РИФ-2006

Секция «Информационная безопасность»

Практика противодействия сетевым атакам на интернет-сайты

Сергей Рыжиков
директор ООО «Битрикс»

Безопасность корпоративного сайта

Веб-сайт - часть корпоративной инфраструктуры.

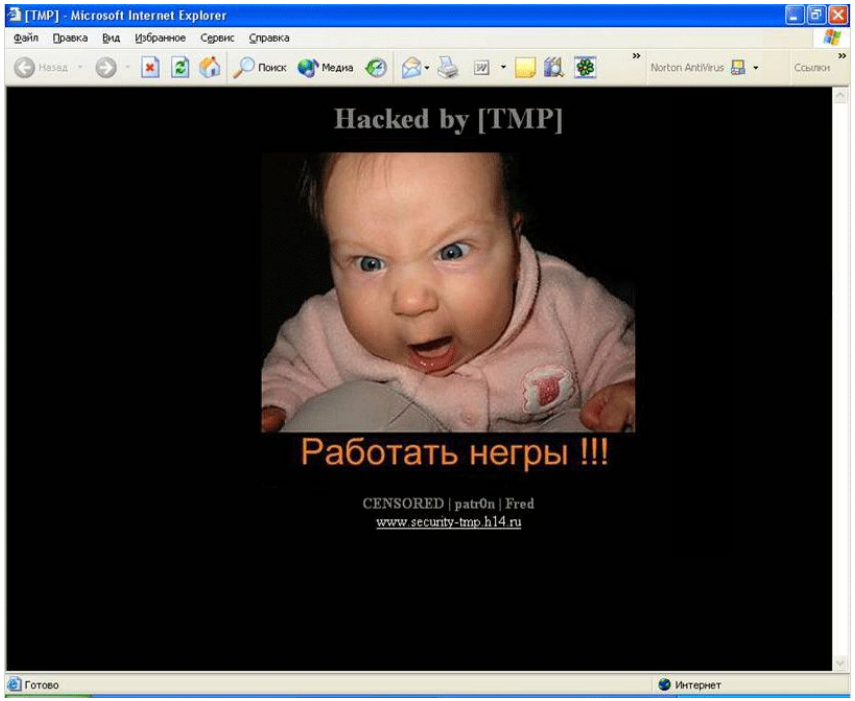
Взлом корпоративного сайта - это **удар по репутации и имиджу** компании. Очень неприятное в подобных событиях - огласка происшествия. Но потеря данных с сайта, информации о клиентах – это уже прямые убытки. И огласка таких происшествий происходит далеко не всегда.

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

Когда сайт – это имидж и репутация

Потенциальные угрозы

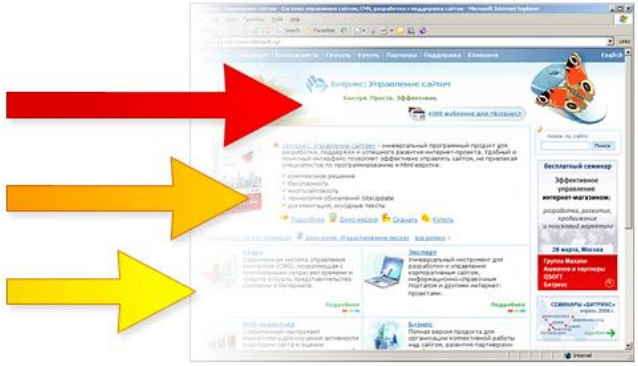
- Взлом **информационной среды** (операционная система, веб-сервер, среда программирования, база данных)
- Взлом **системы управления сайтом**
- Взлом **сторонних веб-приложений**



Что угрожает вашему сайту?

Уровни риска

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)

Безопасность веб-проектов

Интернет-сайт является традиционным программным приложением, которое работает в рамках операционной системы и серверного программного обеспечения, использует сервисные функции операционной системы и других программных продуктов.

Составляющие веб-проекта:

- **Информационная среда**
  - Операционная система
  - Веб-сервер
  - Среда программирования
  - База данных
- **Система управления сайтом**
- **Сторонние веб-приложения**

Очень часто сайты состоят из веб-приложений разных разработчиков (с многочисленными паролями, разными требованиями). В многосайтовом веб-проекте подобная ситуация создает серьезные проблемы.

Как защитить сайт?

Для защиты инфосреды веб-проекта, даже если сайт размещен у хостинг-провайдера, необходимо использовать **специальные средства мониторинга**.

Требуйте **аудита веб-приложений** у разработчиков.

Если сайт разработан студия дизайна, изучайте **политику безопасности**.

Внешний аудит безопасности

Для обеспечения высокого уровня защищенности закажите **независимый аудит информационной безопасности** у сторонних компаний (например, Positive Technologies, «Немесис»).

Непрерывный аудит обеспечит **независимый экспертный надзор** и сохранит уровень безопасности сайта на высоком достигнутом уровне.

Рекомендации

Обеспечение **безопасности информационной среды** - задача сложная и ответственная.

Для обеспечения более высокого уровня безопасности ваших интернет-проектов необходимо комплексно подойти к обеспечению безопасности Информационной среды и веб-приложений.

- поручить задачу обеспечения безопасности дата-центру или хостинг-провайдеру (**DATAFORT**, **Мастерхост и другие**);
- использовать **внешние программы** для надежного мониторинга информационной среды.

Спасибо за внимание!

Отвечу на ваши вопросы.