Лабораторная Работа #3

ПАИТСЗИ  
9 группа  
Крагель Алина

1. Название задания уровня: Warmup

Отсутствует проверка на вредоносность вводимого контента. Подбираем правильный ввод для *alert*, в данном случае – закрываем скобки с обеих сторон от *alert*

1. Название задания уровня: Adobe

См. п. 1, но в данном случае первую закрывающую кавычку экранируем, после alert вводим для слеша для комментирования остатков строки *console.log*

1. Название задания уровня: JSON

Вводимая строка напрямую встраивается в DOM, поэтому можем закрыть выполнение скрипта в *console.log*, после чего добавить начало скрипта с *alert*

1. Название задания уровня: Markdown

Открывающийся тег и кавычки заменяются на html-коды соответствующих символов. Взламываем последнее регулярное выражение, использующее двойные скобки выражения. Первый параметр – название *gif* (содержание неважно), второй же начинается с http:// как *url*, после внедряется обработчик события ошибки *onerror* и исполняемый код (*alert*, например)

1. Название задания уровня: DOM

Вставляет ключевое слово для генерации начала блока комментирования, вторым после решетки вставляем закрытие блока и скрипт для выполнения

1. Название задания уровня: Callback

Взламывается инициализация *userdata*. В случае, если не определено значение, подставляется *alert*

1. Название задания уровня: Scandia

Передаем закрывающиеся теги и открывающий тег фрейма, куда на момент инициализации в виде *uri*-кодировки передаем исполняемый код, дабы обойти перевод в заглавные символы

1. Название задания уровня: Template

*\u003* и *\u003e* – символы ‘<’ и ‘>’ соответственно, используем символьные коды в силу фильтрации их в скрипте, после добавляем *src* и обработчик *onerror*

1. Название задания уровня: JSON 2

Подставляем строку так, чтобы изъятие блока *</script* не нанесло потерь на выполнение основного скрипта

1. Название задания уровня: Callback 2

См. п. 6, но с иным типом открытия комментария

1. Название задания уровня: Scandia 2

Угловые скобки бракуются на ‘-’, строчные буквы переводятся в заглавные. Поэтому обратимся к нотации *JSFuck* (<http://www.jsfuck.com/>) для обхода ограничений

1. Название задания уровня: iframe

*youWon* не определен, в соответствии с этим, если есть определение, и оно не равно *False*, будет выполнен *alert(1)*. Каждый фрейм имеет окно глобального объекта, а имя является атрибутом-членом окна. Должно сработать *name=’youWon’,* но у меня не работает

1. Название задания уровня: TI(S)M

Подставляем блок условного кода с комментированием и открывающий тег

1. Название задания уровня: JSON 3

Передаваемая основному методу строка делится по #, после чего внутренняя функция дублирует вывод *console.log*, в добавок ко всему, теги начала и конца скрипта считаются за один

1. Название задания уровня: Scandia 3

См. п. 11

1. Название задания уровня: RFC4627

Метод фильтрует кучу символов, обходя при этом *Eaeflnrunrstu*. Используем *ValueOf* для *self*, определяя через *the\_easy\_but\_expensive\_way\_out* дважды, ибо после одного применения на возврате *alert(0)*

1. Название задания уровня: Well

Методом фильтруются нужные для *alert* скобки, так что используем метод преобразования из кодировки *utf-16* в символы для скобок

1. Название задания уровня: No

И снова обход *replace* + пометка об отсутствии вызова функции

1. Название задания уровня: K’Z’K

См. п. 11

1. Название задания уровня: K’Z’K

А тут уже п. 11 не действует, ибо фильтруется *!*. Передаем пустую строку через двойное написание, из ");[]["pop"]["constructor"]('alert(1)')()// получаем то, что в ссылке.

1. Название задания уровня: K’Z’K

Опять фильтруются { } ! = < > \, не можем использовать шестнадцатеричный код для обхода

1. Название задания уровня: Fruit

Создаем элемент на основе ввода и удаляем атрибут элемента. Цикл использует *attribute.length* как условие оценки. Это значение представляет собой количество атрибутов в элементе, которое изменяется динамически. Так что просто атрибут перед onload

1. Название задания уровня: Fruit 2

См. п. 22

1. Название задания уровня: Fruit 3

Тут итератор уменьшается в условии внутри цикла, не уверена я что-то, как решить, но варианты двух пунктов выше минус

1. Название задания уровня: Capitals

Во-первых, разделение строки снова по # происходит. Должны выполнить вход в условие во внутренней функции нахождения столицы. Здесь нам помогает значение constructor, тогда в условие нахождения по году передается необходимый скрипт

1. Название задания уровня: Quine

Здесь нужно передать строку, которая каким-то образом во внутренней функции будет отличаться от самой себя, не решила

1. Название задания уровня: Entities

Снова задача обойти замену символов, их тут мало, так что решаемо

1. Название задания уровня: %level%;

Ход через метод replace, где спец символы можно выразить как:  
$` - вставка подстроки влево

$' – вставка подстроки вправо

Решение: https://alf.nu/alert(1)?world=alert&level=i3CRFz2zJKrWV%2Fa-alert-UE0QQjL4riKqBKfSC6jO#accesstoken=ya+fLCVn20m/Pz16Mc9B