УДК 004

ИССЛЕДОВАНИЕ CLICKJACKING АТАК

Полковников И.С.
Научный руководитель: Мыцко Е.А., ассистент кафедры ВТ ИК ТПУ

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: Polkovnikov.Ilya.95@mail.ru

В данной работе приведено исследование clickjacking атак, рассмотрены возможные способы защиты от данного типа атак. Приведена реализация сервиса проверки по двум наиболее популярным ошибкам – не эффективная защита и отсутствие заголовка X–Frame–Options.

This article analyses The Clickjacking attacks and possible ways to defend against them. Also it provides implementation of service which detects the two most common mistakes: the inefficient defence and the absence of X-Frame-Options header.

Key words: *web application vulnerabilities, clickjaking.*

Ключевые слова: у*язвимости веб-приложений, clickjaking.*

Из-за высокого темпами развития интернета возникает всё больше и больше уязвимостей с которыми необходимо бороться. В последнее время стали набирать популярность необычные варианты атак, например, clickjaking.

На русский язык clickjaking можно перевести как «угон клика». Так же в различных источниках можно встретить варианты «перекрытие iframe» и «подмена пользовательского интерфейса».

Данной атаке подвергались такие известные Интернет-ресурсы, как Facebook, Vkontakte, PayPal, и другие.

Основная идея атаки заключается в следующем:

- На атакующей странице посетителю предлагается безобидное действие (посмотреть видео ролик или перейти по ссылке на интересующий ресурс).
- Поверх этого элемента размещается прозрачный iframe с атакуемой страницей.
- Взаимодействуя с атакующим сайтом, посетитель на самом деле взаимодействует с атакуемым.

В данной работе рассмотрены варианты защиты по степени их эффективности.

Самый простой способ защиты – это JavaScript код который запрещает отображение страницы внутри iframe разрушая его (рис. 1).

```
1 if (top != window) {
2   top.location = window.location;
3 }
```

Рис. 1. Старый метод защиты

В данный момент это код больше не является эффективной защитой. Все современные браузеры поддерживают атрибут sandbox. При помощи данного атрибута можно разрешить

во фрейме скрипты (allow–scripts) и отправку форм (allow–forms), но запретить top–навигацию (не указать allow–top–navigation). «Защищённый» iframe будет выглядеть примерно так, как показано на рис. 2.

```
<iframe sandbox="allow-scripts allow-forms" src="example.html"></iframe>
```

Рис. 2. Защищенный iframe

Можно сделать вывод, что эта защита не способна противостать реальной атаке, а так же может скомпрометировать атакуемый сайт.

Рассмотрим подробней более современный способ защиты при помощи заголовка X–Frame–Options. Этот заголовок позволяет разрешить или запретить отображение страницы, если она открыта во фрейме.

У данного заголовка может быть три значения:

- SAMEORIGIN
- DENY
- ALLOW–FROM domain

Clickjaking атаки особенно опасны, поскольку, проектируя интерфейс сайта, обычно никто и не задумывается о том, что клик от имени пользователя может сделать злоумышленник.

Учитывая результаты исследования, был реализован онлайн сервис который проводит проверки по двум наиболее популярным ошибкам – не эффективная защита и отсутствие заголовка X–Frame–Options.

Сервис реализован при помощи библиотеки CURL для языка программирования PHP. По окончанию проверки пользователю предлагается перейти по ссылке «Подробней» и детальней ознакомиться с уязвимостью. На рис. 3 представлен пользовательский интерфейс разработанного сервиса. На рис. 4 представлен пример результата проверки на уязвимость.

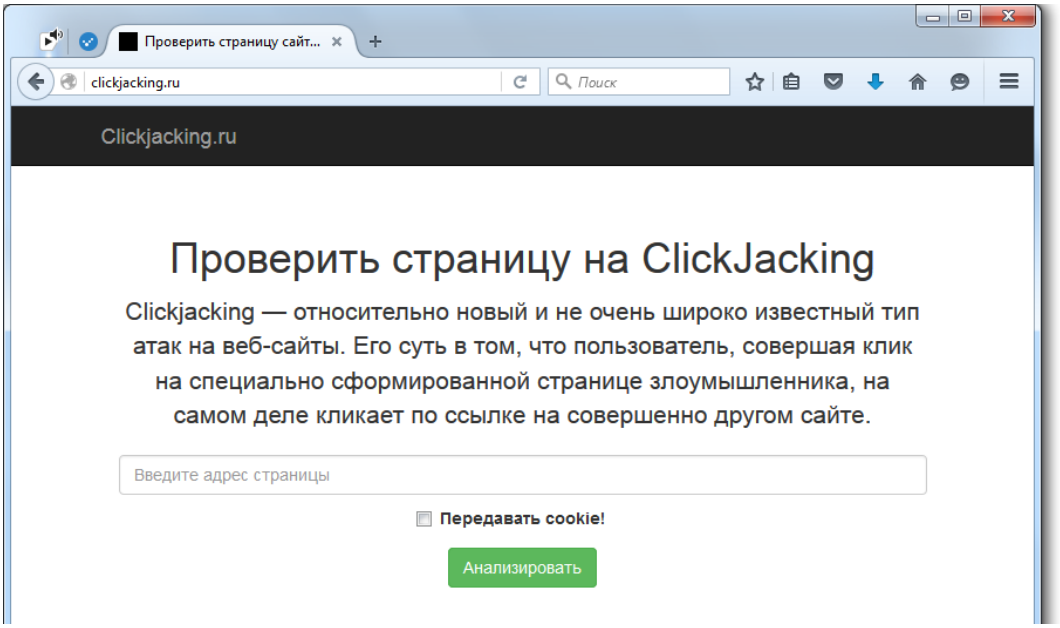

Рис. 3. Пользовательский интерфейс

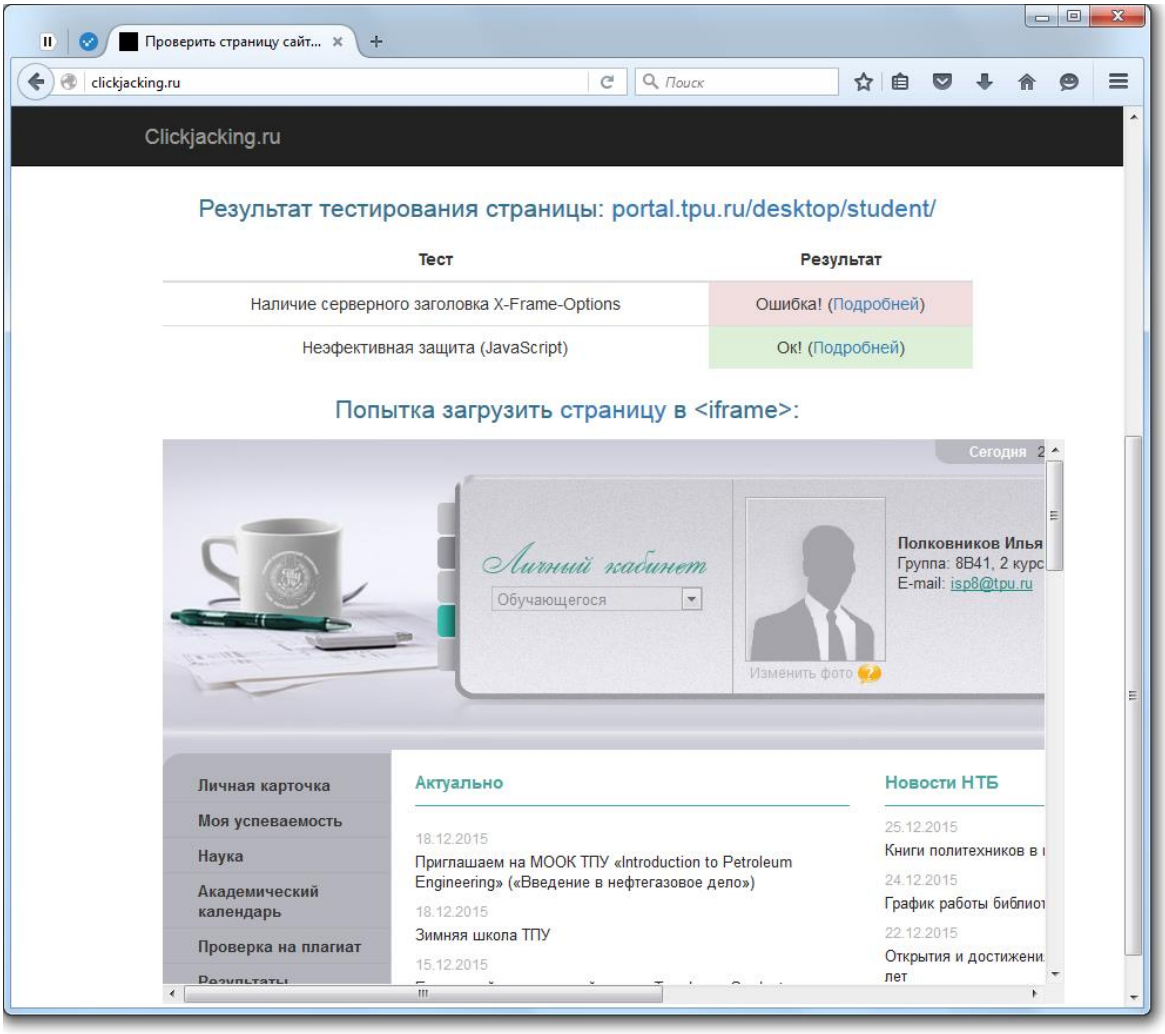

Рис. 4. Результат проверки

Список литературы

1. Атака Clickjacking и защита от неё. [Электронный ресурс]. URL: https://learn.javascript.ru/clickjacking/. [Дата обращения: 25.12.15].
2. За нами следят или clickjacking для бизнеса. [Электронный ресурс]. URL: http://habrahabr.ru/post/238565/. [Дата обращения: 25.12.15].
3. Кликджекинг – Википедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ Кликдже-кинг/. [Дата обращения: 25.12.15].
4. Легальный Clickjacking ВКонтакте. [Электронный ресурс]. URL: http://habrahabr.ru/post/228617/. [Дата обращения: 25.12.15].
5. The Clickjacking attack, X-Frame-Options. [Электронный ресурс]. URL: http://javascript.info/ tutorial/clickjacking/. [Дата обращения: 25.12.15].