

Cross Site Request Forgeries (CSRF) – zarys problemu

Przemek Sobstel (<http://sobstel.org>). SegfaultLabs, maj 2006.

Atak typu *Cross Site Request Forgeries* (CSRF) polega na wykorzystaniu przeglądarki internetowej użytkownika (ofiary ataku) do wysyłania żądań HTTP bez jego wiedzy [John04, s.22]. W polskiej literaturze nie występuje odpowiednik nazwy tego ataku. Prawdopodobnie przyczyną takiego stanu rzeczy jest fakt, że przez wiele źródeł, także zagranicznych, technika ta jest zupełnie pomijana. Tymczasem łatwość z jaką można wykonać CSRF sprawia, że jest on jednym z groźniejszych sposobów atakowania stron internetowych.

Nie należy mylić CSRF z XSS. O ile XSS wykorzystuje zaufanie, które użytkownik ma do strony, o tyle CSRF wykorzystuje zaufanie, które strona ma do użytkownika [Shif03, s.56]. Nie przeszkadza to jednak temu, aby techniki te z powodzeniem były łączone.

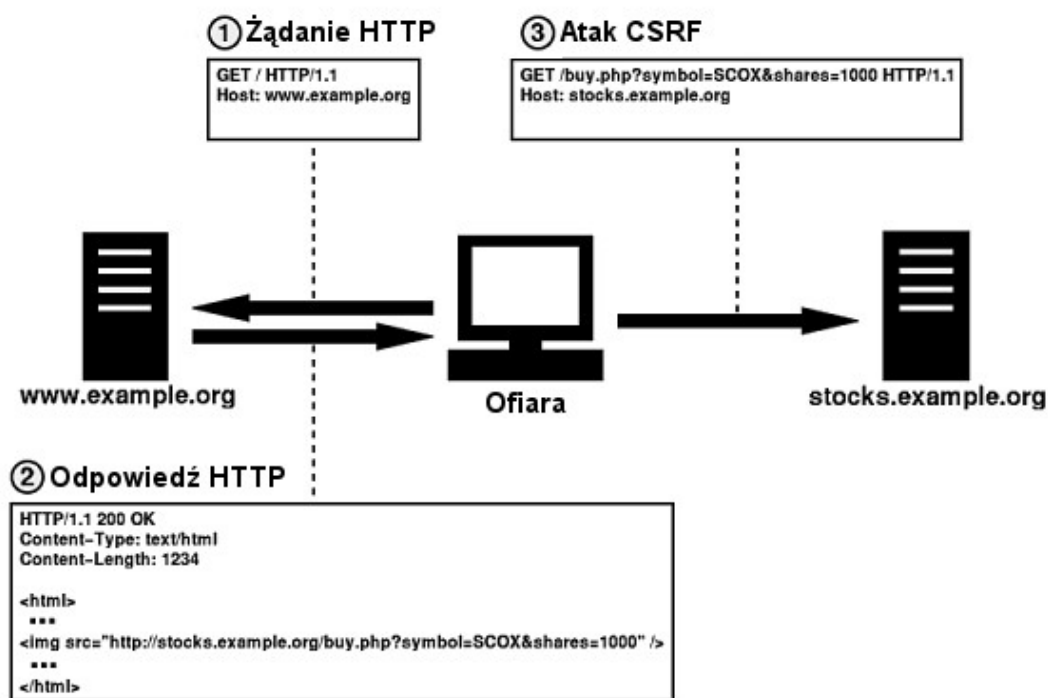
Cross Site Request Forgeries wykorzystuje sposób w jaki przeglądarki stron WWW przetwarzają witryny internetowe. Przeglądarka po odebraniu kodu HTML witryny, analizuje go i pobiera osobnymi zapytaniami (żądzeniami) kolejno wszystkie zasoby, jakie są konieczne do poprawnego wyświetlenia strony, np. pliki stylów, pliki ze skryptami oraz obrazy [Gajd05, s.95]. Przykładowo po napotkaniu pliku graficznego wysyłane jest całkowicie odrębne żądanie w celu jego pobrania. Problem polega na tym, że przeglądarki często wcale nie sprawdzają czy dany zasób jest tym, czym powinien być, czyli czy np. pobierany plik graficzny jest rzeczywiście plikiem graficznym, a nie skrypcem JavaScript czy całkowicie inną stroną internetową.

Na przykład napastnik mógłby wstrzyknąć w stronę następujący wrogi kod : [Shif03, s.58]

```

```

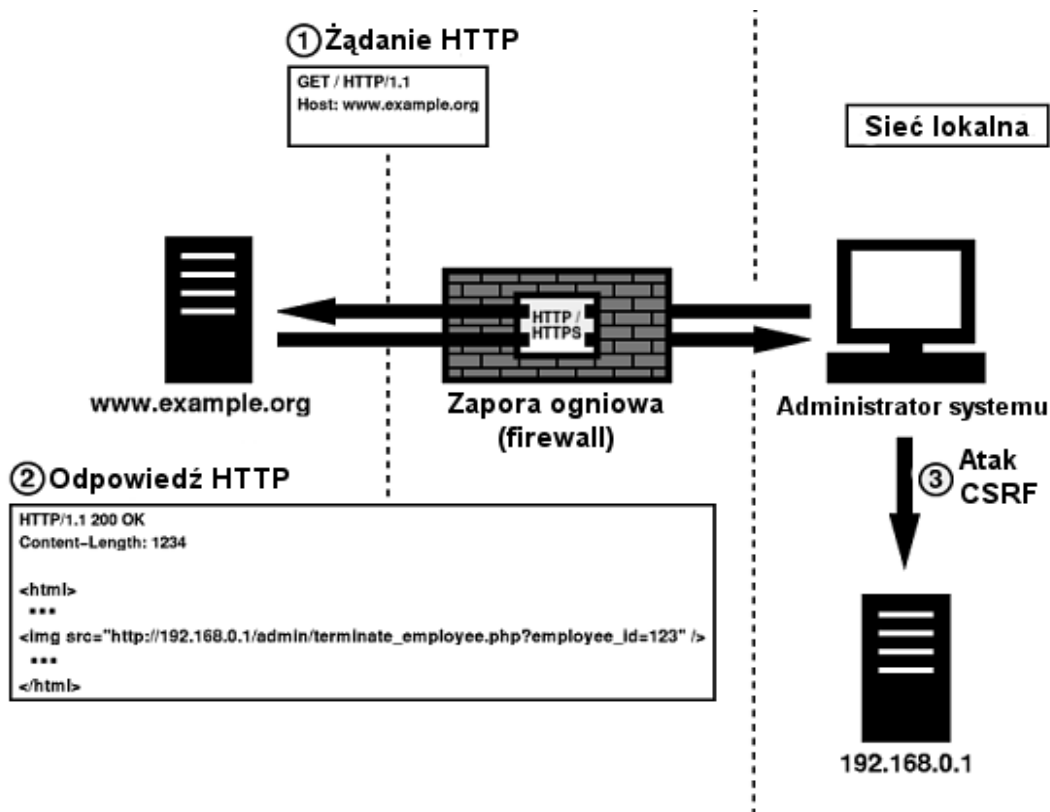
W efekcie, po odwiedzeniu tej strony, każdy zalogowany użytkownik nieświadomie nabyłby dużą ilość udziałów pewnej spółki. W tym samym czasie na stronie zostałaby wyświetlona tylko ikona symbolizująca niepoprawny format pliku graficznego. Proces ten został przedstawiony na rysunku nr 1. Istotne jest, że strony WWW, szczególnie fora internetowe, często umożliwiają umieszczanie obrazków pochodzących z zewnętrznych serwerów, w wyniku czego atakujący nie musi uciekać się do wyszukanych sposobów umieszczenia złośliwego łącza na stronie.



Rysunek 1: Przebieg przykładowego ataku typu Cross Site Request Forgeries
 Źródło: [Shif03, s.58]

Cross Site Request Forgeries może być także wykorzystany do przeprowadzania czynności administracyjnych bez konieczności przechwytywania sesji użytkownika czy łamania haseł dostępu. Wystarczy, że administrator systemu wejdzie na podstronę, na której znajduje się spreparowany odnośnik w ramach znacznika `` i nie musi to być wcale ta sama witryna względem której dokonywany jest atak. Jak wykazał C. Shiflett [Shif03, s.57] w ten sposób podatne na CSRF są także systemy intranetowe (zob. rysunek 2). Na zaprezentowanym rysunku administrator systemu przegląda zasoby Internetu z sieci lokalnej, która oddzielona jest dobrze skonfigurowaną zaporą ogniową (*firewall*). Zostaje skierowany (np. atakujący może wiedzieć, że administrator często odwiedza jakieś forum i umieścić tam swój złośliwy kod) na odpowiednio stronę zawierającą osadzony odnośnik w ramach znacznika obrazka. Odnośnik ten odsyła administratora do aplikacji znajdującej się w sieci lokalnej – w niniejszym przykładzie oznacza on dokładnie zwolnienie z pracy osoby o podanym identyfikatorze. Ponieważ administrator także znajduje się w ramach sieci lokalnej akcja zostanie wykonana i w ten sposób nieświadomie dokona on niepożądanego operacji, nawet tego nie zauważając. Napastnikowi uda się przeprowadzić atak bez konieczności łamania jakichkolwiek zabezpieczeń w ramach sieci lokalnej, z której łączy się administrator.

Najgorsze jest to, że w praktyce CSRF nie wymaga od użytkownika podejmowania żadnych szczególnych akcji, poza zwyczajowym korzystaniem z witryny.



Rysunek 2: Przykład ataku Cross Site Request Forgeries na aplikację znajdującą się w sieci lokalnej chronionej zaporą ogniową

Źródło: [Shif03, s.58]

Do przeprowadzenia ataku CSRF można wykorzystać nie tylko metody z podstawionymi obrazkami w znacznikach IMG, ale także dowolny inny znacznik, którego przetwarzanie wiąże się z automatycznym pobieraniem wskazanego zasobu [Alsh06, s.54]. Obecnie nie ma możliwości zabezpieczenia się przed działaniem przeglądarek [Gajd05, s.96], dlatego to programiści stron internetowych powinni podjąć odpowiednie środki ostrożności na poziomie aplikacji.

Literatura

- [Alsh06a] Alshanetsky I.: *Niebezpieczeństwa ataków XSS i CSRF*, PHP Solutions nr 2/2006, s.48-55.
- [Gajd05] Gajda W.: *Ataki XSS oraz CSRF na aplikacje internetowe*, Internet nr 7/2005, s.95-99.
- [John04] Johnston P.: *Authentication and Session Management on the Web*, GSEC 2004.
http://www.giac.org/certified_professionals/practicals/gsec/4206.php
- [Shif03] Shiflett C.: *Foiling Cross-Site Attacks*, PHP Architect nr 10/2003.