SOP. CSRF

Самосадный Кирилл
https://t.me/kirsamosad
samosad@seclab.cs.msu.su

МГУ 2018

Same Origin Policy

SOP for DOM

- Как в браузерах изолировать две страницы с разных доменов друг от друга?
- Два JS-контекста могут обращаться к DOM друг друга, если совпадают:
  - протоколы
  - домены
  - порты
- Протокол + домен + порт = источник
- RFC 6454 от 2011 года: до сих пор Proposed Standard
- WHATWG HTML Living Standard

SOP for DOM

Originating document	Accessed document	Non–IE browser	Internet Explorer
http://example.com/**a/**	http://example.com/**b/**	Access okay	Access okay
http://example.com/	http://**www.**example.com/	Host mismatch	Host mismatch
http://example.com/	**https**://example.com/	Protocol mismatch	Protocol mismatch
http://example.com**:81**/	http://example.com/	Port mismatch	Access okay

- Интеграция payments.site.com с login.site.com "из коробки" невозможна

SOP for Cookies

- Фундаментальная проблема – несогласованность с SOP для DOM
- Атрибуты:
  - path
  - domain
  - secure
  - httponly
  - samesite (lax, strict) //на ноябрь 2018 умеют браузеры 70% пользователей
- В cookies не учитываются порты
- domain нельзя ограничить конкретным хостом для всех браузеров
- domain можно сделать более широким

SOP for Cookies

Cookie set at *foo.example.com*, *domain* parameter is:	Scope of the resulting cookie	
	Non–IE browsers	**Internet Explorer**
(value omitted)	*foo.example.com* (exact)	**.foo.example.com*
bar.foo.example.com	Cookie not set: domain more specific than origin	
foo.example.com	**.foo.example.com*	
baz.example.com	Cookie not set: domain mismatch	
example.com	**.example.com*	
ample.com	Cookie not set: domain mismatch	
.com	Cookie not set: domain too broad, security risk	

Brad E. Oct 21, 2016 MICROSOFT EDGE TEAM

RFC 2965 was never really adopted by any browser.

RFC 6265 is the current RFC and used by most browsers. Per this RFC the domain attribute ignores leading dots. The only way to get a cookie constrained to a particular domain is to not have a domain attribute which will cause the hostonly flag to be set. Edge plans on adding hostonly support (per RFC 6265) in a later release.

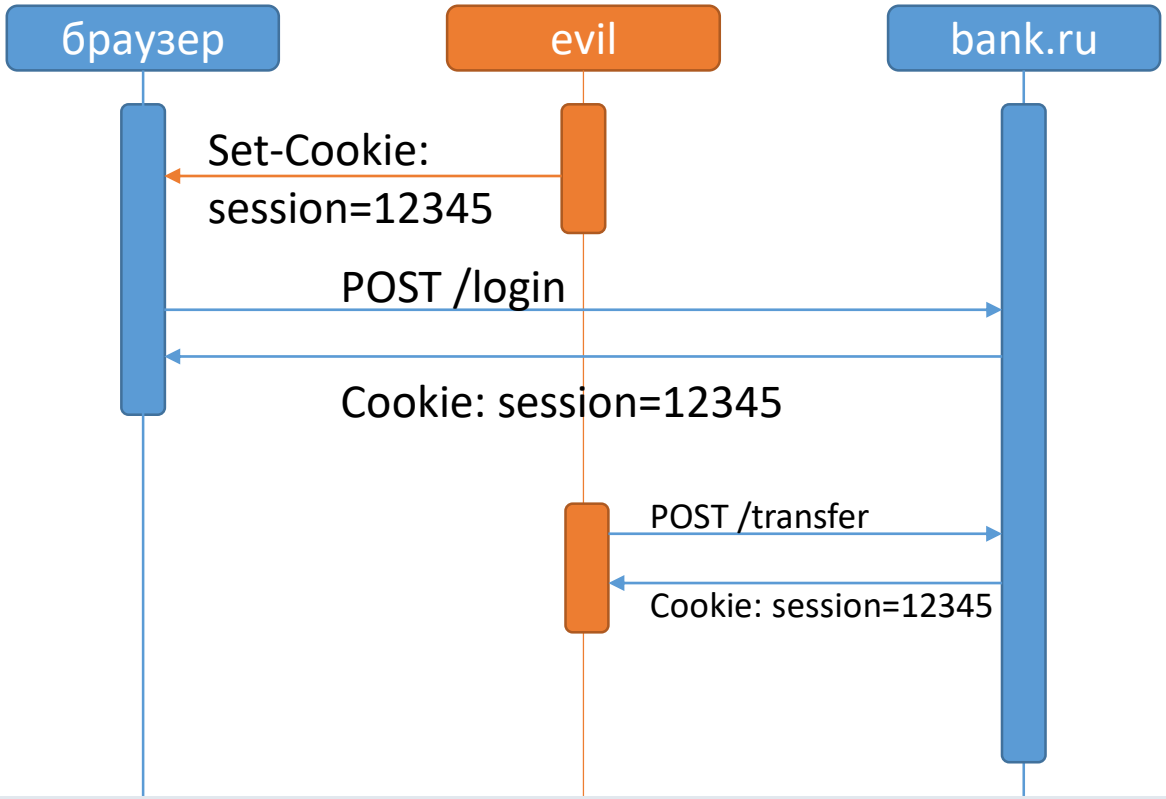
Best,
The MS Edge Team

SOP DOM vs Cookies

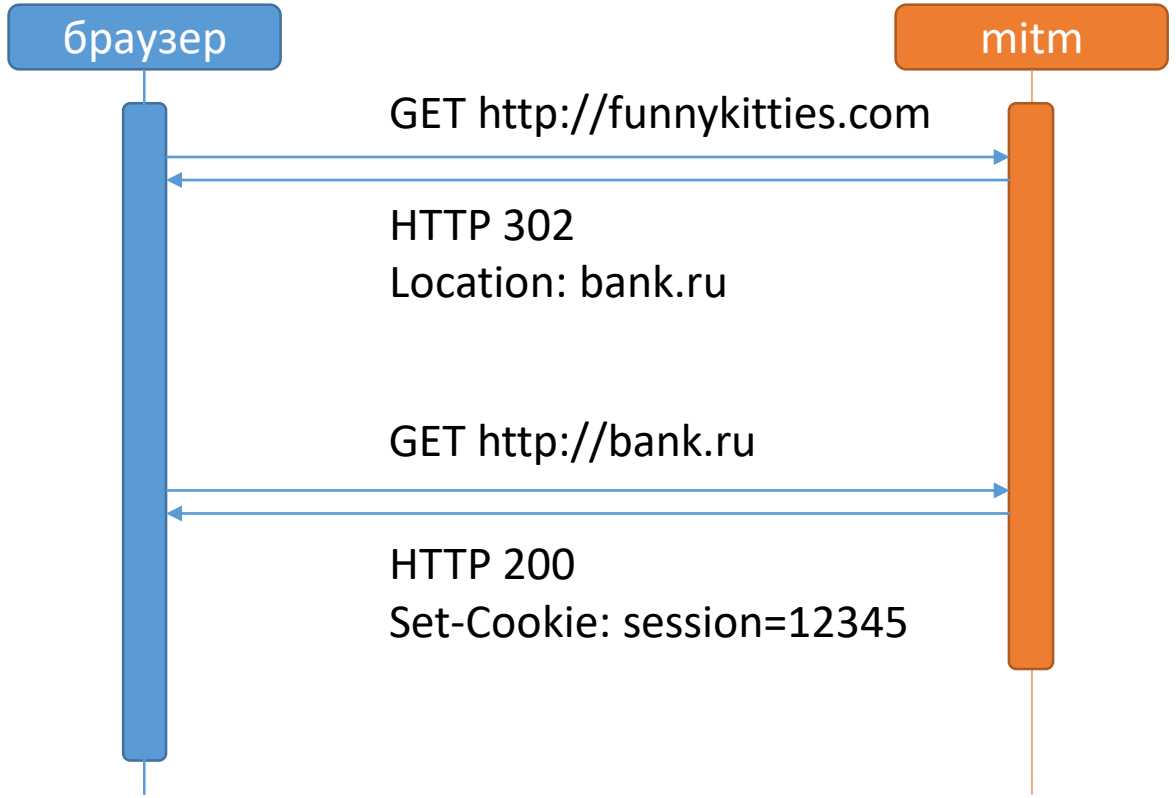
- scheme://domain:port/path?params
- SOP DOM:
  - (scheme, domain, port)
- SOP Cookies:
  - (scheme*, domain*, path*)
- * - не строго

Session fixation

- Фиксация сессии
  - Злоумышленник может поставить пользователю известную ему сессию
  - Пользователь аутентифицируется в своем аккаунте



Session fixation



Как атаковать жертву?

- Cookie с флагами secure и httponly могут быть перезаписаны методом переполнения cookie jar
- Нельзя надежно разделить приложения различного уровня критичности, например:
  - payments.site.com от blogs.site.com
- Пусть на blogs.site.com есть XSS
- Пусть на payments.site.com cookie выставлены как secure, httponly и без domain

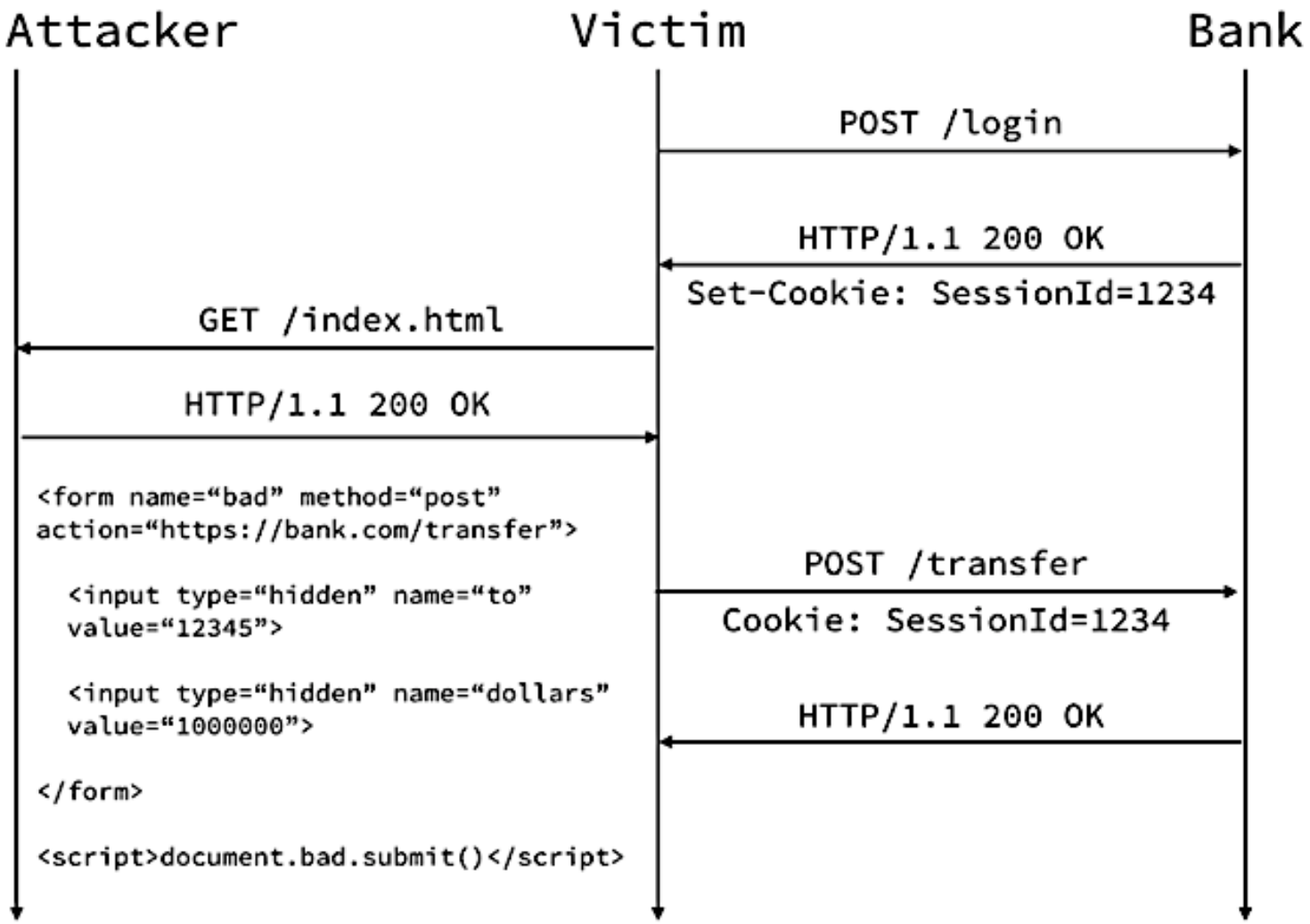
Ответ

- Как атаковать жертву?
  - выставляем через XSS cookie с domain = site.com
  - cookie jar для blogs.site.com переполняется и вытесняет cookies пользователя
  - выставляем свои cookies
  - порядок и кол-во посылаемых cookies зависит от браузера

DEMO: Session fixation

CSRF

Cross Site Request Forgery

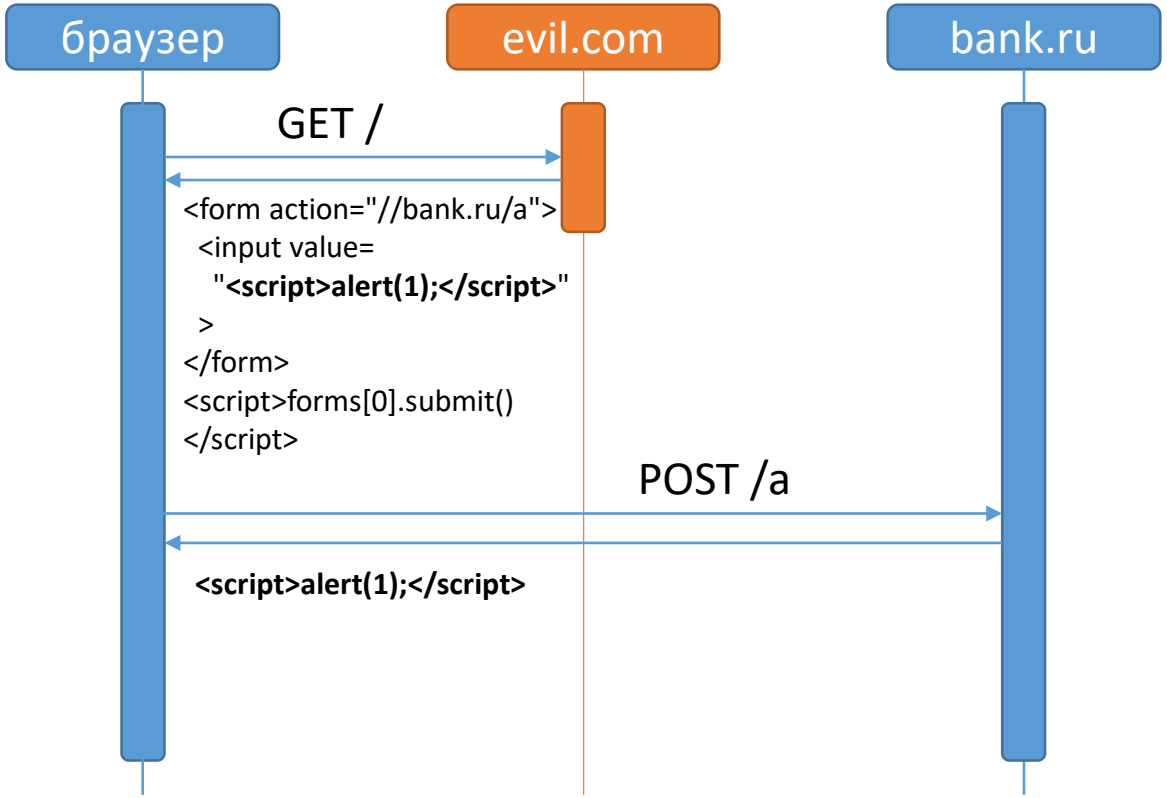


DEMO: CSRF

CSRF: обеспечить проверку аутентичности запросов

- Сделать формат запроса непредсказуемым
  - CAPTCHA
  - Token
  - ввод пароля/дополнительного фактора
- Аутентифицировать источник запроса
  - проверять Referer (плохо)
  - выставлять свои заголовки для XHR и проверять их наличие
- Сделать сессию на заголовках
- Не ошибиться при конфигурации CORS (если актуально)
- Проверять CSRF централизованно

XSS over CSRF



Литература