Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Bypassing Whitelists using Double Extensions in File Uploads

Whitelist Based Approach

```
$allowed = array('gif');

$splitFileName = explode(".", $_FILES["file"]["name"]);

$fileExtension = end($splitFileName);


if($_FILES["file"]["type"] != "image/gif" ||  !in_array($fileExtension, $allowed))
{
        echo "Please upload a GIF file";
}
else{

        echo "Name: ".$_FILES["file"]["name"];
        echo "<br>Size: ".$_FILES["file"]["size"];
        echo "<br>Temp File: ".$_FILES["file"]["tmp_name"];
        echo "<br>Type: ".$_FILES["file"]["type"];

        move_uploaded_file($_FILES["file"]["tmp_name"], "uploads/".$_FILES["file"]["name"]);
}
```

Apache Manual – Double Extensions

Files can have more than one extension, and the order of the extensions is normally irrelevant. For example, if the file welcome.html.fr maps onto content type text/html and language French then the file welcome.fr.html will map onto exactly the same information. If more than one extension is given which maps onto the same type of meta-information, then the one to the right will be used, except for languages and content encodings. For example, if .gif maps to the MIME-type image/gif and .html maps to the MIME-type text/html, then the file welcome.gif.html will be associated with the MIME-type text/html.

http://httpd.apache.org/docs/2.2/mod/mod_mime.html

Apache Manual – Double Extensions

Care should be taken when a file with multiple extensions gets associated with both a MIME-type and a handler. This will usually result in the request being by the module associated with the handler. For example, if the .imap extension is mapped to the handler imap-file (from mod_imap) and the .html extension is mapped to the MIME-type text/html, then the file world.imap.html will be associated with both the imap-file handler and text/html MIME-type. When it is processed, the imap-file handler will be used, and so it will be treated as a mod_imap imagemap file.

http://httpd.apache.org/docs/2.2/mod/mod_mime.html

Insecure Configuration

Secure

```
<FilesMatch ".+\.ph(p[345]?|t|tml)$">
    SetHandler application/x-httpd-php
</FilesMatch>
```

Insecure

```
<FilesMatch ".+\.ph(p[345]?|t|tml)">
    SetHandler application/x-httpd-php
</FilesMatch>
```

Arbitrary File Upload Vulnerable ISO

securitytube:123321

Download

- https://sourceforge.net/projects/arbitraryfileuploados
  - user:pass = securitytube:123321
- created by Ashish Bhangale
- Bugs and Issues:
  - ashish@binarysecuritysolutions.com

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

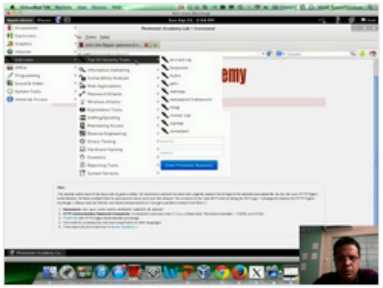
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

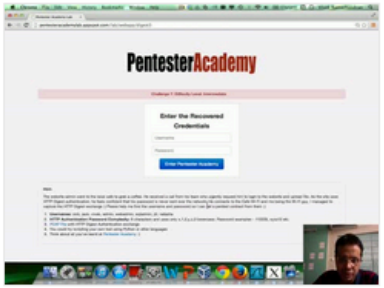
Start Learning Today!

Latest Videos

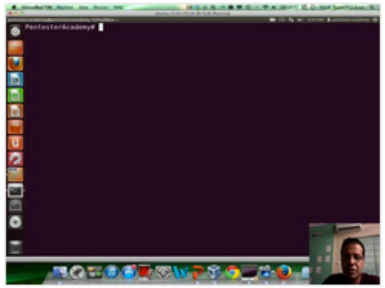
New content added weekly!



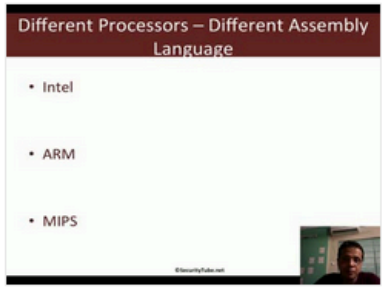
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux