Технический аудит проблемного сайта slowpoke.ru

Срок проведения: 18.05.2017 - 30.05.2017

Содержание

Содержание **2**

Проверка сервера **5**

Операционная система и веб-окружение 5

Отправка почты 8

Нагрузочное тестирование 9

Выводы о настройках и конфигурации сервера 12

Проверка встроенными средствами 1С-Битрикс **13**

Монитор производительности 13

Сканер безопасности 13

Сканер безопасности обнаружил массу проблем 16

Проверка сайта 17

Список файлов, которых следует удалить 18

Неиспользуемые модули 19

Кеширование 20

Исходный код проекта **20**

Публичная часть 20

Заголовок h1 не часть шаблона сайта, смешение модели и представления данных 20

Магические числа 21

Лишний программный код в init.php 22

Api 22

Декларация классов не по стандартам bitrix 23

Неиспользуемые файлы в шаблонах компонентов 23

Мусорные комментарии 23

Лишний вывод 24

Странные присвоения 24

Итерации по коллекциям вместо запроса с группировкой 25

Кеширование в API выключено 26

Прямые обращения к базе данных 26

Нет проверки данных, полученных от пользователя 26

Генерация паролей не учитывает настройки безопасности битрикс 26

Ошибка авторизации 27

Дублирование кода 27

Код не оформлен в компоненты и модули 28

Заключение 28

Каталог товаров 28

Обращение к запросу в шаблоне, уязвимость Content Spoofing 28

Обмен с 1с 29

SEO **30**
Ответ на несуществующий URL 30
Перенаправление на URL с/без WWW 30
Файл robots.txt 31
Файл sitemap.xml 31
Важные html-тэги на страницах и возможность управления ими на страницах доступных поисковым системам 31
Главная страница 31
Корень каталога 31
Список товаров 32
Карточка товара 32
Текстовая страница 33
Список новостей 33
Страница новости 34
Партнеры 34
Вопросы и ответы 35
Список услуг 35
Страница услуги 36
Прайс листы 36
Контакты 37
Проверка Page Speed Insights 37
Шаблон сайта 37
Главная страница 38
Корень каталога 38
Список товаров 38
Карточка товара 38
Список новостей 38
Страница новости 38
Партнеры 39
Вопросы и ответы 39
Список услуг 39
Страница услуги 39
Прайс листы 39
Контакты 39
Битые ссылки, размещенные на страницах сайта 40
Заключение **40**
Список задач **40**

Проверка сервера

Операционная система и веб-окружение

На сервере установлена операционная система CentOS 7 со стандартным пакетом «1С-Битрикс: Веб-окружение» версии 7.0.0. Версия ПО свежая, обновления не требуется.

Некорректные настройки Apache, приводят к быстрому расходу оперативной памяти. В следствии этого, нет памяти для ускорения дисковых операций (см. рисунки 1-4).

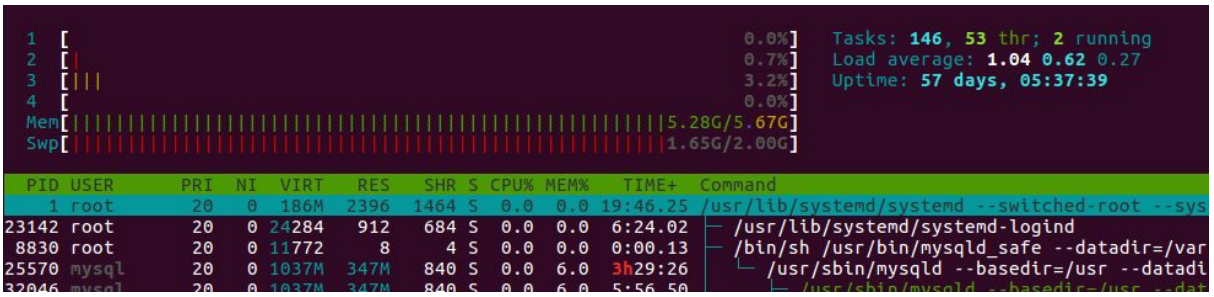

Рисунок 1 — htop - показатели оперативной памяти

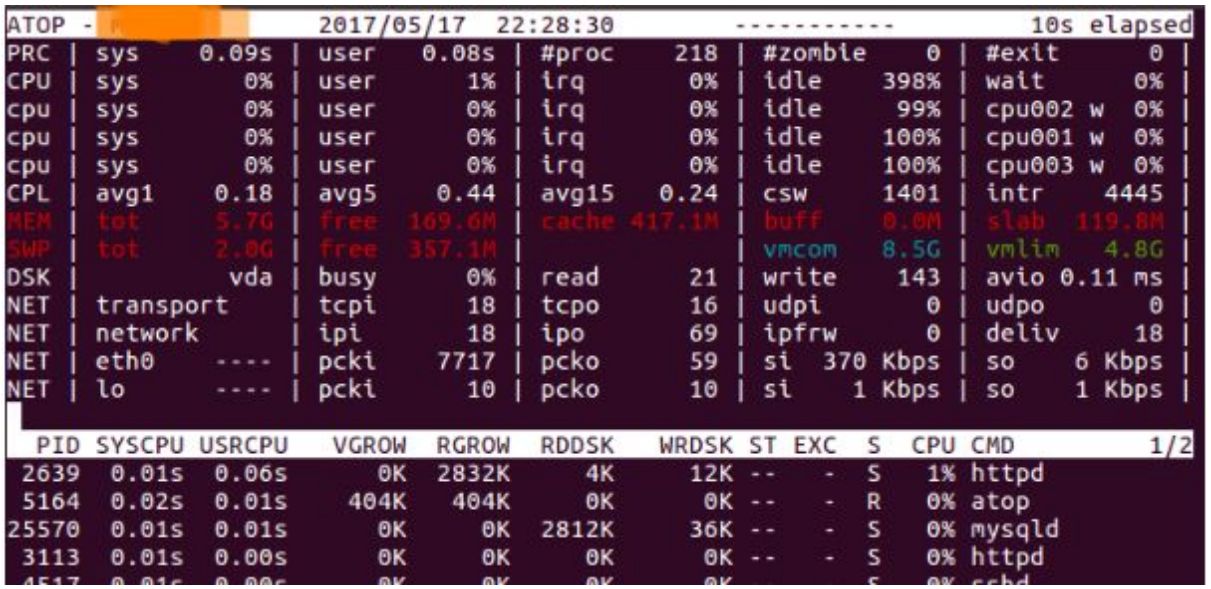

Рисунок 2 — atop - показатели оперативной памяти

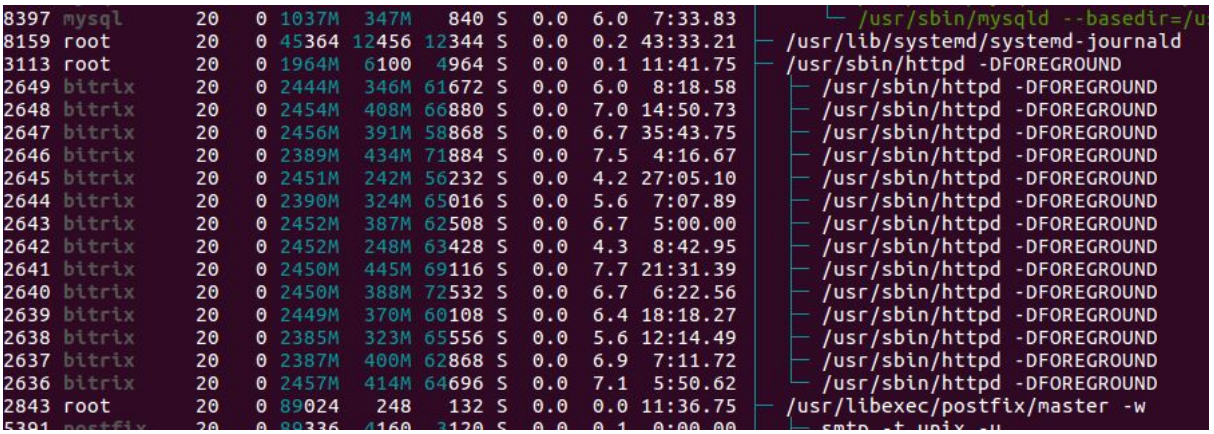

Рисунок 3 — Количество используемой оперативной памяти веб-сервером Apache

Периодически срабатывает OOM(out of memory)-киллер: автоматически завершаются процессы, потребляющие много памяти.

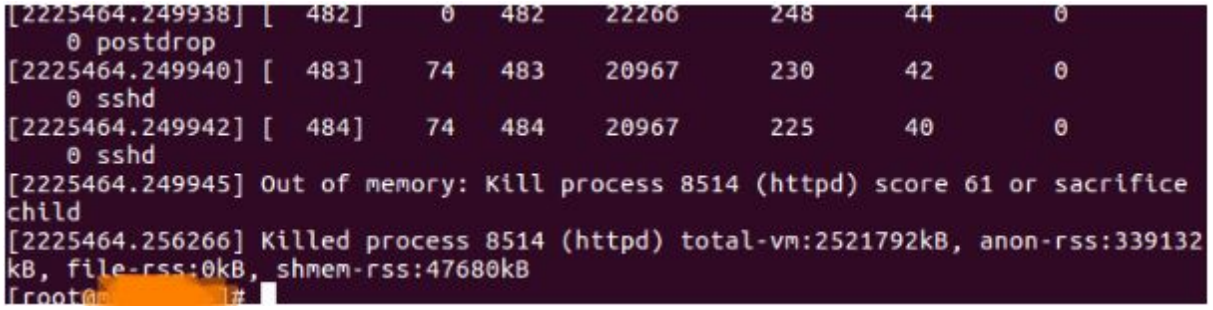

Рисунок 4 — Срабатывание OOM

На каждом из воркеров httpd десятки минут машинного времени. Из-за излишне оптимистичных настроек MaxRequestsPerChild.

Критичность: высокая

Необходимо определить оптимальное значение MaxRequwsrsPerChild и изменить настройки Apache.

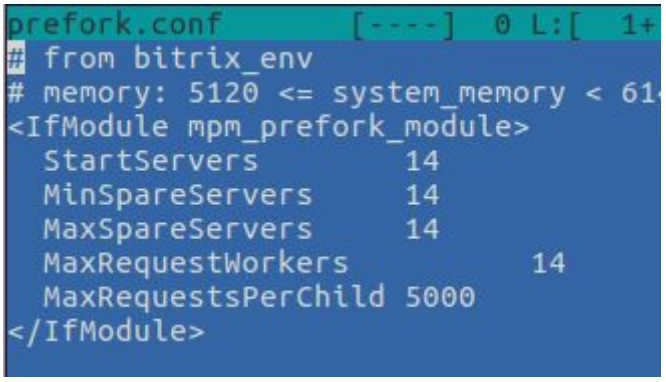

Рисунок 5 — Настройки модуля Prefork

Оперативную память потребляет включенный по умолчанию модуль PHP XDebug (default_enable = On) (см. рисунок 6).

Критичность: высокая.
Необходимо отключить модуль XDebug.

xdebug

xdebug support	enabled
Version	2.5.1
IDE Key	*no value*

Supported protocols	Revision
DBGp - Common DeBuGger Protocol	$Revision: 1.145 $

Directive	Local Value	Master Value
xdebug.auto_trace	Off	Off
xdebug.cli_color	0	0
xdebug.collect_assignments	Off	Off
xdebug.collect_includes	On	On
xdebug.collect_params	0	0
xdebug.collect_return	Off	Off
xdebug.collect_vars	Off	Off
xdebug.coverage_enable	On	On
xdebug.default_enable	On	On

Рисунок 6 — Конфигурация XDebug

В ходе работы базы данных, создается слишком много временных таблиц (см рисунок 7).

Сортировки	1 302 087
Сортировки (диск)	0%
Временные таблицы (диск)	41.17%
Кеш потоков	99.99%
Кеш открытых таблиц	65.5%

Рисунок 7 — Статистика БД

Критичность: средняя
Необходимо либо увеличить параметры tmp_table_size (текущее значение: 128 МБ), либо уменьшить max_heap_table_size (текущее значение: 128 МБ) и перенести папку с временными таблицами в оперативную память.

На сервере большое количество процессов smtp (см. рисунок 8).

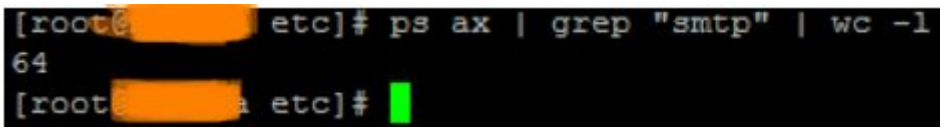

Рисунок 8 — Количество процессов smtp

Которые заняты отправкой почты в странные места (см. рисунок 9).

Рисунок 9 — Лог работы smtp

Это не влияет на скорость работы сайта, но может являться признаком спам-активности. Необходимо исследовать дополнительно.
Критичность: низкая

На сервере присутствует некорректно установленное или не настроенное программное обеспечение. Кто-то пытался поставить APC, но у него не получилось (см. рисунок 10).

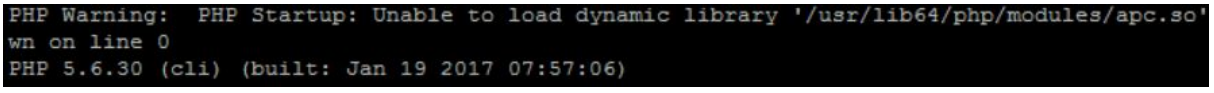

Рисунок 10 — Ошибка установки APC.

Критичность: средняя.
Необходимо удалить APC.

Отправка почты

На сервере не настроена отправка писем из PHP.

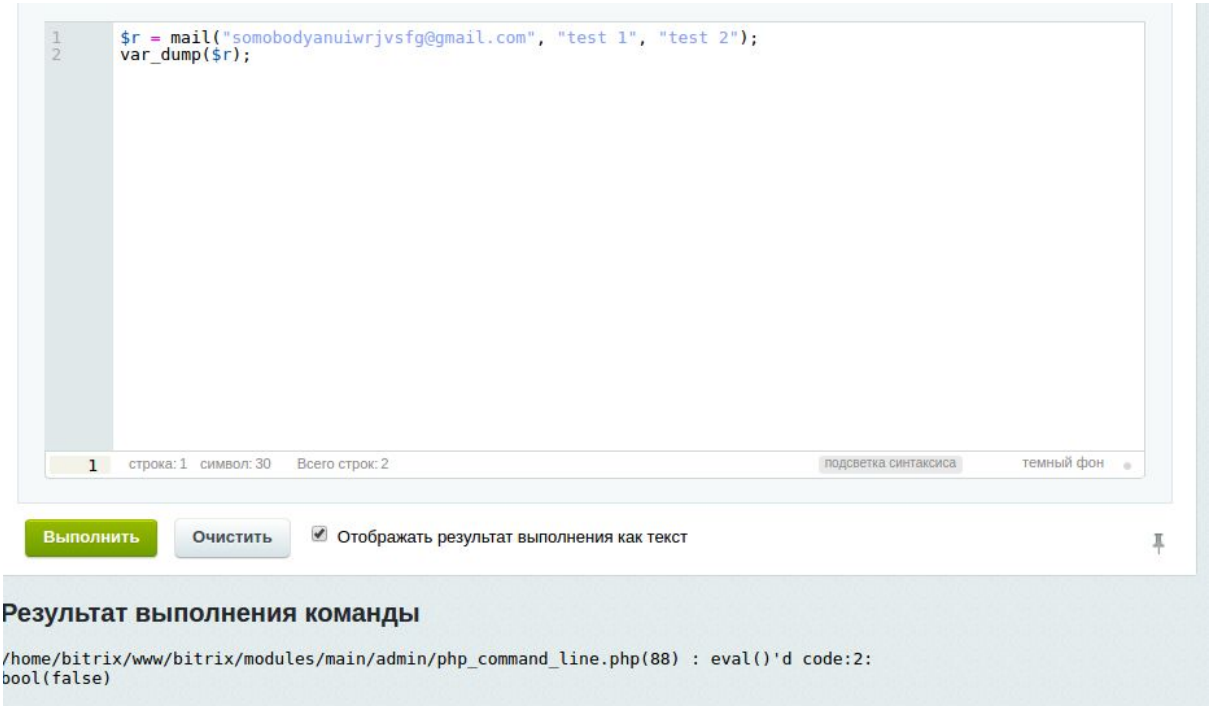

Рисунок 11 — Проверка работы почты

Критичность: высокая.
Необходимо настроить отправку писем.

Нагрузочное тестирование

RPS – количество одновременных запросов к серверу.

Нагрузочное тестирование позволяет определить, при каком количестве одновременных запросов к серверу, он перестает справляться с нагрузкой (после длительного ожидания, пользователи получают сообщения об ошибках вместо страниц сайта).

Нагрузочное тестирование с включенным автокешированием.
По графику видно, что время отдачи страниц выросло до 3,4 сек на 8 RPS (нормальное время отдачи страницы меньше 1 сек)

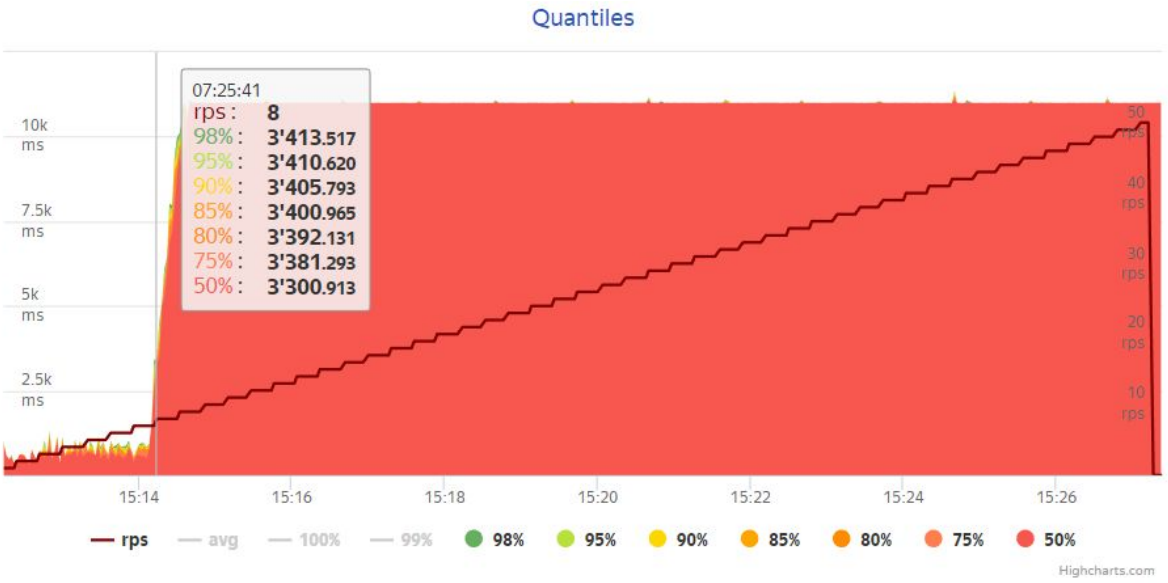

Рисунок 12 — Процентили времени ответа

Первую 500 ошибку получили на 9 RPS(с учетом таймаута отдачи страницы веб-сервером).

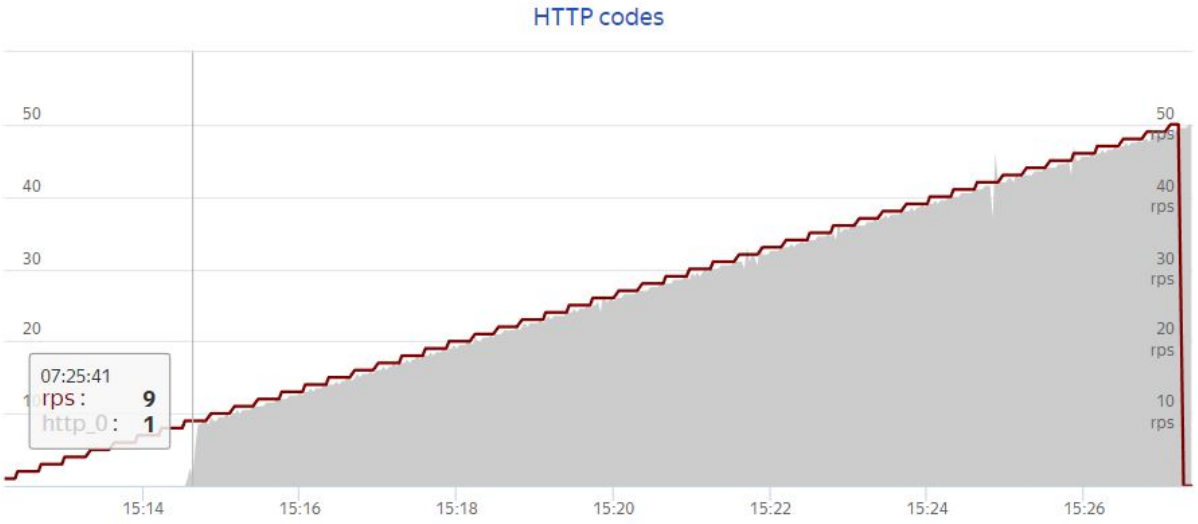

Рисунок 13 — Количественное отношение http-ответов

Во время нагрузочного тестирования подтвердились проблемы с недостаточной производительностью процессора и нерациональном расходом оперативной памяти.

Тестирование с отключенным механизмом автокеширования

Рисунок 14 — Процентили времени ответа

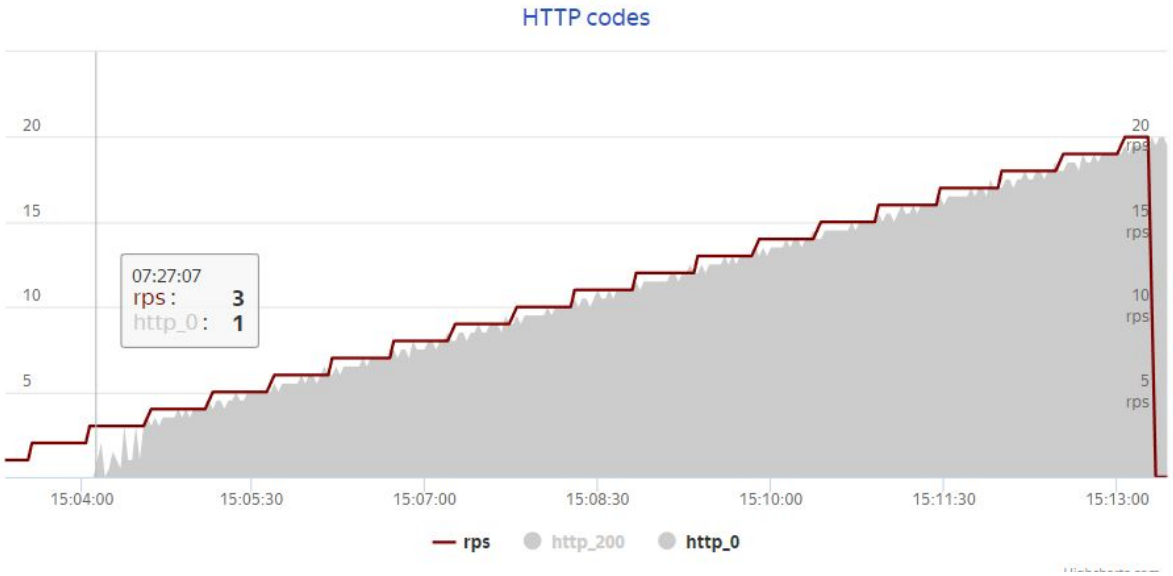

Рисунок 15 — Количественное отношение http-ответов

На графиках ниже видно, что даже при малой нагрузке (3 RPS), сервер расходует всю оперативную память и на 100% загружает процессор.

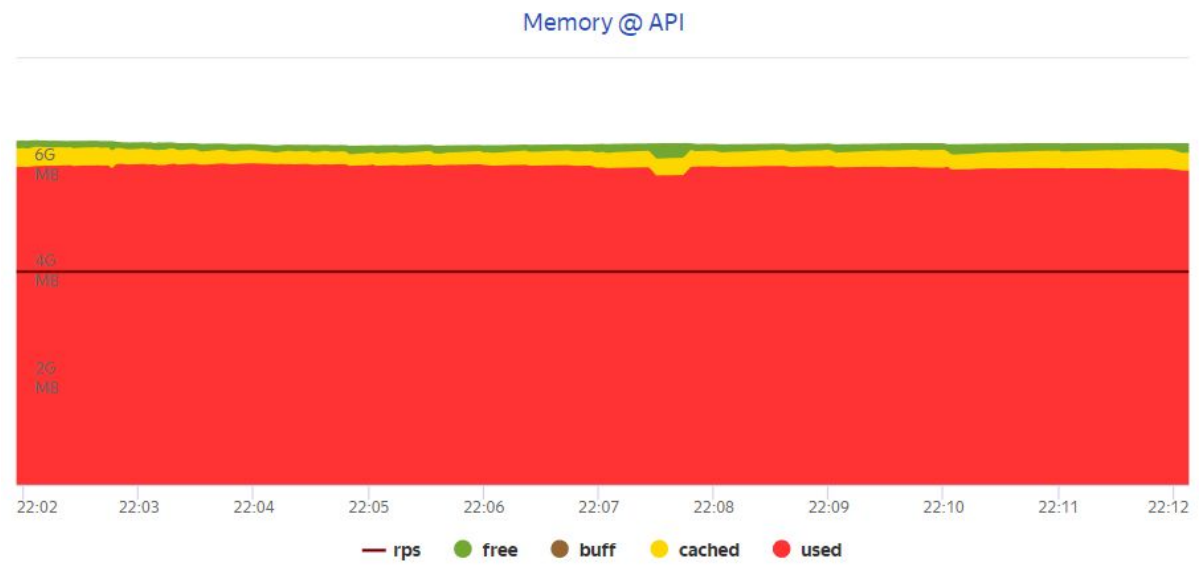

Рисунок 16 — Расход оперативной памяти во время нагрузочного тестирования

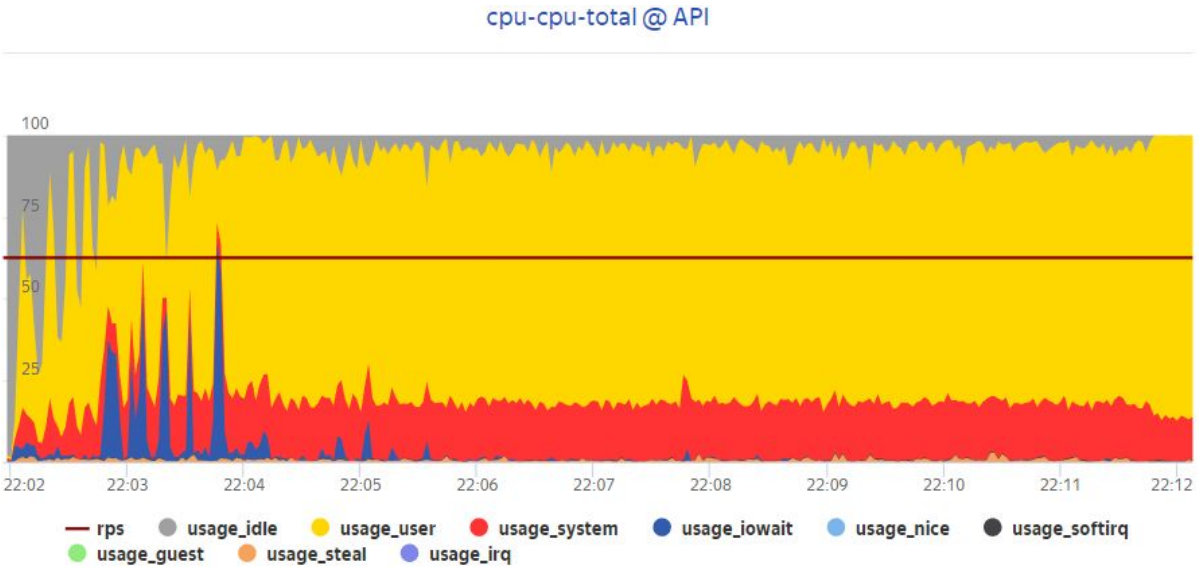

Рисунок 17 — Показатели использования процессора во время нагрузочного тестирования

Выводы о настройках и конфигурации сервера

Сайт работает в режиме дефицита процессора и оперативной памяти. Ресурсов сервера недостаточно для обслуживания запросов пользователей. Имеющиеся ресурсы используются нерационально.
Рекомендации:

1. Обновить php до версии 7.1
2. Заменить процессор на более производительный.
3. Добавить 6Гб оперативной памяти. Это позволит повысить производительность системы кеширования (Memcache, больше выделить места под кеш базы данных)

Проверка встроенными средствами 1С-Битрикс

Монитор производительности

Монитор производительности: низкий интегральный показатель производительности.

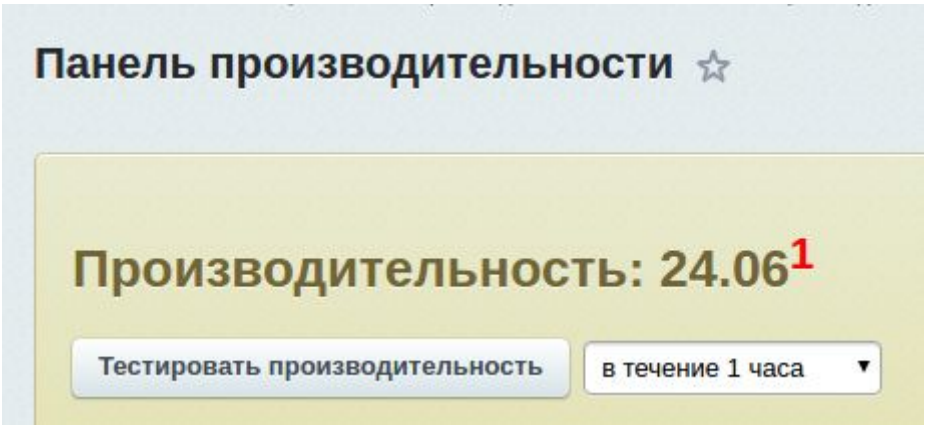

Рисунок 18 — Показатель производительности

Хорошим показателем считаются значения от 50 п.
Критичность: высокая
Необходимо увеличить производительность сервера и устранить проблемы в коде сайта, описанные ниже.

Сканер безопасности

Опасные файлы:
index-1.php
Регистрирует администратора с наперед известными логином и паролем (см. рисунок 19).

Рисунок 19 — Опасный скрипт

Критичность: авария
Необходимо удалить файл.

Лишние файлы
Имеются файлы, ненужные для работы сайта. Файлы restore.php и файлы бэкапов в корне, всевозможные логи. Каталоги temp и temp2 с копиями файлов сайта.

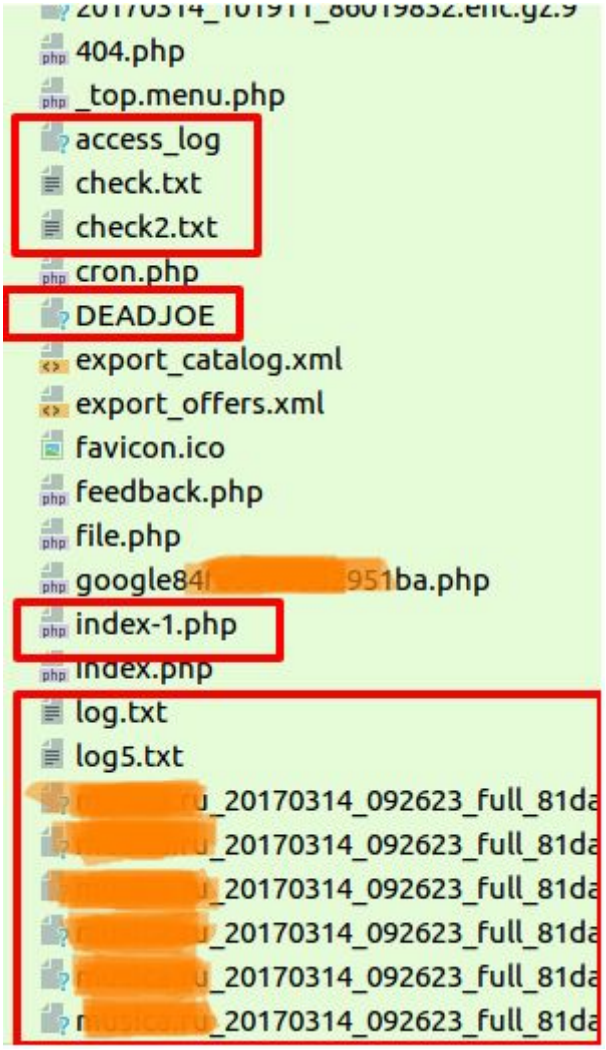

Рисунок 20 — Опасные файлы

Рисунок 21 — Содержимое папки /temp

Критичность: высокая.
Необходимо удалить файлы

Сканер безопасности обнаружил массу проблем

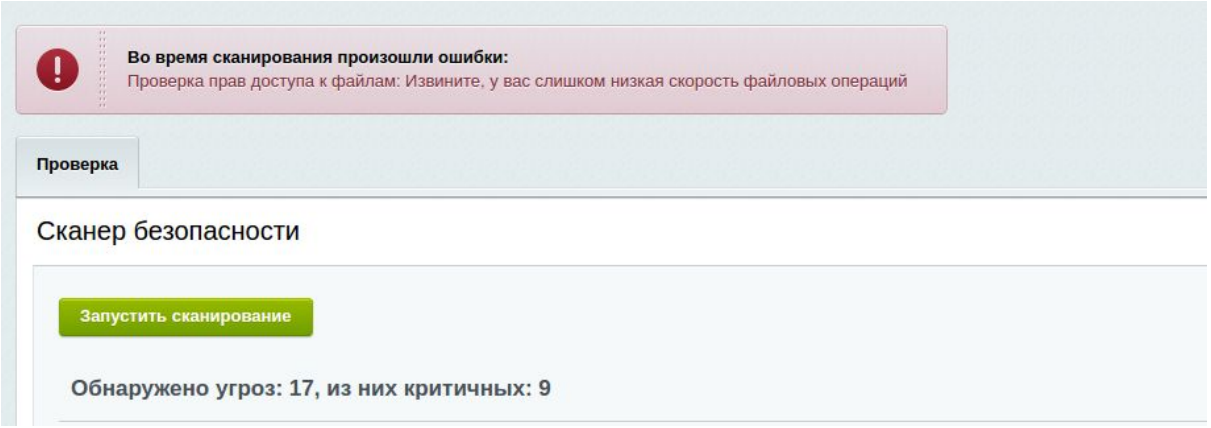

Рисунок 22 — Количество угроз

Все ошибка сканера безопасности должны быть устранены.
Критичность: высокая.

Проверка сайта

Проверка сайта диагностирует ошибки конфигурации:

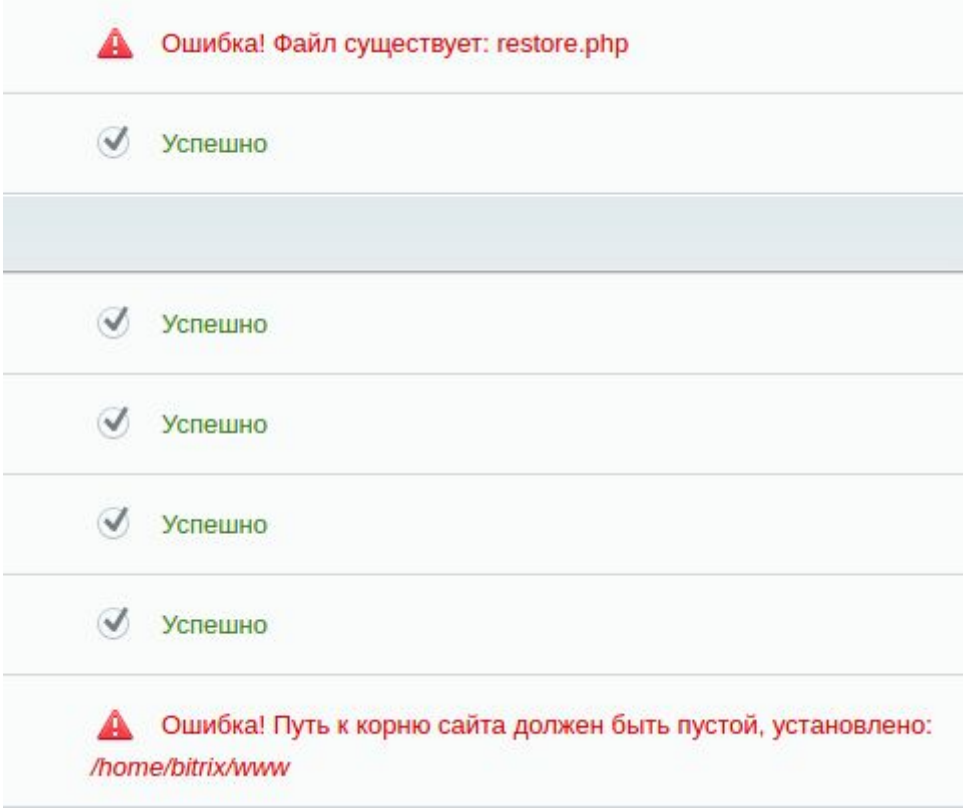

Рисунок 23 — Показания инструмента “Проверка сайта”

Критичность: средняя.
Необходимо устранить ошибки.

Список файлов, которых следует удалить

20170314_101911_86019832.enc.gz
20170314_101911_86019832.enc.gz.1
20170314_101911_86019832.enc.gz.10
20170314_101911_86019832.enc.gz.11
20170314_101911_86019832.enc.gz.12
20170314_101911_86019832.enc.gz.13
20170314_101911_86019832.enc.gz.14
20170314_101911_86019832.enc.gz.15
20170314_101911_86019832.enc.gz.16
20170314_101911_86019832.enc.gz.17
20170314_101911_86019832.enc.gz.18
20170314_101911_86019832.enc.gz.19
20170314_101911_86019832.enc.gz.2
20170314_101911_86019832.enc.gz.20
20170314_101911_86019832.enc.gz.21
20170314_101911_86019832.enc.gz.22
20170314_101911_86019832.enc.gz.23
20170314_101911_86019832.enc.gz.24
20170314_101911_86019832.enc.gz.2.tmp
20170314_101911_86019832.enc.gz.3
20170314_101911_86019832.enc.gz.4
20170314_101911_86019832.enc.gz.5
20170314_101911_86019832.enc.gz.6
20170314_101911_86019832.enc.gz.7
20170314_101911_86019832.enc.gz.8
20170314_101911_86019832.enc.gz.9
access_log
check2.txt
check.txt
DEADJOE
export_catalog_files
export_catalog.xml
export_offers_files
export_offers.xml
folder
google84fe0a156d2951ba.php
index-1.php
log5.txt
login
log.txt
slowpoke_2016_2.sql
slowpoke_2016.sql

slowpoke.ru_20170314_092623_full_81dac83b.tar.gz
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.1
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.10
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.11
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.12
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.13
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.14
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.15
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.16
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.17
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.18
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.19.tmp
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.2
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.3
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.4
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.5
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.6
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.7
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.8
slowpoke.ru_20170314_092623_full_81dac83b.tar.gz.9
ns.txt
restore.php
restore.tar.gz
site_cp
site_ft
site_ft.tar.gz
temp
temp2
test.php
theme_files
update.tar.gz
Критичность: высокая.
Необходимо удалить файлы

Неиспользуемые модули

Много включенных модулей bitrix:
http://slowpoke.ru/bitrix/admin/module_admin.php?lang=ru
Критичность: низкая.
Необходимо отключить и удалить неиспользуемые модули, т.к. они расходуют ресурсы процессора и оперативную память на каждом хите.

Кеширование

HTML-кеширование некорректно настроено

Формально оно включено, но не работает из-за масок включения и исключения.

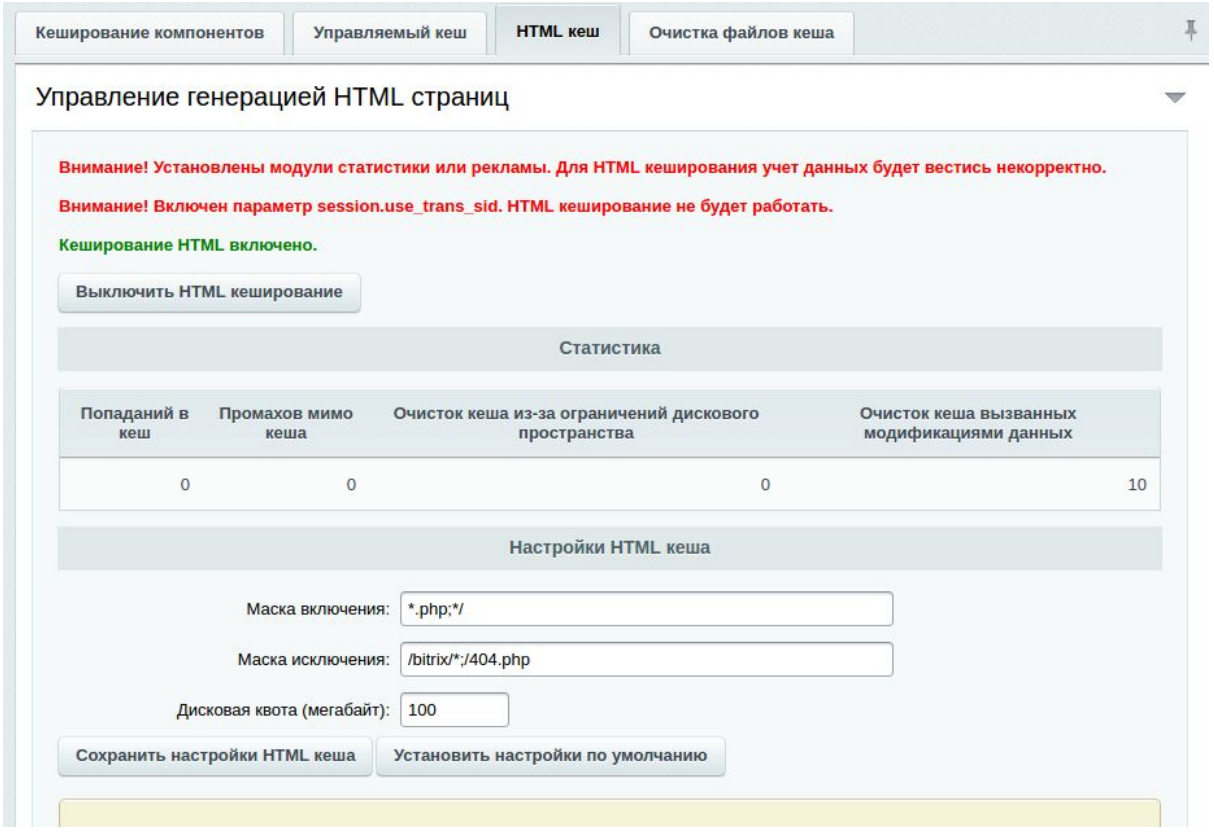

Рисунок 24 — HTML-кэшироние

Критичность: низкая.
Необходимо отключить html-кеширование.

Исходный код проекта

Публичная часть

Заголовок h1 не часть шаблона сайта, смешение модели и представления данных

Пример:
`/about/news/index.php`

Рисунок 25 — Ошибочное расположение заголовка страницы

Критичность: низкая.
Необходимо перенести вывод заголовка h1 в шаблоне сайта.
Правильно: компонент должен определять нужно выводить заголовок или нет, а шаблон - выводить.
Другие страницы с этой проблемой:
about/partners/index.php
about/news/index.php
about/index.php

Магические числа

В коде повсеместно используются числа там, где должны использоваться константы. Использование констант снижает вероятность ошибков при изменениях. Снижает стоимость доработок.
Пример:
`/ajax/add_compare.php`

Рисунок 26 — “Магическое число” 47

Критичность: средняя.
Необходимо вынести значения в константы, заменить использование значений на использование констант.

Другие файлы с проблемой:
`/ajax/compare_array.php`
`/ajax/show_compare.php`

`/ajax/show_compare_line.php`
`/api/auth/receivecode.php`
<очень много>

Лишний программный код в init.php

В файле init.php объявлены служебные функции, использующиеся при отладке сайта. Кроме то, выполняется обширное журналирование работы обмена с 1С, есть закомментированные “для истории” участки. Все это замедляет работу сайта, вносит бардак, затрудняет внесение изменений.
Нужно удалить функции “для разработки”, удалить лишние комментарии.
Критичность: низкая

```php
function PR($o,$toString = false,$ltf=false){...}

function LTF($var,$unlink = false){...}


function PrintAdmin($obj)
{
    global  $USER;
    if($USER->IsAdmin())
    {
      echo "<pre style=\"background-color:#FFF;color:#000;font-siz
      print_r($obj);
      echo "</pre>";
    }
}
```

```php
/*
if(count($arOptPrices["PRICES"])>0)
{
    foreach($arOptPrices["PRICES"] as $key=>$prices)
    {
        if($prices["PRICE"]>0 AND $price>$prices["PRICE"])
        {
            $price=$prices["PRICE"];
            $catalog_group_id=$key;
        }

    }

}
else
{
    $price=0;
}
*/
```

Рисунок 28 — Содержимое файла /bitrix/php_interface/init.php

Api

Декларация классов не по стандартам bitrix

Классы должны быть объявлены в модулях либо компонентах
Пример:
`/api/auth/API.php`
`/oauth/api.class.php`

Критичность: низкая.
Необходимо создать модуль, перенести объявления в него объявление классов, использовать встроенный механизм автозагрузки классов.

Неиспользуемые файлы в шаблонах компонентов

Шаблоны компонентов, используемых в api, содержат файлы ненужные для работы. Они выполняют программный код, результаты которого не используются или который вовсе не исполняется.
Пример:
`/bitrix/templates/slowpoke/components/bitrix/catalog.section/api/result_modifier.php`
`/bitrix/templates/slowpoke/components/bitrix/catalog.section/api/script.js`
`/bitrix/templates/slowpoke/components/bitrix/catalog.section/api/style.css`
`/bitrix/templates/slowpoke/components/bitrix/catalog.section/api/themes/*`
Необходимо убрать все лишние файлы, код в оставшихся очистить от ненужных действий.
Критичность: высокая.

Мусорные комментарии

Из файлы в файл повторяются закомментированный строки кода. Это вносит беспорядок, усложняет чтение файла.
Пример:

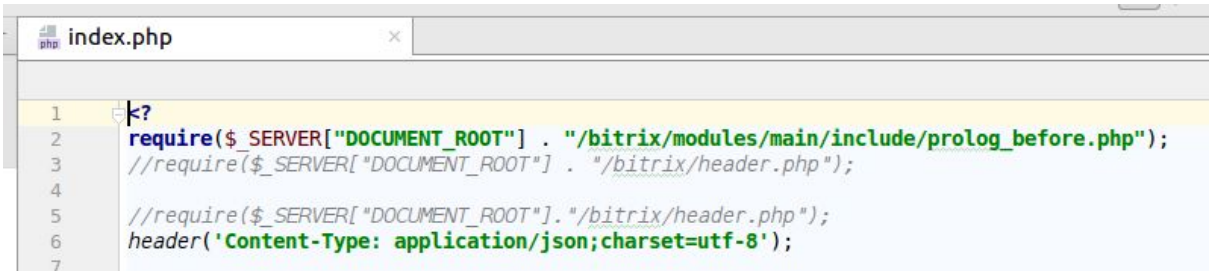

Рисунок 29 — Лишние комментарии

Критичность: низкая.

Необходимо удалить все ненужные комментарии.

Лишний вывод

Файлы, формирующие вывод api в формате json, содержат вывод лишних пробельных символов. Формат json допускает наличие пробельных символов и формально это не ошибка. Но это вносит беспорядок, увеличивает вероятность ошибки при доработках.

```
<?
require($_SERVER["DOCUMENT_ROOT"] . "/bitrix/modules/main/inclu
//require($_SERVER["DOCUMENT_ROOT"] . "/bitrix/header.php");

//require($_SERVER["DOCUMENT_ROOT"]."/bitrix/header.php");
header('Content-Type: application/json;charset=utf-8');

define("NO_KEEP_STATISTIC", true);
define("NOT_CHECK_PERMISSIONS", true);
?>

<?
$page_count=30;
if(!empty($_REQUEST["page"]))
$page_count=$_REQUEST["page"];
?>

<?
global $arrFilter;
?>

<?$APPLICATION->IncludeComponent(
);
?>


<?die;?>
```

Рисунок 30 — Лишний вывод

Такое в каждом файле в каталоге /api/ и в шаблонах компонентов, используемых для API.

Критичность: средняя.

Необходимо убрать весь лишний вывод пробельных символов, отдавать ответ только специальными конструкциями.

Странные присвоения

Усложняют понимание кода, внесение изменений.

Пример:

`/api/reg/user.php:27`

```php
$arResult["MESSAGE"]=iconv("windows-1251","UTF-8",$arResult["MESSAGE

if($arResult["TYPE"]=='ERROR')
{

}
else
{
    $arResult["ID"]=$USER->GetID();
}

    echo $arResult=json_encode($arResult, JSON_UNESCAPED_UNICODE);

?>
```

Рисунок 31 — Странное присвоение

Критичность: низкая.
Необходимо убрать лишние операции в API.

Итерации по коллекциям вместо запроса с группировкой

Вместо запроса количества элементов (запрос с группировкой) выполняется запрос получения элементов и подсчет их количества средствами PHP. Т.е. и СУБД делает лишнюю работу и PHP. Это приводит к лишней нагрузке. Кроме того, скорость получения результата линейно зависит от количества элементов, в то время как при запросе с группировкой постоянна.
Пример:
bitrix/templates/slowpoke/components/bitrix/catalog.section.list/api/result_modifier.php

```php
if(!empty($arParams["ELECTRON"]))
{
    $arSelect = Array("ID");
    $arFilter = Array("IBLOCK_ID"=>$arSection['IBLOCK_ID'],"!PROPERTY_ELECTR_BOOK"
    $res = CIBlockElement::GetList(Array(), $arFilter, false, false, $arSelect);
    while($ob = $res->GetNextElement())
    {
        $count_el++;
    }
```

Рисунок 32 — Неправильный подсчет количества элементов

Необходимо заменить итерирование на запрос с группировкой.
Критичность: высокая.

Кеширование в API выключено

Кеширование позволяет существенно снизить нагрузку на СУБД и сервер в целом. Большинство запросов к API можно кешировать на длительное время, информация всегда будет актуальной благодаря механизму управляемого кеширования. Необходимо включить кеширование в API.
Критичность: высокая.

Прямые обращения к базе данных

Для доступа к данным в БД используются “прямые запросы”. Средства битрикс, обеспечивающие безопасность и быстродействие запросов к БД, не используются.
Пример:
/api/user/sale.php

```
$flag_pay = $_REQUEST["flag_pay"];
$budget = $_REQUEST["budget"];

$data = $conn->query('SELECT * FROM oauth_access_tokens WHERE access_token = '.$conn->quote($token
$result=Array();
```

Рисунок 33 — Прямое обращение к БД

Необходимо использовать средства платформы для доступа к БД.
Критичность: высокая.

Нет проверки данных, полученных от пользователя

Возможны атаки вида “SQL injection”. Например, отправив специальный запрос, можно удалить все записи в таблице book_list_ios.

Критичность: авария
Необходимо проверять все входные параметры, не использовать прямые обращения к БД.
Файлы с этой проблемой:
/api/user/wish.php
/api/user/book.php

Генерация паролей не учитывает настройки безопасности битрикс

Битрикс позволяет предъявить дополнительные требования к сложности паролей пользователей. Например минимальную длину или обязательное наличие не алфавитных символов. Код в файле api/user/foget.php генерирует новый пароль пользователя как большое число. Если изменятся настройки безопасности, то сменить пароль через api станет невозможно.

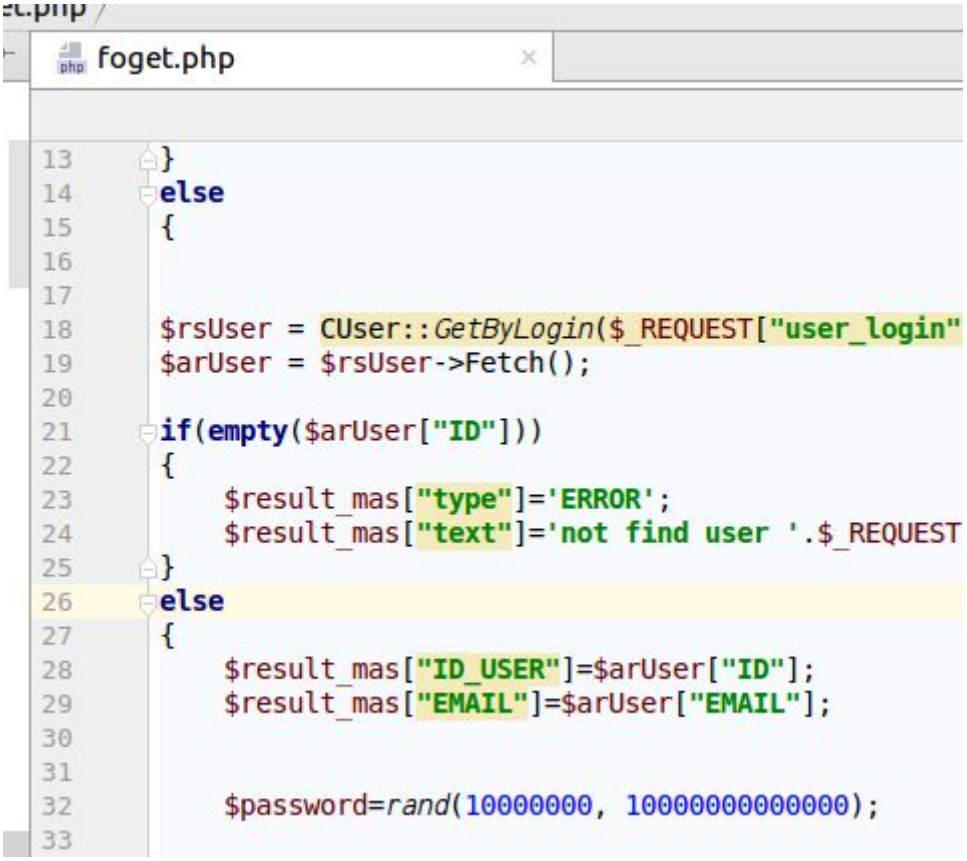

Рисунок 34 — Неправильная генерация пароля

Необходимо сгенерировать пароль средствами битрикс. Тогда он всегда будет соответствовать требованиям безопасности.
Критичность: средняя.

Ошибка авторизации

Любой пользователь может поменять пароль любому другому через API.
Достаточно знать его логин.
Критичность: авария
Необходимо давать сменить пароль только самому себе.

Дублирование кода

Современные подходы к программирования позволяют многократно использовать код. Это позволяет снизить количество ошибок. Такие программы легко изменять.
В коде API из файла в файл повторяются участки, отвечающие за аутентификацию и обработку ошибок и подобные операции.
Критичность: высокая
Необходимо переработать, обобщить. Сделать “несколько многоразовых”, а не “много одинаковых”.

Код не оформлен в компоненты и модули

По стандарту, весь код proerna должен быть разделен на модули, компоненты и их использование. Модули, предоставляют возможности компонентам, компоненты используются для отображения сайта. В разделе /oauth/ подобное разделение отсутствует. Это усложняет развитие проекта.
Нужно переработать раздел, выделить функциональность модуля, компонентов.
Критичность: средняя.

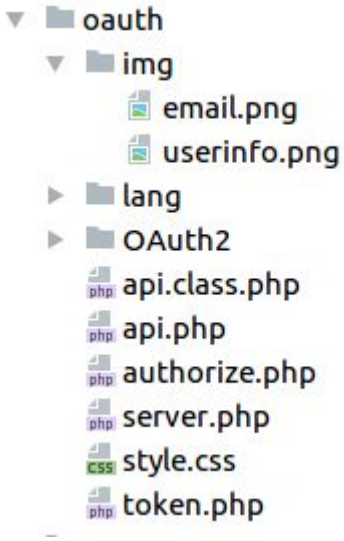

Рисунок 35 — организация файлов в разделе /oauth/

Заключение

API сделано отдельными страницами, что позволяет расширять функциональность методом слепого копирования имеющихся участков кода. Это приводит к повторению проблем.
Мы рекомендуем переработать API, сделав отдельным модулем для внешних систем. Это позволит обобщить механизмы авторизации, аутентификации и кеширования API, уменьшит количество потенциальных ошибок при развитии этого инструмента.

Каталог товаров

Обращение к запросу в шаблоне, уязвимость Content Spoofing

В шаблоне компонента “умный фильтр” выполняется подстановка в тело страницы значения из запроса, без каких-либо проверок на стороне сервера.
Все входящие данные должны быть проверены и экранированы.
Критичность: высокая.

```
<input type="hidden" name="<?echo $arItem["CONTROL_NAME"]?>" id="<?echo $arItem["CONTR
<?endforeach;?>

<input type="hidden" name="tovar_search" value="<?=$_REQUEST["tovar_search"]?>" >

<div class="row">
    <?foreach($arResult["ITEMS"] as $key=>$arItem)//prices
```

Рисунок 36 — Обращение к запросу в шаблоне

Обмен с 1с

Импорт нестандартный, запускается агентом “import_slowpoke25”. Все шаги импорта разбиты на отдельные скрипты, располагаются они в папке /update, которые вызываются с помощью curl’а в агенте. Пример:

```
$ch = curl_init();
$url = "[redacted]";
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_HTTPAUTH, CURLAUTH_BASIC);
    curl_setopt($ch,CURLOPT_USERPWD,$user . ":" . $password);
$Response = curl_exec($ch);
curl_close($ch);
```

Рисунок 37 — Шаг импорта

Шаги импорта:

1. Скрипт catalog-import.php. Подключение к удаленному серверу по ftp, скачивание файлов xml-файлов импорта в папку /upload/1c/.
2. Скрипт update_prop.php. Очистка свойств: VKLYUCHAT_V_KATALOG, VKLYUCHAT_V_INTERNET_MAGAZIN, RAZRESHIT_ELEKTRONNYE_PRODAZHI.
3. Скрипт main.php. Вызов модифицированного 1c_exchange.php с типом catalog и файлом для импорта import.xml. Импорт товаров.
4. Скрипт main_offers.php. Вызов модифицированного 1c_exchange.php с типом catalog и файлом для импорта offers.xml. Импорт торговых предложений.
5. Скрипт section.php. Перемещение товаров в разделы. Изначально разделы товары хранятся в свойствах ITEMATRAZDELNOV1 и ITEMATRAZDELNOV2 в текстовом виде, затем по значениям этих свойств товары переносятся в необходимые разделы, если такого раздела нет, то он создается.
6. Скрипт deactivate_section.php. Деактивация разделов, в которых нет активных товаров.
7. Скрипт picture.php. Подключение к удаленному серверу по ftp, скачивание и добавление изображений к товарам.
8. Скрипт pricelist.php. Обновление элементов инфоблока “Прайс листы”.
9. Скрипт check_book.php. Проставление элементам каталога флаг “Электронные книги” на основе значения свойства RAZRESHIT_ELEKTRONNYE_PRODAZHI.

Качество решения низкое. Код написан не оптимально, присутствуют запросы в цикле, которые увеличивают время импорта. Кроме того, файлы импорта никак не защищены от обращения к ним рядового посетителя или поискового робота. Такое обращение, в общем случае, может нарушать работу импорта, если произойдет во время его выполнения или в момент, когда входящие файлы загружены не полностью.

```
$res = CIBlockSection::GetList(Array(), $arFilter,true, $arSelect);


while($ar_result = $res->GetNext())
{

if($ar_result['ELEMENT_CNT']<=0)
{
    $bs = new CIBlockSection;
    $arFields_section_deactivate = Array(
      "ACTIVE" => 'N',
    );
    $bs->Update($ar_result['ID'],$arFields_section_deactivate);
}
}
```

Рисунок 37 — Запросы к БД в цикле

Критичность: Средняя
Необходимо изучить 1С и сформулировать технические требования к интерфейсу обмена с сайтом.

SEO

Ответ на несуществующий URL

Сервер возвращает 404 Page not found для несуществующих URL. Система работает корректно.

Перенаправление на URL с/без WWW

Перенаправление отсутствует. Необходимо выбрать формат и настроить.
Критичность: высокая
Если сайт будет проиндексирован по 2-м URL, это негативно скажется на его позициях.

Файл robots.txt

Файл отсутствует. Необходимо создать и наполнить согласно специфике сайта.

Критичность: высокая
Файл позволяет ограничить доступ к персональным разделам сайта для поисковых систем, снизить и ограничить нагрузку от поисковиков на сайт.

Файл sitemap.xml

Файл отсутствует. Необходимо создать и наполнить согласно специфике сайта.
Критичность: высокая
Файл содержит карту сайта и позволяет сократить время полного переиндексирования.

Важные html-тэги на страницах и возможность управления ими на страницах доступных поисковым системам

Главная страница

	Значение	Управление
URL	http://slowpoke.ru/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	Есть	Редактирование предусмотрено
H1	**Не заполнен**	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Корень каталога

	Значение	Управление
URL	http://slowpoke.ru/catalog/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено

H1	**Не заполнен**	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Список товаров

	Значение	Управление
URL	http://slowpoke.ru/catalog/######/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	Есть	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено
REL CANONICAL	**Не настроен**	**Не предусмотрен**

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Необходимо настроить вывод <link rel="canonical" href="###" /> на всех страницах постраничной навигации дальше 1-й.
Критичность: высокая.
Это позволит избежать индексирования 2,3…N страниц со списками товаров и предотвратит создание дублей в индексе поисковых систем. Ссылки на карточки товаров будут храниться в файле sitemap.xml

Карточка товара

	Значение	Управление
URL	http://slowpoke.ru/catalog/######/%%%/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	Есть	Редактирование

		предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Текстовая страница

	Значение	Управление
URL	http://www.slowpoke.ru/about/ http://www.slowpoke.ru/knigotorgovlya/ http://www.slowpoke.ru/knigotorgovlya/partners/ http://www.slowpoke.ru/contacts/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Список новостей

	Значение	Управление
URL	http://www.slowpoke.ru/about/news/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено

KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено
REL CANONICAL	**Не настроен**	**Не предусмотрен**

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Необходимо настроить вывод <link rel="canonical" href="###" /> на всех страницах постраничной навигации дальше 1-й.
Критичность: высокая.
Это позволит избежать индексирования 2,3…N страниц со списками товаров и предотвратит создание дублей в индексе поисковых систем. Ссылки на карточки товаров будут храниться в файле sitemap.xml

Страница новости

	Значение	Управление
URL	http://www.slowpoke.ru/about/news/%%%%/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Партнеры

	Значение	Управление
URL	http://www.slowpoke.ru/about/partners/	
TITLE	Есть	Редактирование предусмотрено

DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Вопросы и ответы

	Значение	Управление
URL	http://www.slowpoke.ru/about/faq/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	**Не заполнен**	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Список услуг

	Значение	Управление
URL	http://www.slowpoke.ru/knigotorgovlya/services/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено

H1	**Отсутствует**	**Редактирование не предусмотрено**

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Необходимо запрограммировать вывод h1 и возможность его редактирования **Критичность: высокая.**

В соответствие с рекомендациями Яндекс и Google, на любой странице сайта должен присутствовать заголовок h1.

Страница услуги

	Значение	Управление
URL	http://www.slowpoke.ru/knigotorgovlya/services/%%%%%/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Прайс листы

	Значение	Управление
URL	http://www.slowpoke.ru/knigotorgovlya/prices/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено

KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Контакты

	Значение	Управление
URL	http://www.slowpoke.ru/contacts/	
TITLE	Есть	Редактирование предусмотрено
DESCRIPTION	**Не заполнен**	Редактирование предусмотрено
KEYWORDS	**Не заполнен**	Редактирование предусмотрено
H1	Есть	Редактирование предусмотрено

Следует заполнить значения meta-тэгов и заголовка h1 в соответствие с запросом(ами), по которому(ым) продвигается страница.

Проверка Page Speed Insights

Шаблон сайта

Изображения не оптимизированы (более 20 изображений).

- Сжатие страницы http://slowpoke.ru/include/images/logo_header.png уменьшит ее размер на 19,1 КБ (52 %).
- Сжатие страницы http://slowpoke.ru/…itrix/templates/youshop/img/new_icon.png уменьшит ее размер на 15,7 КБ (84 %).
- Сжатие страницы http://slowpoke.ru/…f2a/f2ab69e371a49f4d5d694df4e5c9ada9.jpg уменьшит ее размер на 11,1 КБ (54 %).
- ...
- Сжатие страницы http://slowpoke.ru/…bitrix/templates/youshop/img/fb_icon.png уменьшит ее размер на 869 Б (89 %).

Критичность: высокая.

Следует сжать изображения на сервере во время сохранения.

Все файлы JS подключены в начале страницы.
Критичность: средняя.
Следует подключать JS в конце HTML, чтобы не блокировать загрузку страницы.

Главная страница

https://developers.google.com/speed/pagespeed/insights/?url=slowpoke.ru

Унаследованы проблемы шаблона.

Корень каталога

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fcatalog%2F
Унаследованы проблемы шаблона.

Список товаров

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fcatalog%2Fdukhovye-instrumenty%2F
Унаследованы проблемы шаблона.

Карточка товара

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fcatalog%2Fdukhovye-instrumenty%2F46478%2F
Унаследованы проблемы шаблона.

Список новостей

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fabout%2Fnews%2F
Унаследованы проблемы шаблона.
У img, в которых выводятся анонсные изображения новостей не определены адтибуты height и width.
Критичность: низкая.
Заранее заданная ширина и высота img сокращает время рендеринга страницы.

Страница новости

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fabout%2Fnews%2F45732%2F
Унаследованы проблемы шаблона.

Партнеры

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fabout%2Fpartners%2F
Унаследованы проблемы шаблона.
У img в которых выводятся логотипы партнеров не определены атрибуты height и width. **Критичность: низкая.**
Заранее заданная ширина и высота img сокращает время рендеринга страницы.

Вопросы и ответы

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fabout%2Ffaq%2F
Унаследованы проблемы шаблона.

Список услуг

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fknigotorgovlya%2Fservices%2F
Унаследованы проблемы шаблона.

Страница услуги

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fknigotorgovlya%2Fservices%2F8615%2F
Унаследованы проблемы шаблона.
Следует избежать загрузки несжатых изображений в визуальные редактор в поле “детальное описание”.
Критичность : низкая
Изображения которые попадают на сайт через визуальный редактор следует предварительно сжать в графическом редакторе.

Прайс листы

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fknigotorgovlya%2Fprices%2F
Унаследованы проблемы шаблона.

Контакты

https://developers.google.com/speed/pagespeed/insights/?url=http%3A%2F%2Fslowpoke.ru%2Fcontacts%2F
Унаследованы проблемы шаблона.

Битые ссылки, размещенные на страницах сайта

Обнаружено 6319 битых ссылок. Следует устранить все битые ссылки со страниц сайта.
Критичность: высокая.
Во время индексирования сайта, поисковые системы будут создавать чрезмерную нагрузку на веб-сервер.
Перечень битых ссылок доступен по ссылке ################

Заключение

Производительность сервера: средняя. Рекомендуем заменить процессор и увеличить количество оперативной памяти.
Производительность сайта: низкая. Сайт не способен выдерживать нагрузку выше 10 запросов в секунду. Необходимо устранить обнаруженные проблемы, настроить веб-сервер и базу данных.
Качество кода: низкое. Всё что запрограммировано поверх готового решения my_shop не соответствует правилам и стандартам кодирования 1С-Битрикс. Код и проекта и директории сайта содержат много мусора и не используемых фрагментов кода.
Безопасность: код сайта и API содержит критические уязвимости, позволяющие сменить пароль администратора сайта, удалить сайт, отредактировать контент.

Список задач

Задача	Критичность	Оценка от (часов)	Оценка до (часов)
Запрограммировать проверку входных параметров в скриптах API	Авария	4	6
Устранить уязвимость, при которой можно сменить пароль любому пользователю через API	Авария	2	3
определить оптимальное значение MaxRequwsrsPerChild и изменить настройки Apache	Высокая	1	1,5
отключить модуль XDebug	Высокая	0,1	0,15
настроить отправку писем	Высокая	2	3
Удалить мусор и резервные копии из корня сайта	Высокая	4	6
Устранить ошибки обнаруженные	Высокая	4	6

“сканером безопасности 1С-Битрикс”			
Устранить уязвимости в компоненте “Умный фильтр”	Высокая	1	1,5
Выбрать основное “зеркало” сайта и запрограммировать перенаправление пользователей с www.slowpoke.ru-> slowpoke.ru или наоборот	Высокая	0,5	0,5
Создать robots.txt и наполнить согласно специфике сайта	Высокая	0,5	0,5
Создать файл sitemap.xml	Высокая	0,5	0,5
В каталоге настроить вывод <link rel="canonical" href="###" /> на всех страницах постраничной навигации дальше 1-й	Высокая	1	1
В новостях настроить вывод <link rel="canonical" href="###" /> на всех страницах постраничной навигации дальше 1-й.	Высокая	1	1
Удалить битые ссылки со страниц сайта (6319 шт.)	Высокая	4	6
Заменить итерирование на запрос с группировкой в API	Высокая	4	6
включить кеширование в API	Высокая	16	24
Заменить код взаимодействующий напрямую с базой данный в API	Высокая	16	24
Устранить дублирование кода в API	Высокая	8	12
увеличить параметры tmp_table_size (текущее значение: 128 МБ), либо уменьшить max_heap_table_size (текущее значение: 128 МБ) и перенести папку с временными таблицами в оперативную память	Средняя	2	3
удалить APC	Средняя	0,1	0,15
Обновить php до версии 7.1	Средняя	24	36
Устранить ошибки обнаруженные “проверкой сайта 1С-Битрикс”	Средняя	2	3
вынести значения в константы, заменить использование значений на	Средняя	8	12

использование констант			
Оптимизировать изображения в шаблоне и на страницах сайта	Средняя	3	4,5
Перенести JS в конец страниц	Средняя	4	6
Изучить особенности 1С, сформулировать требования к интеграции, переделать интеграцию	Средняя	40	60
Запрограммировать генерацию паролей средствами 1С-Битрикс в API	Средняя	2	3
переработать api Oauth, выделить функциональность модуля, компонентов	Средняя	12	18
Исследовать работу большого количества запущенных процессов SMTP	Низкая	4	6
отключить и удалить неиспользуемые модули	Низкая	2	3
перенести вывод заголовка h1 в шаблоне сайта	Низкая	2	3
Удалить все ненужные комментарии	Низкая	2	3
Указать размеры изображений на странице “список новостей”	Низкая	0,5	0,75
Указать размеры изображений на странице “партнёры”	Низкая	0,5	0,75
убрать лишние операции в API	Низкая	4	6
отключить html-кешрование	Низкая	0,5	0,75
удалить функции “для разработки”, удалить лишние комментарии из init.php	Низкая	1	1,5

Итого: От 183 до 273 часов работы.

*Если будет меняться сервер, объем работ по переносу сайта на новый сервер 8 часов.
*На наш взгляд, рациональнее полностью переделать API. Объем всех работ 40 часов, это меньше чем точечно исправлять все обнаруженные проблемы.