path / file: /home/mrt/Desktop/test/ subdirs
verbosity level: 1. user tainted only vuln type: _All scan
code style: phps bottom-up /regex/: search
windows
files user inp
stats function
RIPS 0.55

File: /home/mrt/Desktop/test/2.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
 18: move_uploaded_file move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path))
      6: $target_path .= basename($_FILES['uploaded']['name']);
           5: $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";

     requires:
           3: if(isset($_POST['Upload']))
          15: if(($uploaded_type == "image/jpeg" || $uploaded_type == "image/png") && ($uploaded_size < 100000))
```

hide all

File: /home/mrt/Desktop/test/4.php

File Disclosure

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
 34: imagecreatefrompng $img = imagecreatefrompng($uploaded_tmp);
      13: $uploaded_tmp = $_FILES['uploaded']['tmp_name'];

     requires:
           3: if(isset($_POST['Upload']))
          26: if((strtolower($uploaded_ext) == 'jpg' || strtolower($uploaded_ext) == 'jpeg' || strtolower($uploaded_ext) == 'png') && ($uploaded_size < 100000) && ($uploaded_type == 'image/jpeg' || $uploaded_type == 'image
              /png') && getimagesize($uploaded_tmp))
          33: if($uploaded_type == 'image/jpeg') else
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
 40: rename rename($temp_file, (getcwd() . DIRECTORY_SEPARATOR . $target_path . $target_file))
      20: $temp_file .= DIRECTORY_SEPARATOR . md5(uniqid() . $uploaded_name) . '.' . $uploaded_ext;
           19: $temp_file = ((sys_get_temp_dir()) : (ini_get('upload_tmp_dir')));
           9: $uploaded_name = $_FILES['uploaded']['name'];
          10: $uploaded_ext = substr($uploaded_name, strrpos($uploaded_name, '.') + 1);
               9: $uploaded_name = $_FILES['uploaded']['name'];
               9: $uploaded_name = $_FILES['uploaded']['name'];
      16: $target_path = DVWA_WEB_PAGE_TO_ROOT . 'hackable/uploads/';
      18: $target_file = md5(uniqid() . $uploaded_name) . '.' . $uploaded_ext;
           9: $uploaded_name = $_FILES['uploaded']['name'];
          10: $uploaded_ext = substr($uploaded_name, strrpos($uploaded_name, '.') + 1);
               9: $uploaded_name = $_FILES['uploaded']['name'];
               9: $uploaded_name = $_FILES['uploaded']['name'];

     requires:
           3: if(isset($_POST['Upload']))
          26: if((strtolower($uploaded_ext) == 'jpg' || strtolower($uploaded_ext) == 'jpeg' || strtolower($uploaded_ext) == 'png') && ($uploaded_size < 100000) && ($uploaded_type == 'image/jpeg' || $uploaded_type == 'image
              /png') && getimagesize($uploaded_tmp))
```

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
 51: unlink unlink($temp_file);
      20: $temp_file .= DIRECTORY_SEPARATOR . md5(uniqid() . $uploaded_name) . '.' . $uploaded_ext;
           19: $temp_file = ((sys_get_temp_dir()) : (ini_get('upload_tmp_dir')));
           9: $uploaded_name = $_FILES['uploaded']['name'];
          10: $uploaded_ext = substr($uploaded_name, strrpos($uploaded_name, '.') + 1);
               9: $uploaded_name = $_FILES['uploaded']['name'];
               9: $uploaded_name = $_FILES['uploaded']['name'];

     requires:
           3: if(isset($_POST['Upload']))
          26: if((strtolower($uploaded_ext) == 'jpg' || strtolower($uploaded_ext) == 'jpeg' || strtolower($uploaded_ext) == 'png') && ($uploaded_size < 100000) && ($uploaded_type == 'image/jpeg' || $uploaded_type == 'image
              /png') && getimagesize($uploaded_tmp))
          50: if(file_exists($temp_file))
```

hide all

File: /home/mrt/Desktop/test/3.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
 20: move_uploaded_file move_uploaded_file($uploaded_tmp, $target_path))
      12: $uploaded_tmp = $_FILES['uploaded']['tmp_name'];
      6: $target_path .= basename($_FILES['uploaded']['name']);
           5: $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";

     requires:
           3: if(isset($_POST['Upload']))
          17: if((strtolower($uploaded_ext) == "jpg" || strtolower($uploaded_ext) == "jpeg" || strtolower($uploaded_ext) == "png") && ($uploaded_size < 100000) && getimagesize($uploaded_tmp))
```

hide all

File: /home/mrt/Desktop/test/1.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
  9: move_uploaded_file move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path))
      6: $target_path .= basename($_FILES['uploaded']['name']);
           5: $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";

     requires:
           3: if(isset($_POST['Upload']))
```

hide all