Basic Web Security for Developers

About Me

Working with Web Developer
Since 1996

Working with Unix (FreeBSD, Linux)
System Admin Since 1996

Bachelor of Engineering Program
in Computer KMITL
(Room D KMITL #39)

System Engineer @GMMD

Senior System Engineer
@Weloveshopping.com

Specialist @EGG Digital

Introduction

What's happened about my site?

What's Web Security?
Why Web Security?

How to do Web Security?

Web Vulnerability Scanner Tools?

Topics Today

Server Information robots.txt, phpinfo(), Directory Listing, .git

Web Session & Cookies Management

Command Injection

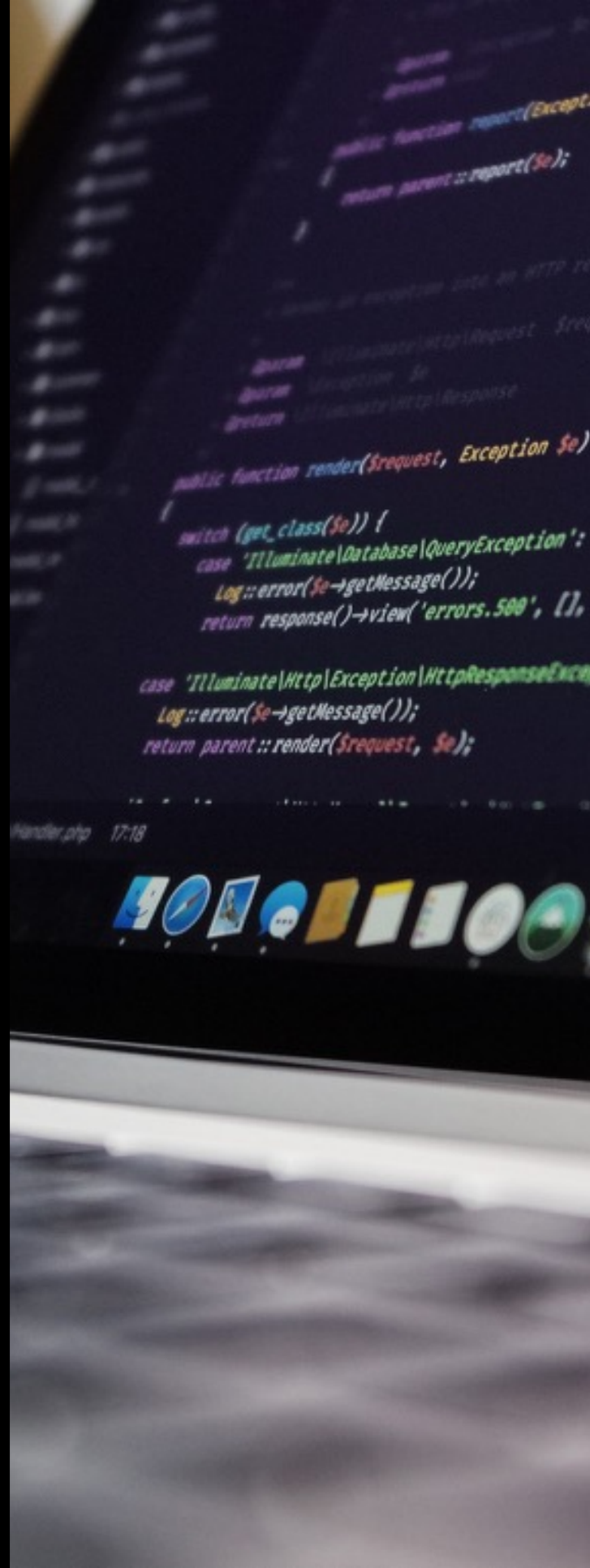
File Upload, PHP Shell (b374k, c99, r57)

Default Setting phpMyAdmin

SQL Injection

Cross-Site Scripting (XSS)

Web Vulnerability Scanner Tools



Server Information

nmap -A tonblog.com
./nikto.pl -h http://tonblog.com

robots.txt

phpinfo.php

.git

Web Session &
Cookies Management

```php
<?php
if ((($_POST['uid']=="admin") && ($_POST['pwd']=="1234!")) || base64_decode($_COOKIE['login'])=="admin") {
    setcookie("login", base64_encode("admin"), time()+60*60*24*365, "/", $_SERVER['HTTP_HOST'], 0);
    echo "<center><img src=images/admin_profile_image.jpg?".rand()." border=0><br>\n";
    echo "[ <a href=formupdatepic.php>Update Profile Picture</a> ] [ <a href=logout.php>Logout</a> ]\n";
    echo "<h1>You are Admin :P</h1>\n";
    echo "<form action=ping.php method=GET>\n";
    echo "Ping: <input type=text name=ip><input type=submit value=ping!!!>\n";
    echo "</form></center>\n";
    exit;
} else {
    setcookie("login", base64_encode("guest"), time()+60*60*24*365, "/", $_SERVER['HTTP_HOST'], 0);
    echo "<center><h1>You are Guest :(</h1>\n";
    echo "[ <a href=index.php>Login</a> ] </center>\n";
}
?>
```

Command Injection

```php
<?php
if(isset($_GET['ip'])) {
    $output = shell_exec("ping -c1 ".$_GET['ip']);
    echo "<pre>$output</pre>";
}
?>
```

SQL Injection

File Upload

Cross-Site Scripting (XSS)

<script>alert(‘H’);</script>

search.php:

```
<?php echo "Your query:
$_GET['query'] returned $num
results." ?>
```

Web Vulnerability Scanner Tools

Tools

- Nmap
- Nikto
- Acunetix
- Sqlmap
- Metasploit
- Kali Linux

Thanks :)

EGG Digital.

http://webblaze.cs.berkeley.edu

http://highscalability.com

http://hitcon.org

http://packetstormsecurity.com

http://zone-h.org

http://www.exploit-db.com

https://www.hackthis.co.uk


INKSECURE PTE LTD. All Rights Reserved.


I
travel


I
travel

Contact Us

My Blog: http://ton.packetlove.com/blog/

FB: https://www.facebook.com/pornpasok

E-Mail: ton@packetlove.com

Mobile: +66868885195