Cross-Site Framing VUNERABILITY in phpMyAdmin 2.11.7

Discovered by: Aung Khant
Date: July 13, 2008
Product: PhpMyAdmin 2.11.7 (http://phpmyadmin.net)
Vulnerability Type: Cross-Site Framing
Risk: **low~medium**
Threats: Sensitive Information Exposure to Third Parties

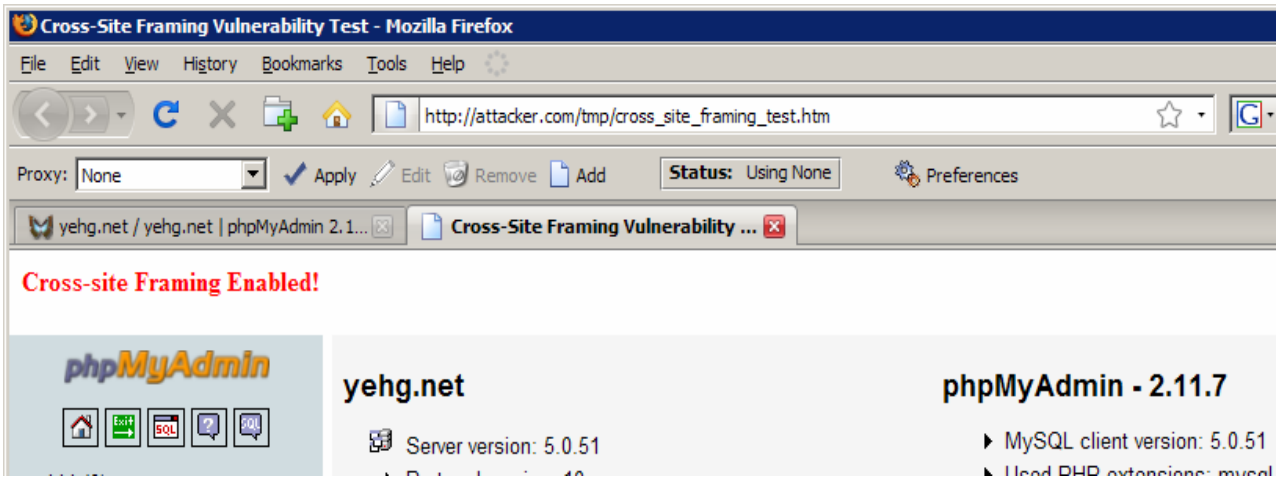
Proof-Of-Vulnerability:

phpMyAdmin protects cross-site framing only in index.php page.

```
<script type="text/javascript">
//<![CDATA[
// show login form in top frame
if (top != self) {
    window.top.location.href=location;
}
//]]>
</script>
```

Due to its frame-friendly pages, it cannot protect framing to other pages by third-parties. Cross-site Framing is controlled by index.php. Attackers may take advantage of this and can do phishing or fooling user if the victim has authenticated. Cross-frame reading access is denied but a zero-day exploit can read across/**control** several frames contents. For example, please read Jar Protocol issue.

```
<frameset cols="200,*" rows="*" id="mainFrameset">
        <frame frameborder="0" id="frame_navigation"
        src="http://victim.com/navigation.php "
        name="frame_navigation" />
        <frame frameborder="0" id="frame_content"
        src=" http://victim.com/main.php"
        name="frame_content" />
</frameset>
```



A simple JavaScript checking can solve this issue.

```
// Phishing protection
try
{
        // can't access by phpMyaAdmin because it's on different domain
        var topdomain = top.document.domain;
        // but double-check to ensure
        if(topdomain !=self.document.domain)
        {
                alert("The parent domain mismatches to self domain.\nThis is a
        potential security issue.\nYou\'ll be redirected to correct page.");
                top.location.replace(self.document.URL.substring(0,self.document
        .URL.lastIndexOf("/")+1));
        }

}
catch(e)
{
        alert("The parent domain mismatches to self domain.\nThis is a potential
security issue.\nYou\'ll be redirected to correct page. \nError:\n"+e);
        top.location.replace(self.document.URL.substring(0,self.document.URL.la
stIndexOf("/")+1));
}
```

jar: Protocol XSS Security Issues

16 November 2007

Issue

jar: protocol is not restricted to java archives and will open any zip format file. An attacker can use this to evade filtering on sites that allow users to upload content and use this initiate a cross site scripting attack.

Impact

Firefox supports the Java Archive URI scheme that allows the addressing of the contents of zip archives. An attacker may upload a zip format file to a trusted site that allows users to upload content. The victim clicks on a link on the attackerâ€™s website or in an email that links to the uploaded content on a trusted site. Since the content is loaded from the trusted site, content from the zip file runs in the context of the trusted site. This may allow the attacker to access information stored on the trusted site without the victimâ€™s knowledge.

There is a second issue that if a zip archive is loaded from a site through a redirect, Firefox uses the context from the initiating site. This allows an attacker to take advantage of a site with an open redirect and **host content on their own malicious site that will execute with the permissions of the redirecting site.**

There is a proof of concept that demonstrates these issues in an attack against Gmail that allows the attacker **access to the victim's stored Gmail contacts**.

Status

In future versions Firefox will only support the jar scheme for files that are served with the correct application/java-archive MIME type. Firefox will also adjust the security context to recognize the final site as the source of the content. This will be addressed in Firefox 2.0.0.10, which is currently in testing.

You can follow our work in bugzilla:

https://bugzilla.mozilla.org/show_bug.cgi?id=369814

https://bugzilla.mozilla.org/show_bug.cgi?id=403331