Лекция 14. Безопасность веб-приложений

Цель лекции: познакомиться с безопасностью веб-приложений и с аудитом безопасности.

План лекции:

1. Безопасность веб-приложений
2. Уязвимости веб-проектов
3. Аудит безопасности

Сайт - часть корпоративной инфраструктуры. Взлом корпоративного сайта - это удар по репутации и имиджу компании. Очень неприятное в подобных событиях - огласка происшествия. Но потеря данных, информации о клиентах – это уже прямые убытки. И огласка таких происшествий происходит далеко не всегда.

Чем серьезнее компания и известнее ее имя и продукты, тем существеннее бывают риски и убытки от взлома корпоративного портала.

Что угрожает вашему сайту?

- Взлом информационной среды (операционная система, веб-сервер, среда программирования, база данных)
- Взлом системы управления корпоративным порталом
- Взлом сторонних веб-приложений

Степень угроз можно разделить на три уровня риска:

Минимальный – получение доступа к не конфиденциальной информации, к которой не санкционирован доступ, возможность создания косметических проблем и помех в работе проекта.

Средний уровень – получение частичного доступа к конфиденциальной информации, частичный обход системы авторизации расширяющий полномочия.

Высокий уровень – полный обход системы авторизации, получение неограниченного доступа к системе или приложению, возможность запуска несанкционированных приложений, возможность просмотра или подмены конфиденциальной информации.

Уязвимости веб-проектов

Автоматизированный подбор

- Недостаточная аутентификация (Insufficient Authentication)

- Небезопасное восстановление паролей (Weak Password Recovery Validation)

Авторизация

- Предсказуемое значение сессии (Credential/Session Prediction)
- Недостаточная авторизация (Insufficient Authorization)
- Отсутствие таймаута сессии (Insufficient Session Expiration)
- Фиксация сессии (Session Fixation)

Атаки на клиента

- Подмена содержимого (Content Spoofing)
- Межсайтовое выполнение сценариев (Cross-site Scriptin - XSS)

Выполнение кода

- Переполнение буфера (Buffer Overflow)
- Атака на функции форматирования строк (Format String Attack)
- Внедрение операторов (LDAP Injection)
- Выполнение команд ОС (OS Commanding)
- Внедрение команд SQL (SQL Injection)
- Внедрение серверных расширений (SSI Injection)
- Внедрение операторов XPath (XPath Injection)

Разглашение информации

- Индексирование директорий (Directory Indexing)
- Утечка информации (Information Leakage)
- Обратный путь в директориях (Path Traversal)
- Предсказуемое расположение ресурсов (Predictable Resource Location)

Логические атаки

- Злоупотребление функциями (Abuse of Functionality)
- Отказ в обслуживании (Denial of Service)
- Недостаточное противодействие автоматизации (Insufficient Anti-automation)
- Недостаточная проверка процесса (Insufficient Process Validation)

Как защитить сайт?

- Для защиты инфосреды веб-проекта необходимо использовать специальные средства мониторинга.
- Требуйте аудита веб-приложений у разработчиков.

- Если сайт разработан студией дизайна, изучайте политику безопасности.

Аудит безопасности

Различные баги, ошибки и бреши в безопасности WEB-приложений обеспечивают широкие возможности для злоумышленников. Все это позволяет раскрывать защищенную информацию, копировать персональные данные и проникать в сети, вызывая сбои в работе программного обеспечения и т.д.

Статистика показывает, что более 72% организаций было скомпрометировано именно через уязвимости, найденные в программной части приложений. Чтобы защититься от неприятных инцидентов в сфере ИБ, нужен качественный анализ.

К анализу уязвимостей подходят комплексно – мероприятия по аудиту защищенности веб-приложений и анализу уязвимостей (WEB) проходят по всем правилам и последовательно. В процессе выполняются несколько основных задач:

- Выявление уязвимостей, которые могут быть использованы злоумышленником в корыстных целях.
- Проверка уровня безопасности программного обеспечения или сервиса.
- Оценка качества применяемых способов защиты.

Основные методы аудита похожи на действия злоумышленника и включают в себя:

- Разведку и сбор информации об атакуемой системе: в ход идут специальные поисковые запросы (google dork), обнаружение почтовых адресов сотрудников, профилей компании на сайтах вакансий (по вакансиям можно определить используемые технологии), поиск информации в кеше поисковиков, сканирование портов;
- Выявление защитных средств сайта — IDS/IPS/AntiDDoS/WAF систем;
- Сканирование веб-приложения популярными утилитами и сканерами — здесь достаточно широкий выбор, как платных, так и бесплатных программ, например веб-сканер w3af;
- Сканирование директорий веб-сайта для поиска чувствительной информации (файлы, бэкапы базы данных и прочее) — к примеру утилитой dirbuster;
- Ручной анализ уязвимостей — с помощью проксирующих средств происходит обработка запросов и анализ на предмет наличия потенциальных уязвимостей, одна из популярных утилит — Burpsuite.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582

5. Carl A. Sunshine. Computer Network Architectures and Protocols. — Springer Science & Business Media, 2013-06-29. — 542 с. — ISBN 978-1-4613-0809-6.