Basic Web Security

Knowledge Is Free.
We Are Anonymous.
We Are Legion.
We Do Not Forgive.
We Do Not Forget.
Expect Us.

EGG DIGITAL

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)
- Senior Engineer @Weloveshopping.com
- Specialist @EGG Digital

YOU HAVE BEEN

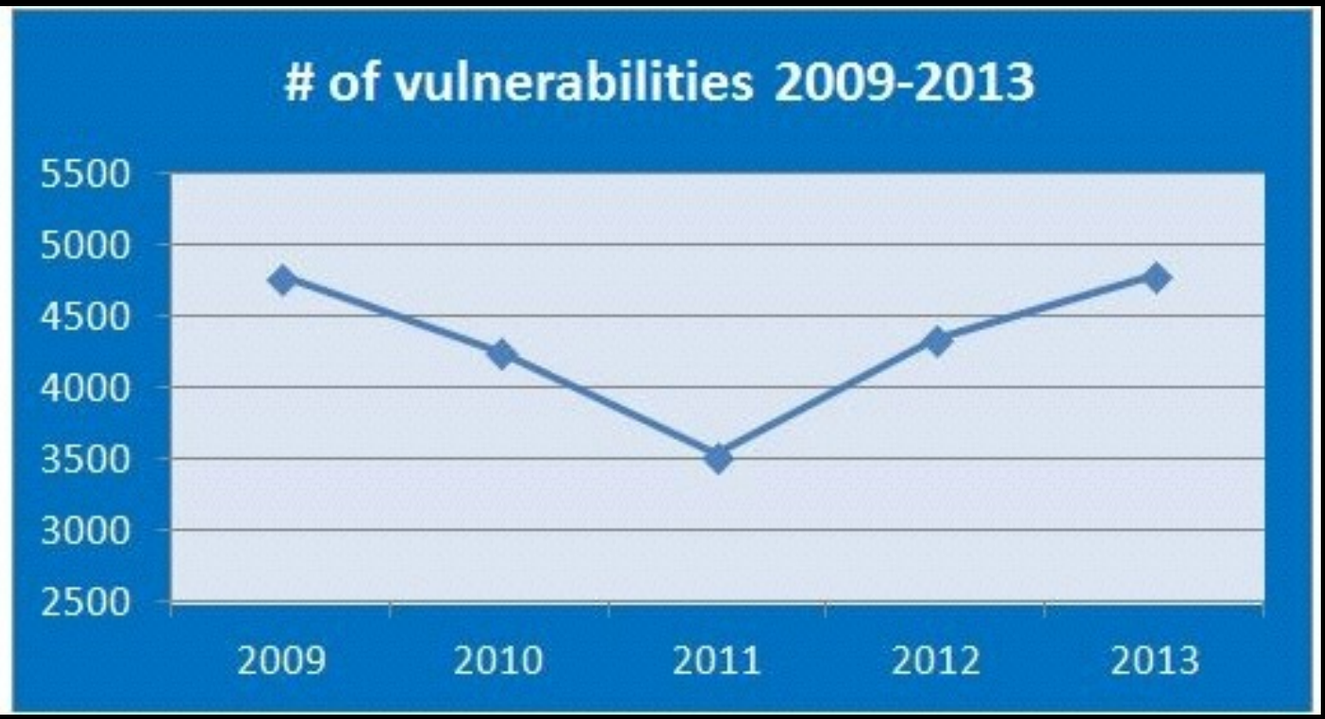
HACKED !


الله أكبر
الله أكبر
SECURITY COMPROMISED BY
Muslim Liberation
Army
-.- UNITED WE STAND DIVIDED WE FALL -.-
XtReMiSt, KillerMind Haxor, Jerry Hassan,
Syed Zaadaa,
Faisy Ali Laghari, Zarb-E-Momin, HyP3r-Boy
techtree
.com

Introduction

- What’s happened about my site?
- What’s Web Security? Why Web Security?
- How to do Web Security?
- Web Vulnerability Scanner Tools?

Year	# of vulnerabilities
2009	4783
2010	4258
2011	3532
2012	4347
2013	4794



The number of reported security vulnerabilities in 2013
Source: National Vulnerability Database (NVD)
http://nvd.nist.gov

Topics Today

- Server Information
- Web Session & Cookies Management
- Command Injection
- SQL Injection
- Cross-Site Scripting (XSS)
- Web Vulnerability Scanner Tools

Server Information

nmap -A IP
./nikto.pl -h http://www.google.com
robots.txt
phpinfo.php

Web Session & Cookies Management

index.php :

```
if ((($_POST['uid']=="admin") && ($_POST['pwd']=="1234!")) || $_COOKIE['login']=="admin") {
        setcookie("login", "admin", time()+60*60*24*365, "/", $_SERVER['HTTP_HOST'], 0);
        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>\n";
        exit;
}
else {
        setcookie("login", "guest", time()+60*60*24*365, "/", $_SERVER['HTTP_HOST'], 0);
        echo "<h1>You are Guest </h1>\n";
}
```

Command Injection

ping.php?ip=127.0.0.1
ping.php :

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

SQL Injection

login.php :

```
$query = "SELECT * FROM users WHERE (uid = '$_GET[user]' AND pwd =
'$_GET[pwd]')";
$result = mysql_query($query);
$arr=mysql_fetch_array($result);

if (mysql_num_rows($result) > 0) {
        echo "<h1>Success</h1>\n";
        echo "You are Admin :P <br>\n";
        print_r($arr);
}
else {
        echo "<h1>Wrong User or Password!!!</h1>\n";
        print_r($arr);

}
```

Cross-Site Scripting (XSS)

<script>alert(‘H’);</script>
search.php
<? echo “Your query: $_GET[‘query’] returned $num results.” ?>

Web Vulnerability Scanner Tools

Tools
- nmap
- nikto
- metasploit
- Kali Linux
- Acunetix

FireFox Add-ons
- User Agent Switcher
- FireBug
- Web Developer

Thanks :)

EGG Digital Team.
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