Title Goes Here

Dimos Stamatakis, Dimitrios Chasapis

Department of Computer Science,
University of Crete,
P.O. Box 2208, Heraklion, GR 71409, Greece
{dstamat,hassapis}@csd.uoc.gr

February 9, 2012

1 Abstract

In this report we briefly explain how Cross-Site Request Forgery (CSRF), a common exploit used to attack websites, works. In addition, We present the most well known defenses against this attack and explain how each one works. We conducted an analysis on the top 100,000 web sites, as rated by alexa.com, as to which defense they implement to counter any CSRF attacks and present the results. To meet this end we implemented a tool that crawls the web, parses http headers and html body of each site to deduct which defense is employed.

2 Introduction

Cross Site Request Forgery (CSRF) is an attack which maliciously forces the users web application to sent a request to a website, on which the user is authenticated, thus fooling the server that he, the attacker is actually an authenticated user. The severity of a CSRF attack varies as it depends upon the level of access the victim user has. For instance a simple user can only compromise his data, while an administrator user can compromise the entire site infastructure. A common way to launch a CSRF attack is to fool the user, through means of social engineering, to click on a link from a fraud website/email, made or sent by the attacker, which redircects to a website that the user has an open session with, thus hijacking that session. Due to the difficulty of achieving these prequirements (user has a running session with target, social engineering), many regard a CSRF attack as an unlikely scenario, undermining its importance. This misconception could not be further from the trueth. CSRF is ranked as the 909th most dangerous software bug ever found (REFERENCE HERE) and it is among the twenty most exploited security-vulnerabilities in 2007.

The most common CSRF countermeasures are the following:

1. Secret Validation Token
2. Referer Header

3. Custom XMLHtmlHeader
4. Origin Header
5. Content Security Policy (CSP)

References