



conf

RootConf – 2009

Профессиональная конференция
системных администраторов

Безопасность Интернет- проектов: основные проблемы разработки и пути решений

«1С-Битрикс»

Сергей Рыжиков, генеральный директор

Сайты сегодня – набор запчастей

Большая часть современных сайтов - набор запчастей.

- низкий уровень стандартной разработки
- отсутствие единой концепции безопасности
- несколько аккаунтов для одного пользователя
- не обновляемое ПО, особенно после модификации



Разработчики интернет-приложений зачастую не задумываются о безопасности.

О безопасности сайта думают в последнюю очередь!

- индивидуальные разработчики думают о безопасности сайтов в самую последнюю очередь
- клиенты не готовы платить за безопасность интернет-проектов
- подразумевается, что разработчик должен этим заниматься, но у него не остается ни времени, ни бюджета

Хостинг часто не защищен

- зачастую уровень администрирования серверов и хостинга *критически низкий*
- редко используются системы автоматического мониторинга



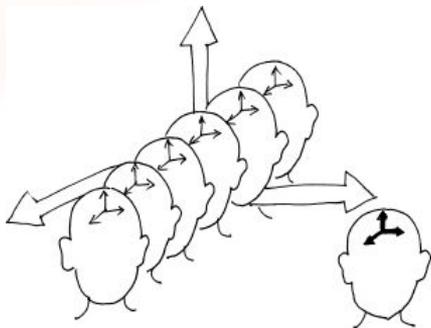
Цикл разработки

- I. Перед выпуском модуля идет обязательное тестирование разработчиками на внутренних серверах с разными базами данных, операционными системами и версиями PHP.
- II. Отдел тестирования проверяет на соответствие бизнес-функциональности и наличие ошибок.
- III. Отдел безопасности проверяет на наличие уязвимостей.
- IV. Модуль поступает в бета-тестирование клиентам и партнерам.

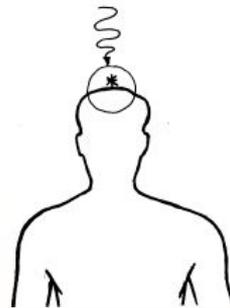
Разработчики работают в компании по 5-8 лет, но все равно допускают ошибки в безопасности. Почему?

Психология хакера и разработчика

Психология хакера и разработчика принципиально отличаются:



Как мыслит разработчик...



... и как мыслит хакер

Профессиональным веб-разработчик становится только через 3-5 лет и при активном контроле со стороны специалиста по веб-безопасности.

Категории хакеров

Студенты, ИТ специалисты начального уровня



- пробуют силы на первых попавшихся сайтах
- нет понимания последствий для жертвы
- нет осознания юридической личной ответственности
- редко зарабатывают на хакерстве как на бизнесе

Профессиональные специалисты



- прекрасный технический багаж
- никогда не светятся в тусовках, не кривляются
- делают только на заказ и только за деньги
- активно работают на службы безопасности крупных компаний

Соотношение разработчиков к хакерам 1:100

Платный аудит безопасности

- Индивидуальная проверка проектов специалистами по веб-безопасности
- Большой объем работы
- Постоянные изменения вносимые в интернет-проекты
- Нехватка специалистов
- Отсутствие сформированной практики аудитов

Аудит профессиональными компаниями - услуга комплексная, сложная и зачастую не подходит для массового рынка.

Новый подход к концепции веб- безопасности

- *Проактивная защита* – это комплекс технических и организационных мер, которые объединены общей концепцией безопасности и позволяют значительно расширить понятие защищенности и реакции веб-приложения на угрозы.
- Панель безопасности
- Проактивный фильтр (Web Application Firewall)
- Технология одноразовых паролей (OTP)
- Защита авторизованных сессий
- Контроль активности
- Шифрование канала передачи через SSL
- Журнал вторжений
- Защита административных разделов по IP
- Стоп-листы
- Контроль целостности
- Рекомендации по настройке безопасности
- Защита редиректов от фишинга
- Монитор обновлений



Проактивная защита

1С-Битрикс: FrameWork

Платформа «1С-Битрикс» - это комплексное решение с единой системой безопасности:

- единая политика безопасности;
- единая система авторизации;
- единый бюджет пользователя для всех модулей;
- трехуровневая система разграничения прав доступа;
- независимость системы контроля доступа от бизнес-логики страницы;
- смена пароля;
- запомнить авторизацию;
- возможность шифрования информации при передаче;
- система обновлений SiteUpdate;
- независимое журналирование выполняемых страниц в модуле Статистики;
- политика работы с переменными и внешними данными;
- методика двойного контроля критически опасных участков кода;
- политика работы с пластиковыми картами.

Панель безопасности

Панель безопасности

Рабочий стол > Настройки > Проактивная защита > Панель безопасности

Текущий уровень безопасности: Стандартный.

Уровень безопасности: Стандартный

Параметр	Значение	Рекомендации
Проактивный фильтр (Web Application Firewall)	Включен	
Исключения из проактивного фильтра	Нет	
Журнал вторжений за последние 7 дней	1	Просмотреть записи
Контроль активности	Включен	
Уровень безопасности группы администраторов	Повышенный	
Использовать CAPTCHA при регистрации	Да	
Режим вывода ошибок (error_reporting):	Только ошибки	

Уровень безопасности: Высокий

Параметр	Значение	Рекомендации
Журналирование событий главного модуля	Не все включены	Включить
Защита административной части	Выключена	Включить
Хранение сессий в базе данных	Выключено	Включить
Смена идентификатора сессий	Выключена	Включить

Уровень безопасности: Повышенный

Оценка уровней безопасности веб-проекта

Проактивный фильтр Web Application FireWall

Проактивный фильтр распознает большинство опасных угроз и блокирует вторжения на сайт.

- XSS - cross site scripting (CSS)
- SQL инъекции
- PHP Including
- часть атак, связанных с обходом каталогов

- Экранирует приложение от наиболее активно используемых атак
- Фиксирует попытки атаки в журнале
- Информировывает администратора о случаях вторжения

Технология одноразовых паролей

Технология одноразовых паролей (One Time Password - OTP) с использованием брелков Aladdin eToken PASS позволяет быть однозначно уверенным, что на сайте авторизуется именно тот человек, которому выдали брелок.

Корректность работы электронных ключей eToken PASS для системы «1С-Битрикс: Управление сайтом 8.0» подтверждается соответствующим сертификатом компании Aladdin, выданным на основании серии испытаний.



eToken
YOUR KEY TO SECURITY



Aladdin
SECURITY SOLUTIONS

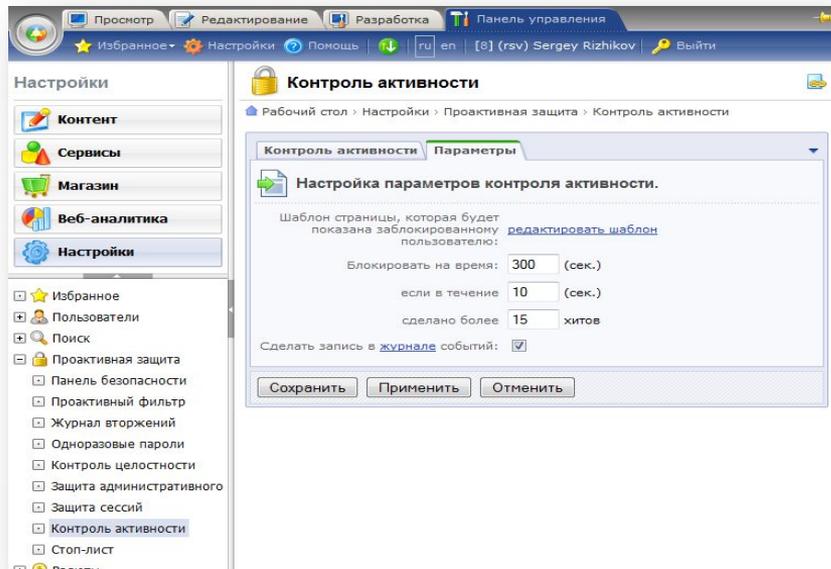
Технология защиты авторизованных сессии

Сессия пользователя – это ключевой объект атаки на веб-сайт с целью получения сессии авторизованного пользователя.

В повышенных режимах безопасности сессия будет полностью меняться раз в несколько минут (в зависимости от настройки).

Механизм хранения сессий в базе данных для исключения ошибок конфигурирования виртуального хостинга, ошибок настройки прав доступа в временным каталогам и ряда других проблем настройки операционной среды.

Контроль активности



Обеспечивает защиту от DDoS атак на веб-приложения, от автоматизированных роботов, которые извлекают контент, спамят и всячески подстраиваются под посетителей.

Шифрование данных

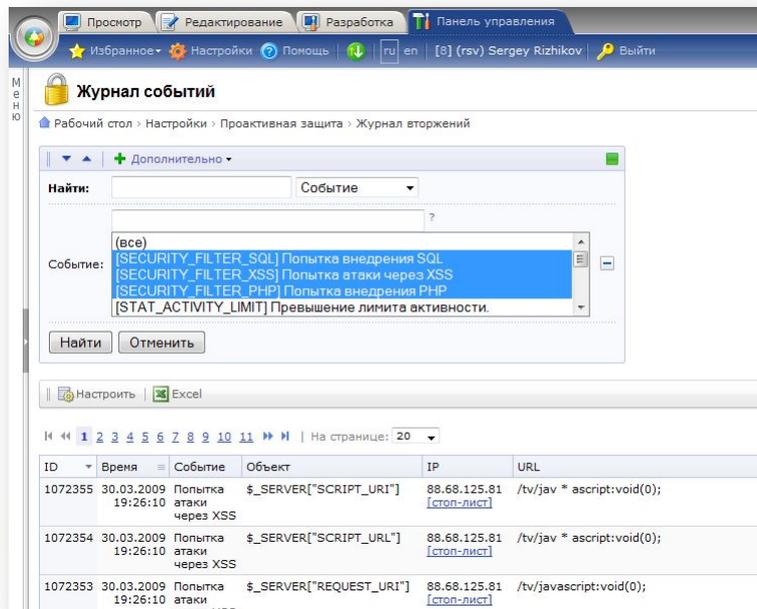
Полная поддержка работы по SSL

Один из ключевых вариантов обеспечения защищенности проекта – шифрование данных и сессионных значений при передаче между пользователем и сайтом.

Зачастую разделяются режимы работы пользователей и администратора.

Новые параметры позволят использовать несколько режимов работы с сайтом для пользователей при установленном SSL сертификате.

Журнал вторжений



Журнал событий

Рабочий стол > Настройки > Проактивная защита > Журнал вторжений

Найти: Событие

Событие:

- (все)
- [SECURITY_FILTER_SQL] Попытка внедрения SQL
- [SECURITY_FILTER_XSS] Попытка атаки через XSS
- [SECURITY_FILTER_PHP] Попытка внедрения PHP
- [STAT_ACTIVITY_LIMIT] Превышение лимита активности.

Найти Отменить

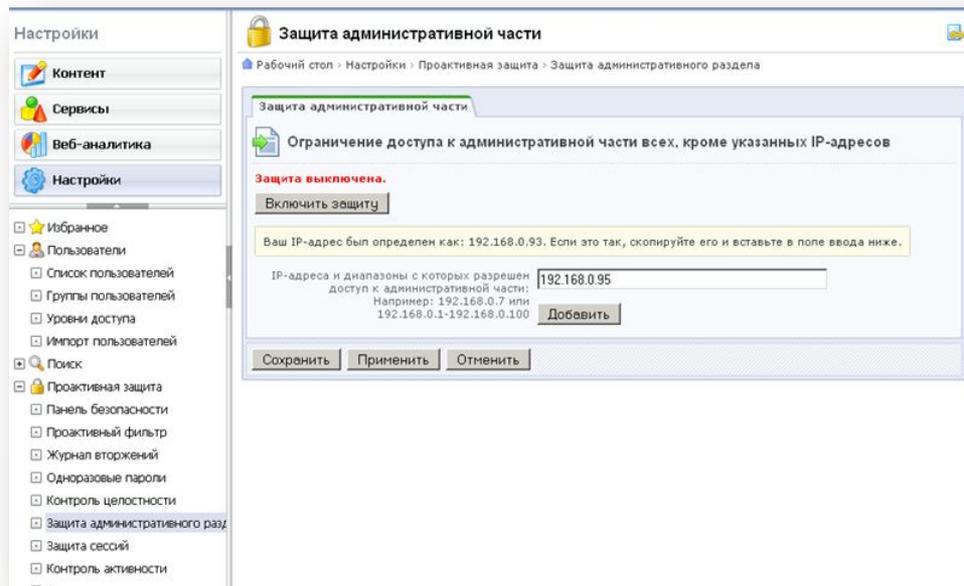
Настроить Excel

На странице: 20

ID	Время	Событие	Объект	IP	URL
1072355	30.03.2009 19:26:10	Попытка атаки через XSS	\$_SERVER["SCRIPT_URI"]	88.68.125.81 [стоп-лист]	/tv/jav * ascript:void(0);
1072354	30.03.2009 19:26:10	Попытка атаки через XSS	\$_SERVER["SCRIPT_URL"]	88.68.125.81 [стоп-лист]	/tv/jav * ascript:void(0);
1072353	30.03.2009 19:26:10	Попытка атаки через XSS	\$_SERVER["REQUEST_URI"]	88.68.125.81 [стоп-лист]	/tv/javascript:void(0);

В журнале вторжений ведется запись попыток внедрения SQL, атак через XSS и внедрения PHP.

Защита административных разделов по IP



Защита позволяет строго регламентировать сети, которые считаются безопасными и из которых сотрудникам разрешается администрировать сайт.

Стоп-листы

<input type="checkbox"/>		ID	Статус активности	Начало	Акт.	Сайт	IP адрес сети	Маска сети	Стат.
<input type="checkbox"/>		72		25.01.2006 19:57:33	Да	(все)	192.168.1.100	255.255.255.255	Нет
<input type="checkbox"/>		74		26.01.2006 16:58:56	Да	(все)	192.168.1.100	255.255.255.0	Нет
<input type="checkbox"/>		70		16.12.2005 16:52:12	Да	(все)	192.168.1.100	255.255.255.255	Нет
<input type="checkbox"/>		2		13.02.2004 18:58:15	Да	(все)	192.168.1.100	255.255.255.255	Нет

Стоп-лист ограничивает доступ посетителей к содержимому сайта. Все пользователи, которые попытаются зайти на сайт с IP адресами, включенными в стоп-лист, будут заблокированы.

Контроль целостности системы

Контроль целостности системы управления и страниц сайта:

- Механизм расчета контрольных сумм всего проекта
- Раздельное вычисление для статических страниц и кода с возможностью видеть, когда менял обычный пользователь и когда менял веб-разработчик
- Пароль проверки не хранится на сайте
- Файл контрольных сумм можно отдельно сохранить у себя для проверки

В любой момент вы можете проверить целостность ядра, системных областей, публичной части продукта.

Защита от фишинга

Защита редиректов с сайта от фишинга

Фи́шинг (англ. *phishing*, от *password* — пароль и *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, например, от имени социальных сетей (Facebook, ВКонтакте), банков (Ситибанк, Альфа-банк), прочих сервисов (Rambler, Mail.ru). В письме часто содержит прямая ссылка на сайт, внешне не отличимый от настоящего. Оказавшись на таком сайте, пользователь может сообщить мошенникам ценную информацию, позволяющую получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанной на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

При включенной защите все ссылки с сайта через редиректы защищаются дополнительным параметром индивидуальным для сайта и для этого перехода. Внешние переходы не будут работать.

Групповые политики безопасности

Выполняется проверка на длину пароля и на вхождение в пароль определенных групп символов (латинские буквы, цифры, знаки препинания).

Маска сети для привязки сохраненной авторизации:	<input checked="" type="checkbox"/> Не переопределять	<input type="text"/>
Срок хранения авторизации, запомненной на компьютере пользователя (минут):	<input checked="" type="checkbox"/> Не переопределять	<input type="text"/>
Срок действия контрольного слова для восстановления пароля (минут):	<input checked="" type="checkbox"/> Не переопределять	<input type="text"/>
Минимальная длина пароля:	<input checked="" type="checkbox"/> Не переопределять	<input type="text"/>
Пароль должен содержать латинские символы верхнего регистра (A-Z):	<input checked="" type="checkbox"/> Не переопределять <input type="checkbox"/>	
Пароль должен содержать латинские символы нижнего регистра (a-z):	<input checked="" type="checkbox"/> Не переопределять <input type="checkbox"/>	
Пароль должен содержать цифры (0-9):	<input checked="" type="checkbox"/> Не переопределять <input type="checkbox"/>	
Пароль должен содержать знаки пунктуации (.,<>/?;:"'[]{} \ ' ~ ! @ # \$ % ^ & * () _ + =):	<input checked="" type="checkbox"/> Не переопределять <input type="checkbox"/>	
Количество попыток ввода пароля до показа CAPTCHA:	<input checked="" type="checkbox"/> Не переопределять	<input type="text"/>

Регистрация и авторизация

- 1) Подтверждение регистрации по email
- 2) Поддержка авторизации OpenID и LiveID
- 3) Детальная настройка CAPTCHA
- 4) Вывод CAPTCHA после N неуспешных авторизаций

Настройка параметров отображения CAPTCHA

Профиль:

Прозрачность текста в процентах от 0 до 100:

Нижняя граница случайного цвета фона:

Верхняя граница случайного цвета фона:

Количество кругов:

Нижняя граница случайного цвета круга:

Верхняя граница случайного цвета круга:

Линии поверх текста:

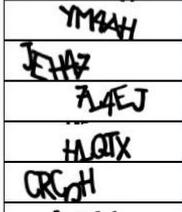
Количество линий:

Нижняя граница случайного цвета линии:

Верхняя граница случайного цвета линии:

Отступ текста слева:

Размер шрифта:



Журнал событий

В журнал заносятся события, связанные с авторизацией и регистрацией пользователей. Детально настраиваются фиксируемые события.

Настройка параметров журнала событий

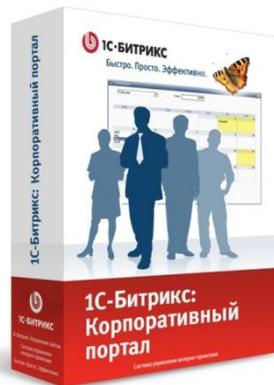
Сколько дней хранить события:

События для записи в журнал

- Записывать выход из системы
- Записывать успешный вход
- Записывать ошибки входа
- Записывать регистрацию нового пользователя
- Записывать ошибки регистрации
- Записывать запросы на смену пароля
- Записывать смену пароля
- Записывать удаление пользователя

Модуль «Проактивная защита» включен в состав программных продуктов:

- «1С-Битрикс: Управление сайтом» (все редакции, кроме «Старт»)
- «1С-Битрикс: Корпоративный портал»





RootConf – 2009

Профессиональная конференция
системных администраторов

Спасибо за внимание! Вопросы?

Сергей Рыжиков
rsv@1c-bitrix.ru

www.1c-bitrix.ru