

The logo for EGGG DIGITAL, featuring the word "EGGG" in a large, white, sans-serif font above the word "DIGITAL" in a smaller, white, sans-serif font. The text is centered within a bright yellow oval. The background of the entire image is a dark teal color with a faint, glowing geometric pattern of white lines and dots, resembling a network or data structure. In the center, a person wearing a dark hoodie is shown from the chest up, with their face obscured by shadow, creating a mysterious and somewhat ominous atmosphere. The overall lighting is dim, with the yellow logo and the white text providing the primary points of focus.

EGGG
DIGITAL

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

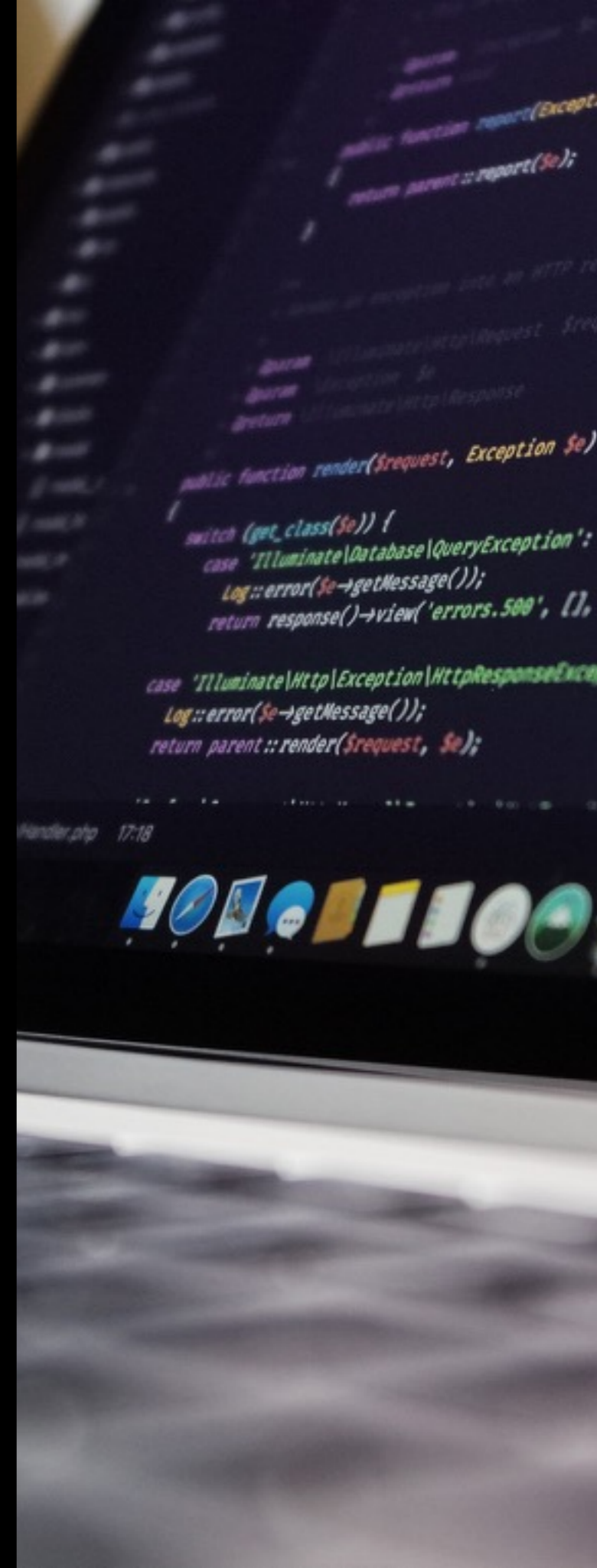
File Upload, PHP Shell (b374k, c99, r57)

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

```
1 <?php
2 if ((($_POST['uid']=="admin") && ($_POST['pwd']=="1234!")) || base64_decode($_COOKIE['login']=="admin") {
3     setcookie("login", base64_encode("admin"), time()+60*60*24*365, "/", $_SERVER['HTTP_HOST'], 0);
4     echo "<center><img src=images/admin_profile_image.jpg?\".rand().\" border=0><br>\n";
5     echo "[ <a href=formupdatepic.php>Update Profile Picture</a> ] [ <a href=logout.php>Logout</a> ]\n";
6     echo "<h1>You are Admin :P</h1>\n";
7     echo "<form action=ping.php method=GET>\n";
8     echo "Ping: <input type=text name=ip><input type=submit value=ping!!!>\n";
9     echo "</form></center>\n";
10    exit;
11 } else {
12     setcookie("login", base64_encode("guest"), time()+60*60*24*365, "/", $_SERVER['HTTP_HOST'], 0);
13     echo "<center><h1>You are Guest :( </h1>\n";
14     echo "[ <a href=index.php>Login</a> ] </center>\n";
15 }
16 ?>
```

Command Injection

```
1 <?php
2 if(isset($_GET['ip'])) {
3     $output = shell_exec("ping -c1 ".$_GET['ip']);
4     echo "<pre>$output</pre>";
5 }
6 ?>
```

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>



Contact Us

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

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

E-Mail: ton@packetlove.com

Mobile: +66868885195

