SOC
FORUM
2023

Как атакуют Битрикс: от А до Я

Технический директор
«Перспективный мониторинг»
Пушкин Александр

SOC
FORUM
2023

Пушкин Александр, CTO

АО «Перспективный мониторинг»

План выступления

SOC FORUM 2023

1. Битрикс и его архитектура
2. Встроенные механизмы безопасности
3. Известные уязвимости платформы
4. Как атакуют сайты на Битрикс
5. Советы по реагированию
6. Демонстрация атаки и защиты на учебно-тренировочной платформе

Используемые материалы

SOC FORUM 2023

KAZHACKSTAN TURAN – 2023

«Выйди и зайди нормально!»

Anton Lopanitsyn

Уязвимости и атаки на CMS Bitrix

Май 23, 2022 - Версия 1.0

CYBEROK

Собственные исследования и опыт реагирования на атаки Битрикс

Рекомендации
по применению компенсирующих мер и реагированию на атаки, связанные с CMS «1С-Битрикс: Управление сайтом»

www.cyberok.ru

SOC FORUM 2023

Битрикс и его архитектура

Архитектурное наследие

SOC FORUM 2023

1. Кодовая база начала формироваться в 00-х
2. Эмуляция Register Globals
3. Легальное выполнение PHP-кода в админке
4. Определение версии CMS
5. Разные эндпоинты аутентификации и регистрации
6. Мультидоменность

SOC FORUM 2023

Встроенные механизмы безопасности

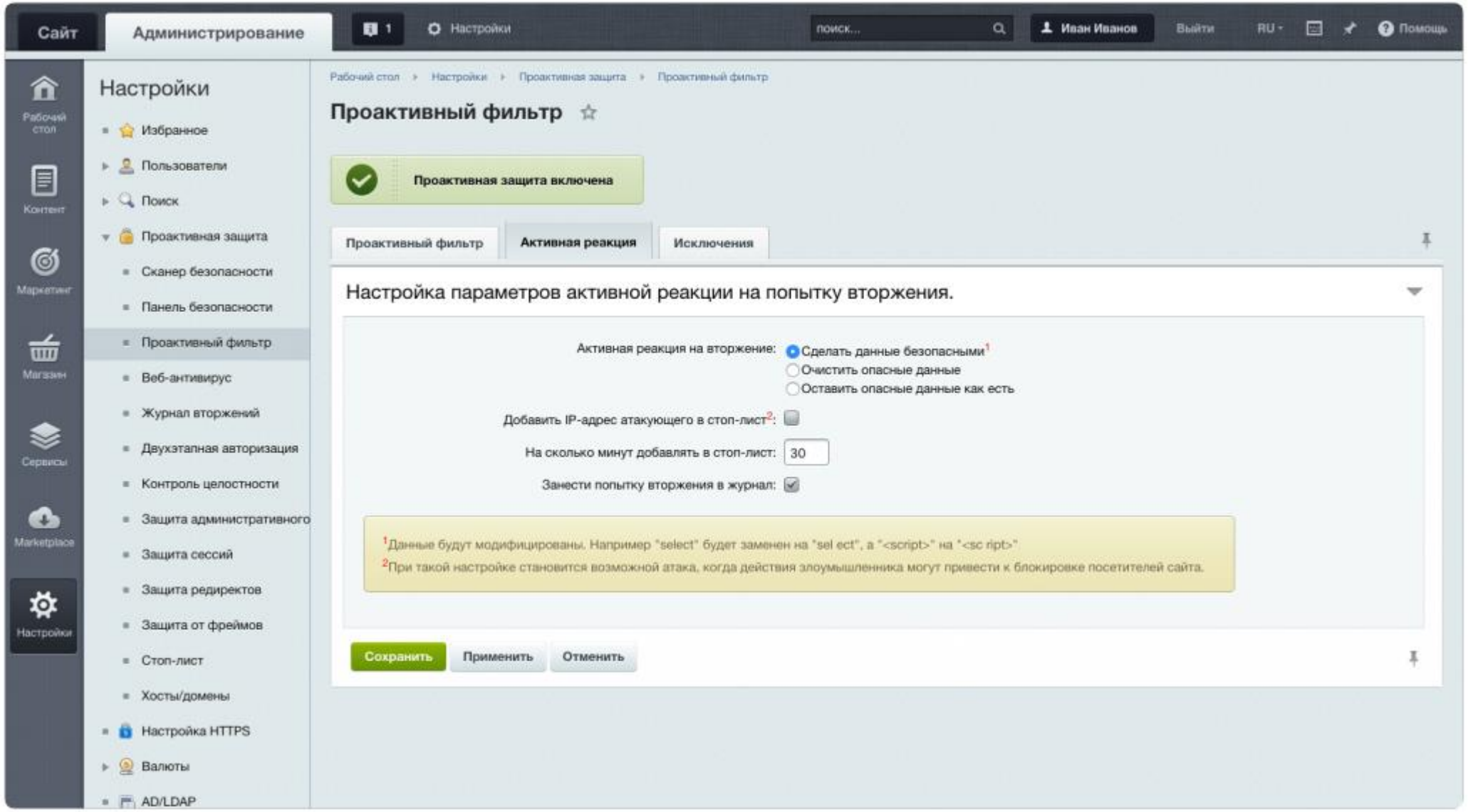
Механизмы безопасности и как они устроены

SOC FORUM 2023

1. Встроенный WAF
2. Сканер безопасности
3. Аудит кода
4. Многослойная валидация данных
5. Журнал вторжений
6. Контроль целостности

Встроенный WAF

SOC FORUM 2023



SOC FORUM 2023

Известные уязвимости платформы

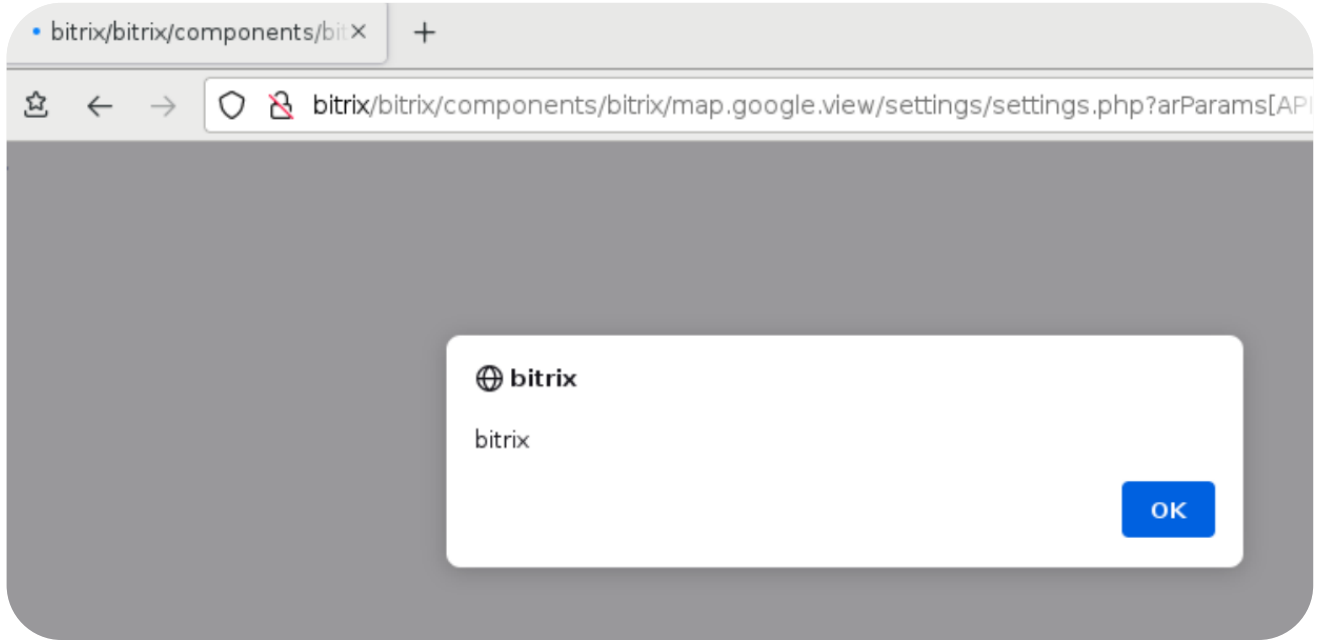
Менее опасные

SOC FORUM 2023

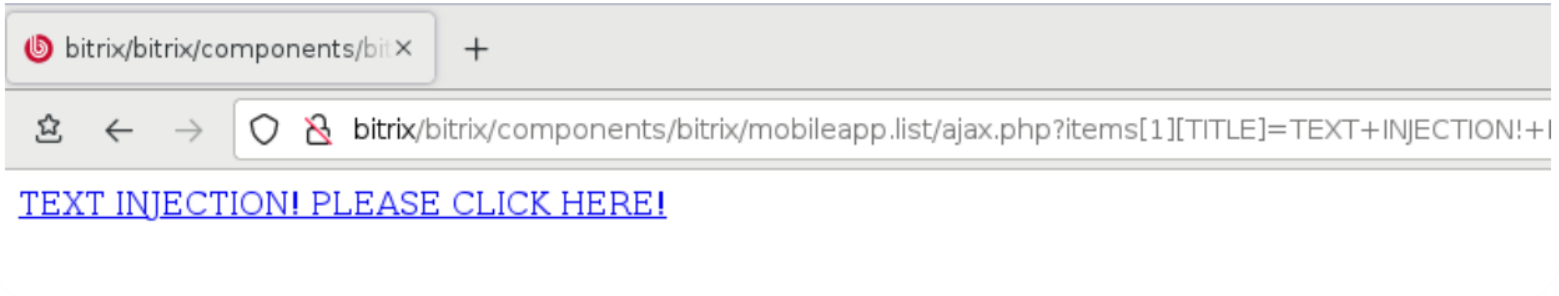
1. **Reflected XSS** (map.google.view, photogallery_user)
2. **Account Enumeration**
3. **Open Redirect** (rk.php, redirect.php, track_mail_click.php)
4. **Content Spoofing** (mobileapp.list, Imagepg.php, swfpg.php, rest.marketplace.detail)
5. **SSRF** (main.urlpreview, html_editor_action.php)
6. **Local File Disclosure / Include** (virtual_file_system.php)

Менее опасные

SOC FORUM 2023




```
http://site/bitrix/components/bitrix/mobileapp.list/ajax.php?items[
1][TITLE]=TEXT+INJECTION!+PLEASE+CLICK+HERE!&items[1][DETAIL_LINK]=
http://google.com
```



Критические уязвимости

SOC FORUM 2023

1. **Arbitrary Object Instantiation** (vote/uf.php - CVE-2022-27228)
2. **Arbitrary File Writer** (html_editor_action.php)
3. **Remote Code Execution** (landing)

Критические уязвимости

SOC FORUM 2023

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испыт
институт проблем технической защиты информаци

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Главная / Список уязвимостей / BDU:2023-05857

BDU:2023-05857: Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом, позволяющая нарушителю выполнить команды ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть

Вид

Описание уязвимости	Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить команды ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть
Вендор	ООО «1С-Битрикс»
Наименование ПО	1С-Битрикс: Управление сайтом (запись в едином реестре российских программ №35)
Версия ПО	до 23.850.0
Тип ПО	Прикладное ПО информационных систем
Операционные системы и аппаратные платформы	Данные уточняются

SOC FORUM 2023

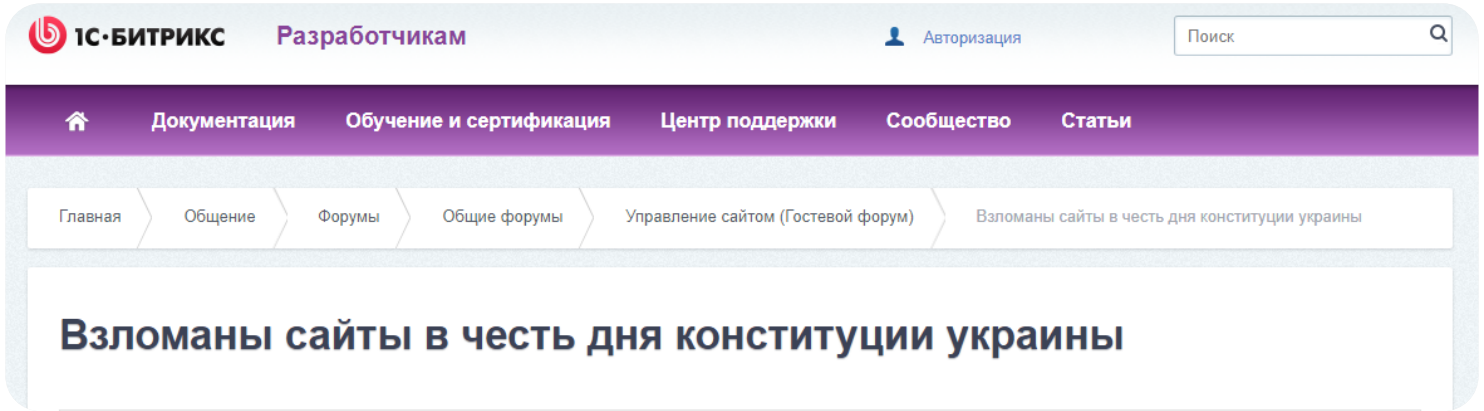
Как атакуют сайты на Битрикс

Массовые инциденты

SOC FORUM 2023

1. **26.05.2023** - массовый дефейс веб-серверов национального сегмента РФ
2. **весна 2023** - множественные утечки ПДн с сайтов на Битрикс

- интернет-магазина Gloria Jeans,
- книжного интернет магазина book24.ru,
- магазина матрасов "Аскона" (askona.ru),
- книжного интернет-магазина "Буквоед",
- интернет-магазина "Леруа Мерлен",
- сайта кулинарных рецептов edimdoma.ru,
- интернет-магазина одежды "ТВОЕ",
- интернет-аптека "Вита".



Кастомные вектора

SOC FORUM 2023

1. RCE via SQL Injection
2. RCE via PHP Object Injection (signer_default_key)
3. RCE via PHP Object Injection (site_checker.php)
4. Использование **restore.php**
5. Уязвимости в **самописных** модулях

Постэксплуатация

SOC FORUM 2023

1. Замена **index.php** в корневой директории WEB-приложения
2. Встраивание **вредоносного кода** в существующие компоненты
3. Создание новых файлов с **вредоносным кодом**
4. **Удаление данных** из таблиц базы данных (b_iblock, b_iblock_element, b_iblock_element_property)

SOC FORUM 2023

Советы по реагированию

Идентификация

SOC FORUM 2023

1. Проверка средствами «1С-Битрикс:Поиск троянов»
2. Проверка по журналам доступа к Web-серверу
3. Поиск новых и модифицированных файлов с вредоносным содержимым
4. Поиск следов закрепления

Хотфиксы

SOC FORUM 2023

1. **Модификация кода** CMS Битрикс
2. **Ограничение доступа** к уязвимым файлам средствами WAF/NGFW
3. **Отключение** уязвимых плагинов/модулей
4. Блокировка доступа к файлам на **уровне сервера**

Очистка зараженного сервера

SOC FORUM 2023

1. Использование механизмов **контроля целостности** файлов
2. Проверка **резервной** копии
3. Остановка подозрительных процессов
4. Очистка **кэша** Web-приложения

Повышение уровня защищенности

SOC FORUM 2023

1. Обновление PHP до 8 ветки
2. Обновление Битрикс
3. Настройка встроенного WAF и модуля «Контроль активности»
4. Проверка встроенным Сканером безопасности
5. Регулярный мониторинг событий WAF и логов веб-сервера

SOC FORUM 2023

Демонстрация атаки на учебно-тренировочной платформе

Тренировка

AMPIRE

ОСНОВНАЯ ИНФОРМАЦИЯ | ИНЦИДЕНТЫ | УЧАСТНИКИ | СХЕМА ШАБЛОНА | ЛОГИ СОБЫТИЙ АТАКИ

SOC FORUM 2023

Основная информация о тренировке

Название	Битрикс - видео 3
Шаблон	Офис (Конфигуратор)
Сценарий	Защита сайта на Битрикс
Статус	Готова к запуску
Доступные действия	УДАЛИТЬ ТРЕНИРОВКУ НАЧАТЬ ТРЕНИРОВКУ

Длительность 90 мин.

ПРОГРЕСС АТАКИ 0%

Схема шаблона

Скачать методические материалы

Участники

Группа	Тестовая группа	
Команда мониторинга	в сети	0 / 1
Команда реагирования	в сети	0 / 0
Лидер реагирования	не в сети	

- Bitrix vote RCE — Редактировать ответственных
- Bitrix deface — Редактировать ответственных

Инциденты

Новые	0/0
В работе	0/0
Закрытые	0/0
Цепочек кибератаки	0/1

Доступные ресурсы

Удалённое рабочее место	10.10.210.60
ViPNet IDS NS	10.10.210.180

Спасибо за внимание!

@Nesergeevich

amonitoring.ru