Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье
Дата лекции: __01.10.2020_____ Дата сдачи: ___15.10.20_____

Выполнил(а) Сенина М.М., № группы *P3112*, оценка _____
Фамилия И.О. студента — не заполнять

Название статьи/главы книги/видеолекции
Фундаментальная уязвимость HTML при встраивании скриптов

ФИО автора статьи (или e-mail)	**Дата публикации (не старше 2018 года)**	**Размер статьи (от 400 слов)**
Александр Карпинский (https://habr.com/users/homm/)	*"12"_февраля 2018 г.*	*2034 слов*

Прямая полная ссылка на источник и сокращённая ссылка
https://habr.com/ru/post/348558/

Теги, ключевые слова или словосочетания
HTML, уязвимость

Перечень фактов, упомянутых в статье

1. *Уязвимость языка гипертекстовой разметки HTML состоит в том, что у HTML и встраиваемых в него скриптов, разные синтаксисы и HTML не всегда может правильно определить, где начинаются и заканчиваются теги, в которых лежат скрипты (JavaScript как самого частого случай, вообще не только его).*
2. *Эта уязвимость возникает, если после последовательности </script> в скрипте идёт считывание данных, введённых пользователем, это позволяет злоумышленнику ввести в поле зловредный код.*
3. *Так же опасна ситуация, когда в скрипте присутствуют символы "<!--", обозначающие в HTML многостраничный комментарий, т.к. парсер HTML будет воспринимать весь последующий код, как комментарий.*
4. *Выходит, что чтобы HTML был безопасным его автор должен точно знать, что за скрипт он встраивает и имеет возможность его менять, чтобы экранировать строки вызывающие ошибки, что, очевидно, возможно далеко не всегда.*

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)

1. *Ошибку (2) разработчик может заметить благодаря подсветке синтаксиса HTML.*
2. *Если данные из строк скрипта дальше разбирать в JSON, можно экранировать, нежелательные строки уже в самом JSON, потому что на его структуру методы экранирования HTML случайно повлиять не могут.*
3. *Автор предлагает ввести новый тег - <safescript> который будет полностью подчиняться синтаксису HTML, и будет автоматически экранировать код скрипта по правилам HTML.*

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)

1. *Ошибку (3) разработчику редактор не подсветит и никак в этом не поможет.*
2. *(3) отличие от (2) может встретиться и в самом коде, не только в строковых литералах.*
3. *Приходится подстраивать JavaScript под HTML, чтобы обезопасить ситуацию, что очень неудобно.*

Ваши замечания, пожелания преподавателю *или* анекдот о программистах[1]
— Папа, а хакеры хорошо получают?
— Хорошо, сынок, лет эдак пятнадцать…