

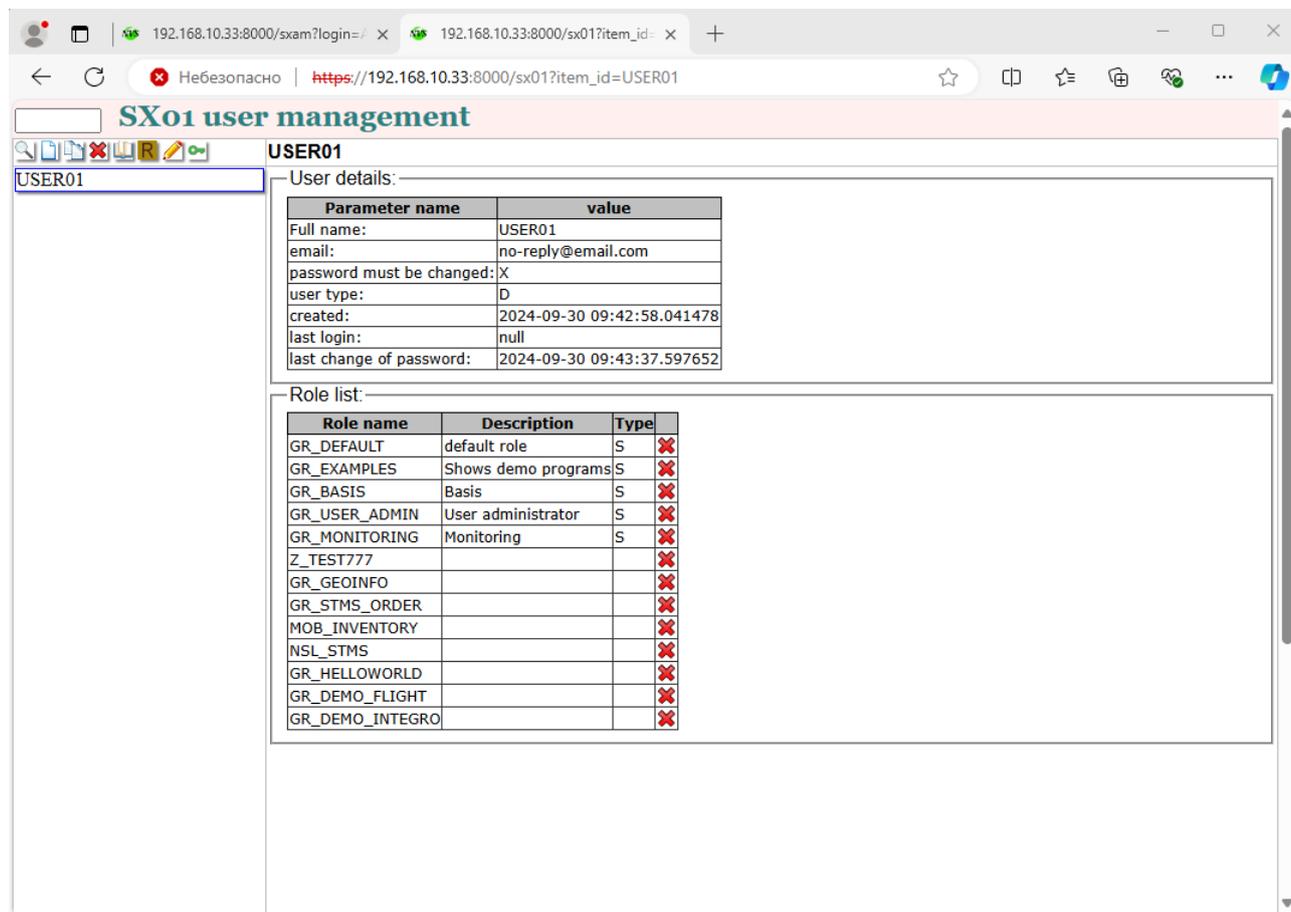
NVS Greenex

Первый вход в систему

Создание пользователя администратором.

Первоначально пользователь с достаточными полномочиями (администратор) создает нового пользователя в транзакции SX01, присваивает ему роли и устанавливает начальный пароль. Подробное описание процесса выходит за рамки данной инструкции.

В примере имя пользователя USER01 и начальный пароль Initial12



The screenshot shows a web browser window with the URL https://192.168.10.33:8000/sx01?item_id=USER01. The page title is "SX01 user management". On the left, there is a search bar containing "USER01". The main content area is titled "USER01" and contains two sections:

User details:

Parameter name	value
Full name:	USER01
email:	no-reply@email.com
password must be changed:	X
user type:	D
created:	2024-09-30 09:42:58.041478
last login:	null
last change of password:	2024-09-30 09:43:37.597652

Role list:

Role name	Description	Type	
GR_DEFAULT	default role	S	✖
GR_EXAMPLES	Shows demo programs	S	✖
GR_BASIS	Basis	S	✖
GR_USER_ADMIN	User administrator	S	✖
GR_MONITORING	Monitoring	S	✖
Z_TEST777			✖
GR_GEOINFO			✖
GR_STMS_ORDER			✖
MOB_INVENTORY			✖
NSL_STMS			✖
GR_HELLOWORLD			✖
GR_DEMO_FLIGHT			✖
GR_DEMO_INTEGRO			✖

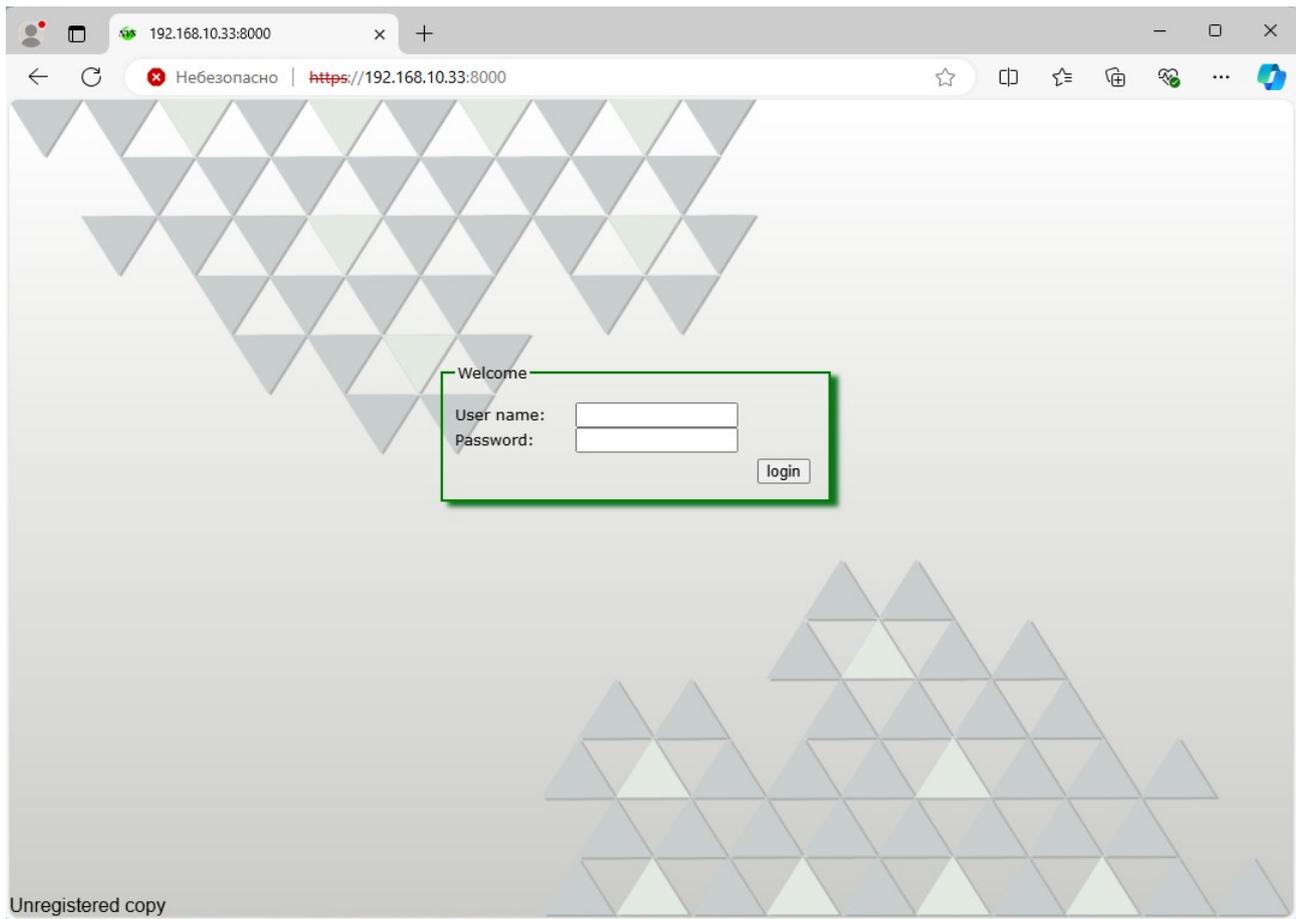
Первый вход в систему нового пользователя.

Для входа в систему необходима ссылка (URL) и данные об имени пользователя и начальном пароле, которые пересылаются по почте.

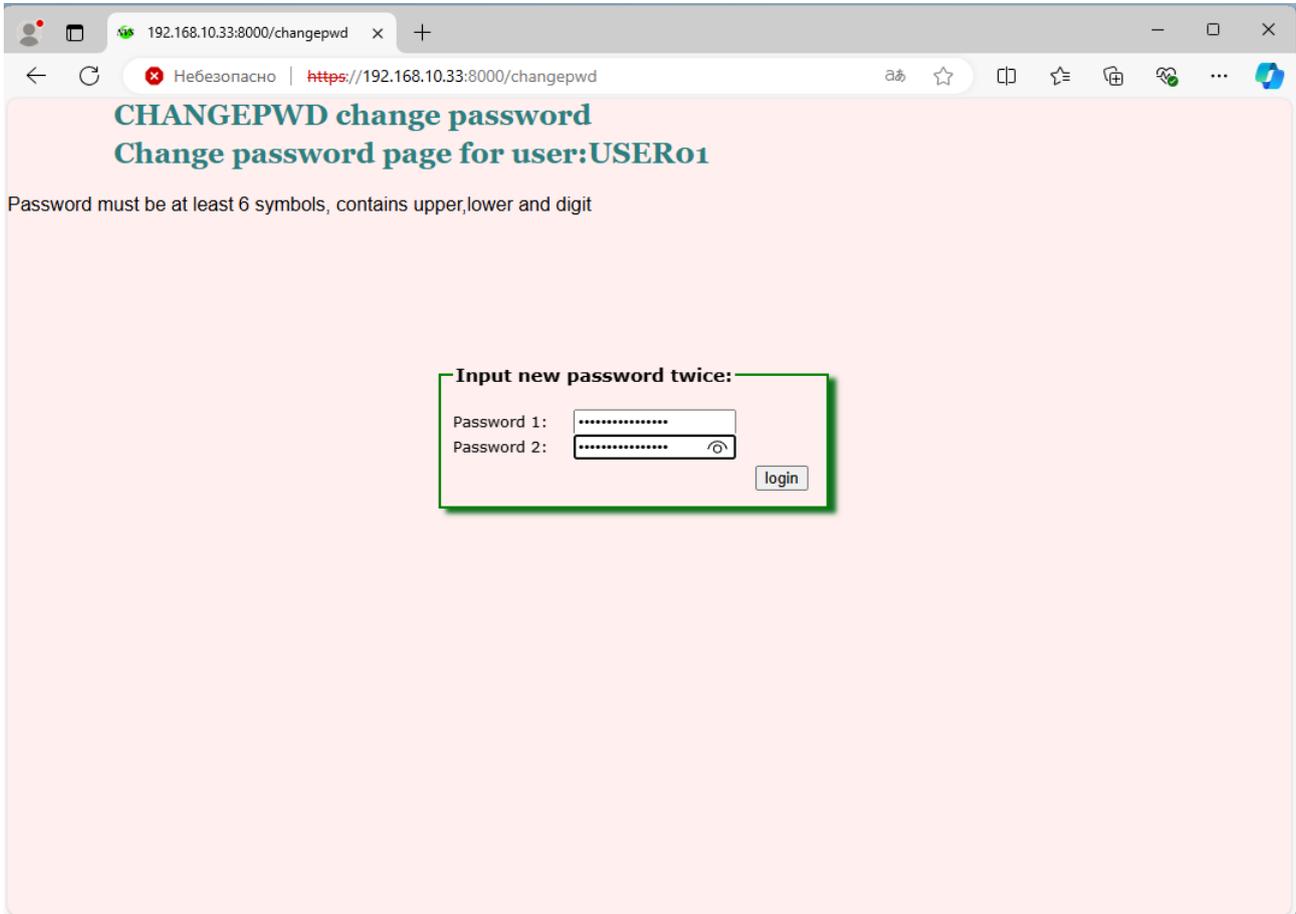
Например:

<https://192.168.10.33:8000/>

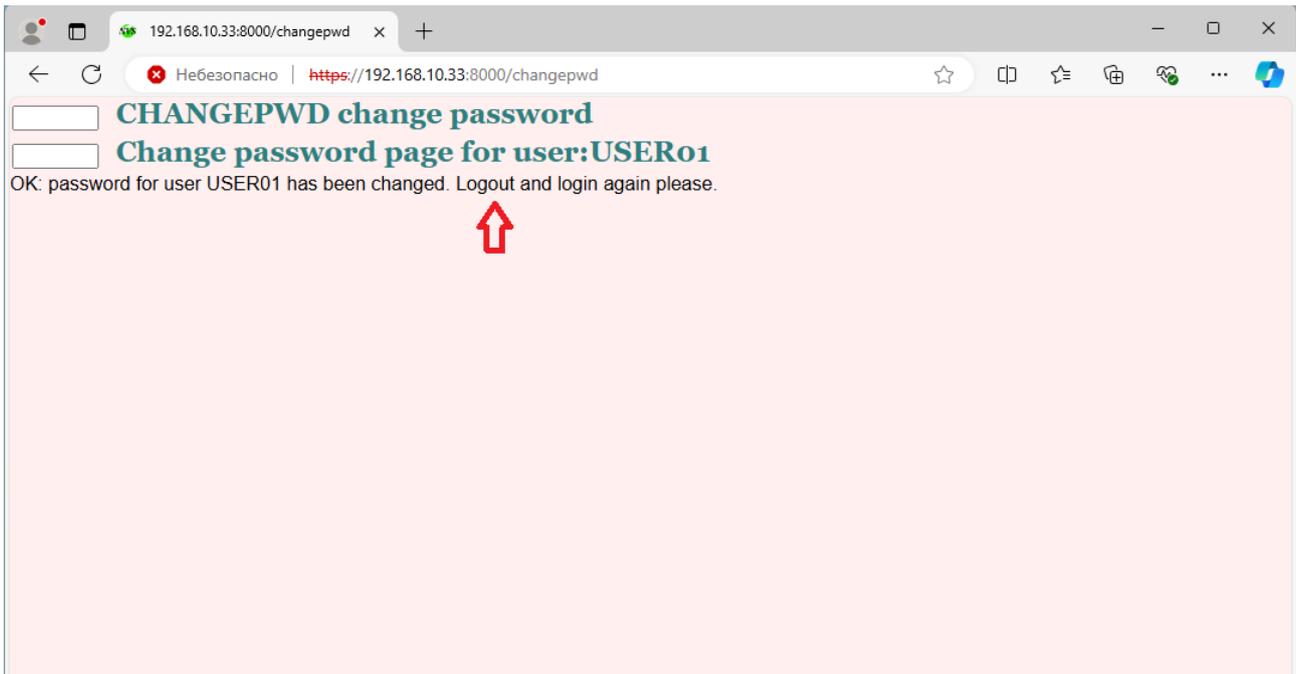
внешний вид экрана приглашения может выглядеть так:



Пользователю следует ввести имя и начальный пароль вручную, после чего он будет перенаправлен на страницу ввода нового пароля. Цвет фона зависит от настроек системы.



После смены пароля следует закрыть браузер. В примере это Microsoft Edge и войти заново с уже постоянным паролем.

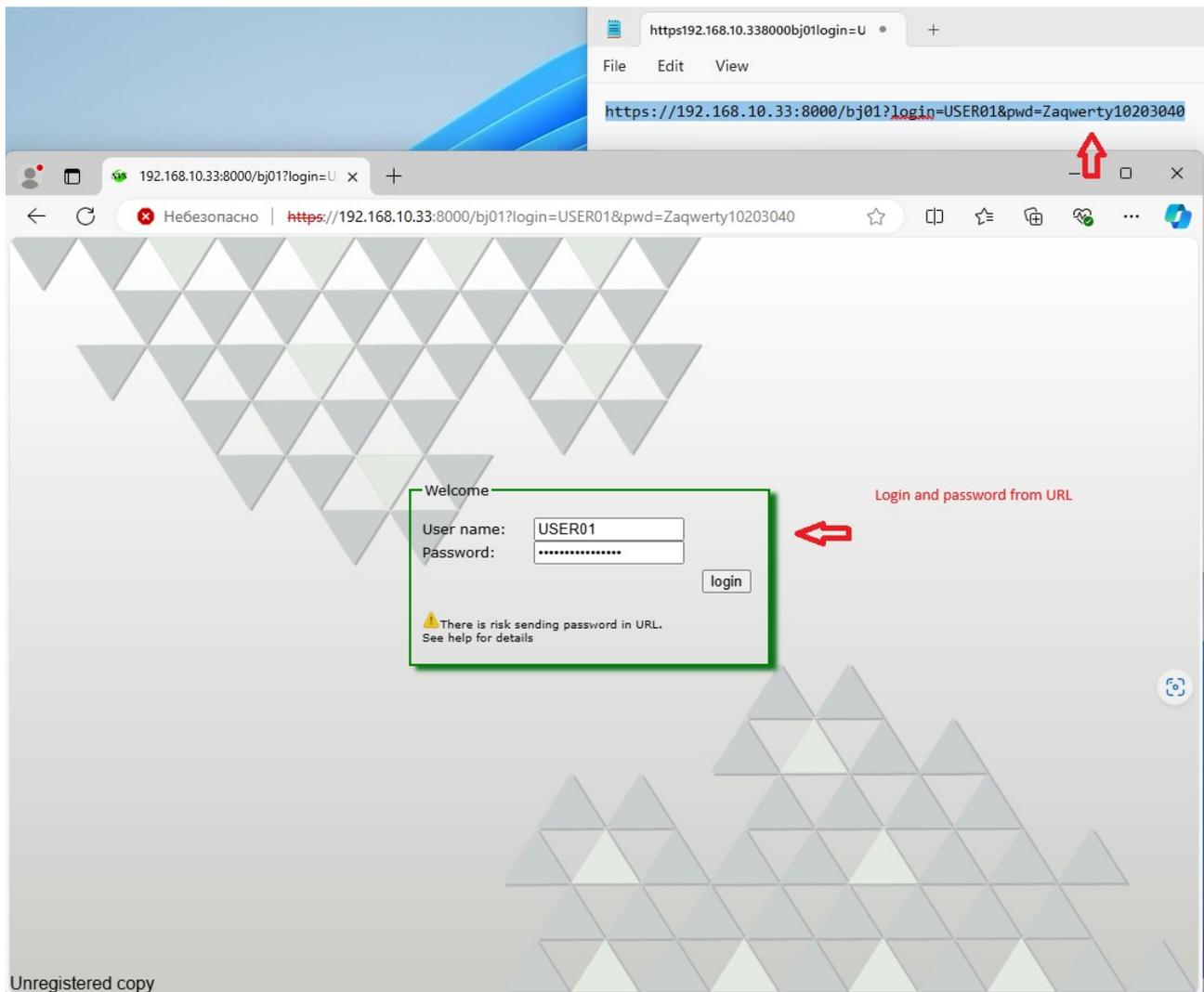


Лайфхак 1: Авторизация через URL параметры.

В тестовых системах можно передавать логин пароль через параметры строки вызова (URL). Хотя при передачи данных по сети строка происходит шифрование SSL(TLS v1.2) и строка URL не доступна для перехвата, она все еще может быть видна в логах сервера и на скриншотах при неаккуратном обмене информацией по почте.

Пример вызова первым способом:

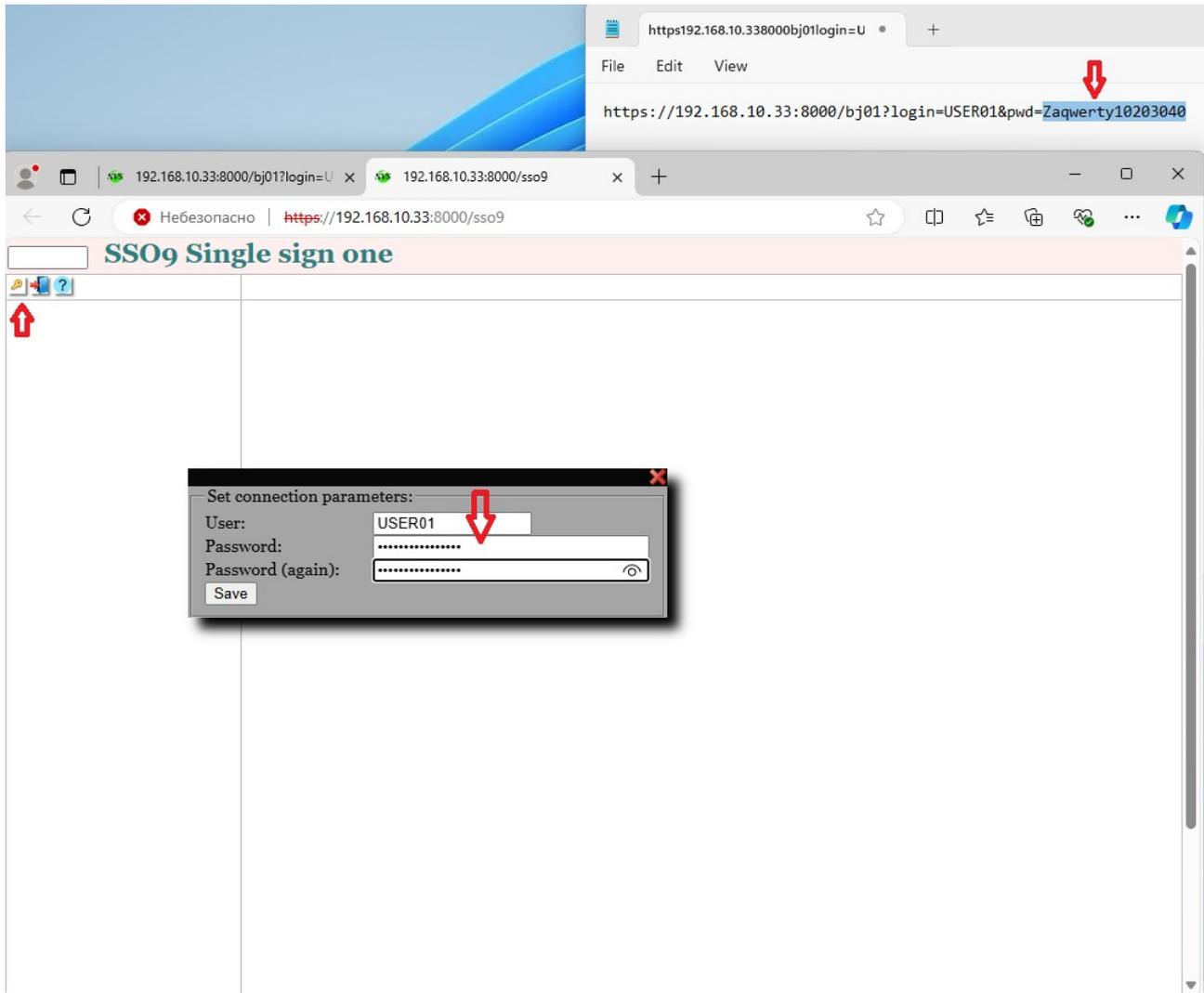
<https://192.168.10.33:8000/bj01?login=USER01&pwd=Zaqwerty10203040>



Лайфхак 2: Авторизация через ключ.

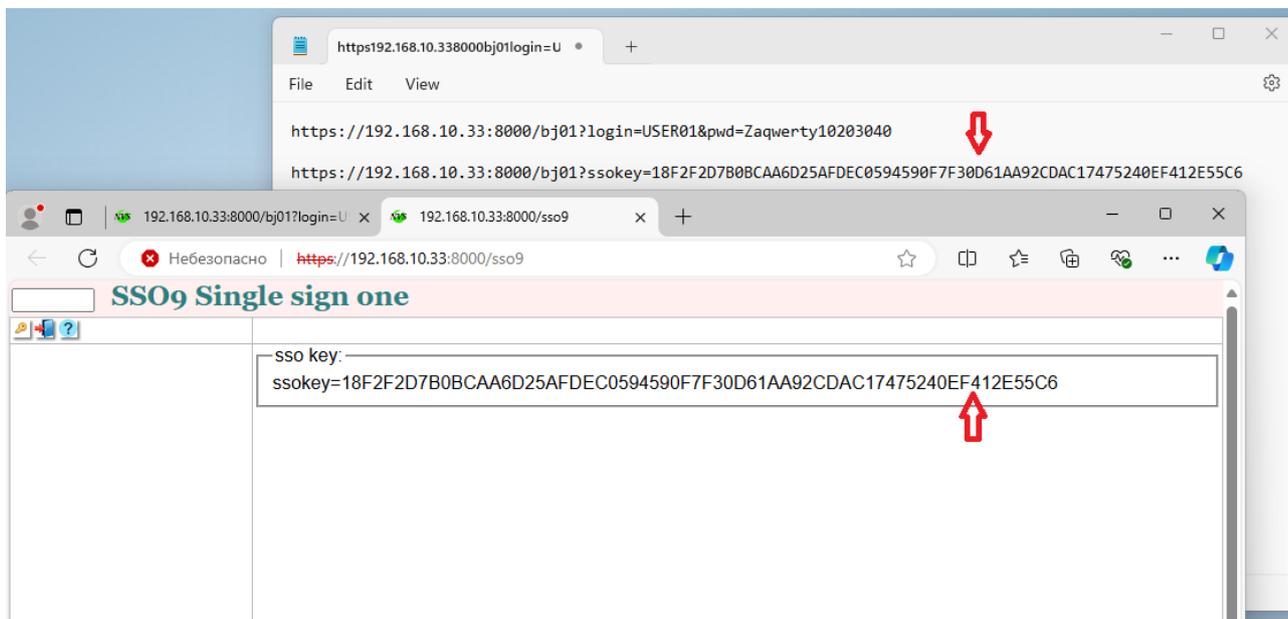
Более безопасным способом передачи является ключ ssokey который пользователь может сгенерировать с помощью транзакции SSO9 на основе имени пользователя и пароля.

Извлечение логина и пароля происходит самой системой и является более продвинутым способом, чем первый.



В результате строка вызова выглядит так:

<https://192.168.10.33:8000/bj01?login=USER01&pwd=Zaqwerty10203040>
[ssokey=18F2F2D7B0BCAA6D25AFDEC0594590F7F30D61AA92CDAC17475240EF412E55C6](https://192.168.10.33:8000/bj01?ssokey=18F2F2D7B0BCAA6D25AFDEC0594590F7F30D61AA92CDAC17475240EF412E55C6)



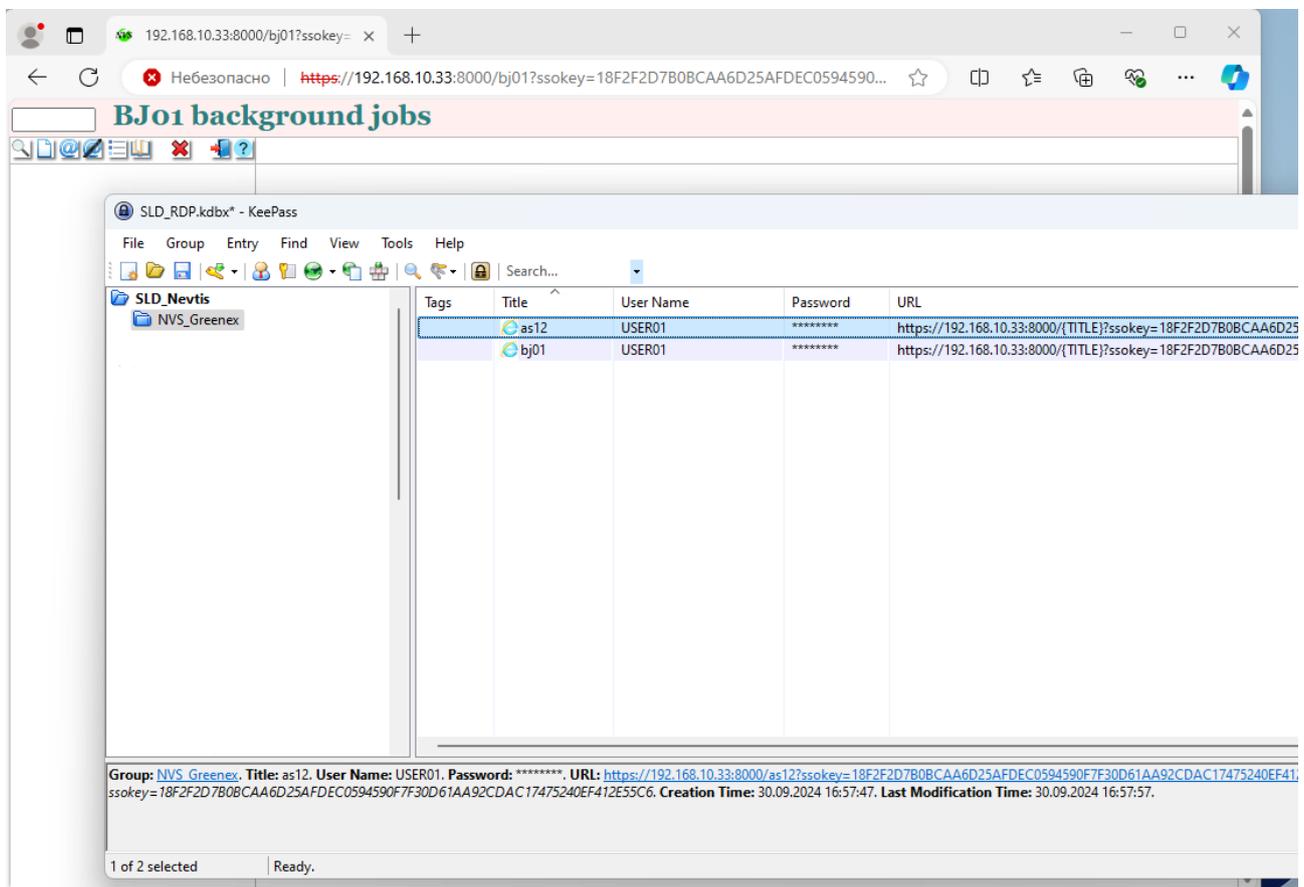
Но следует признать, что самым безопасным способом является стандартный ввод пароля в окне приглашения и передача его на сервер через POST запрос.

Каким способом воспользоваться решать пользователю на основе важности данных в конкретной системе.

Лайфхак 3: Использование вспомогательной программы KeePass.

Наряду с основным предназначением хранения паролей, этот Open-source менеджер предоставляет удобный способ доступа ко многим приложениям путем автоматического запуска браузера (в данном случае) с одновременной подстановкой параметров.

Использование KeePass позволяет организовать работу наиболее удобным способом, снижая риск ошибок и уменьшая необходимость ручного ввода.



Заключение

При работе с NVS Greenex важно понимать основные принципы работы с пользовательским интерфейсом правильно выбирая баланс между безопасностью и удобством работы.