

Мастер класс по заданиям СТФ

Коротко и доступно про анализ трафика, стенографию, OSINT и веб-технологии.



Рудакова Екатерина Евгеньевна

учитель информатики

МАОУ «Гимназии №80 города Челябинска»

Образовательные события по теме «Информационная безопасность»

1 ВсОШ

Направление с 2025/2026 учебного года, ранее модуль Технология

2

Киберщит. CTF (Capture the Flag)

На базе ЧРТ (Челябинский радиотехнической колледж) 4-й год.

5

InnoCTF Junior

Университет Иннополис.
9 – 11 классы.

3 Олимпиада им. И.Я. Верченко

по информатике и компьютерной безопасности. Академия ФСБ России, МТУСИ, Институт криптографии.

4

Олимпиада по математике, информатике, криптографии

имени академика А.М. Ильина проводится для учащихся 5-8 классов ОУ города Челябинска.

6

«Звезда»

Направление Информационная безопасность.

КВИЗ-ТУРНИР

МИР КРИПТО

РЕГИСТРАЦИЯ

Проведение открытого квиз-турнира запланировано на
20 декабря 2025 года с 08:00 до 18:00
по московскому времени, участие бесплатное.
Турнир будет проведен в онлайн формате

ПОЛОЖЕНИЕ

CTF — ЧТО ЭТО?

Соревнования по кибербезопасности в форме игры Capture The Flag проходят в 2 форматах: task-based и classic. В формате Task-Based (или Jeopardy) игрокам предоставляется набор заданий (тасков), к которым требуется найти и отправить ответ. Ответ даётся в виде флага, состоящего из набора символов или произвольной фразы. `ib2024{FLAG}` За верное выполнение каждого задания команда получает очки, количество которых зависит от сложности таска.



pt	Forensics	Reverse	M
65	100	50	5
50	150	100	1
50	150	150	1
00	200	200	1
57	200	300	2
34	250	300	3
00	347	400	
30	350		

Crypto



Криптография — наука о методах обеспечения конфиденциальности, целостности данных, аутентификации и шифрования. Для решения задач данного типа понадобятся различные декодеры, знание отличительных признаков различных кодировок.

Cryptography

stitution
cipher

Stream C

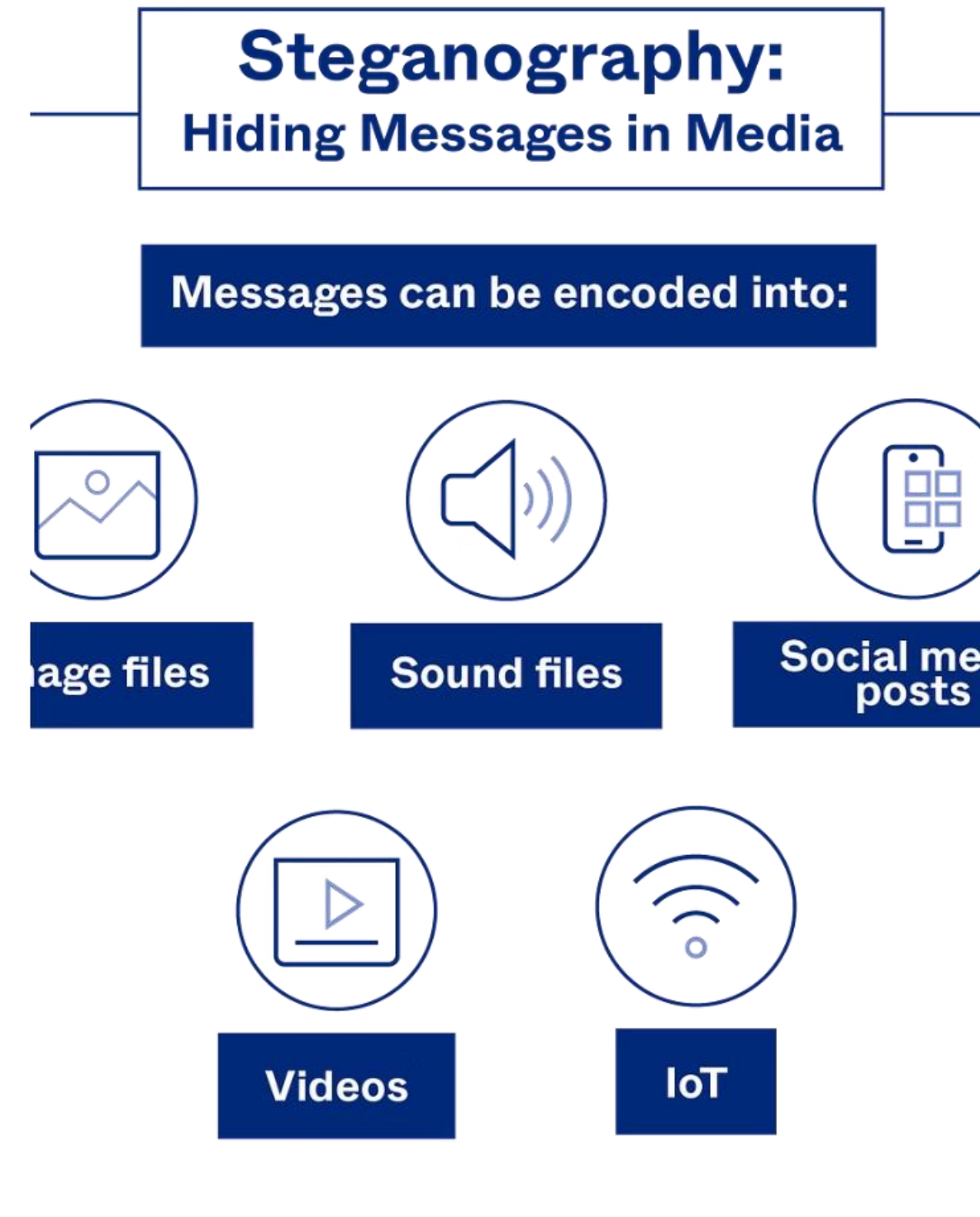
Salad

Нам на почту прислали поврежденную [картинку](#). Сможешь понять, что с ней не так?



Stegano/stego

Стеганография – защита информации посредством скрывания самого факта ее наличия. В CTF используются 4 типа контейнеров: изображения, текстовые файлы, видео файлы и аудио-файлы.



Sounds of the future

Думаю, примерно [так](#) будет звучать музыка в 2500 году.

<https://spectrogram.birdiememory.com/>

OSINT (Open Source Intelligence)

В данном типе задач представлена информация какого-то формата, и суть задания состоит в том чтобы найти флаг посредством поиска в открытых источниках.

Advanced Sciences and Technologies for Security Applications

Babak Akhgar
P. Saskia Bayerl
Fraser Sampson *Editors*

Open Source Intelligence Investigation

From Strategy to Implementation

 Springer

ВО{ }Ш

**ВСЕРОССИЙСКАЯ
ОЛИМПИАДА
ШКОЛЬНИКОВ**

Web

Это одна из категорий задач, включающая в себя анализ получаемых и передаваемых web приложению (или серверу) данных, поиск и эксплуатирование уязвимостей и т.д.



telnet

telnet аутентификация.

(формат флага: ib2024{FLAG}, будьте внимательны!)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet bytes Narrow & Wide Case sensitive String password

No.	Time	Source	Destination	Protocol	Length	Info
38	4.126630	192.168.196.16	192.168.196.1	FTP	90	Response: 331 Please specify the password.
39	4.167701	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
40	5.424998	192.168.196.1	192.168.196.16	FTP	78	Request: PASS Buck3tH4TF0RM3!
41	5.425034	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
42	5.432387	192.168.196.16	192.168.196.1	FTP	79	Response: 230 Login successful.
43	5.432801	192.168.196.1	192.168.196.16	FTP	62	Request: SYST
44	5.432834	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
45	5.432937	192.168.196.16	192.168.196.1	FTP	75	Response: 215 UNIX Type: L8
46	5.478790	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=42 Ack=97 Win=1050880 Len=0
47	6.309628	192.168.196.1	192.168.196.16	FTP	84	Request: PORT 192,168,196,1,212,140
48	6.309655	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=97 Ack=70 Win=64256 Len=0
49	6.309874	192.168.196.16	192.168.196.1	FTP	107	Response: 200 PORT command successful. Consider using PASV.
50	6.310514	192.168.196.1	192.168.196.16	FTP	62	Request: LIST
51	6.311053	192.168.196.16	192.168.196.1	FTP	95	Response: 150 Here comes the directory listing.
52	6.311479	192.168.196.16	192.168.196.1	FTP	80	Response: 226 Directory send OK.
53	6.311640	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=76 Ack=211 Win=1050880 Len=0

File Transfer Protocol (FTP)

- 331 Please specify the password.\r\n
 Response code: User name okay, need password (331)
 Response arg: Please specify the password.

```

[Current working directory: /]
0000 00 04 00 01 00 06 00 0c 29 83 20 a6 00 00 08 00 ..... ).....
0010 45 00 00 4a 73 76 40 00 40 06 bd d4 c0 a8 c4 10 E..Jsv@. @.....
0020 c0 a8 c4 01 00 15 d4 8b 1b 22 5c ea 60 81 78 5f ..... "\. `x_
0030 50 18 01 f6 09 a0 00 00 33 33 31 20 50 6c 65 61 P..... 331 Plea
0040 73 65 20 73 70 65 63 69 66 79 20 74 68 65 20 70 se speci fy the p
0050 61 73 73 77 6f 72 64 2e 0d 0a ..... assword. ..

```



robots

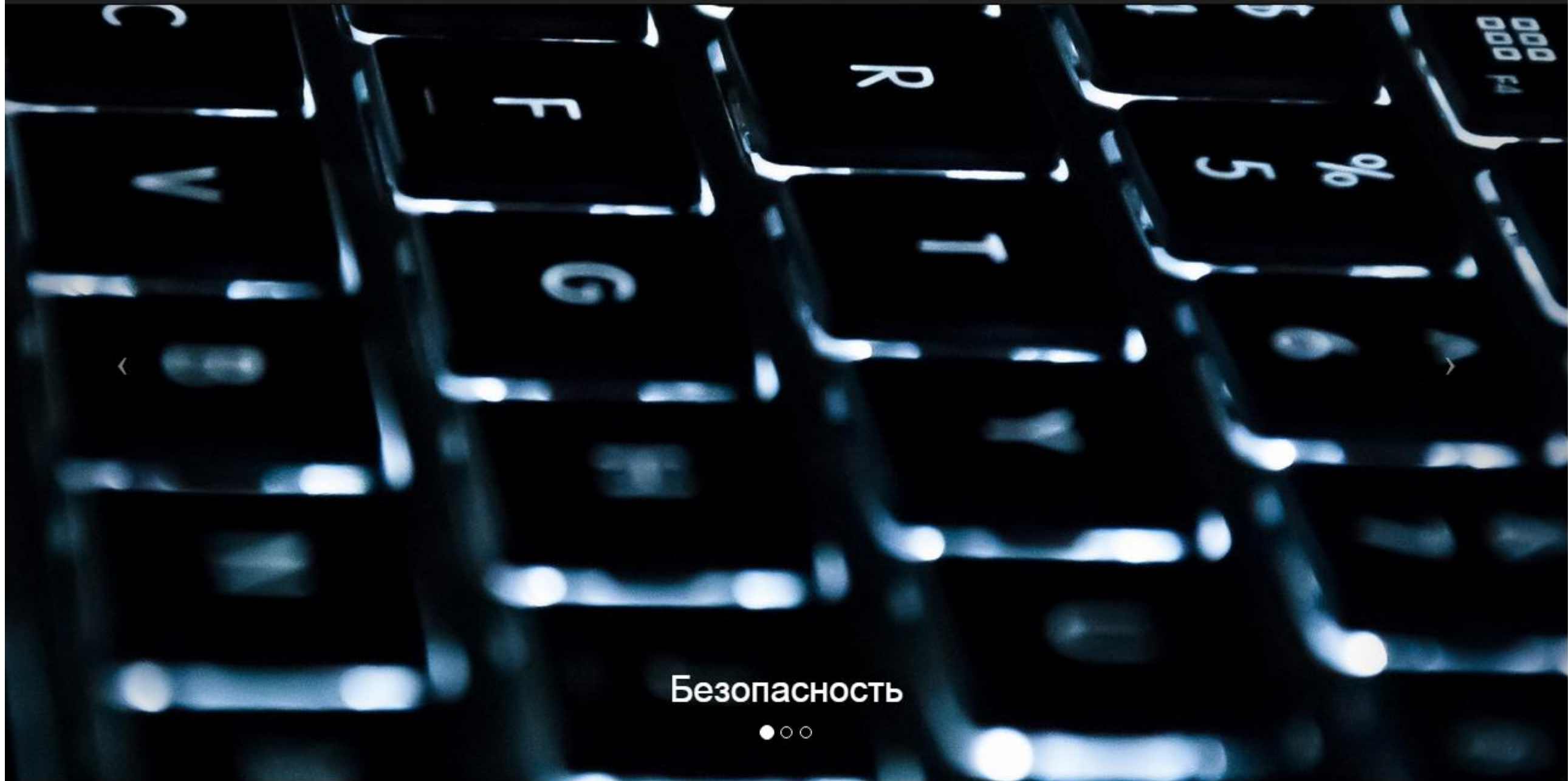
50

24 solves

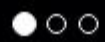
Are you robot?

[Vuln board](#)

Submit



Безопасность



← → ↻ ctfboard.ml/robots.txt   ☰

ctfboard.ml/robots.txt

🔍 ctfboard.ml/robots.txt - Поиск Google



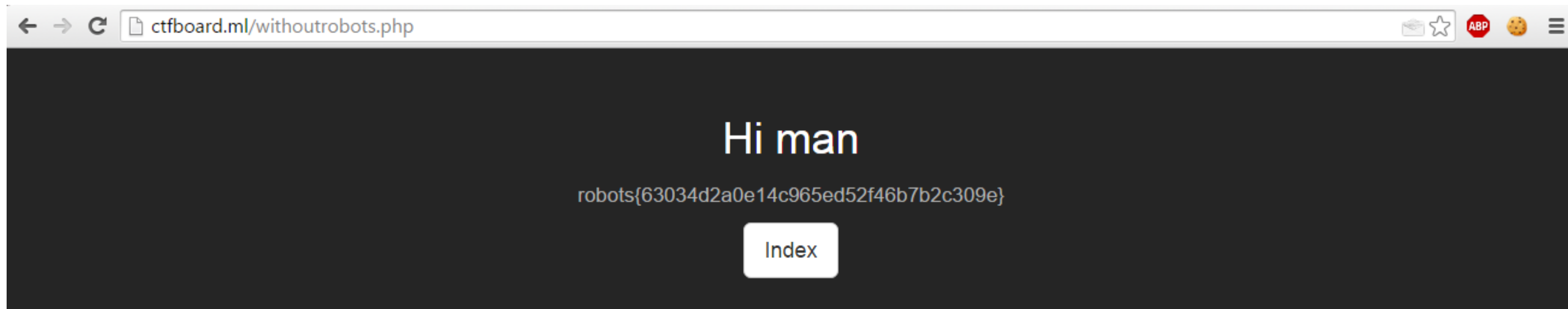
← → ↻ ctfboard.ml/robots.txt



```
User-Agent: *
Disallow: /withoutrobots.php
Disallow: /search
Allow: /search/about
Disallow: /sdch
Disallow: /groups
Disallow: /catalogs
Allow: /catalogs/about
Allow: /catalogs/p?
Disallow: /catalogues
Allow: /newsalerts
Disallow: /news
Allow: /news/directory
Disallow: /nwshp
Disallow: /setnewsprefs?
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=*%
Allow: /?hl=*%&gws_rd=ssl$
Disallow: /?hl=*%&gws_rd=ssl
Allow: /?gws_rd=ssl$
Allow: /?pt1=true$
Disallow: /addurl/image?
Allow: /mail/help/
Disallow: /mail/
Disallow: /pagead/
Disallow: /relpage/
Disallow: /relcontent
Disallow: /imgres
Disallow: /imglanding
Disallow: /sbd
Disallow: /keyword/
Disallow: /u/
Disallow: /univ/
Disallow: /cobrand
Disallow: /custom
Disallow: /advanced_group_search
Disallow: /googlesite
Disallow: /preferences
Disallow: /setprefs
Disallow: /swr
Disallow: /url
Disallow: /default
Disallow: /m?
Disallow: /m/
... ..
```


```
← → ↻ ctfboard.ml/robots.txt
User-Agent: *
Disallow: /withoutrobots.php
Disallow: /search
Allow: /search/about
Disallow: /sdch
Disallow: /groups
Disallow: /catalogs
Allow: /catalogs/about
Allow: /catalogs/p?
Disallow: /catalogues
Allow: /newsalerts
```

Это запись означает, что файл withoutrobots.php не должен индексироваться какими-либо поисковыми роботами, т.е. кто-то очень хотел его спрятать, но сделал это не так, как надо было:)
Переходим к этому файлу:



Полезные интернет-ресурсы

- <https://vserosolimp.edsoo.ru> - Официальный сайт ВсОШ
- <https://vsosh.miem.hse.ru/main/> - Высшая школа экономики
- <https://zsfond.ru/vsosh/regionalnyj-etap/tehnologiya-regionalnyj-etap/> - Фонд «Золотое сечение» (методика оценки и ключи)
- <https://ikb.mtuci.ru> - Межрегиональная олимпиада школьников им. И.Я. Верченко по информатике и компьютерной безопасности
- <https://ctfd.io> - фреймворк Capture The Flag для обучения разработчиков и студентов
- <https://stepik.org/course/132488/syllabus> - Базовый курс по CTF
- <https://stepik.org/course/61237/syllabus> - Task-Based CTF для новичков (недоработан)
- <https://www.dcode.fr> - это универсальный сайт для расшифровки закодированных сообщений, решения головоломок и многого другого
- <https://www.youtube.com/watch?v=VCoB1P3kIW0> – разбор заданий CTF "Новый учитель новой информатики. Перезагрузка" 2020 (две части)
- <https://github.com/acisoru/mircrypto> - ответы квиз-турнира Мир Крипто
- <https://sites.google.com/view/ctftraineronline> - сайт с заданиями CTF Хашимовой Дианы ученицы 9-2 класса МАОУ «Гимназии №80 г.Челябинска»



Кажется,
вы интересуетесь
инфобезом.
ДОБРО ПОЖАЛОВАТЬ!

Интересные задания

Письмо?

Не кажется ли Вам оно каким-то странным?

Может быть, ему не хватает цвета?

Поиграем с заливкой? В ответе напишите полное имя агента.

