DataArt

Security Audit: жизнь до и после

Yaroslav Vorontsov, PhD
Software Architect, Security Architect

yvorontsov@dataart.com

About me

DataArt

- ВГУ, ФКН: 2007-2012
  - Продолжение: 2012-2015 (PhD)
  - Там же: ассистент каф. ПиИТ
  - С 2016 – спецкурс на каф. ИТУ
- DataArt: 2010 – по настоящее время
  - Intern->Junior->Middle->Senior iOS
  - Team and Tech Lead
  - Software Architect
  - Security Analyst

Agenda

DataArt

- Аудит безопасности
  - Место в модели BSIMM (OWASP SAMM)
  - Признаки и цели
  - Применимость
- Основные темы аудита
  - Компоненты приложения
  - Инфраструктура, конфигурация
  - …И немного об эпичных промахах
- Жизнь после
  - Приоритизация задач

Об аудите

BSIMM и OWASP SAMM

DataArt

Building Security in Maturity Model

- Compliance and Policy, CP2.3
  - Implement and track controls for compliance

Software Assurance Maturity Model

- Policy & Compliance, PC2B
  - Establish project audit practice

«А как называете его вы?»

DataArt

Ключевые признаки

DataArt

- Частота
  - однократно, раз в квартал/полгода/год,…
- Участники
  - ключевые лица проекта
- Темы для разговора
  - компоненты продукта
  - инфраструктура (+политики обслуживания)
  - процессы и compliance (если нужно)
- Чеклист
  - внутренние и клиентские стандарты
- Итог: список пробелов и проблем

Когда аудит не нужен

DataArt

Абсолютно новый, начатый с нуля проект

- Моделирование угроз (Threat modeling)
  - Attack Trees (Schneier)
  - STRIDE -> Elevation of Privilege (Shostack)
  - CAPEC (Mitre)
  - DREAD
- Оценка рисков (Risk assessment)
  - Количественные модели
  - Качественные

Короткоживущий проект

- Не связанный с обработкой и хранением критичных данных (sensitive data)

Team augmentation

- У вас отсутствует возможность принятия ключевых управленческих решений

Впопыхах перед внешней проверкой (или во время, что ещё хуже)

- Пустая трата денег и сил

Темы аудита (и наиболее частые проблемы)

User management

DataArt

ID	Picture	Login	Nickname	Full name	Gender	Country	Collections	Source	Registered
1		admin		Johnny Admin	M	United States	1		07/23/17
2		mary		Mary Wilson	F	United States			07/23/17
3		jay		Jay Parker	M	United States	2		07/22/17
4		dave		David Miller	M	United States	2		07/22/17
5		paul		Paul Jones	M	United States	2		07/21/17
6		larry		Larry Smith	M	United States			07/20/17
7		kate		Kate Adams	F	United States			07/20/17

- **Scope of admin responsibilities**
  - manage users
  - enable/disable users
  - reset credentials
  - view audit log
- **Credential policies**
  - secure distribution and change
  - secure storage
  - inactivity lockout
  - *password rotation and complexity*
  - **no default credentials**

User Authentication

DataArt

Authentication Mechanism

- Generic error on login
- Anti brute force
- SSO and MFA
- Re-authentication for sensitive actions
- Secure password recovery

Token Security

- Token generation
- Token transmission
- Token signature
  - Keys should not be reused
- Token reissue

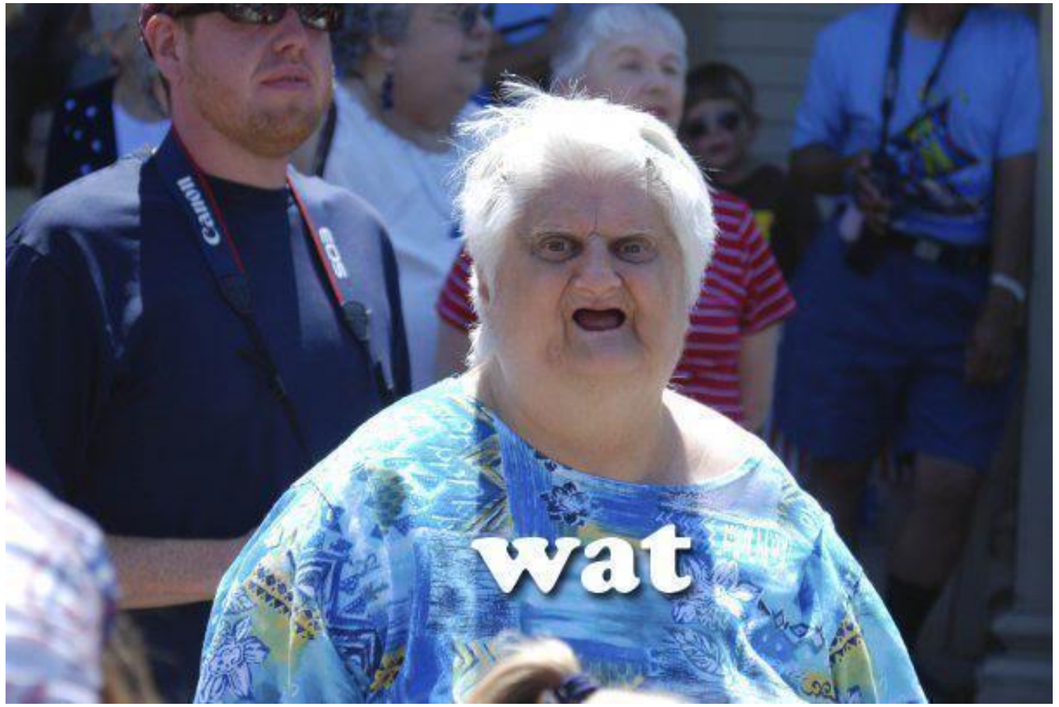
Session Anti-hijack

- Explicit termination
- Inactivity termination
- Absolute termination
- Termination on password change and reset
- CSRF mitigation

Access Control

DataArt

- Access control model
  - Components used for implementation
- Access control enforcement
  - For static resources as well
- Data contextual access control
  - aka Data Permissions
- Additional restrictions (IP, geo…)
- **Audit**



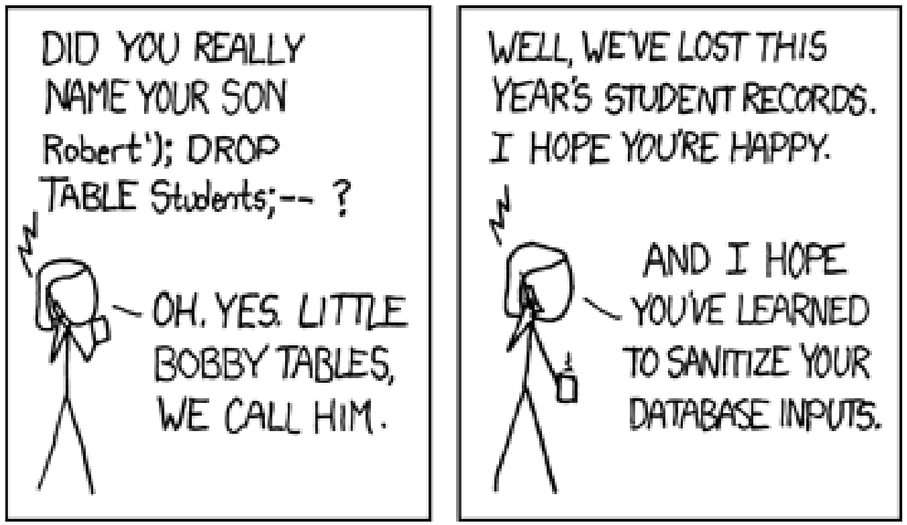
Data Protection

DataArt

- Secure connections to internal services and databases
- Encryption of sensitive data at rest (with appropriate key management policies)
  - Non-compromised ciphers and cipher suites
- Disclosure of sensitive information
  - in non-authenticated area
  - in logs
  - in VCS (3rd party credentials)
  - via verbose error messages
  - via code (obfuscation, minification)
  - via client-side caches
- **Storage of PII according to regulatory guidelines (GDPR, HIPAA,…)**

Input handling

DataArt



- Separate DTO
- Server-side validation (whitelist, blacklist)
- Prepared statements
- File Upload
  - File name and content checks
  - Content type and size limitations
- Output encoding
- Validated server-side redirects

Environment Configuration

DataArt

Web server

- HTTP verbs
- CORS configuration
- Security HTTP headers
- Platform headers
- HTTP redirect to HTTPS
- TLS configuration

Network security

- Inventory (diagram?)
- Environment isolation
- NAT and firewalls
- Redundancy of critical components

Host security

- Account management
- Unused services
- File system monitoring
- Antivirus scanning
- Clock synchronization
- Transparent encryption
- Auditable, time-limited remote access

Processes

DataArt

Logging and Monitoring

- Centralized logging
  - Various sources
  - Retention policy
  - Log integrity
  - Access control
- Traffic monitoring
- WAF, IDS, IPS
- Alerting

Backups

- Documented policy
  - Retention policy
- Relevance
- Encryption
- Recovery procedures
  - Alerting in case of failure
  - Test periodically

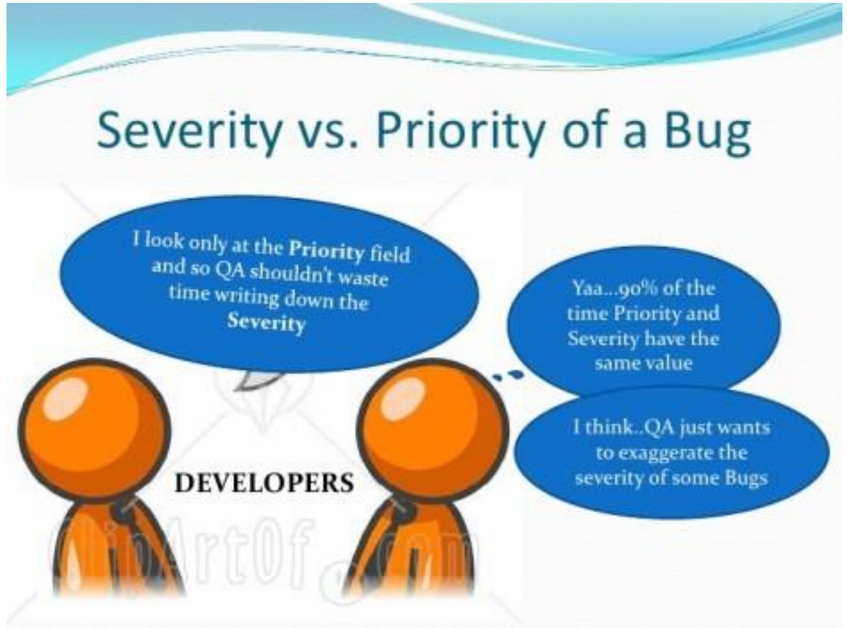
Maintenance

- Patching
- Vulnerability scanning
- Code scanning
- Risk assessment
- Penetration testing

Приоритизация

Шеф, усё пропало?

DataArt



Пирамиды Маслоу

Пирамида Маслоу, первая версия

Приоритеты

DataArt

1. Человеческий фактор: логины и пароли по умолчанию, секретные URL…
2. Защита данных: шифрование, меры против SQL Injection…
3. Аутентификация, управление сессиями и базовый аудит
4. Безопасная конфигурация окружения (ОС, веб-сервер, сеть)
5. Авторизация и расширенный аудит
6. Anti-XSS, Anti-XSRF, CORS
7. Аудит 3rd party кода и компонентов
8. Прочие мелкие настройки
9. …

1. Аудит – скучная, но нужная вещь
2. Вы тоже занимаетесь им
3. Не является панацеей
4. Требует подготовки
5. Расставьте приоритеты
6. Жизнь до аудита – есть
7. И после – тоже ☺

DataArt

Security Audit: жизнь до и после

Yaroslav Vorontsov, PhD
Software Architect, Security Architect

yvorontsov@dataart.com