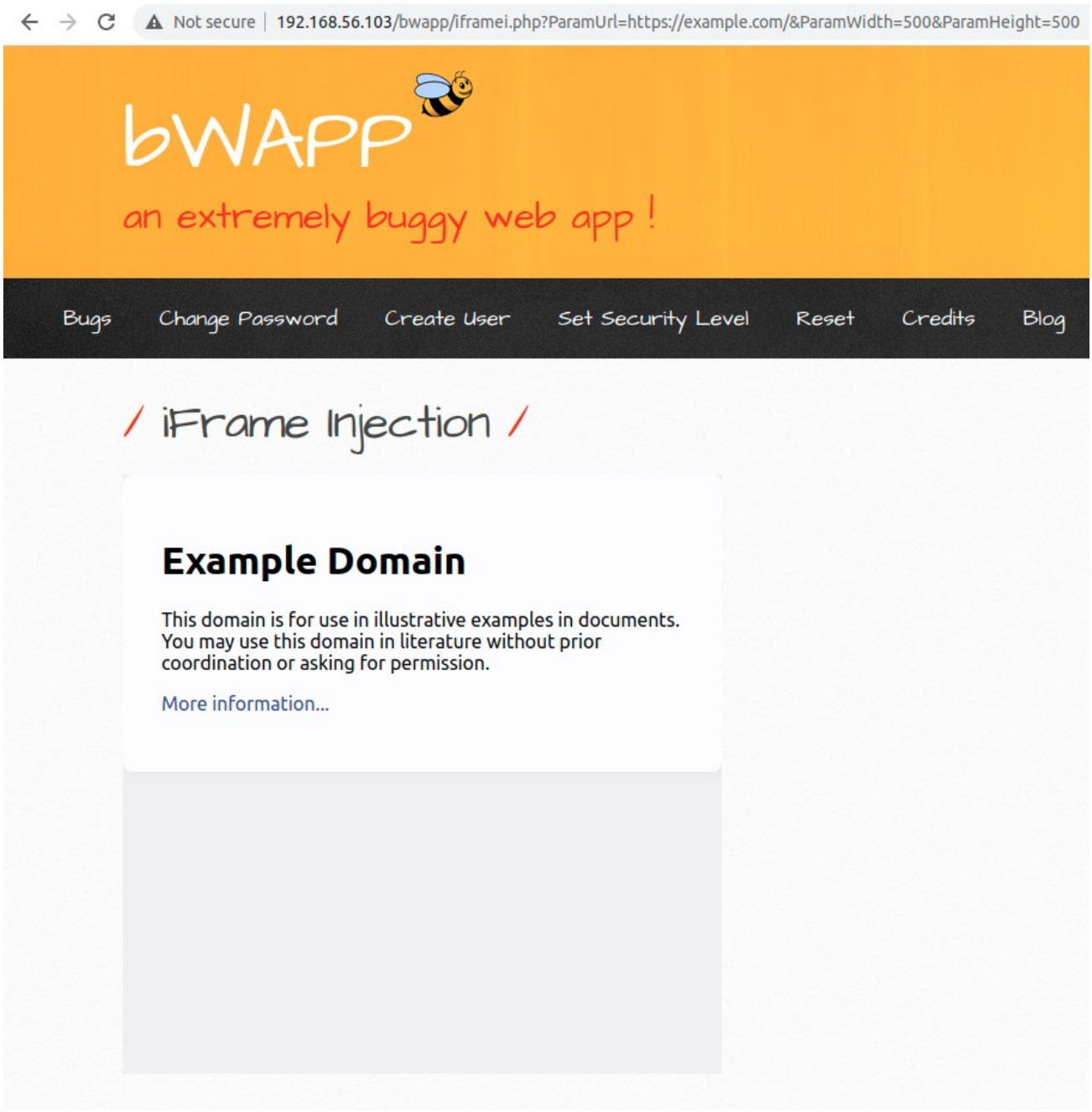
Урок 8. Прочие уязвимости на клиенте

Задание 1:

Изучите пример страницы iframe injection проекта bWAPP (iFrame Injection), уровень сложности Low. Какие можно провести атаки на данную страницу?

Ответ:

Есть возможность загрузить во фрейме вредоносную страницу, указав в GET-параметре **path** ссылку на evil-page.



Задание 2:

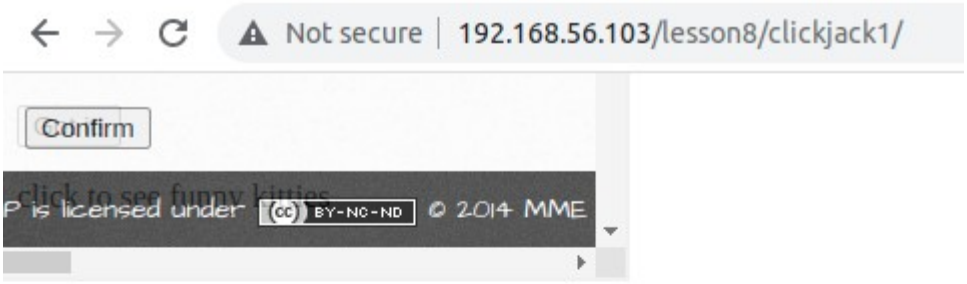
Изучите пример страницы Clickjacking проекта bWAPP (ClickJacking (Movie Tickets)), уровень сложности Low. Какие можно провести атаки на данную страницу?

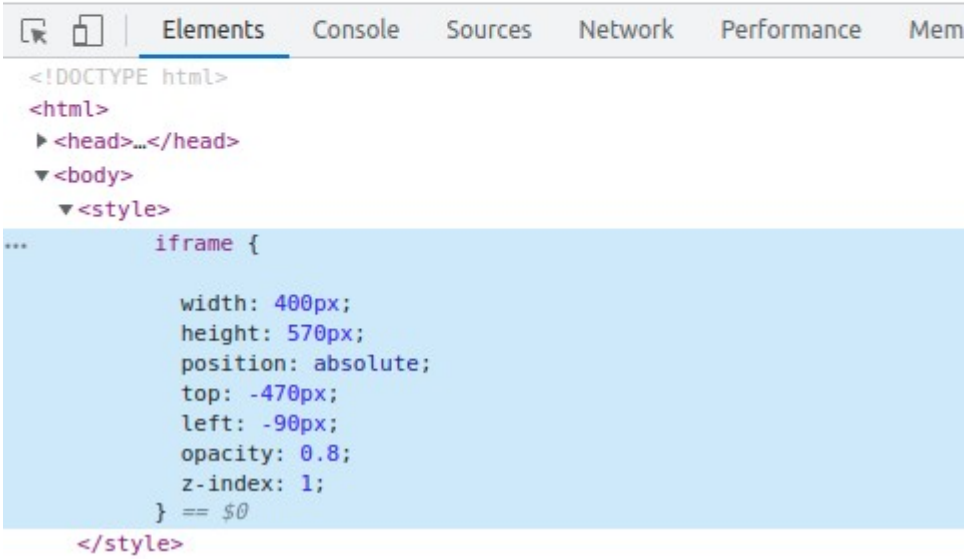
Ответ:

Угон клика, как не страно.

Думаешь что посмотришь смешных котов

А на самом деле ты что-то купил…





Задание 3:

Изучите пример страницы, содержащей возможность редиректа, из проекта OWASP Mutillidae (Owasp 2013 – A10 – Credits). Какие можно провести атаки на данную страницу?

Ответ:

Атаки Open Redirect.

На сервере никак не проверяется ссылка, указанная в соответствующем параметре. Её можно заменить на любую другую.

Рекомендуется использовать отдельные сценарии для редиректа, проверять Referer, предупреждать пользователя о редиректе.