Задание выполнил студент группы 2345 Романенко Кирилл

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

Clickjacking: Тип атаки, при котором хакер использует невидимый iframe, чтобы обманом заставить пользователей нажать на кнопку или ссылку, которая выполняет вредоносное действие, такое как загрузка вредоносного ПО или обмен личной информацией.

Кража учетных данных: Злоумышленник может внедрить iframe на страницу входа в систему, чтобы захватить учетные данные пользователя, включая имена пользователей и пароли. Украденные учетные данные могут быть использованы для доступа к конфиденциальной информации, такой как банковские счета или учетные записи электронной почты.

Доставка вредоносного ПО: Злоумышленник может внедрить в iframe вредоносный код, который автоматически загружает и устанавливает вредоносное ПО на устройство жертвы. Затем вредоносная программа может быть использована для кражи данных, мониторинга активности или удаленного управления устройством.

Фишинг: Злоумышленник может использовать iframe для перенаправления пользователей на поддельную страницу входа в систему или другой фишинговый сайт, предназначенный для кражи личной информации, такой как номера кредитных карт или социального страхования.

Важно отметить, что внедрение iframe - это лишь один из многих потенциальных векторов атаки, которые могут быть использованы для компрометации веб-сайта или приложения. Крайне важно внедрить строгие меры безопасности, такие как использование методов безопасного кодирования, регулярное обновление программного обеспечения и внедрение протоколов безопасности, таких как HTTPS, для защиты от кибератак.

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

Нажатие на скрытую кнопку: страница может содержать скрытую кнопку, о которой пользователь не знает. Злоумышленник может наложить прозрачный слой на кнопку и сделать так, чтобы она выглядела так, как будто пользователь нажимает на что-то другое, например, на безобидное изображение. Когда пользователь нажимает на изображение, он фактически нажимает на скрытую кнопку, которая может выполнить непреднамеренное действие, например, отправить конфиденциальную информацию.

Наложение фрейма: Злоумышленник может использовать iframe для наложения законного веб-сайта на вредоносный. Пользователь может полагать, что он взаимодействует с законным веб-сайтом, но на самом деле он взаимодействует с вредоносным веб-сайтом. Это может позволить злоумышленнику украсть конфиденциальную информацию, такую как учетные данные для входа в систему или номера кредитных карт.

Социальная инженерия: Злоумышленник может использовать методы социальной инженерии, чтобы обманом заставить пользователя нажать на кнопку или ссылку, которые выполняют непреднамеренное действие. Например, злоумышленник может создать убедительное поддельное сообщение об ошибке, в котором пользователю предлагается нажать на кнопку, чтобы устранить проблему. Когда пользователь нажимает на кнопку, он выполняет непреднамеренное действие, например загружает вредоносное ПО на свой компьютер.

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

XSS: Злоумышленник может внедрить вредоносные скрипты на страницу кредитов проекта OWASP Mutillidae, которые могут быть выполнены ничего не подозревающими пользователями, посещающими страницу. Это может позволить злоумышленнику украсть токены сеанса пользователя, учетные данные и личную информацию.

SQL-инъекции: Используя уязвимость страницы Credits проекта OWASP Mutillidae, злоумышленник может вводить вредоносные SQL-запросы в базу данных, потенциально позволяя им получать доступ, изменять или удалять конфиденциальную информацию из базы данных.

CSRF: Злоумышленник может создать вредоносную веб-страницу, которая обманом заставляет пользователей отправлять запрос на страницу кредитов уязвимого проекта OWASP Mutillidae, что приводит к непреднамеренным действиям.

SSRF: Злоумышленник может использовать уязвимость страницы кредитов проекта OWASP Mutillidae, чтобы заставить сервер веб-приложений отправлять запросы на другие внутренние или внешние серверы, что приводит к раскрытию информации или краже данных.

RCE: Злоумышленник может воспользоваться уязвимостью страницы Credits проекта OWASP Mutillidae для выполнения произвольного кода на сервере веб-приложений, что может привести к полному контролю над сервером.