Актуальные вопросы информационной безопасности веб-приложений

Сергей Рыжиков
генеральный директор
компании «1С-Битрикс»

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

Web-приложения и анализ рисков

- Анализ рисков. Где статистика?
- В 2006 году впервые количество обнаруженных Web-уязвимостей превысило «стандартные» проблемы

  MITRE, анализ списка CVE

- **Больше 7% Web-сайтов может быть «взломано» автоматически**
- **При экспертном анализе вероятность обнаружения критической уязвимости превышает 60%**

  Web Application Security Consortium

По данным компании Positive Technologies

Исследование уязвимости Web-приложений, 2008 г.

- Объем исследования:
  - В автоматическом режиме – около 10000 узлов
  - Детальный анализ – около 1000 узлов

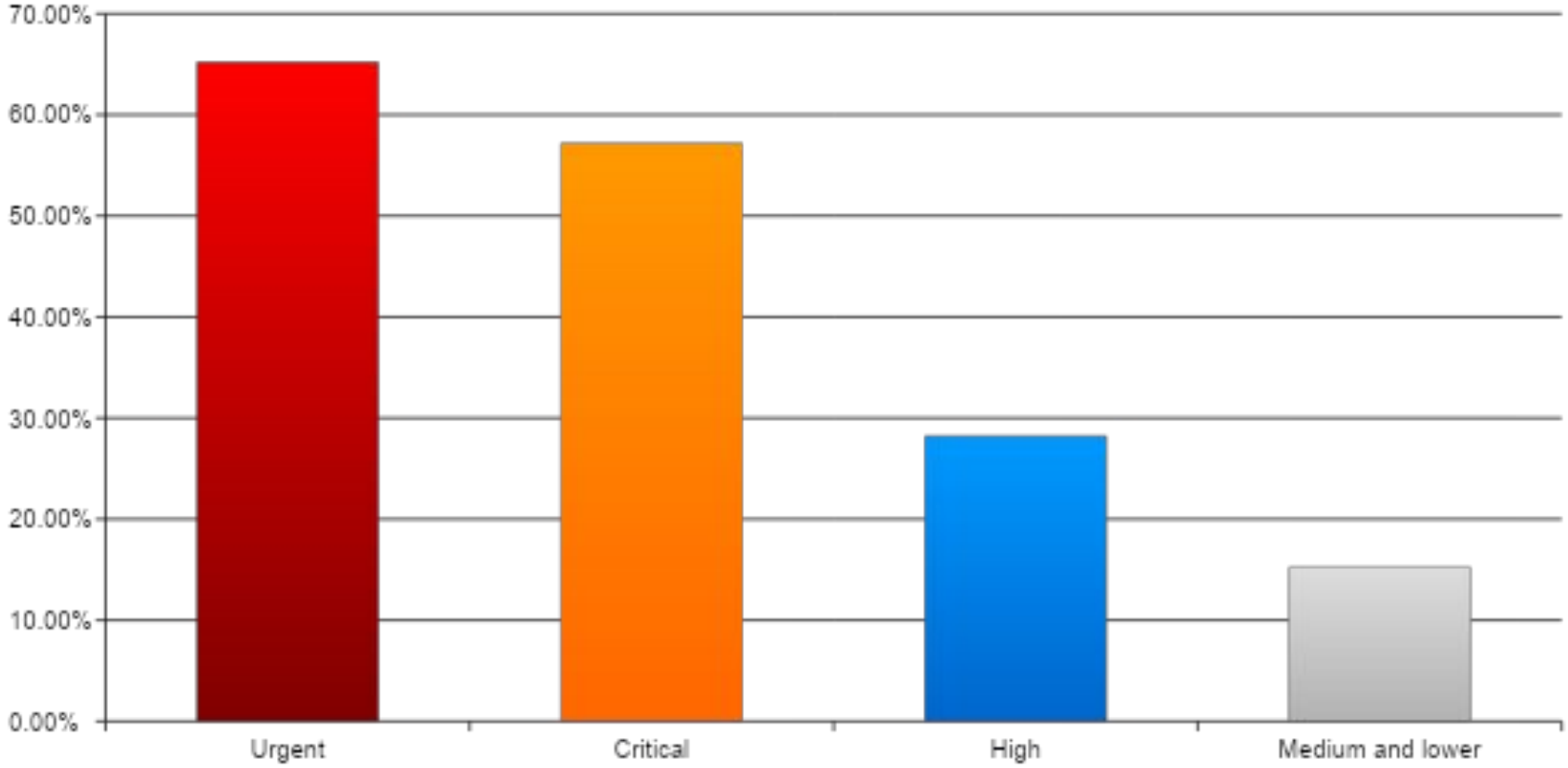
Результаты исследования:

- **Низкий уровень защищенности большинства Web-сайтов**
- **Автоматизация методов выявления и эксплуатации уязвимостей**

Web Application Security Consortium
предварительные данные

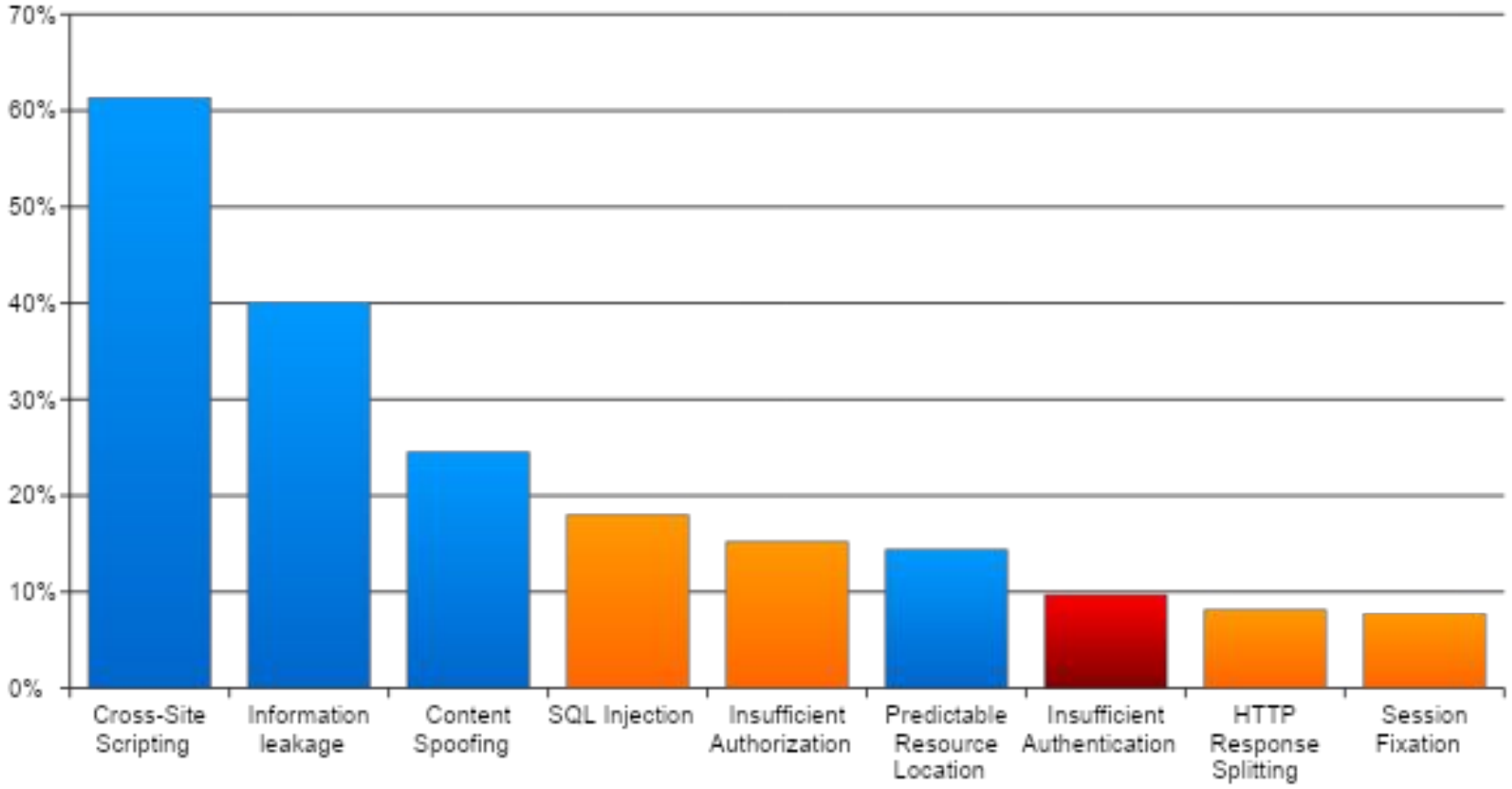
По данным компании Positive Technologies

Распределение веб-сайтов по уровню найденных уязвимостей (2008 г.)



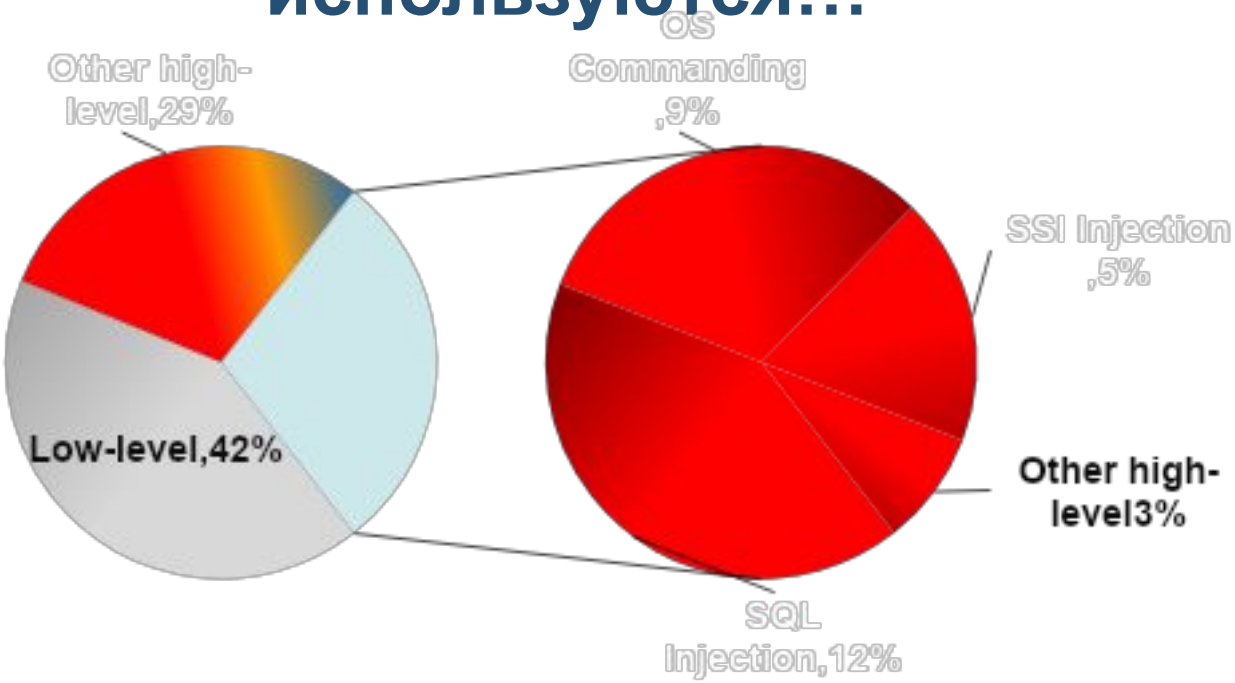
По данным компании Positive Technologies

Наиболее распространенные уязвимости



По данным компании Positive Technologies

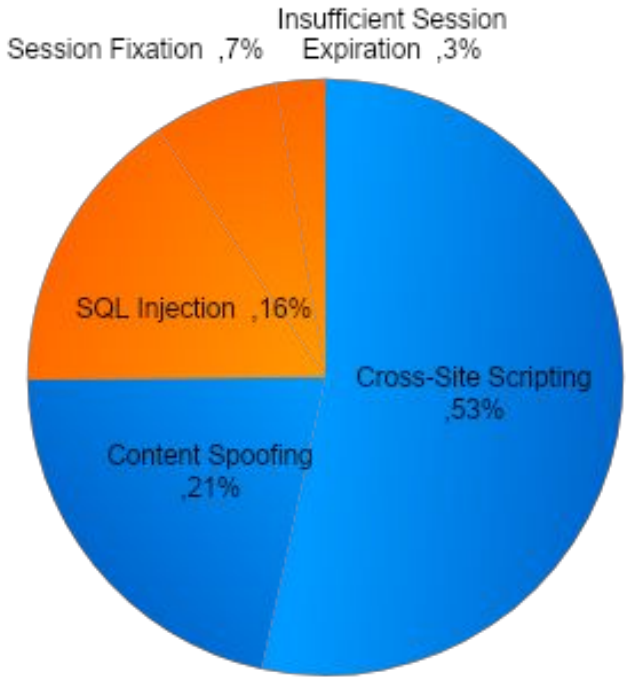
Для атаки на Web-сайт обычно используются…



При анализе скомпрометированного Web-сайта обнаруживается “букет” уязвимостей, треть из которых могла быть использована нарушителем для атаки

По данным компании Positive Technologies

Для атаки на пользователей Web-сайта обычно используются…



По данным компании Positive Technologies

А как оперативно устраняются эти проблемы?

Class of Attack	% resolved	severity
Information Leakage	50%	urgent
Insufficient Authorization	42%	urgent
SQL Injection	66%	urgent
HTTP Response Splitting	83%	urgent
Directory Traversal	31%	urgent
Insufficient Authentication	26%	critical
Cross-Site Scripting	55%	critical
Abuse of Functionality	41%	critical
Cross-Site Request Forgery	48%	critical
Session Fixation	11%	critical
Brute Force	8%	high
Content Spoofing	26%	high
HTTP Response Splitting	31%	high
Information Leakage	34%	high
Predictable Resource Location	31%	high

Whitehat Security

По данным компании Positive Technologies

Нашли «дыру»… Взломали… Что делать?

- Всех уволить!
- Найти эту дыру и закрыть ее!
- Проверить другие приложения
- Осознать проблему и заняться безопасностью

Осознали… Что дальше?

- Периодический аудит
- Развитие внутренних компетенций
- Внедрение дополнительных средств защиты
- Создание собственных средств защиты

Что дает проактивная защита?

- Страховка от возможных ошибок
- Безопасность сторонних разработок
- Своевременное обнаружение атак
- Соответствие PCI DSS

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.**

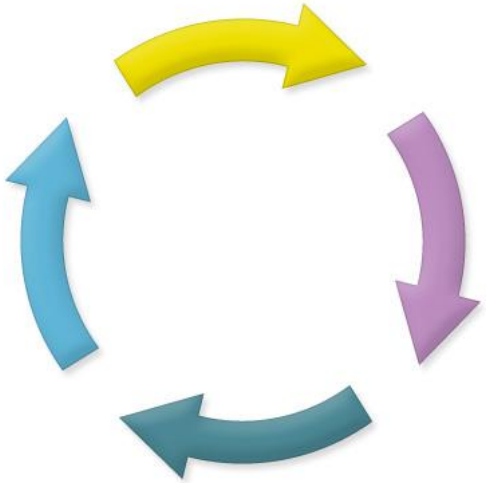
Цикл разработки

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**.

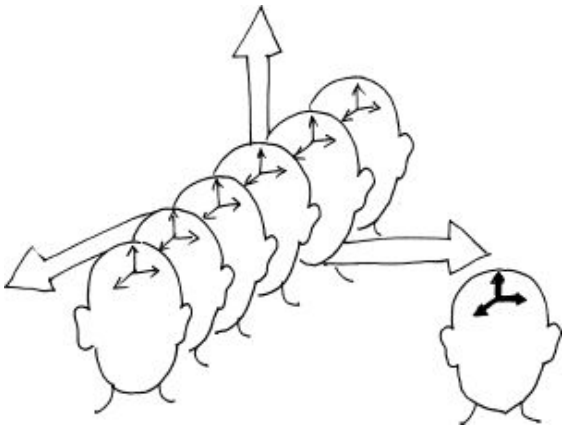
IV. Модуль поступает в **бета-тестирование клиентам и партнерам**.



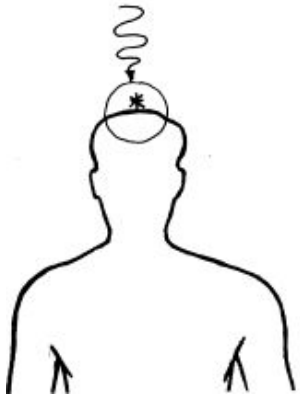
Разработчики работают в компании по 5-8 лет, но все равно допускают ошибки в безопасности. Почему?

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 - такими как Positive Technologies - услуга комплексная, сложная и зачастую не подходит для массового рынка.

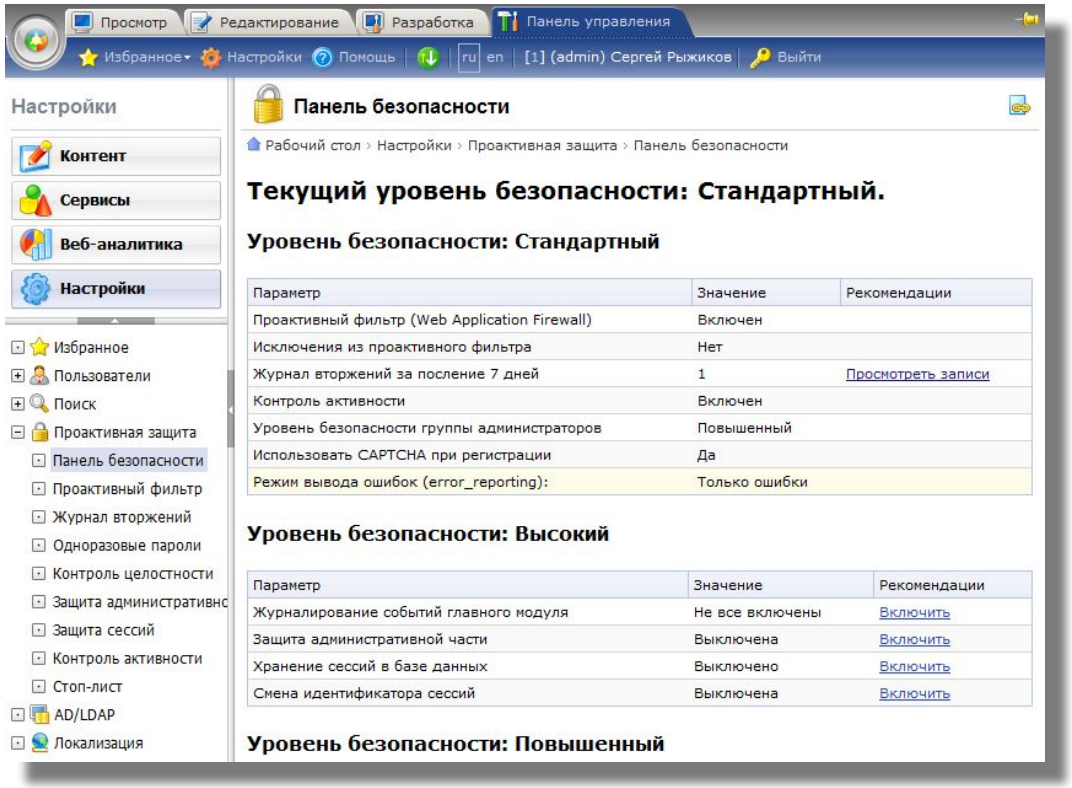
Новый подход к концепции веб-безопасности

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**
- **Защиту административных разделов по IP**
- **Стоп-листы**
- **Контроль целостности**
- **Рекомендации по настройке безопасности**
- **Защиту редиректов от фишинга**
- **Монитор обновлений**
- **Внешний контроль информационной среды**

Проактивная защита

Панель безопасности



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
- Информирует 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.

eToken
YOUR KEY TO eSECURITY

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

Aladdin
SECURITY SOLUTIONS

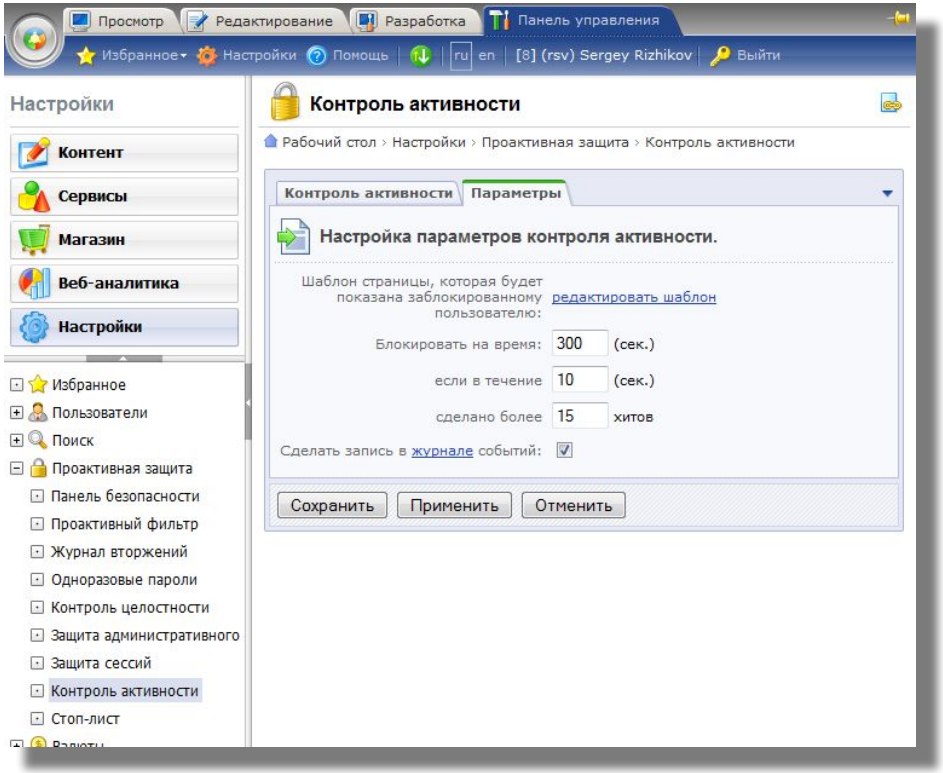
Технология защиты авторизованных сессии

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

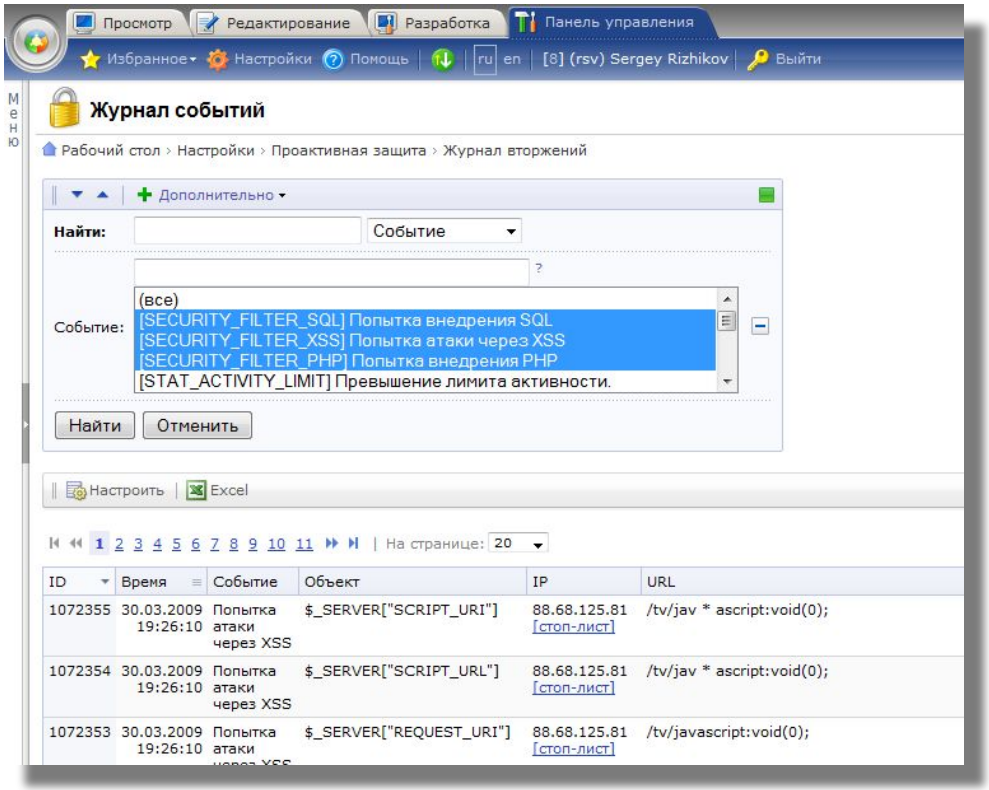
Полная поддержка работы по SSL

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**.

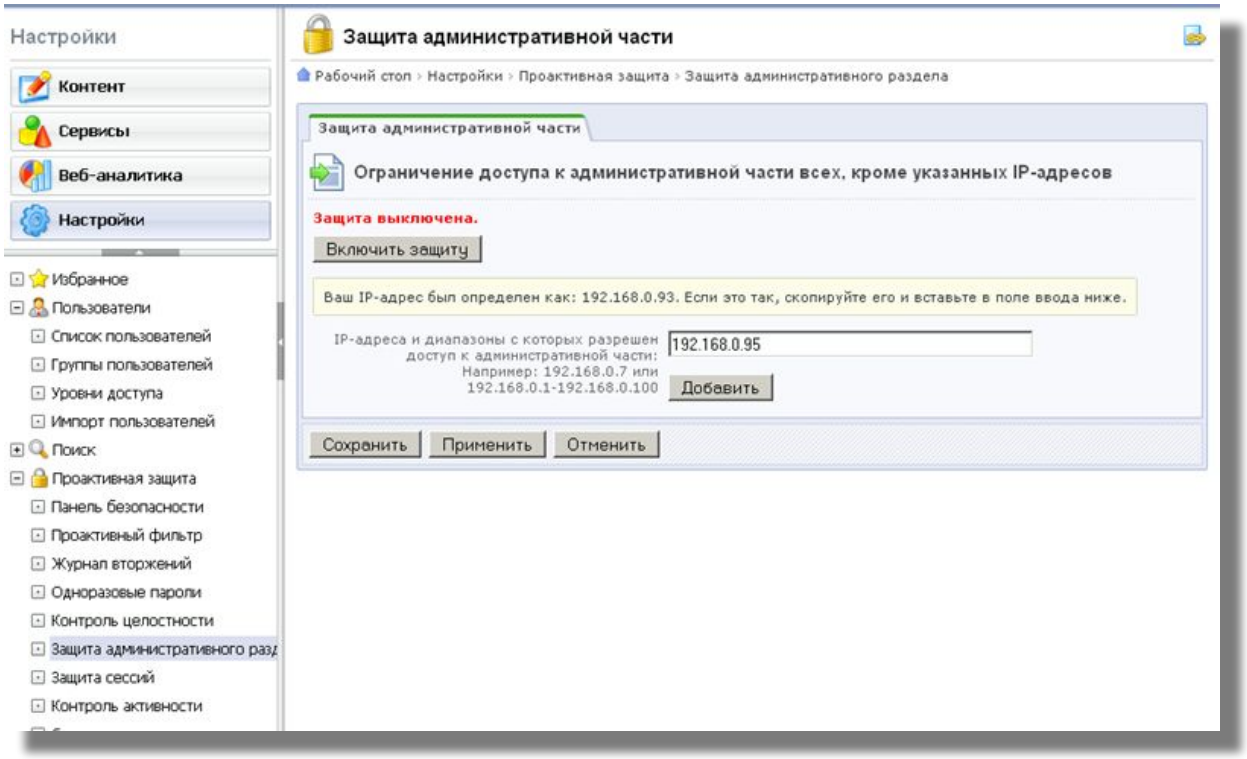
Новые параметры позволят использовать несколько режимов работы с сайтом для пользователей при установленном SSL сертификате.

Журнал вторжений



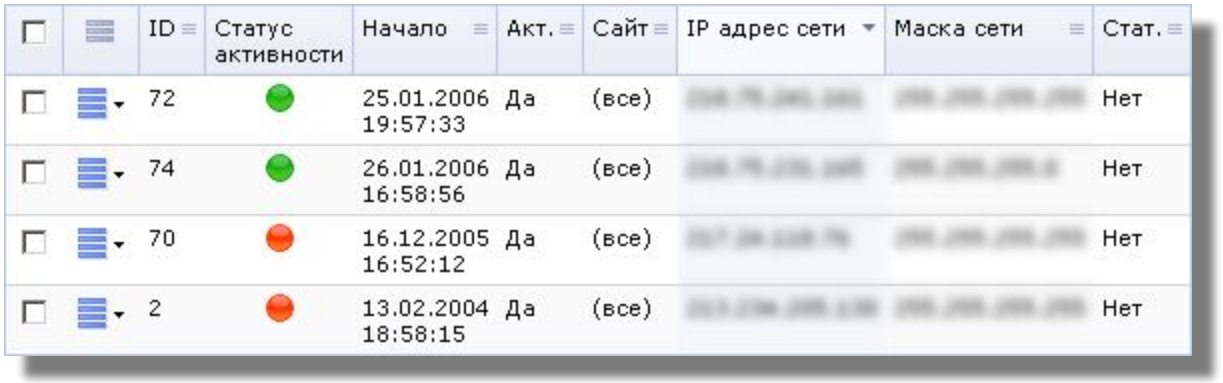
В журнале вторжений ведется запись попыток внедрения SQL, атак через XSS и внедрения PHP.

Защита административных разделов по IP



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

Стоп-листы



	ID	Статус активности	Начало	Акт.	Сайт	IP адрес сети	Маска сети	Стат.
	72		25.01.2006 19:57:33	Да	(все)	[redacted]	[redacted]	Нет
	74		26.01.2006 16:58:56	Да	(все)	[redacted]	[redacted]	Нет
	70		16.12.2005 16:52:12	Да	(все)	[redacted]	[redacted]	Нет
	2		13.02.2004 18:58:15	Да	(все)	[redacted]	[redacted]	Нет

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

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.

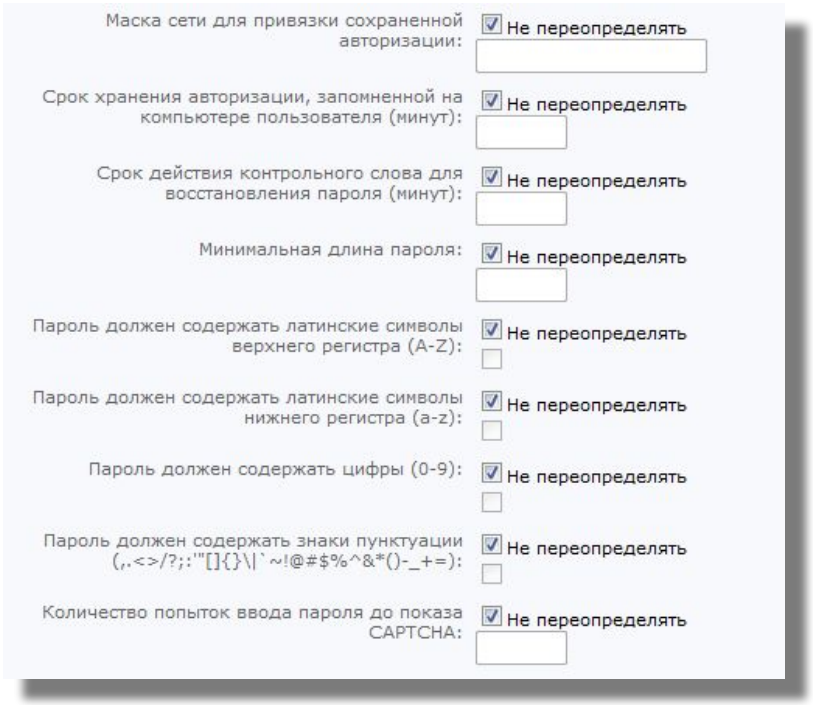
Защита от фишинга

Защита редиректов с сайта от фишинга

Фи́шинг (англ.Фи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернетФи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничестваФи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинамФи́шинг (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 рассылокФи́шинг (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 писемФи́шинг (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 брендовФи́шинг (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 сетейФи́шинг (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 (FacebookФи́шинг (англ. phishing, от password — пароль и fishing — рыбная

Групповые политики безопасности

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



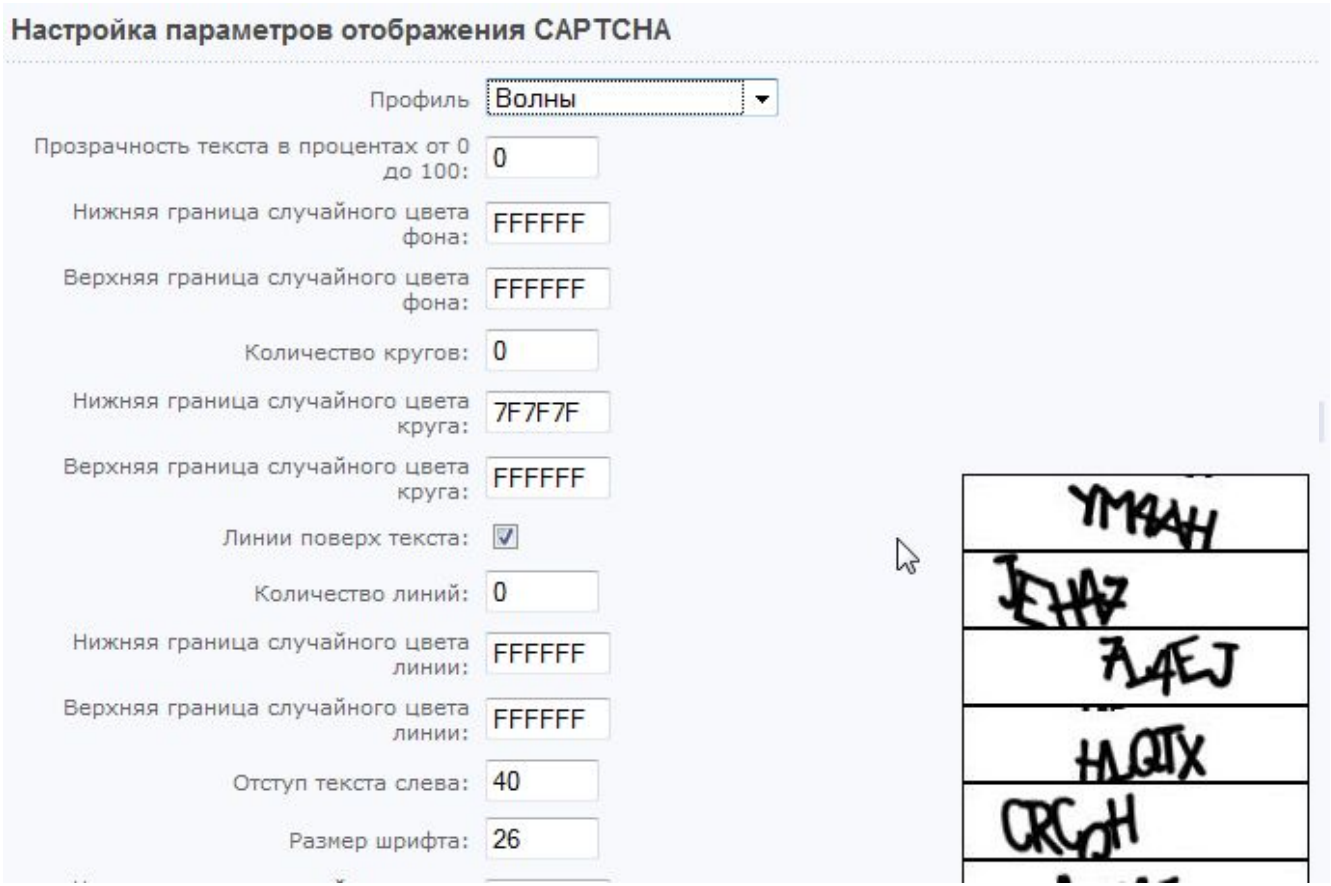
Регистрация и авторизация

1) Подтверждение регистрации по email

2) Поддержка авторизации OpenID и LiveID

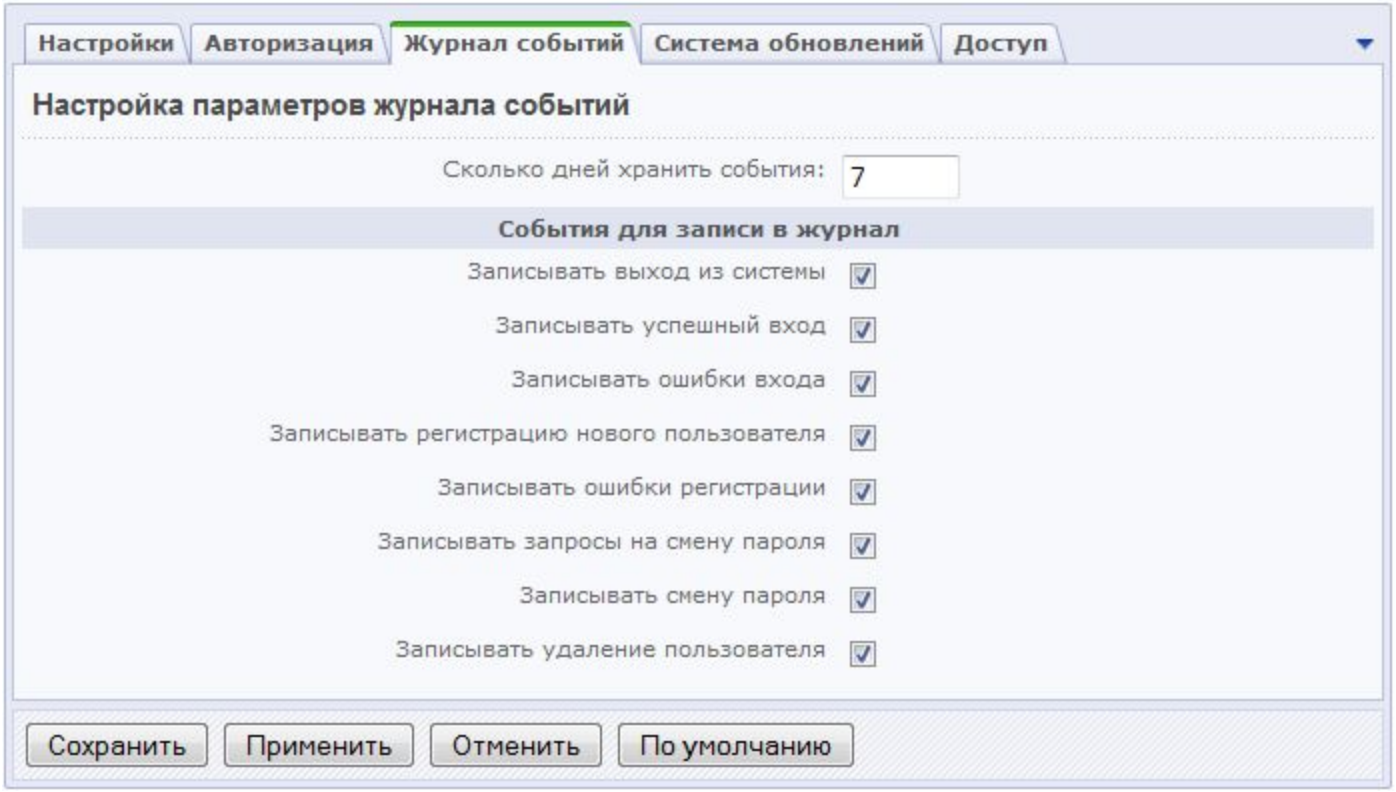
3) Детальная настройка CAPTCHA

4) Вывод CAPTCHA после N неуспешных авторизаций



Журнал событий

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



Модуль «Проактивная защита» включен в состав программных продуктов:

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

Спасибо за внимание! Вопросы?

Сергей Рыжиков
rsv@1c-bitrix.ru

www.1c-bitrix.ru