Эксплуатируем Open Redirect. Как открытый редирект использует для фишинга и DDoS

Автор: Ivanov Andrey — 14 февраля — 14:00

Предисловие статьи

Что Вы прочитаете в статье:
- Что такое Open Redirect?
- Как использовать Open Redirect?
- Как использовать Open Redirect для фишинга?
- Как использовать Open Redirect для DDoS?
- Как найти Open Redirect?
- Как исправить Open Redirect?

Что Вы должны знать:
- Основы HTTP
- Основы HTML
- Основы JavaScript

Привет, я — Andrey Ivanov, Senior Security Engineer. Я занимаюсь тестированием на проникновение и исследованиями уязвимостей. Сейчас я работаю в Positive Technologies. Ранее я занимался тестированием на проникновение в Positive Technologies, Kaspersky Lab, Yandex и ряде других компаний. Я — автор нескольких статей на Habr, выступаю на конференциях, пишу PoC-эксплойты и иногда выступаю в роли CTF-игрока.

Сегодня я расскажу Вам про такую уязвимость, как open redirect — и на примерах того, как злоумышленники могут использовать open redirect для фишинга и DDoS. Также я расскажу, как найти и исправить open redirect. Материал рассчитан на начинающих специалистов по информационной безопасности и разработчиков.

ВНИМАНИЕ

Все приведенные материалы предоставлены исключительно для ознакомления. Ни редакция журнала, ни автор статьи не несут ответственности за любой вред, нанесенный в результате использования данной информации.

Злоумышленник может использовать Open Redirect для фишинга и для DDoS. Open Redirect — это уязвимость, которая позволяет перенаправлять пользователя с одного сайта на другой. Злоумышленник может использовать open redirect для фишинга, чтобы обманывать пользователей и крадут их данные. Также open redirect может использовать для DDoS-атаки, чтобы перенаправлять трафик на сайт жертвы.

Сегодня я расскажу, как использовать open redirect для фишинга и DDoS — на примерах. Я покажу, как найти open redirect, как его использовать для фишинга и DDoS, как исправить open redirect. Материал рассчитан на начинающих специалистов по информационной безопасности и разработчиков. Я постараюсь сделать материал понятным даже для тех, кто только начинает изучать ИБ.

Что такое Open Redirect?

Open Redirect — это уязвимость, которая позволяет перенаправлять пользователя с одного сайта на другой. Злоумышленник может использовать open redirect для фишинга, чтобы обманывать пользователей и крадут их данные. Также open redirect может использовать для DDoS-атаки, чтобы перенаправлять трафик на сайт жертвы.

Например, если сервер использует параметр `redirect` для перенаправления, то злоумышленник может использовать такой URL, чтобы перенаправить пользователя на свой сайт:

```
https://example.com/login?redirect=https://evil.com
```

Если сервер не проверяет, куда перенаправляет пользователя, то злоумышленник может использовать open redirect для фишинга — например, отправить ссылку жертве, которая выглядит как ссылка на сайт example.com, но на самом деле перенаправляет на evil.com.

Злоумышленники используют Open Redirect?

Злоумышленники используют Open Redirect для фишинга, для DDoS-атак и для обхода фильтров. Open Redirect — это простая уязвимость, но она может быть использована для многих атак. Ниже я расскажу, как злоумышленники используют open redirect для фишинга и DDoS.

Open Redirect — простая уязвимость.

Злоумышленники используют Open Redirect для фишинга, для DDoS-атак и для обхода фильтров. Open Redirect — это простая уязвимость, но она может быть использована для многих атак. Ниже я расскажу, как злоумышленники используют open redirect для фишинга и DDoS.

Open Redirect для фишинга

Open Redirect — это уязвимость, которая позволяет перенаправлять пользователя с одного сайта на другой. Злоумышленник может использовать open redirect для фишинга, чтобы обманывать пользователей и крадут их данные. Например, если сервер использует параметр `redirect` для перенаправления, то злоумышленник может использовать такой URL, чтобы перенаправить пользователя на свой сайт:

```
https://example.com/login?redirect=https://evil.com
```

Если сервер не проверяет, куда перенаправляет пользователя, то злоумышленник может использовать open redirect для фишинга — например, отправить ссылку жертве, которая выглядит как ссылка на сайт example.com, но на самом деле перенаправляет на evil.com.

Open Redirect для фишинга — простая уязвимость, но она может быть использована для многих атак.

Open Redirect для DDoS

Open Redirect — это уязвимость, которая позволяет перенаправлять пользователя с одного сайта на другой. Злоумышленник может использовать open redirect для DDoS-атаки, чтобы перенаправлять трафик на сайт жертвы. Например, если сервер использует параметр `redirect` для перенаправления, то злоумышленник может использовать такой URL, чтобы перенаправить пользователя на свой сайт:

```
https://example.com/login?redirect=https://victim.com
```

Если сервер не проверяет, куда перенаправляет пользователя, то злоумышленник может использовать open redirect для DDoS — например, отправить ссылку жертве, которая выглядит как ссылка на сайт example.com, но на самом деле перенаправляет на victim.com.

Open Redirect для DDoS — простая уязвимость, но она может быть использована для многих атак.

Как найти Open Redirect?

Чтобы найти open redirect, нужно:
- Проверить все параметры, которые сервер использует для перенаправления.
- Проверить, что сервер не проверяет, куда перенаправляет пользователя.
- Проверить, что сервер не использует white-list для разрешенных перенаправлений.
- Проверить, что сервер не использует black-list для запрещенных перенаправлений.
- Проверить, что сервер использует только относительные пути, а не абсолютные.
- Проверить, что сервер использует только HTTPS, а не HTTP.
- Проверить, что сервер использует только доверенные домены, а не любые.
- Проверить, что сервер использует только доверенные пути, а не любые.

Чтобы найти open redirect, нужно проверить все параметры, которые сервер использует для перенаправления, и проверить, что сервер не проверяет, куда перенаправляет пользователя.

ВНИМАНИЕ

Предложение доступно только для участников

Абонент 12 Месяцев для любителей чтобы Обновить Свой Статус

Получите 12 месяцев на самые удобные условия! Цена всего 1000 рублей вместо 1320 рублей. Вы сэкономите 320 рублей. Не упустите свой шанс, пока акция доступна! Спешите!

1 год	1 месяц
1000 р.	120 р.
Подробнее	Подробнее

или

Абонент 12 Месяцев Бесплатно

Бесплатный доступ к ресурсу на 12 месяцев по цене 0 рублей. Абонент 12 месяцев бесплатно. Вы сэкономите 1320 рублей. Не упустите свой шанс, пока акция доступна! Спешите!

Подробнее

Скрыть Больше не показывать

Abonent 12
Абонент 12 месяцев

Профиль Лента Диалоги Друзья Сообщества Фото Сообщения Видео

Все Комментарии 4 Сначала новые

Показать ответы на комментарии

Сортировка: Лучшие Новые Старые

Kirill Sokolov 2 часа назад
Спасибо! Все рассмотренные Open Redirect у меня есть на сервере, но я не знал, что с ними можно сделать DDoS.
Ответить · Нравится · 1

Mikhail Petrov 1 час назад
Статья — 5 из 5. Единственное замечание: в разделе «Как исправить» не хватает примера для Nginx. Apache есть, Nginx нет — а у половины продакшенов как раз Nginx.
Ответить · Нравится · 2

Olga Nikitina 1 час назад
Спасибо! Я тестировщик, и мне часто приходится проверять open redirect. Раньше я делала это вручную, теперь у меня есть чек-лист. Статья сохранена.
Ответить · Нравится · 1

Andrey Ivanov 1 час назад
Mikhail, спасибо! Nginx — это хорошо, добавлю в следующей версии. Kirill, DDoS через open redirect — редкая, но красивая атака. Olga, чек-лист — отлично!
Ответить · Нравится · 3