
TSARKA
WWW.CYBERSEC.KZ

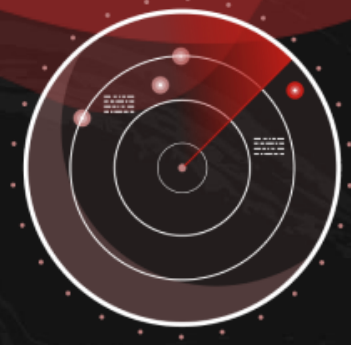
О КОМПАНИИ

ЧАСТНЫЙ CERT (ЦЕНТР РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ) В КАЗАХСТАНЕ

OSCP (OFFENSIVE SECURITY CERTIFIED PROFESSIONAL), CEH (CERTIFIED ETHICAL HACKER), OSWP (OFFENSIVE SECURITY WIRELESS PROFESSIONAL), ISO 27001, ETC
ОПЫТ РАБОТЫ: 10 ЛЕТ

1-2 МЕСТА НА PHDAYS 2017, 2018, 2019

НАШИ УСЛУГИ



АУДИТ ИНФОРМАЦИОННЫХ СИСТЕМ

АУТСОРСИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

ОБУЧЕНИЕ ИБ

ПЕНТЕСТ (ТЕСТ НА ПРОНИКНОВЕНИЕ)

СЕРТИФИКАЦИЯ

ВНЕДРЕНИЕ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАЗРАБОТКА БЕЗОПАСНОГО ПО

СЕССИЯ НА ПЯТЕРОЧКУ

КАК ПОВЫСИТЬ УСПЕВАЕМОСТЬ,
НЕ ВЫХОДЯ ИЗ ДОМА

АВТОР

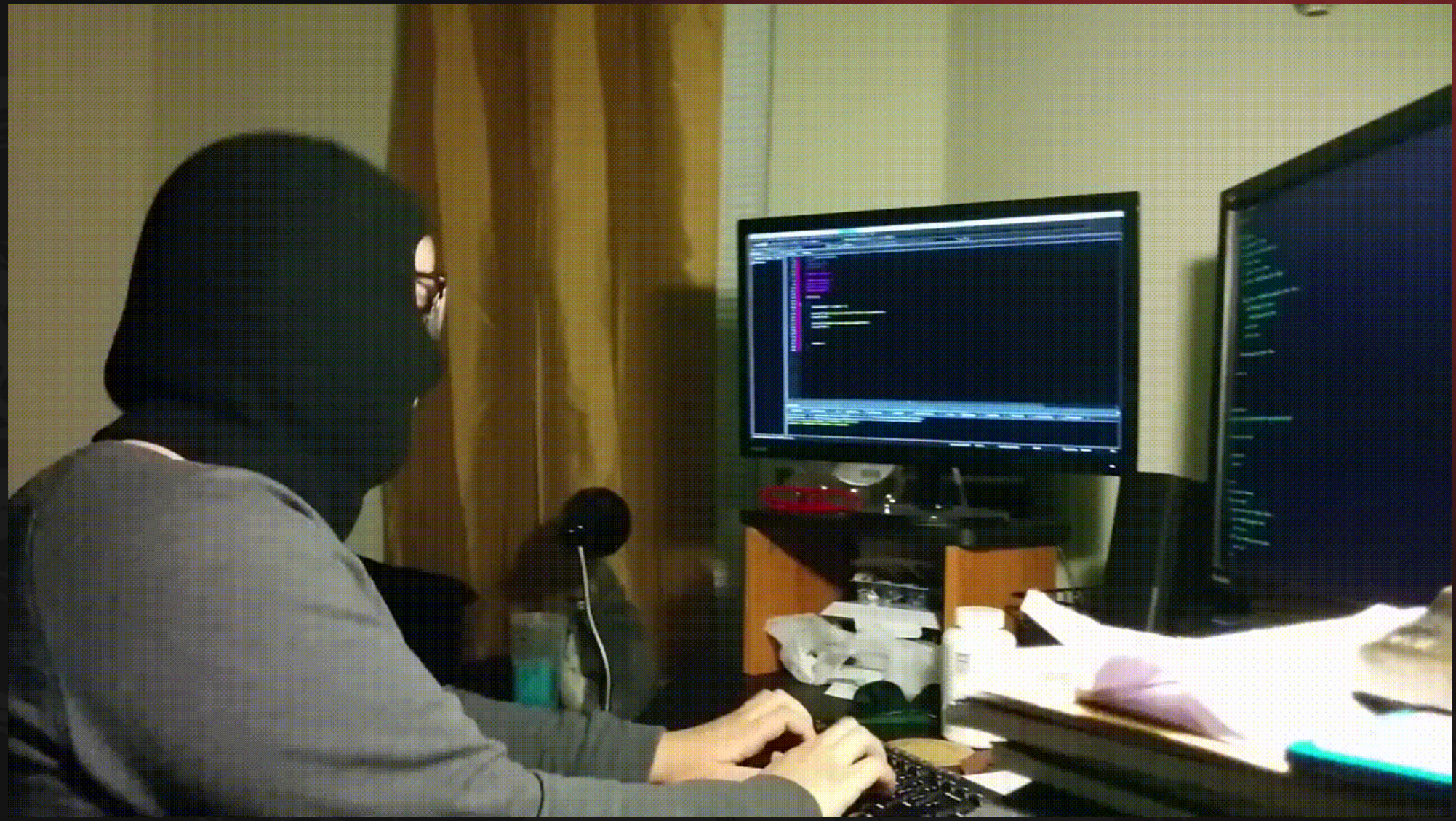
АВТОР: @EVILMORTY
HTTPS//T.ME/MORTYCHANNEL

ВНИМАНИЕ!

ВСЕ СОБЫТИЯ И ПЕРСОНАЖИ ВЫМЫШЛЕНЫ. СОВПАДЕНИЯ СЛУЧАЙНЫ.

ПРЕДЫСТОРИЯ

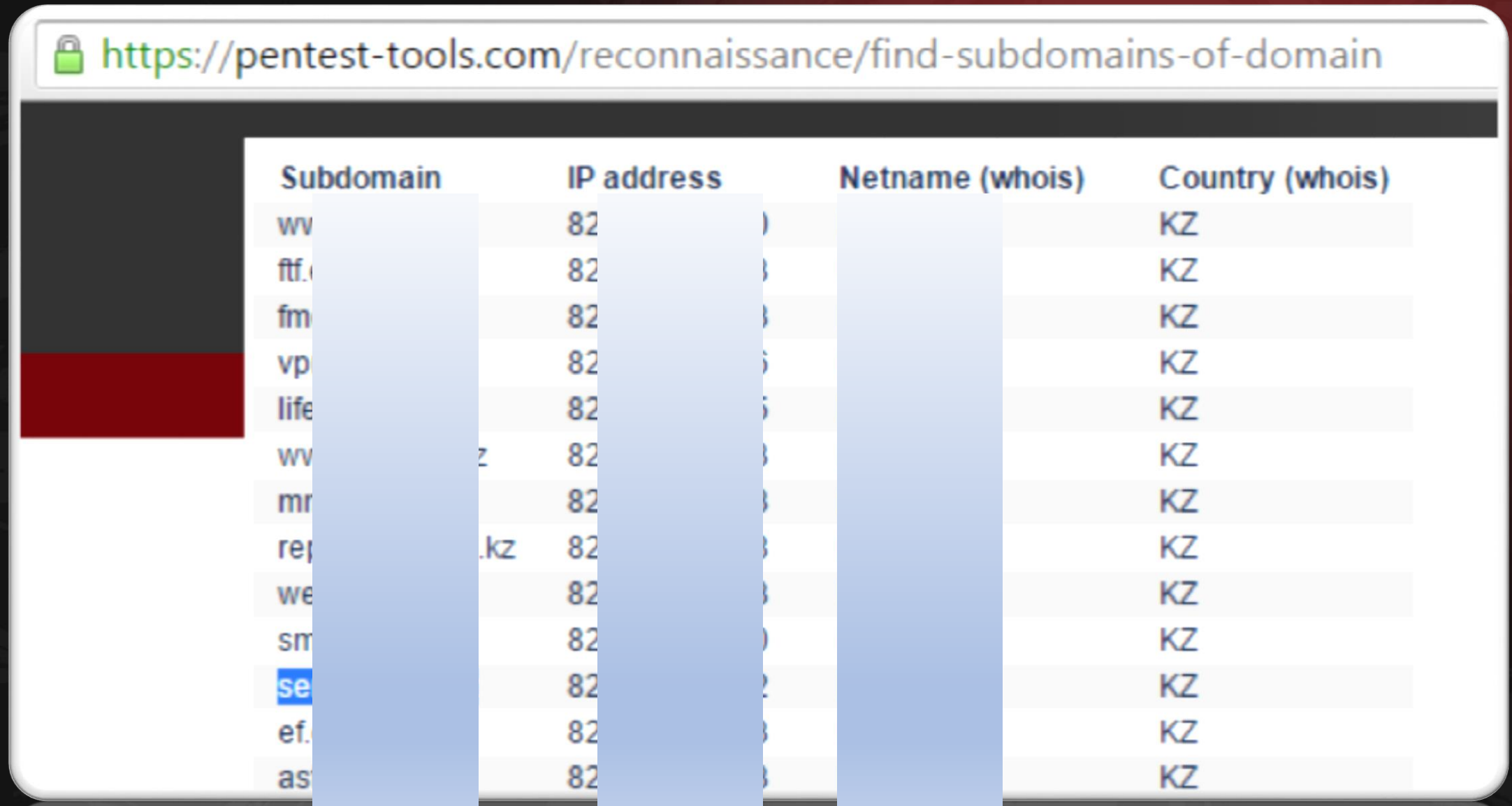
ПРЕДЫСТОРИЯ



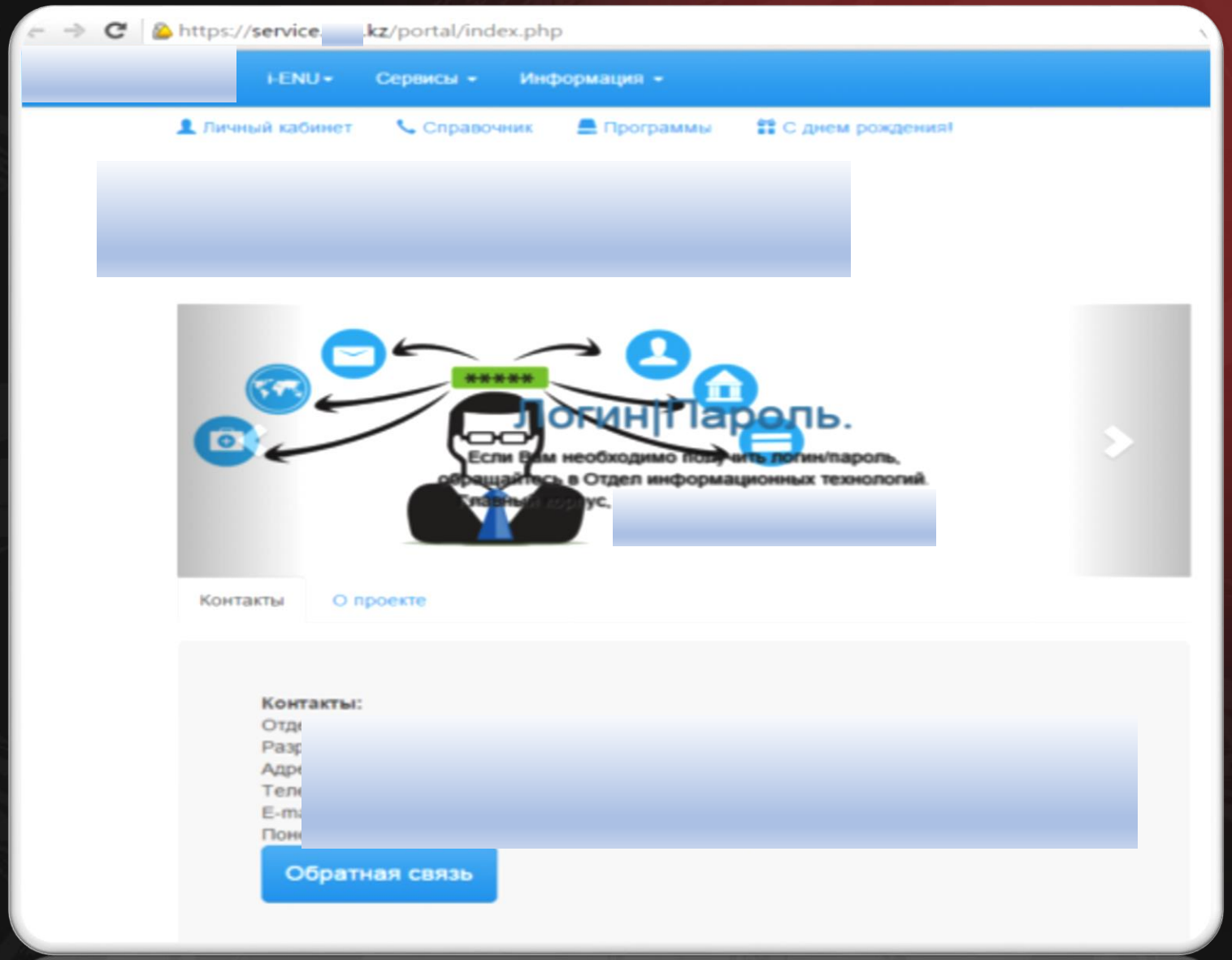
ПРЕДЫСТОРИЯ

```
54:48 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 10390
55:02 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 7858
56:32 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 10392
56:45 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 4258
56:48 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 3611
56:54 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 3619
57:29 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 4258
57:32 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 3577
57:38 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 4215
57:52 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 13030
57:59 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 3986
58:01 +0600] "POST [redacted]image8.jpg.php HTTP/1.0" 200 107072
```

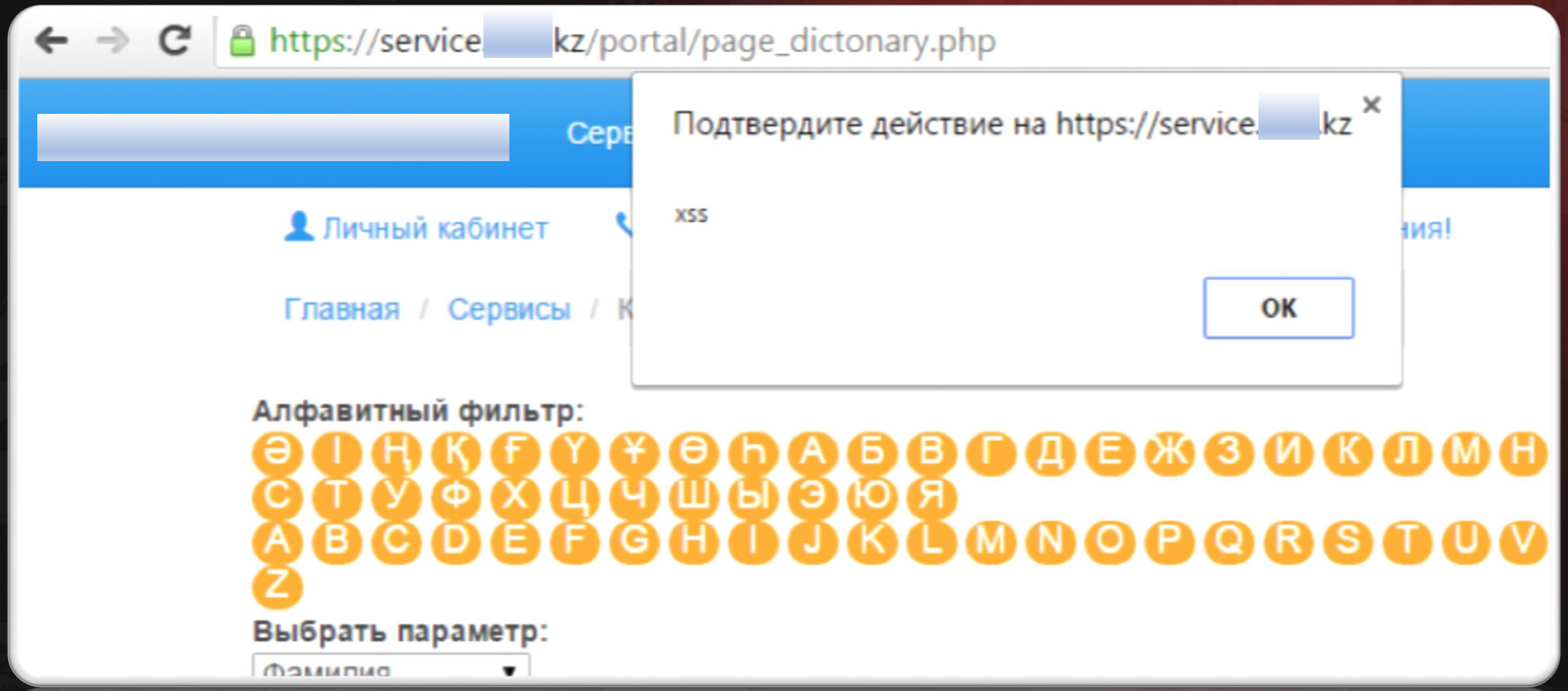
ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ



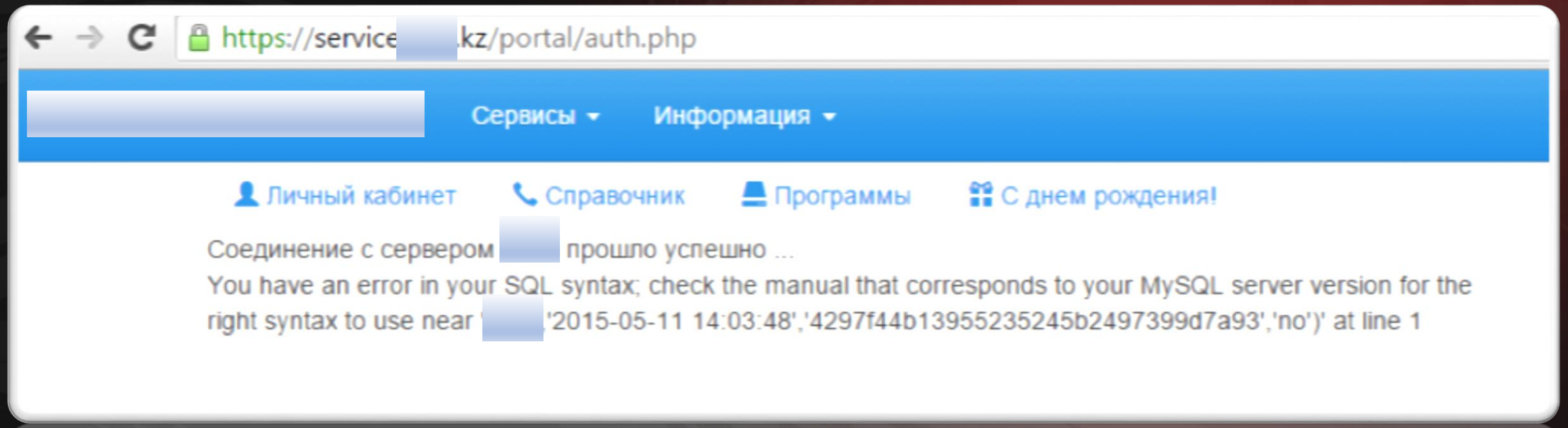
ЦЕЛЬ НАЙДЕНА



ЦЕЛЬ НАЙДЕНА



ПРОВЕДЕНИЕ АТАКИ



ПРОВЕДЕНИЕ АТАКИ

```
[13:34:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: PHP 5.6.7, Apache 2.4.10
back-end DBMS: MySQL 5.0
[13:34:09] [INFO] fetching database names
[13:34:09] [INFO] the SQL query used returns 5 entries
[13:34:09] [INFO] resumed: information_schema
[13:34:10] [INFO] resumed: dictonary
[13:34:10] [INFO] resumed: request
[13:34:10] [INFO] resumed: service
[13:34:10] [INFO] resumed: skd
available databases [5]:
[*] dictonary
[*] information_schema
[*] request
[*] service
[*] skd
```

ПОЛУЧЕНИЕ ИНФОРМАЦИИ

```
Database: service
[24 tables]
+------------------+
| aboniment        |
| auth             |
| counter_ip       |
| counter_pages    |
| enuskd           |
| ldap_fields      |
| ldap_logs        |
| ldap_users       |
| ldap_users_role  |
| links            |
| menu_main        |
| news             |
| news_type        |
| openbook         |
| openip           |
| pages            |
| res_type         |
| resurs           |
| status_abon      |
| tutors_staff_1c  |
| view_ldap_role   |
| vuz_moduls       |
| vuz_spec         |
| vuz_umk          |
+------------------+
```

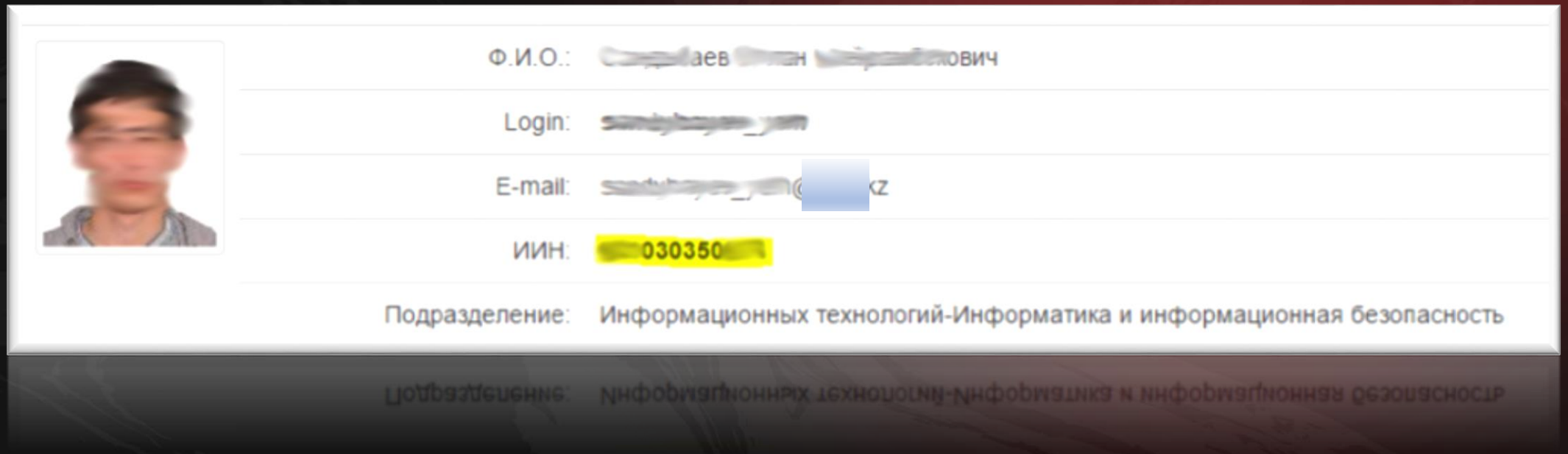
ПОЛУЧЕНИЕ ИНФОРМАЦИИ

```
Database: service
Table: auth
[8 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| auth_dt       | datetime     |
| auth_status   | varchar(3)   |
| id            | int(11)      |
| user_fio      | varchar(255) |
| user_ip       | varchar(255) |
| user_login    | varchar(255) |
| user_password | varchar(255) |
| user_role     | varchar(255) |
+---------------+--------------+

[13:41:23] [INFO] fetched data logged to text files under 'C:\Users\On\.sqlmap\output\service.     .kz'

[*] shutting down at 13:41:23
```

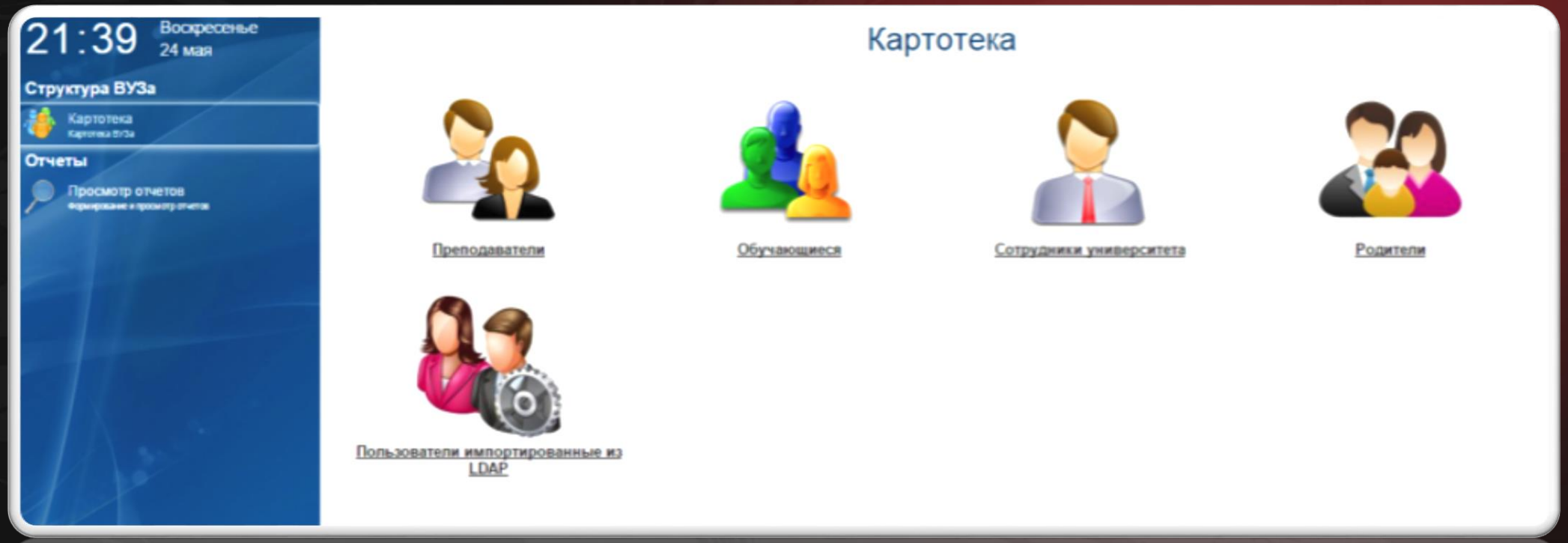
ПОЛУЧЕНИЕ ИНФОРМАЦИИ

id	user_login	user_password
1	nurzhanov_eb	0cd0b44bb27d248200a8964cd0a6a05b

ДОСТУП К ПАНЕЛИ АДМИНИСТРАТОРА



ДОСТУП К ПАНЕЛИ АДМИНИСТРАТОРА



ЧТО БЫЛО ДАЛЬШЕ?

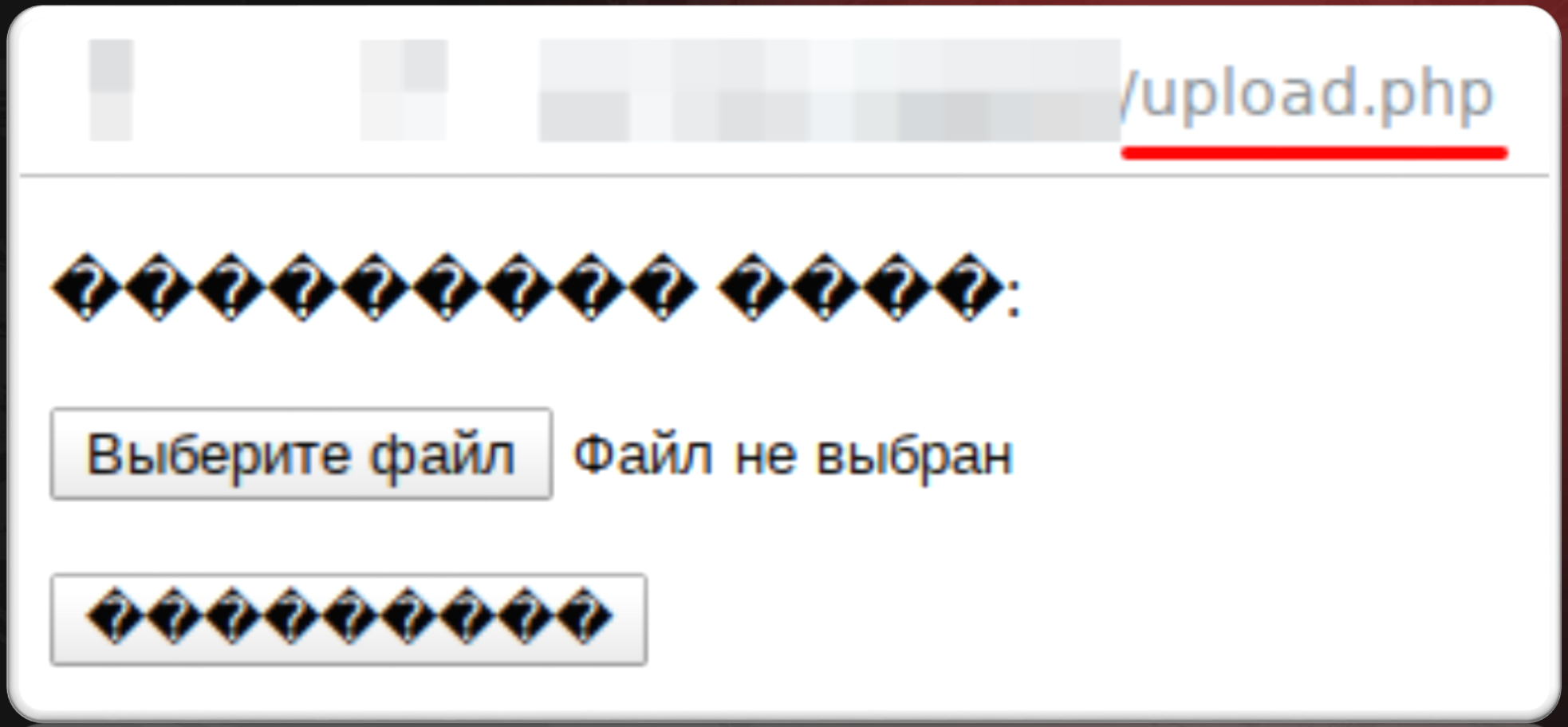
1. УПРАВЛЕНИЕ НАД СЕРВЕРОМ
2. ФИШИНГОВЫЕ АТАКИ
3. MITM
4. ОТЧИСЛЕНИЕ ИЗ ВУЗА
5. ...
6. ДАННАЯ ПРЕЗЕНТАЦИЯ

РАССЛЕДОВАНИЕ ИНЦИДЕНТА

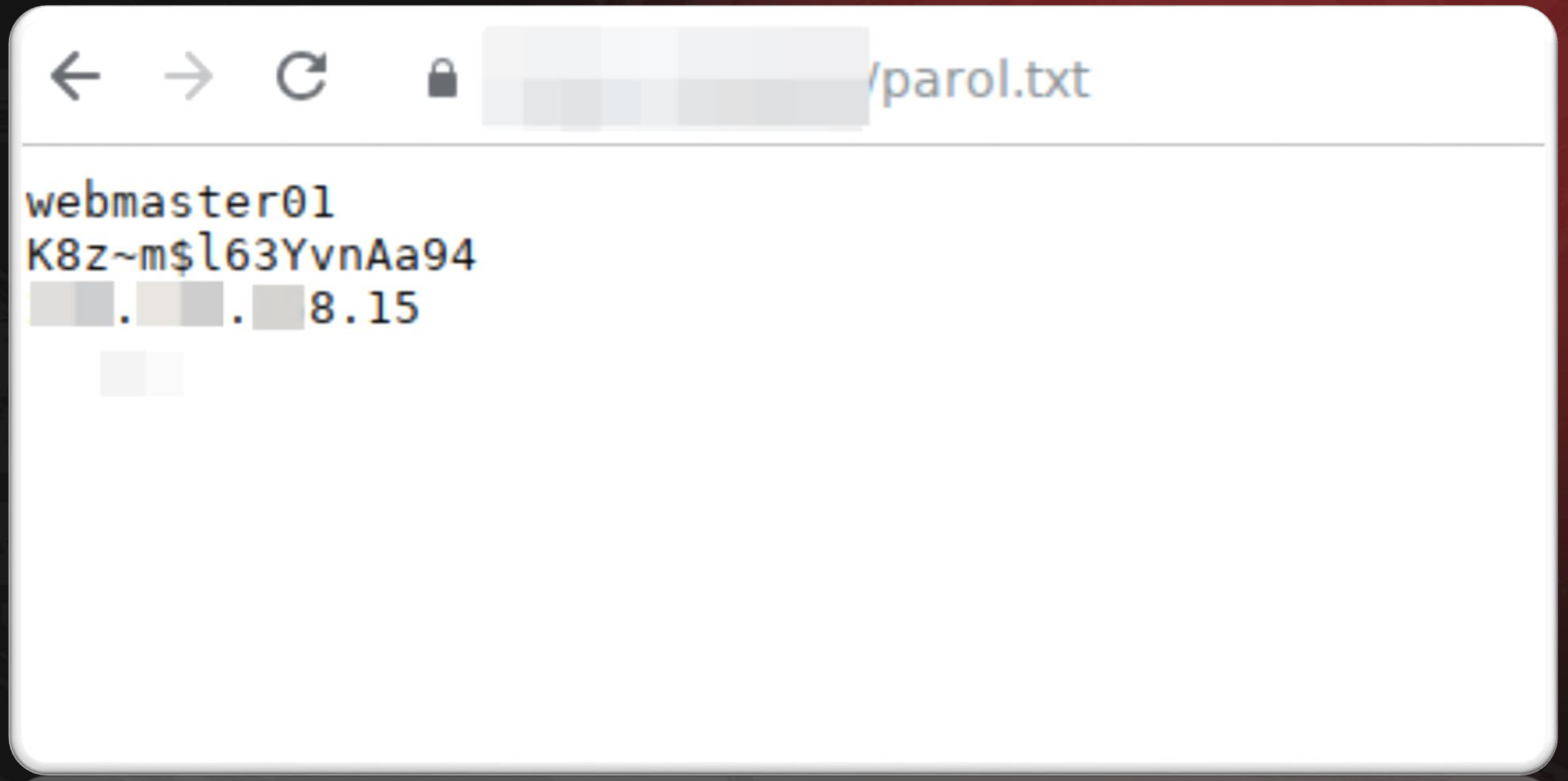
ЧТОБЫ ПОЙМАТЬ ХАКЕРА, НУЖНО ДУМАТЬ КАК ХАКЕР

АВТОР: WILSON & D3N_AMAN

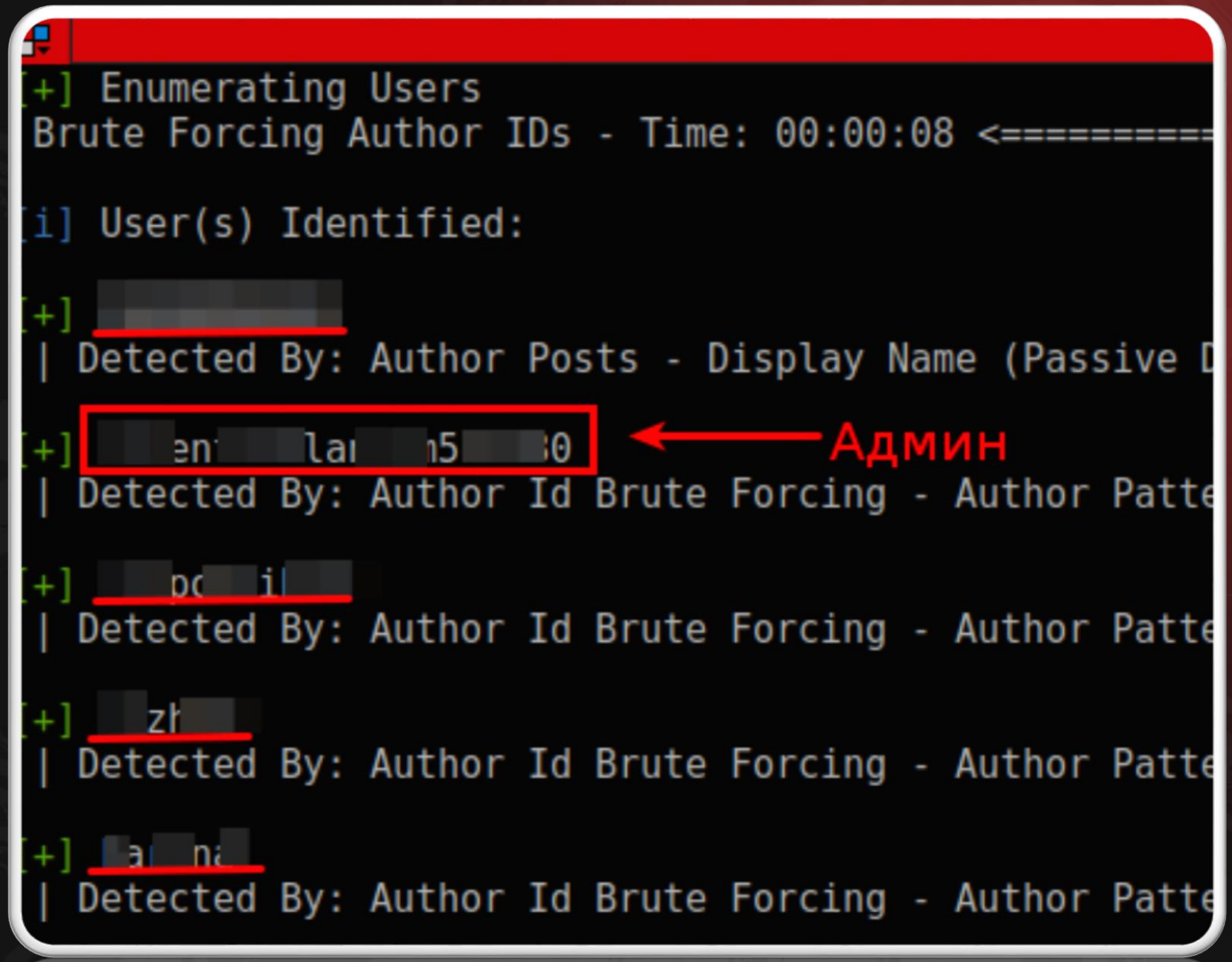
АУДИТ РЕСУРСА



АУДИТ РЕСУРСА



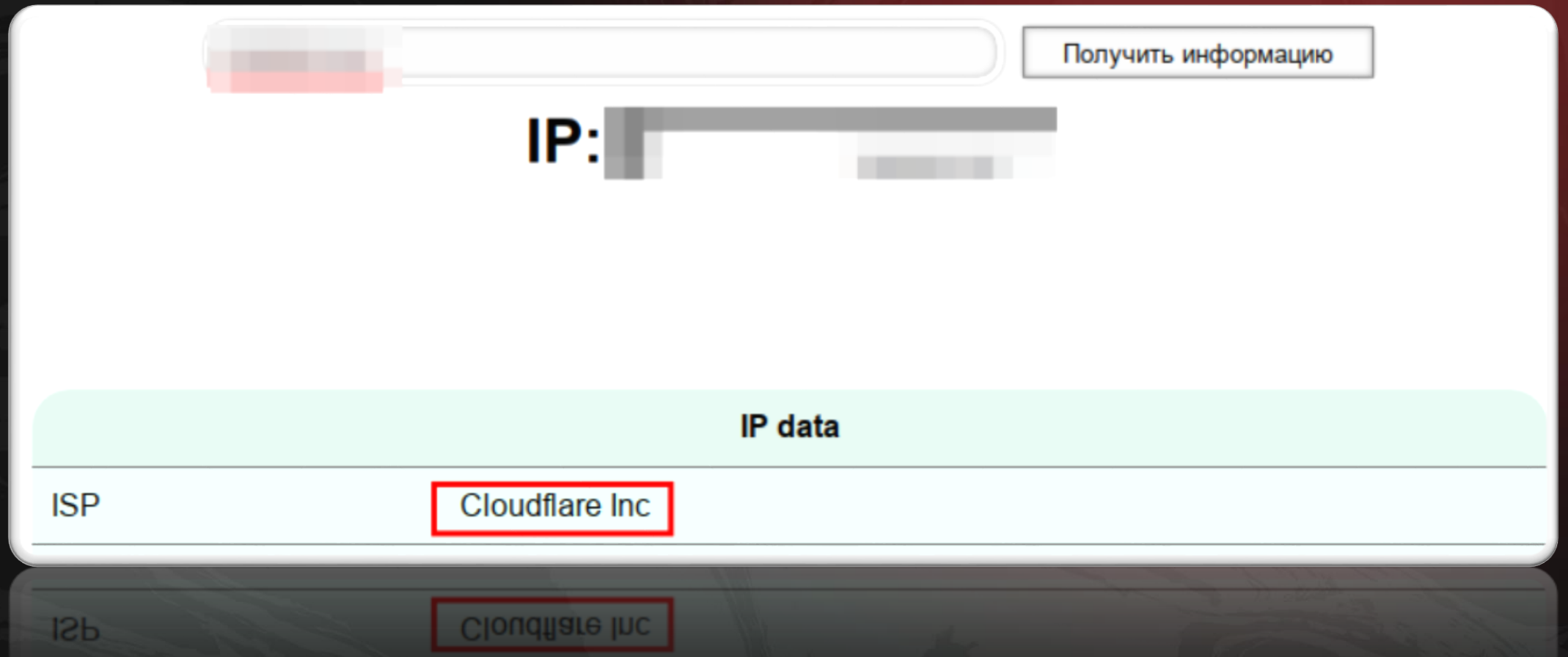
АУДИТ РЕСУРСА



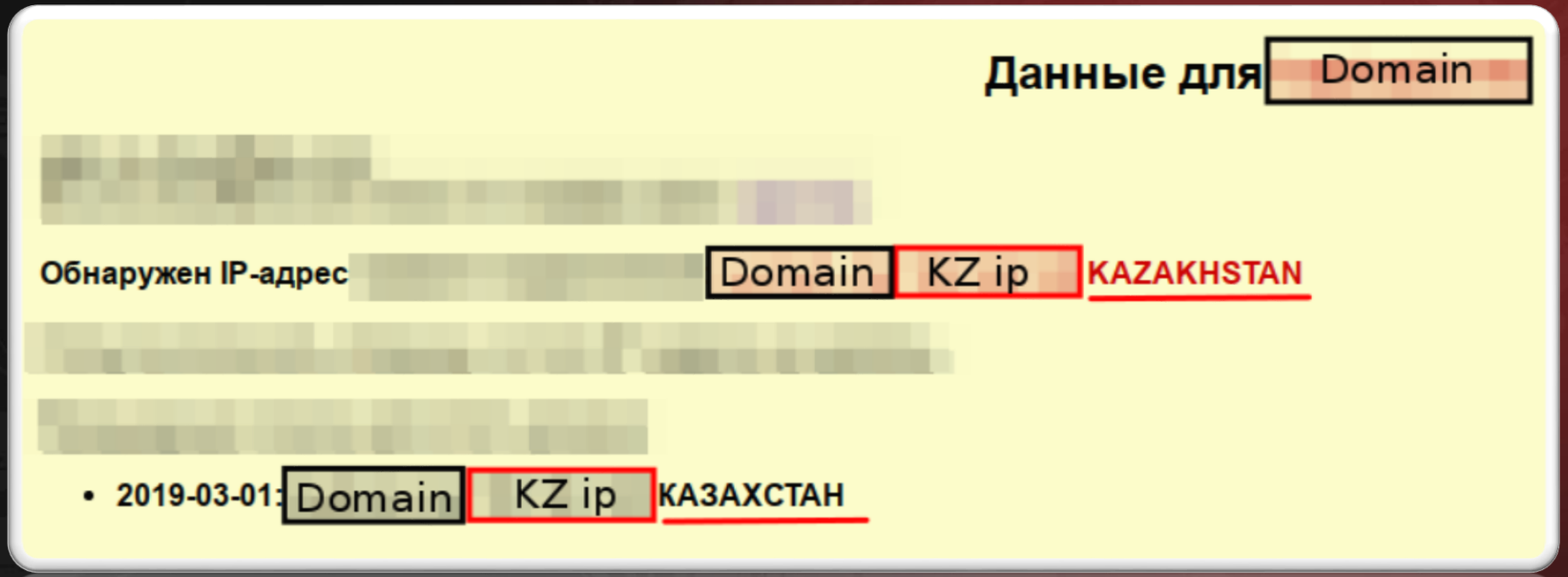
АУДИТ РЕСУРСА

Request ▲	Payload	Status	Error	Timeout	Length
4	2d34d234d	200	☐	☐	3917
5	2d34d23d4	200	☐	☐	3917
6	5f435f34f5	200	☐	☐	3917
7	2x34d23d4	200	☐	☐	3917
8	f53f345f	200	☐	☐	3917
9	23f423f23	200	☐	☐	3917
10	g56g546g54	200	☐	☐	3917
11	d234d234d23	200	☐	☐	3917
12	g345g34g534	200	☐	☐	3917
13	d234d234d23	200	☐	☐	3917
14	g34g534g53	200	☐	☐	3917
15	34g534g534g	200	☐	☐	3917
16	d24d23d423	200	☐	☐	3917
17	g5345g3g434	200	☐	☐	3917
18	d23d423d42	200	☐	☐	3917
19	h45h645h	200	☐	☐	3917
20	d234d23d423	200	☐	☐	3917
21	f345f34f534	200	☐	☐	3917
22	h45h645h4	200	☐	☐	3917
23	23423d23	200	☐	☐	3917
24	1234567	302	☐	☐	0
25	rwerwe	200	☐	☐	3917
26	rwerwerwer	200	☐	☐	3917
27	werwerwe	200	☐	☐	3917

ПОИСК ЗЛОУМЫШЛЕННИКА



ПОИСК ЗЛОУМЫШЛЕННИКА



ВЫВОДЫ?

КОНТАКТЫ

КАЗАХСТАН, Г. НУР-СУЛТАН

УЛ. МАНГИЛИК ЕЛ Д.19/2

+7 (7172) 47-84-13

INFO@YBERSEC.KZ

СПАСИБО ЗА ВНИМАНИЕ!

*ИЗВИНИТЕ, ЧТО НЕ УЛОЖИЛСЯ В ТАЙМИНГ ВЫСТУПЛЕНИЯ