КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

КЛИКДЖЕКИНГ ДЛЯ ДЕАНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ

ИЛЬДАР КУДАШЕВ

МОСКВА

Вступление

Кликджекинг(социальный фишинг) – технология обмана посетителей сайтов, которая состоит в том, что на страницу сайта наслаивается другая, невидимая информация, которая однако активна и совершает действия против пользователя(Получая его конфиденциальную информацию, подписывая на платные сервисы и так далее). Элемент управления (кнопка, ссылка), необходимый для осуществления требуемого действия, совмещается с видимой ссылкой или кнопкой, нажатие на которую ожидается от пользователя. При этом человек ни о чём не догадается, поскольку с его стороны произошло лишь нажатие на элемент веб-страницы. Обычно, кликджекинг(А ведь он является разновидностью фишинга) настраивается на копии популярного ресурса для большей конверсии.

Интересные Разновидности социального фишинга :

- **Лайкджекинг** нацелен на сбор лайков в социальных сетях — пользователи фактически ставят отметку «Мне нравится» на нужной странице. Это может увеличить базу пользователей и поднять просмотры страницы.
- **Курсорджекинг** — курсор мыши находится не там, где он отображается в окне браузера, то есть пользователь может щелкнуть на чем-то одном, в то время как фактический курсор щелкает в другом месте.
- **Кукиджекинг** - Разновидность, ориентированная на cookie-файлы.

Общие моменты

Если говорить о деанонимизации, то с помощью кликджекинга можно получать также аккаунты социальных сетей.
Рассмотрим мы этот процесс на примере ВКонтакте.
Сразу оговорюсь, что мы будем получать не пароли, номера телефонов, скрытые электронные почты, а лишь публичные данные в виде ID, имени и аватара. Однако даже такие данные могут оказаться ключевыми при поимке киберпреступника, о чём я расскажу позже.
Для начала нужно создать сайт, на который пользователь будет завлечён. Создавать его стоит на основе интересов, убеждений, предпочтений человека, если таковые имеются, если нет - использовать более универсальные тематики.
Получать данные профиля мы будем используя официальный виджет для авторизации от соц.сети.
В методике не будет описания настройки отправки полученных данных, тут кому как удобнее - Можно в базу добавлять, или присылать сразу сообщением в телеграм.

Теперь нужно добавить на сайт виджет авторизации через ВК. Процесс подробно описан в официальной методичке : https://dev.vk.com/widgets/auth
Никакой верификации - к любому пустому сайту можно приделать этот функционал, проверено собственным опытом.

Если кратко, то добавить код в head :

```
<script src="https://vk.com/js/api/openapi.js?169" type="text/javascript"></script>
```

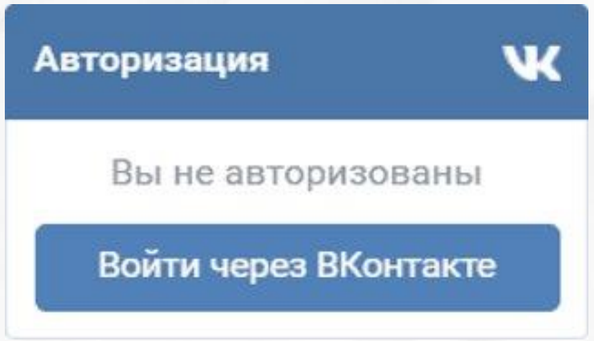
Этот в body :

```
<div id="vk_auth"></div>
<script type="text/javascript"> window.onload = function () { VK.init({apiId:идентификатор}); VK.Widgets.Auth('vk_auth', {}); }
</script>
```

Теперь нужно найти внизу страницы apiId, привязанный к аккаунту.
Находится он там, где замазано моё значение :

```
<!-- Put this script tag to the <head> of your page -->
<script
 type="text/javascript"
 src="https://vk.com/js/api/openapi.js?168"
 charset="windows-1251"
></script>
<script type="text/javascript">
 VK.init({ apiId: [redacted] });
</script>
```

После добавления кода, на сайте у вас должна появится такая кнопка :



Виджет успешно добавлен!

Обычный веб-разработчик на этом этапе бы и остановился, но нам нужно сделать кнопку авторизации невидимой и вставить поверх нее какое-нибудь привлекательное изображение, чтобы пользователь прошел авторизацию, не заметив этого. Например, можно поставить поверх какую-то другую кнопку. Такой вариант событий однако возможен только если пользователь до этого уже заходил в аккаунт с браузера и сохранял данные.

1) Зайдите в браузер
2) Наведите курсор на кнопку авторизации и нажмите правую кнопку мыши
3) Нажмите "Просмотр кода"
4) Теперь найдите следующий абзац :

```
... ▼<iframe name="fXD821bc" frameborder="0" src="https://vk.com/widget_auth.ph
    p?app=8234333&width=200px&_ver=1&url=http%…f99d6a2…&title=My%20first%20styl
    ed%20page&1826898d7b4" width="200" height="134" scrolling="no" id="vkwidget
    1" style="overflow: hidden;height: 116px;opacity: 0.0;"> == $0
```

Теперь чтобы кнопка стала невидимой в окне CSS надо добавить:

opacity : 0.0

По итогу должно получится :

```
element.style {
    overflow: ▸ hidden;
    height: 116px;
    opacity: 0.0;
}
```

Ну а теперь мы просто копируем код, составленный во фрейме(С уже прописанной прозрачностью) и вставляем его в код сайта(находящийся на хостинге непосредственно), соответственно удаляя весь код добавленный ранее для подключения виджета.
Таким образом, мы всё так же взаимодействуем с ВК, однако процесс отображения фрейма(кнопки)происходит на нашей стороне и мы имеем возможность этот фрейм изменять.

Хочу отметить, что эта уязвимость скорее всего никогда не будет исправлена, так как по правилам платформы таковой и не является.
Но зачем вообще нужна эта "фича" и как её применить в деле? - Многие люди пытаются сохранять анонимность, при этом оставляя свои учётные записи с опубликованными фото, списками друзей и так далее.
Данный метод позволяет подобных личностей раскрывать.

А что насчёт закона?

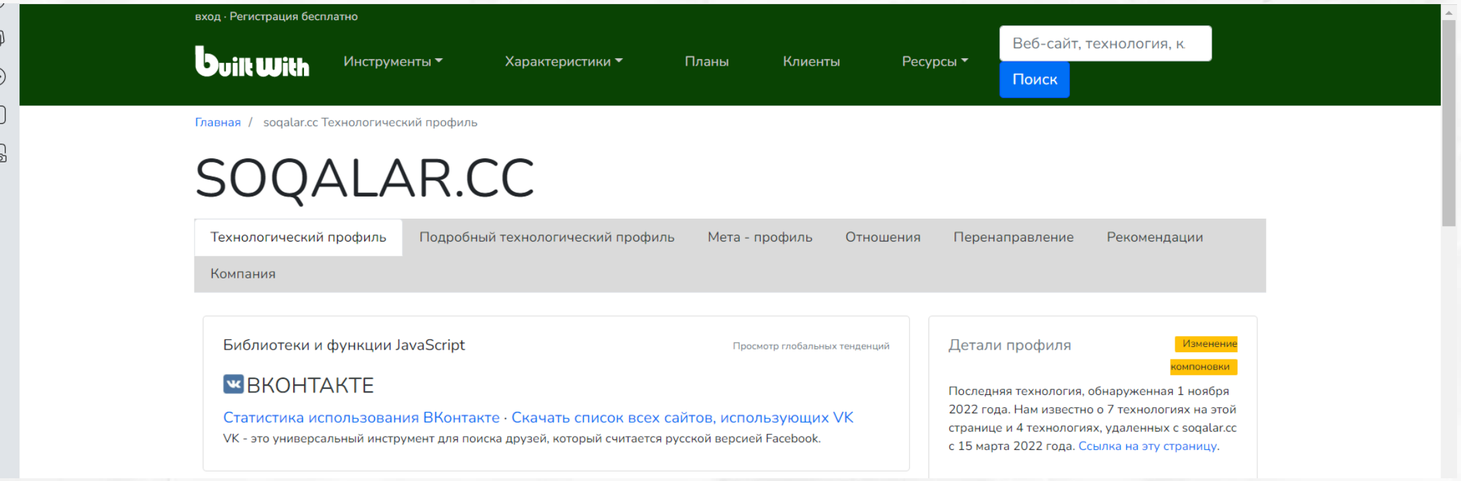
- Всё чисто, ведь получаемые данные никак не могут являться персональными данными.

Для убеждения приведу перечень информации, передаваемой запросом(Цитируя официальное руководство от ВКонтакте) :

- *uid (integer) — идентификатор пользователя;*
- *first_name (string) — имя;*
- *last_name (string) — фамилия;*
- *photo (string) — URL фотографии профиля пользователя шириной 200 px;*
- *photo_rec (string) — URL фотографии профиля пользователя шириной 50 px;*
- *hash (string) — служебный параметр, необходимый для проверки авторизации на удаленной стороне.*

Обезопасим себя от кликджекинга

Существуют сайты, которые обнаруживают используемые на сайте технологии, в том числе и ВК.
Один из таких - https://builtwith.com/



Если сервис нашёл что-то, проверьте, нет видных элементов, связанных с этой технологией на сайте. Если нет - заходите в "Просмотр кода" и ищите по ключевому словосочетанию - opacity : 0.0
Возможно, вы наткнулись на кликджекинг

Готов ответить
на ваши вопросы

QR-Код на вступление
в телеграм канал

E-mail: onlinesearchagency@gmail.com
Telegram - @DigitalScouter