Python & Django

Безопасность

Антон Мазун

Антон Мазун

Full-stack python developer

Тренер-консультант CBS

Безопасность

Виды атак :

- Межсайтовый скриптинг (XSS)
- Межсайтовая подделка запроса(CSRF)
- SQL-injection
- SSL/HTTPS

Межсайтовый скриптинг (XSS)

Тип атаки на веб-системы_, заключающийся во внедрении в выдаваемую веб-системой страницу вредноносного кода .

Специфика подобных атак заключается в том, что вредоносный код может использовать авторизацию пользователя в веб-системе для получения к ней расширенного доступа или для получения авторизационных данных пользователя. Вредоносный код может быть вставлен в страницу как через уязвимость в веб-сервере , так и через уязвимость на компьютере пользователя.

CSRF

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 аутентифицирована на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны пользователя , которое не может быть проигнорировано или подделано атакующим скриптом.

Вася : Привет, Алиса! Посмотри, какой милый котик:

```
<img src="http//bank.example.com/withdraw?account=Alice&amount=1000000&for=Vasya">
```

SSL/HTTPS

При отсутствии HTTPS злоумышленник имеет возможность перехватывать аутентификационные данные или любую другую информацию, передаваемую между клиентом и сервером. А в случае **активной** атаки — может даже изменять данные, передаваемые в любом направлении.
Если вам нужна защита, предоставляемая HTTPS, и на сервере произведена соответствующая настройка ПО, то надо выполнить ещё несколько шагов, чтобы быть уверенным в защите своей информации:

- SECURE_PROXY_SSL_HEADER = True
- SECURE_SSL_REDIRECT = True
- SESSION_COOKIE_SECURE = True
- SCRF_COOKIE_SECURE = True

Спасибо за внимание!

Информационный видеосервис для разработчиков программного обеспечения

ITVDN

IT VIDEO DEVELOPERS NETWORK

TestProvider PROMETRIC TEST CENTER CyberBionic systematics Microsoft Partner Silver Learning Windows Azure Cloud Partner EBA European Business Association