

Урок 9. Отчет по домашнему заданию

1. Найти нешифрованный HTTP-сайт, где есть регистрация и логин. Отправить фейковые данные. Сможет ли злоумышленник перехватить пароль?

При попытке входа на странице <http://samlib.ru/cgi-bin/login> с фейковыми данными:

Login: leaked_login

Password: leaked_password

Журнал "Самиздат": Управление

["Самиздат": \[Регистрация\] \[Найти\] \[Рейтинги\] \[Обсуждения\] \[Новинки\] \[Обзоры\] \[Помощь\] \[Техвопросы\]](#)

ВНИМАНИЕ! Для правильной работы системы авторизации в Вашем браузере должна быть разрешена поддержка cookies. Она разрешена по умолчанию, если Вы не отключали ее специально. [Забыли пароль? Вам сюда](#)

Если вы зарегистрированный пользователь, введите свой login и пароль:

Login (Логин):

Password (Пароль):

Или, если Вы новичок, зарегистрируйтесь:

Ваш логин для входа (login name, только латинские буквы и цифры)

Пароль (только латинскими буквами и цифрами)


E-mail (Не публикуется. На него высылается забытый пароль)

В Wireshark был отслежен POST запрос, по протоколу http. В теле запроса содержались логин и пароль в открытом виде.

Вывод: данные, переданные по незашифрованному протоколу http могут быть перехвачены злоумышленником.

2. Найти нешифрованный HTTP-сайт со множеством картинок. Рекомендуются использовать Google Chrome. Сколько TCP-соединений будет открыто и почему?

Была загружена страница <http://begin-english.ru/images/>



Begin English

Теория

- [С чего начать](#)
- [Самоучитель](#)
- [Грамматика](#)
- [Слова](#)

Практика

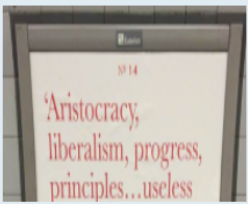
- [Аудио](#)
- [Видео](#)
- [Статьи](#)
- [Топики](#)
- [Тесты](#)
- [Радио](#)
- [Картинки](#)
- [Форум](#)
- [Перевод песен](#)
- [Подборки слов](#)
- [Разговорник](#)
- [Переводчик](#)
- [Анекдоты](#)
- [Тексты англ.](#)
- [Озвучка](#)
- [еще...](#)





Английский язык в картинках

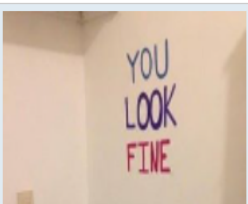
В этом разделе собраны различные картинки на английском, фотоприколы, смешные надписи на фото и картинках, которые помогут набрать **словарный запас по английскому** и просто весело провести время. Изучайте английский с удовольствием!

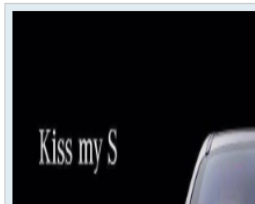
Возможно, некоторые из этих картинок вы уже видели в Интернете. Обычно бывает так: кто-то опубликовал картинку с английской надписью на форуме, при этом в лучшем случае 30% оценили юмор, а остальным пользователям, без знания английского, остается только догадываться в чем прикол. Знакомо, да?))




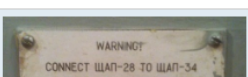


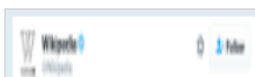















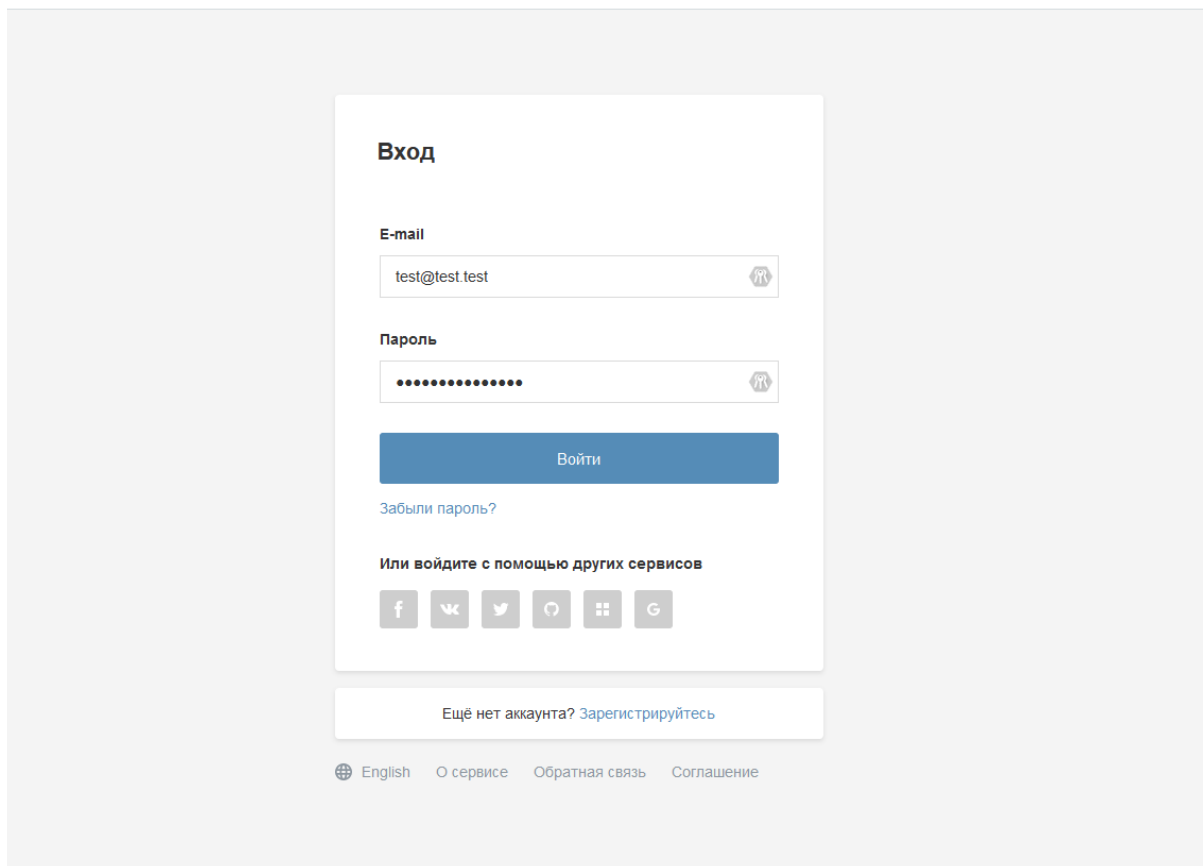
Доставка доступна только для комплектов сим-карт с технологией саморегистрации (недоступно для ряда регионов). Приложение биллайн (12+) – для абонентов биллайн (физ. лиц). Правила использования сервисами могут изменяться. Пополнение счета осуществляется в соответствии с правилами услуги «Онлайн-платеж». ПАО «ВымпелКом», РФ, 127083, г. Москва, ул. 8 Марта, д. 10, стр. 14, ОГРН 1027700166636. Подробнее о сервисах, территории доставки, об ограничениях при пополнении баланса – на beeline.ru

В Wireshark по фильтру `ip.addr == 5.9.97.143 && http` были отслежены TCP сессии. Была открыта 21 сессия. Несколько сессий было открыто для ускорения отображения страницы. Страница отображается после загрузки js файлов, css файлов и картинок со страницы и несколько сессий позволяют загружать составные части страницы одновременно.

3. Повторите п.1 с TLS. Вопрос тот же.

При попытке входа с фальшивыми данными на странице
https://account.habr.com/login/?state=18f2465267177af6a94f0cce8fde2047&consumer=habr&hl=ru_RU

Хабр Аккаунт

The image shows a screenshot of the Habr login page. At the top, it says "Хабр Аккаунт". Below that is a white login form with the title "Вход". It contains two input fields: "E-mail" with the value "test@test.test" and "Пароль" with masked characters. There is a blue "Войти" button. Below the button is a link "Забыли пароль?". Underneath is a section "Или войдите с помощью других сервисов" with icons for Facebook, VK, Twitter, GitHub, and Google. At the bottom of the form is a link "Ещё нет аккаунта? Зарегистрируйтесь". At the very bottom of the page, there are links for "English", "О сервисе", "Обратная связь", and "Соглашение".

В Wireshark были отслежены TCP соединения с сайтом habr.com . Данные в сессиях зашифрованы. Имея только перехваченный трафик с сайтом, перехватить пароль злоумышленник не сможет.