- **Java** — читаю код

Отчетность и методология

- Составление отчетов по результатам аудита
- Подготовка write-up’ов
- Описание уязвимостей и рекомендаций по устранению

- Понимание базового цикла пентеста: разведка, перечисление, эксплуатация, анализ, отчетность

Практический опыт

Согласованный аудит безопасности веб-приложения

Практический проект / независимый аудит
2026 г.
[03.08.2026 17:46] Александр: - Провел авторизованный аудит безопасности веб-приложения на основании соглашения с владельцем / уполномоченным представителем ресурса.
- Работы проводились в рамках согласованной области, правил взаимодействия и подтверждающей документации.
- По результатам аудита выявил:
- 1 Critical-уязвимость
- 1 High-уязвимость
- 2 Medium-уязвимости
- 2 Info-уязвимости
- Подготовил отчет с описанием найденных проблем, уровнем риска и рекомендациями по устранению.
- Передал заказчику и разработчикам понятное техническое описание уязвимостей.
- Оформил write-up’ы и материалы по результатам аудита на GitHub.
- Использовал инструменты web-пентеста: Burp Suite, ffuf, Gobuster, SQLMap, curl.
- Анализировал логику работы веб-приложения, параметры запросов и возможные векторы атак в рамках согласованного scope.

Avito Tech 2026 — участник соревнований по ИБ

2026 г.

- Принял участие в соревнованиях по информационной безопасности.
- Решил **5 заданий**.
- Занял **135 место из 345 участников**.
- Выполнял задания самостоятельно, без команды.
- Работал с задачами по веб-безопасности и анализу сетевого трафика.
- Проводил анализ данных из Wireshark, восстанавливал полезную информацию и использовал её для дальнейших этапов решения.
- В рамках соревновательной среды эксплуатировал уязвимость XSS.
- Продемонстрировал навыки самостоятельного анализа, поиска информации и доведения задач до результата.

Дополнительная практика

CTF и уязвимые стенды

2026 г.

- Регулярно участвую в CTF-соревнованиях и практических заданиях по ИБ.
- Работаю с уязвимыми Linux-машинами: разведка, поиск точек входа, эксплуатация, повышение привилегий.
- Анализирую сетевой трафик в Wireshark и извлекаю данные, необходимые для решения задач.
- Изучаю основы Active Directory и перечисления в Windows-окружениях с помощью enum4linux.
- Использую GTFOBins для понимания возможностей повышения привилегий в Linux.
- Веду GitHub, где публикую write-up’ы, решения и материалы по безопасности.

Образование

Автономная некоммерческая организация “Национальный институт бизнеса”

Специальность: Менеджмент / Управление бизнесом
Год окончания: 2026
Уровень образования: Бакалавр

Дополнительное образование и самообучение

- Самостоятельное изучение основ информационной безопасности
- Практика на уязвимых машинах и CTF-задачах
- Изучение OWASP Top 10
- Практика с Linux, Kali Linux, сетевыми инструментами
- Ведение GitHub с write-up’ами и материалами по безопасности
- Участие в CTF-соревнованиях

Языки

- **Русский** — родной
- **Английский** — A2

О себе

- Интересуюсь offensive security, web-пентестом, CTF и анализом уязвимостей
- Стараюсь участвовать в CTF-соревнованиях
- Веду GitHub, где публикую write-up’ы и практические материалы
- Умею объяснять найденные уязвимости простым языком для заказчика
- Могу подготовить понятное техническое описание уязвимости и рекомендации для разработчиков
- Быстро учусь и готов развиваться в направлении пентеста / application security

---

Направления интересов

- Web Application Security
- Penetration Testing
- CTF
- Linux Security
- Network Traffic Analysis
- Социальная инженерия в рамках этичного тестирования
- Active Directory Security — базовый уровень