Безопасность веб-проектов
Защита сайтов от взломов и атак

Сергей Рыжиков
директор компании «Битрикс»

Безопасность веб-проектов

Сайт - часть корпоративной инфраструктуры.

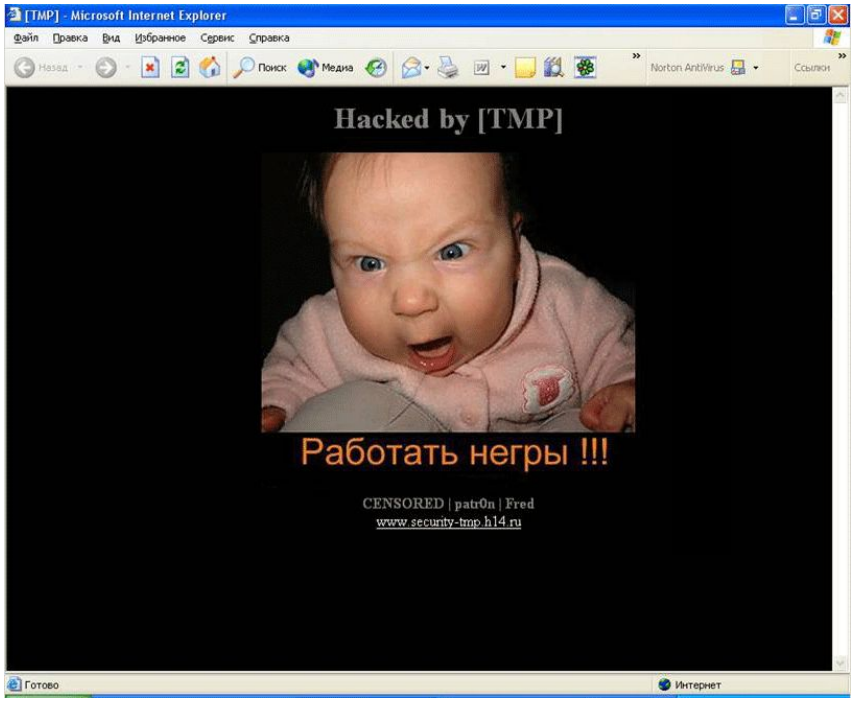
Взлом корпоративного сайта - это **удар по репутации и имиджу** компании. Очень неприятное в подобных событиях - огласка происшествия. Но потеря данных, информации о клиентах – это уже прямые убытки. И огласка таких происшествий происходит далеко не всегда.

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

Когда сайт – это имидж и репутация

Потенциальные угрозы

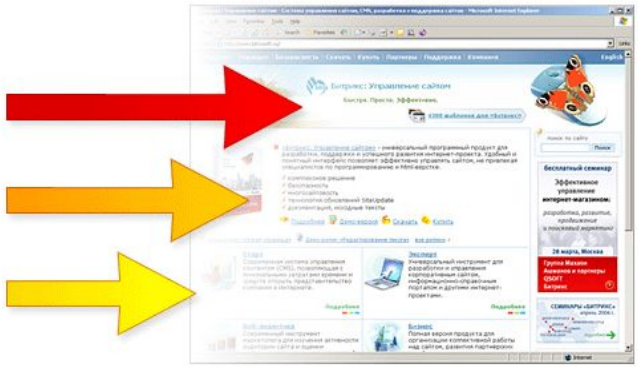
- Взлом **информационной среды** (операционная система, веб-сервер, среда программирования, база данных)
- Взлом **системы управления корпоративным порталом**
- Взлом **сторонних веб-приложений**



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

Портал 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 порталом**
- **Сторонние веб-приложения**

Иногда порталы 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 необходимо использовать **специальные средства мониторинга**.

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

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

Аудит безопасности

Для обеспечения высокого уровня защищенности закажите **независимый аудит информационной безопасности** у сторонних компаний.

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

Внутри компании «Битрикс» создан отдел информационной безопасности, который выполняет:

- аудит информационной среды (сервера, ОС, распределение прав доступа);
- аудит веб-приложений;
- тестовый взлом системы;
- постоянный мониторинг проекта.

За 4 месяца работы отдела при аудите внешних систем в 100% случаях получен максимальный доступ к системе.

Архитектура безопасности продукта

При проектировании программного продукта «Битрикс: Управление сайтом» вопросам безопасности продукта уделялось особое значение на всех этапах разработки и тестирования.

- Единая система авторизации
- Единый бюджет пользователя для всех модулей
- Двухуровневая система разграничение прав доступа
- Независимость системы контроля доступа от бизнес-логики страницы
- Возможность шифрации информации при передаче
- Система обновлений SiteUpdate
- Журналирование
- Политика работы с переменными и внешними данными
- Методика двойного контроля критически опасных участков кода

Единая система авторизации

- Управление пользователями
- Управление группами пользователей
- Надежная идентификация пользователя
- Механизм безопасной смены пароля
- Возможность запомнить авторизацию
- Невозможность подсмотреть пароль пользователя

Система разграничения прав доступа

В программном продукте «Битрикс: Управление сайтом» реализована **двухуровневая система разграничения прав доступа**:

Уровень 1: доступ к файлам и каталогам

Уровень 2: доступ к модулям и логическим операциям в модулях

Независимое журналирование выполняемых пользователями страниц в модуле статистики.

Независимость системы контроля доступа от бизнес-логики страницы

Система авторизации **работает независимо** от бизнес-логики, размещенной в рабочей области страницы.

Принцип независимости системы авторизации от исполняемой части страницы обеспечивает гарантированную защиту приложениям от несанкционированного доступа и исполнения и означает, что если пользователь не будет иметь прав на доступ к странице, ему не удастся обойти систему авторизации.

Шифрация данных

Использование **алгоритмов шифрации** позволяет исключить целый класс потенциальных рисков, связанных с возможностью перехвата информации в канале передачи.

Промышленным стандартом для защиты веб-приложений является **SSL-шифрация** в рамках протокола HTTPS. Данный протокол поддерживается всеми браузерами и не требует установки дополнительных компонент для клиентов.

В качестве сертифицированных **ГОСТ алгоритмов**, на основе которых строится защита веб-ресурса, используются российские стандарты шифрования данных:

- **ГОСТ Р 34.10-94** и **ГОСТ Р 34.11-94** — операции создания и проверки электронной цифровой подписи (ЭЦП) для аутентификации клиента, а также авторизация и обеспечение юридической значимости электронных документов при обмене ими по TLS соединению;
- **ГОСТ 28147-89** — операции шифрования данных и имитозащита для обеспечения конфиденциальности и контроля целостности передаваемой информации по TLS соединению.

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**, **.masterhost и другие**);
- использовать **внешние программы** для надежного мониторинга информационной среды.

Спасибо за внимание!

Отвечу на ваши вопросы.