ADAS-EU R(12)OP02

ADAS-EU
ADAS for fusion in Europe

Grant: 224607

Hugh Summers, Martin O'Mullane, Francisco Guzman and Luis Menchero

OPEN-ADAS report 2

February 2012

Workpackages : 26-2-2
Category : PU

OPEN-ADAS report 2

Hugh Summers, Martin O'Mullane, Francisco Guzman and Luis Menchero

Department of Physics, University of Strathclyde, Glasgow, UK

Abstract: *The report reviews OPEN-ADAS activities for project months 18-36*

Contents

Preface

The report is one of a series of four such reports, deliverable under the ADAS-EU project, which assemble documentary material of OPEN-ADAS for the applicable year. Each comprises a summary of OPEN-ADAS user activity, developments and release notes.

M G O'Mullane
February 2012

Chapter 1

Overview

OPEN-ADAS is the name of the path for release of ADAS data and support software into the public domain. It is an agreed and shared project between ADAS and the International Atomic Energy Agency, Atomic and Molecular Data Unit, Nuclear Data Section (IAEA) in Vienna. As agreed in the ADAS-EU proposal, OPEN-ADAS is to be used for public domain release of fundamental and derived atomic data which enters the ADAS databases from ADAS-EU activities. The web server is located at the Physics Department, University of Strathclyde and is linked via the IAEA web pages.

The development of OPEN-ADAS was substantively finished with the addition of the free-form search capability. Since the first 18 month reporting period the number of users increased steadily each month and came from very many countries. The principal aims of the project had been realized and it had settled down to high-availability but low-maintenance web service.

It is possible to contact OPEN-ADAS via a web contact form which emails the request to the web site administrator. A few requests via this form were received every few weeks and were not burdensome on staff time. Requests from web presence optimization companies are ignored. However in June 2010 there was a flood of email, of hundreds of emails per hour. The usual way of ameliorating such an attack is via a captcha. Before implementing such a system a simpler text challenge field was tried: we ask the correspondent to type 'not spam' into the appropriate box. This has proved to be successful so the more invasive captcha system was not deployed.

The OPEN-ADAS web site required a simple sign-up resulting in an account with a password. The name and email address were not verified before creating the account so a degree on anonymity was possible. This enabled us to produce accurate usage statistics since the number of hits is a very poor metric. Reports that a list of the OPEN-ADAS user names and passwords were available on the 'pastebin' web site came to us in the first week of June 2011. Individual users and the IT services at FZJ, ITER and NASA were the first to pick-up on a possible breach of our security.

The OPEN-ADAS and ADAS-EU websites are on the same server and the underlying framework is PHP with a MySQL back-end. The webserver logs showed a few SQL injection attacks every few weeks which is not unexpected on the public internet. However around the end of May 2011 the volume rose sharply. The reasons are unclear but news of a successful exploit probably circulates quickly in the anarchistic world of web breaking.

The origin of the SQL injection attempts were varied. Table 1.1 details the date and ISP/organization associated with some of these attacks. The last entry in table 1.1 was also the most aggressive with just under 1500 requests over a 20 minute period. The identification of the owner of the IP addresses is from querying the whois service, which we note could be spoofed by the attackers.

Most of the attacks targeted the ADAS-EU (www.adas-fusion.eu) rather than the OPEN-ADAS (open.adas.ac.uk) website but since they shared a database server the users database for OPEN-ADAS was easily compromised.

It is unlikely that the attack was targeted specifically at the ADAS websites but there was a series of widescale web vandalism under the 'lulz' banner during the summer of 2011. The database of users was commented upon but tellingly there was little interest in the atomic database.

Date	IP	*whois* de-reference
02/Jan/2011	60.177.241.7	CHINANET-ZJ-HZ, China
10/Feb/2011	78.39.192.62	Shahid Chamran University of Ahvaz, Iran
17/Feb/2011	95.59.148.41	JSC Kazakhtelecom, KAZAKHSTAN
27/Feb/2011	123.23.109.163	Vietnam Posts and Telecommunications (VNPT)
10/Mar/2011	81.88.222.51	MARYNONET-NAT, Russia
22/Mar/2011	91.218.39.217	Infium Ltd., UKRAINE
24/Mar/2011	94.96.228.165	SAUDINET_DSL_POOL, Saudi Arabia
27/Mar/2011	77.30.4.146	also SAUDINET_DSL_POOL
18/May/2011	41.34.68.233	All-Zone-DS, Egypt
19/May/2011	2.90.221.75	SAUDINET_DSL_POOL again

Table 1.1: Date and origin of some SQL injection attempts.

The OPEN-ADAS and ADAS-EU websites were taken down on 11 June 2011 and replaced with a 'Down for maintenance page' while we contemplated the best strategy to prevent a recurrence.

During this down period the injection attacks continued and on 20 June 2011 the webserver computer suffered a serious and non-recoverable hard disk failure. It is not possible to say whether the continuing attacks were related to the hardware failure.

A redeployed computer, freed up by a departing PhD student, was used as a temporary replacement server.

The website developer, Allan Whiteford, was no longer with the team so the hardening of the PHP code took longer than desired as we had to acquire a sufficient familiarity with the language in order to modify the site and, in particular, to harden the security.

It was decided that the most effective way to prevent a further occurrence was to remove the registration requirement. All data from OPEN-ADAS can now be downloaded anonymously. The removal of the code for registration, sanitizing the MySQL queries and trapping all input resulted in the OPEN-ADAS website being unavailable until 4 September 2011 — a two month interruption which also displaced other activities.

The disadvantages in not knowing the OPEN-ADAS users are the loss of statistics and the ability to inform people who downloaded data of any subsequent improvements. Given the time pressures on the staff and the (merely competent web development) skill set available this is an acceptable compromise.

One upside to the interruption of OPEN-ADAS web service was that it was brought into line with v3.1 of ADAS. In particular electron impact excitation R-matrix data for the He-like, Ne-like and Na-like sequences in addition to W^{+44}, W^{+45} and W^{+46} are now available.

The temporary replacement server has suffered no ill effects and the number of SQL injection attacks has diminished to its previous level. However this computer is outside its warranty period so new hardware was ordered in December 2011 to provide more robust facilities. Scientific Linux was chosen as the operating system because of its long term support and frequent security updates. It is currently under testing and the switch over to the new server is scheduled for early March 2012.

Chapter 2

Work package reports

2.1 Work package 26-2-1

The work package task comprises the preparation of this report.