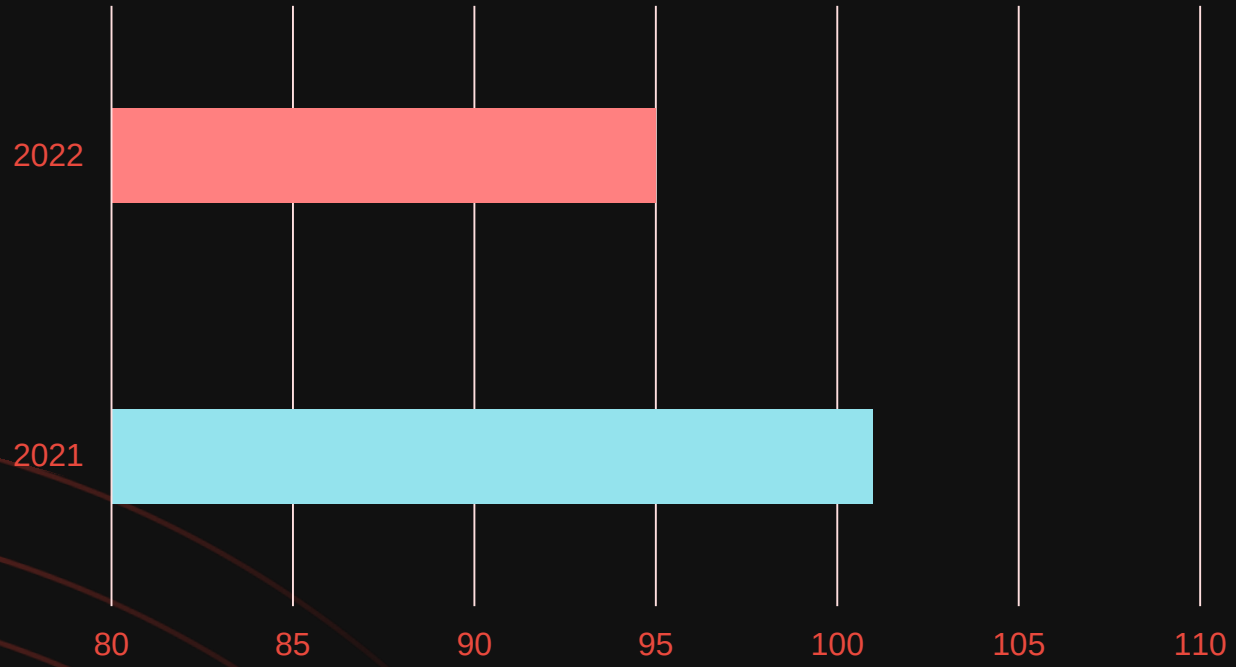
Ломаем бизнес-логику в современных веб-приложениях

2022
ALMATY
KAZAKHSTAN

196

Уязвимостей в бизнес-логике было
найдено за 2021-2022 годы

Статистика багов в пентестах



Experience by vulnerability type 1566 vulnerability types	Submissions Count	Bounties Total	Criticals Submitted	Reputation Change
Insecure Direct Object Reference (IDOR) CWE-639	33	$9,550	12	259
Business Logic Errors CWE-840	28	$6,407	3	288
Violation of Secure Design Principles CWE-657	26	$8,150	5	272
Improper Access Control - Generic CWE-284	22	$14,400	0	291
Improper Restriction of Authentication Attempts CWE-307	19	$9,600	1	334

Проблема

Проблема

- Неопытные разработчики
- Неправильная реализация бизнес-логики
- При масшабировании сложно уследить за безопасностью
- Часто не воспринимают безопасность всерьез

Кто я?

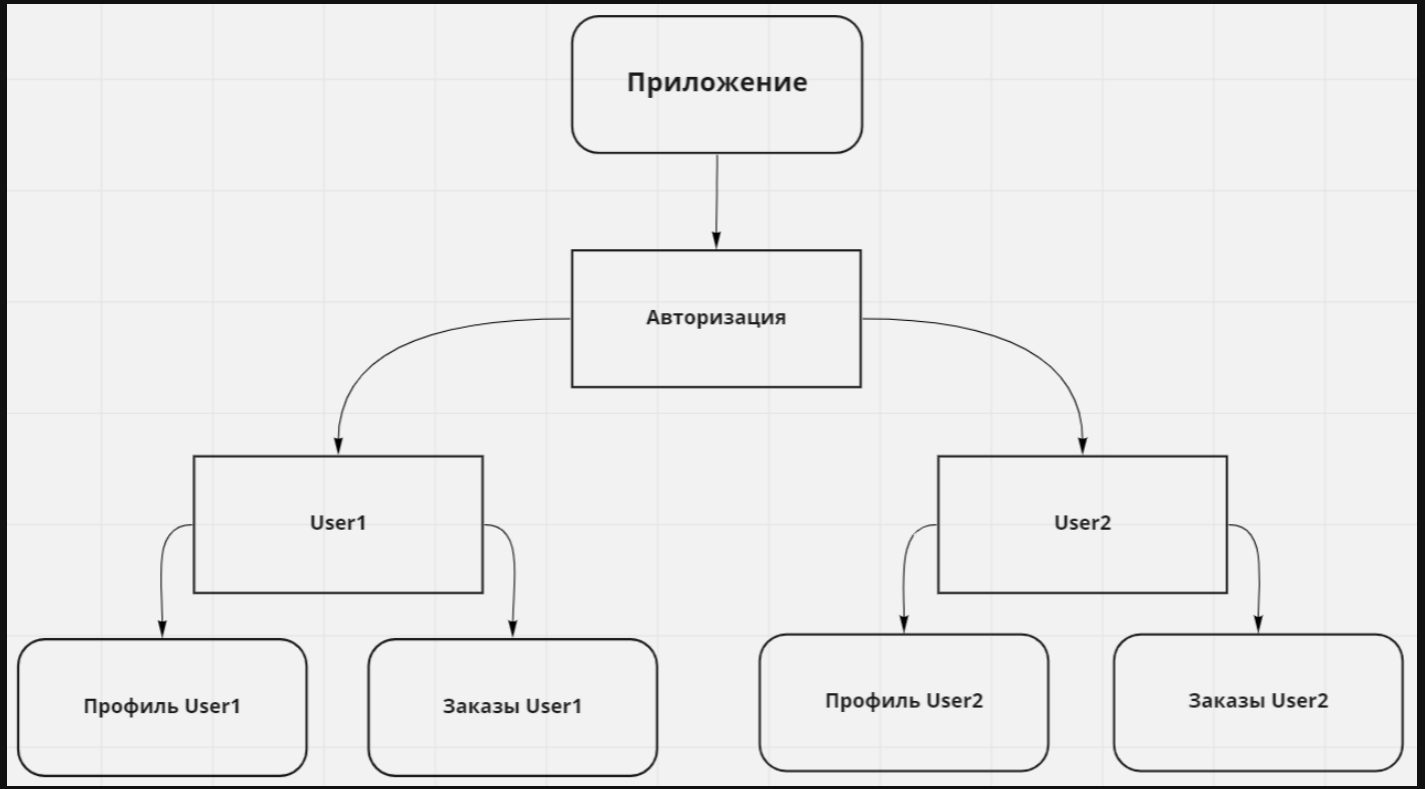
- Рамазанов Рамазан (@r0hack)
- Пентестер и TechLead в DeteAct
- Багхантер
- Большой любитель изучать и ломать бизнес-логику приложений

Бизнес-логика

Как выглядит эта логика?

— Что такое бизнес-логика?

Как выглядит эта логика?



Зачем нам эта логика?

- Что такое бизнес-логика?
- Понимание принципа работы бизнес-логики в приложении

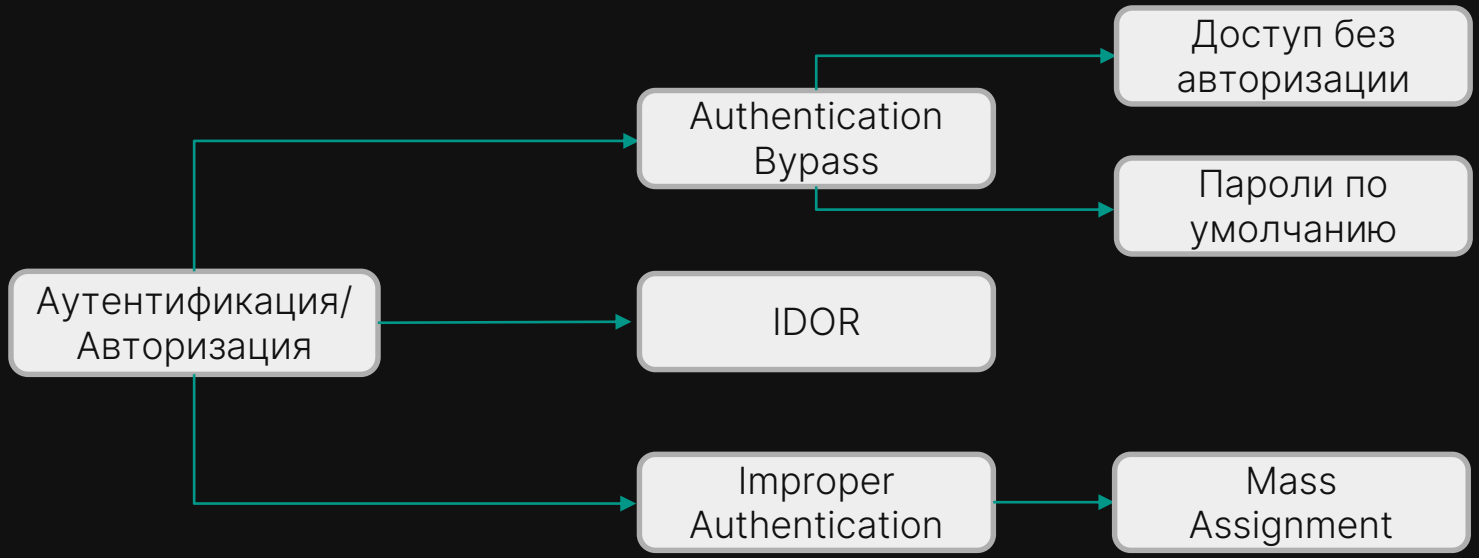
Типы багов

Типы логических багов

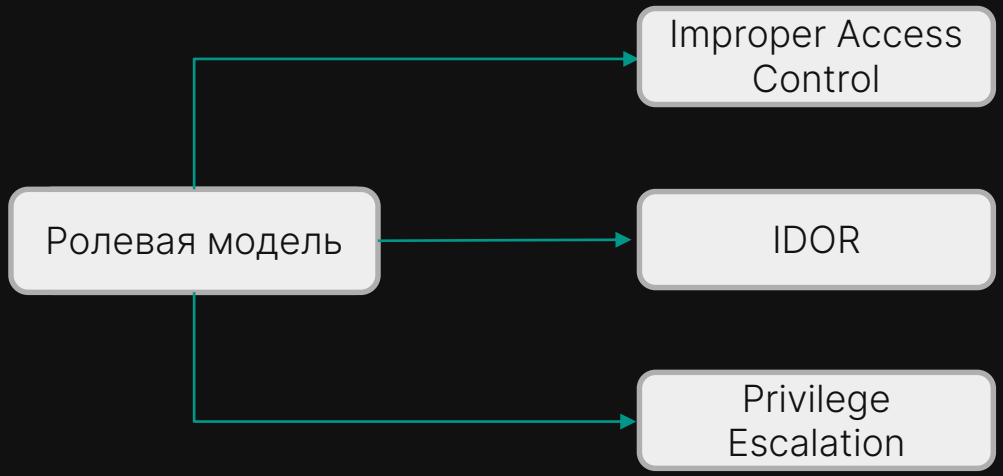
- Improper Access
- Race Condition
- Authentication Bypass
- Privilege Escalation
- Improper Authentication
- Improper Input Validation
- IDOR
- SSRF
- Path Traversal

Ломаем логику

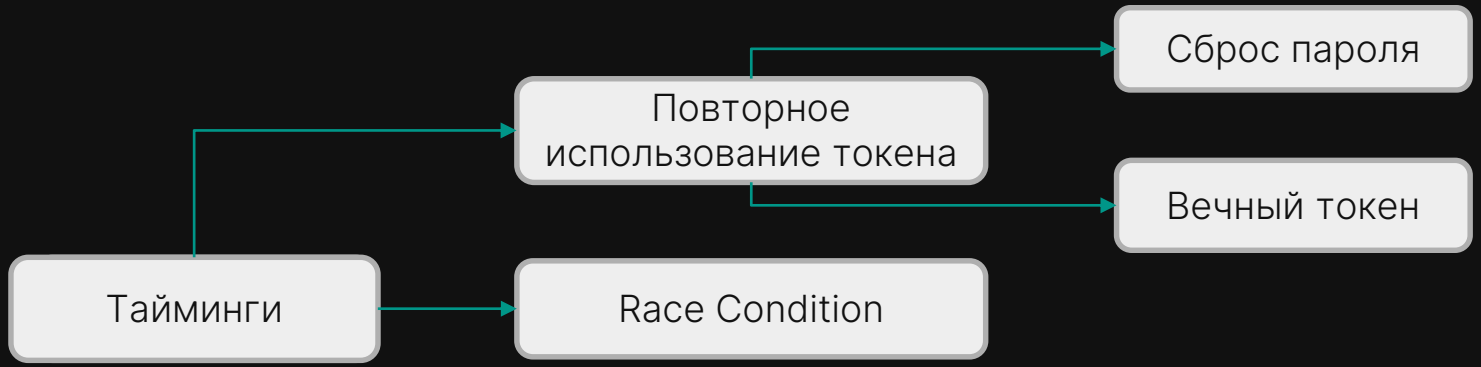
Ломаем логику – Аутентификация/Авторизация



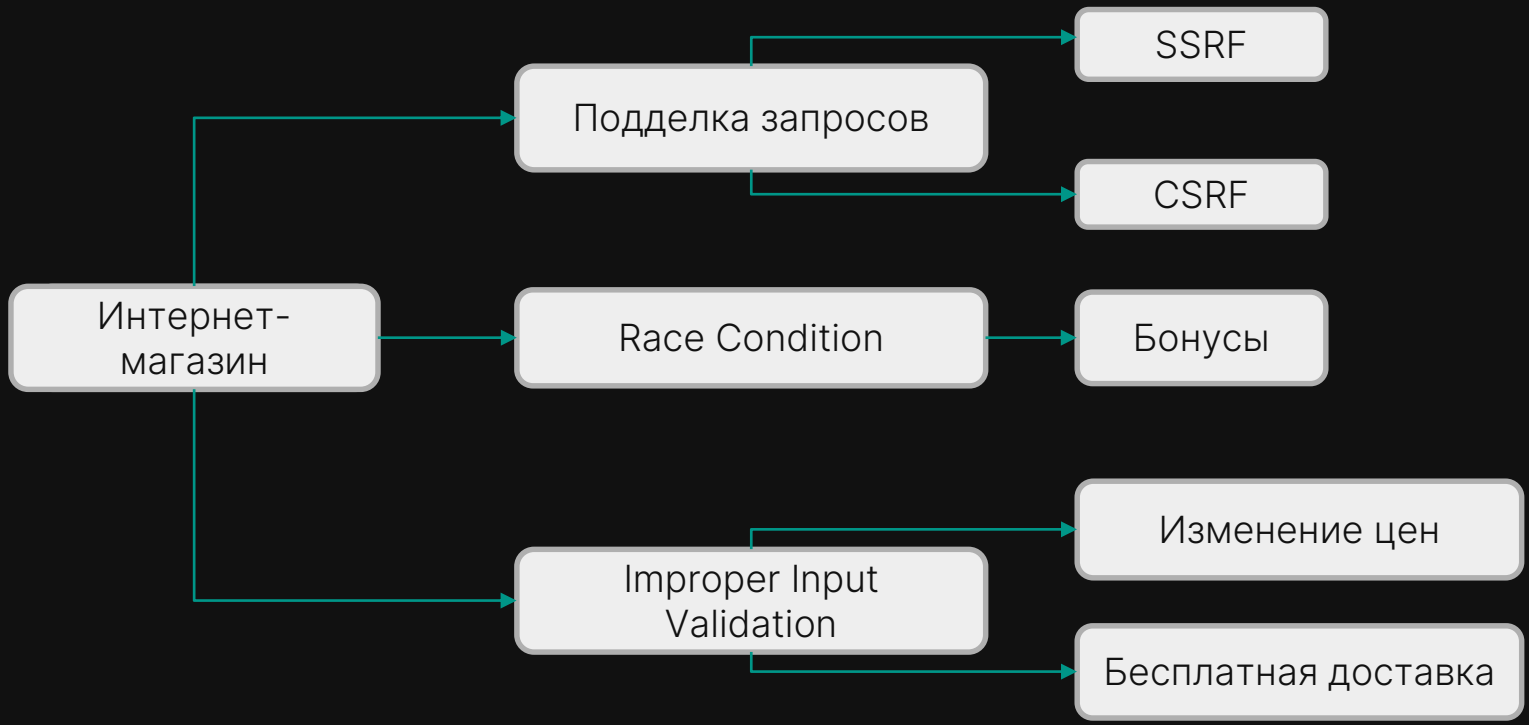
Ломаем логику – Ролевая модель



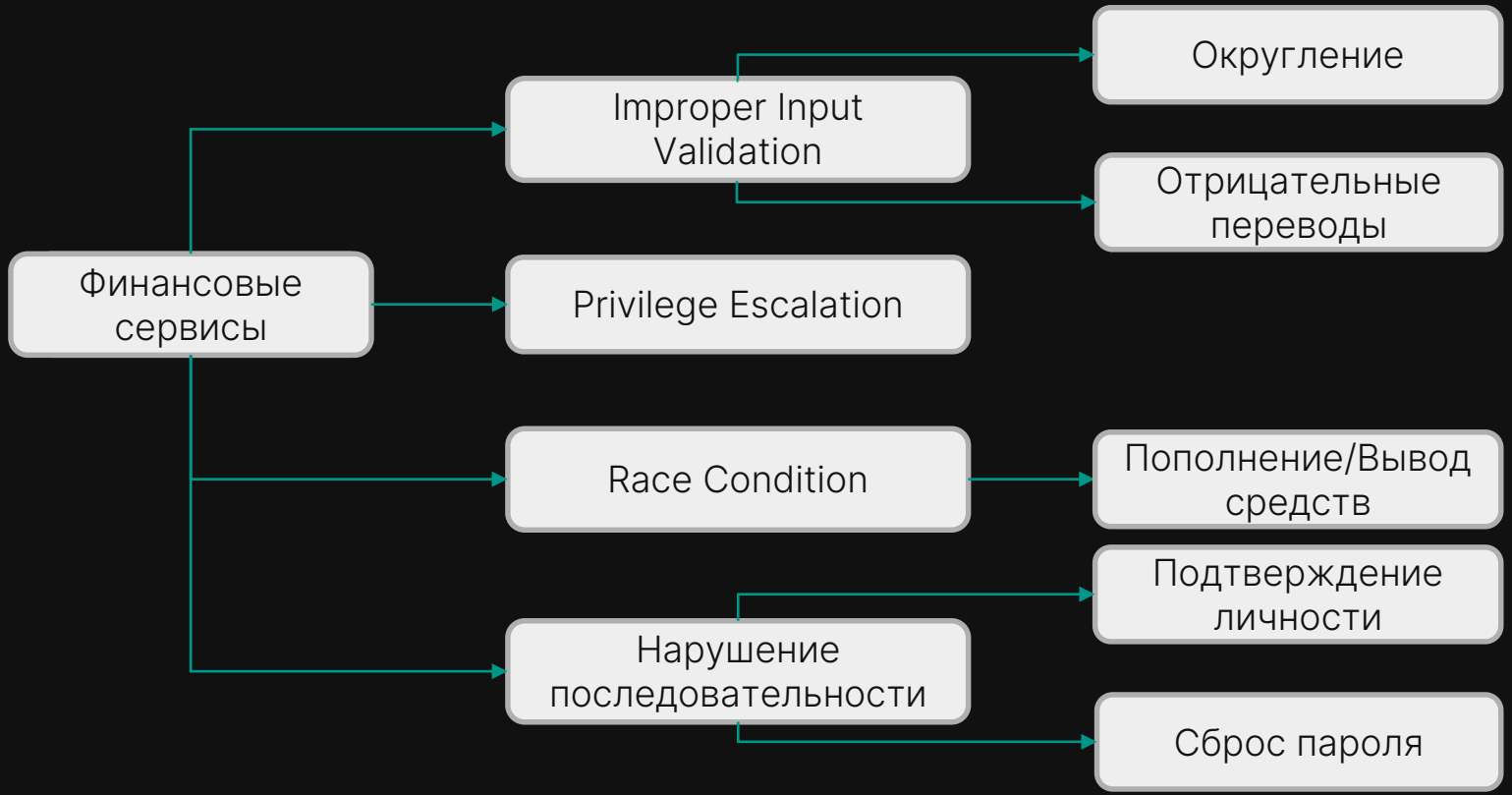
Ломаем логику - Тайминги



Ломаем логику – Интернет-магазина



Ломаем логику – Финансовые сервисы



Инструменты

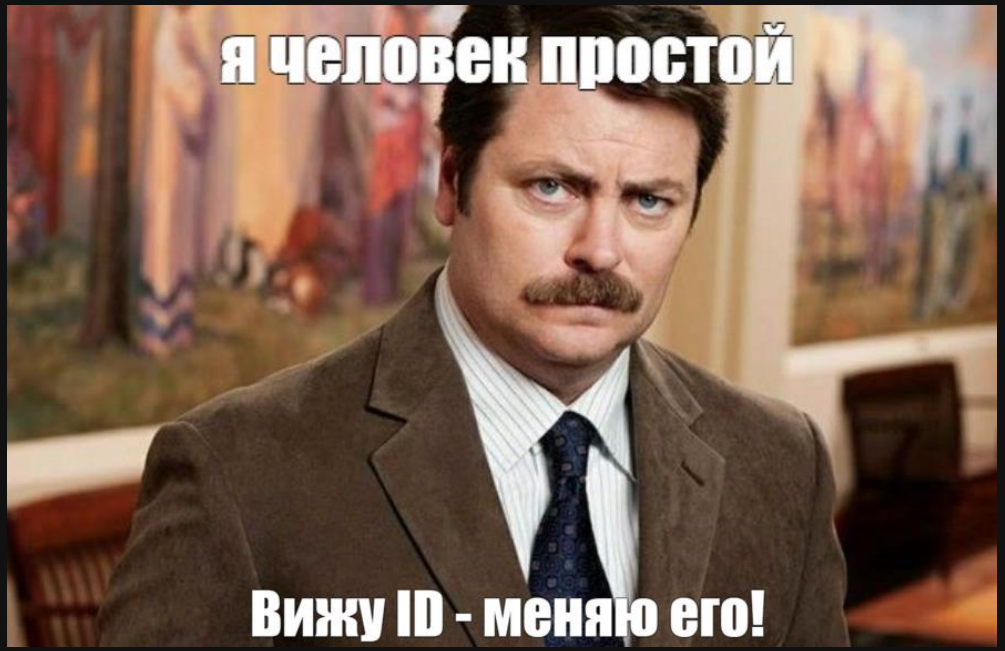
Инструменты

- BurpSuite
- Autorize
- Turbo Intruder
- Param Miner
- Arjun
- mitmproxy
- HTTP Mock

Выводы

Выводы

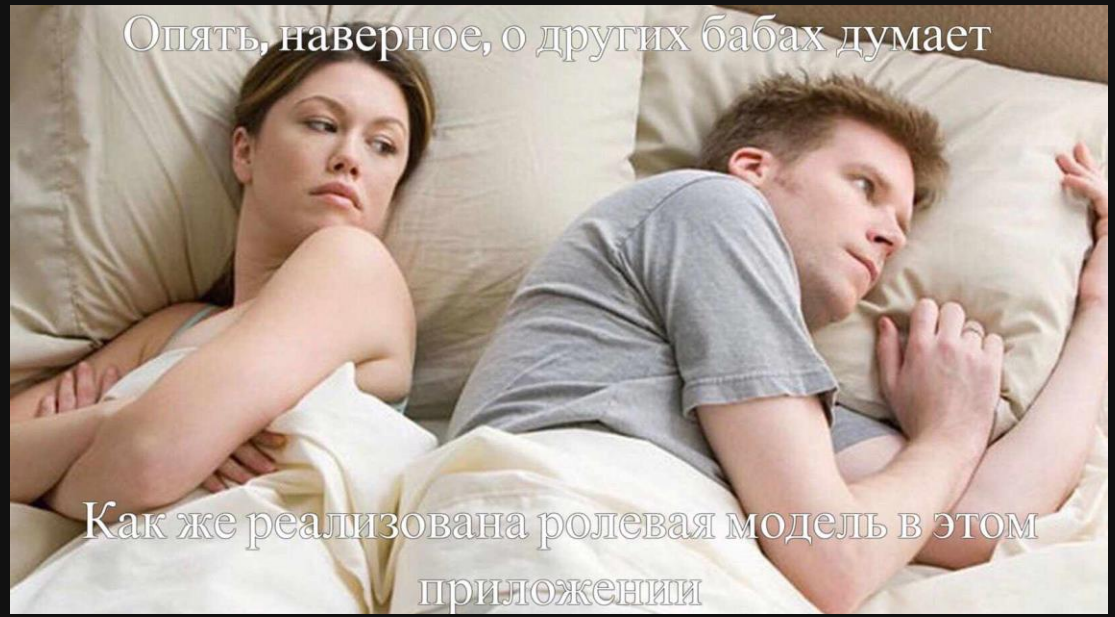
—— Начните с простого



Выводы

—— Начните с простого

—— Вникайте в логику



Выводы

—— Начните с простого

—— Вникайте в логику

—— Продумывайте сложные векторы

Выводы

—— Начните с простого

—— Вникайте в логику

—— Продумывайте сложные векторы

—— Полезные ссылки

Полезные ссылки

—— https://blog.deteact.com/

—— https://t.me/BountyOnCoffee - Много интересного про логику

—— https://habr.com/ru/company/oleg-bunin/blog/412855/ - CSRF атаки

—— https://www.wallarm.com/what/business-logic-flaw - еще вам бизнес векторов

—— https://bo0om.ru/race-condition-ru - подробнее про рейсы

—— https://bit.ly/3qwDIIN - самый подробный материал по SSRF

—— https://gist.github.com/zmts/802dc9c3510d79fd40f9dc38a12bccfc - про токены

—— https://blog.intigriti.com/ - много интересных статей

—— HackerOne Хактивити

——https://medium.com/purplebox/broken-access-control-f82235ddf888

Всем рахмет!

Вопросы?

TG: r0hack

BountyOnCoffe