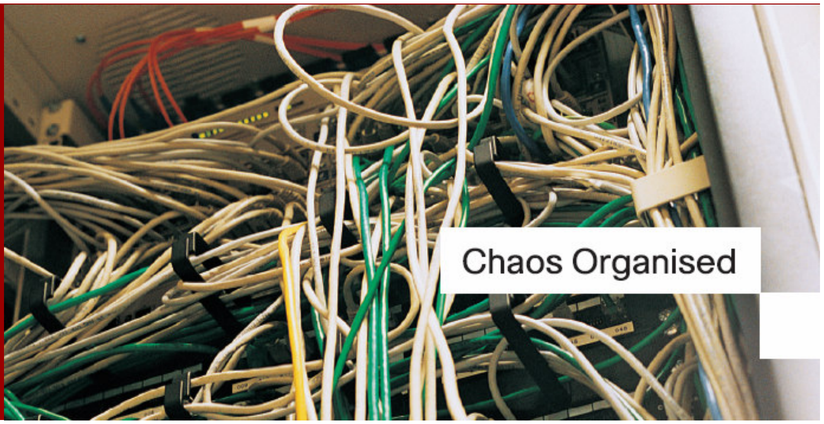
Cisco Data Center Day 2007

Web Application Security


Chaos Organised

Leo Chan
Product Manager – Application Networking Services
Cisco Systems APAC

Session agenda

- Web Application Security: background
- Top Web Application Attacks:
  - Input validation bypass
  - SQL injection
  - Cross-Site Scripting (XSS)
  - Cookie Tampering / Session Hijacking
- Cisco's Web Application Firewall
  - Cisco AVS

Web Application Security: *background*

Applications: the Weak Link to the Crown Jewels

Data Disclosure

Customer Confidentiality

Customer List

Name	Main Contact	YTD Revenue
ACME Corp	John Michaels	$893, 5
Anderson Technologies	Sandra Watson	$599,67
Azure Systems	Mitch Wilson	$395,00
Best Industries	Muchael Le	
Cascade Inc.	Rob Smith	
Diamond Technology	Bruce Leah	
Echelon Manufacturing	Jennifer Bl	

User ID:

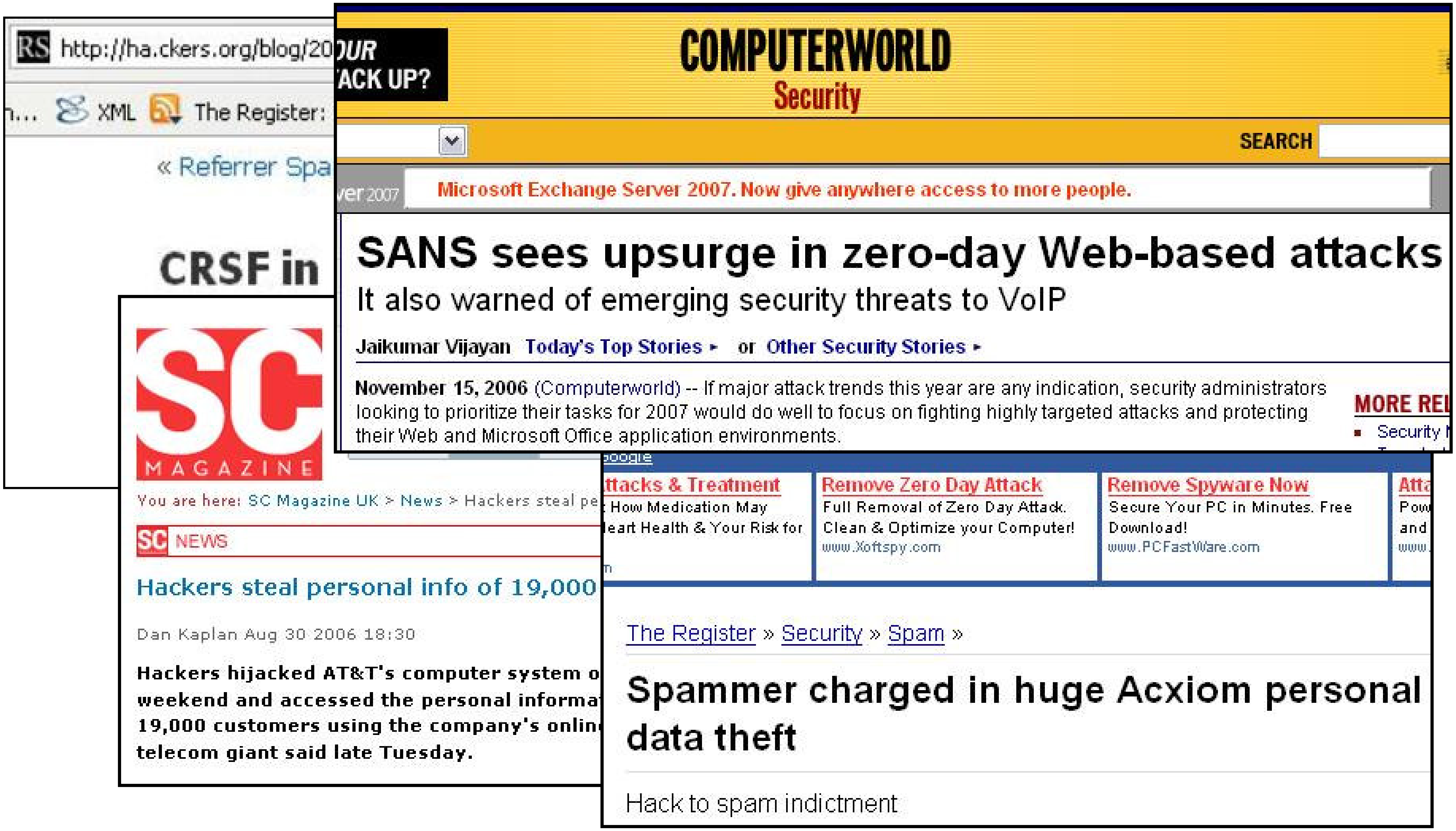
Password:

Applications Give Unprecedented Access to Critical Business Data

Identity Theft

Service Disruption

Just off the press



RS http://ha.ckers.org/blog/20

h... XML The Register:

« Referrer Spa

CRSF in

OUR

ACK UP?

COMPUTERWORLD

Security

SEARCH

ver 2007

SANS sees upsurge in zero-day Web-based attacks

It also warned of emerging security threats to VoIP

Jaikumar Vijayan Today's Top Stories ▸ or Other Security Stories ▸

November 15, 2006 (Computerworld) -- If major attack trends this year are any indication, security administrators looking to prioritize their tasks for 2007 would do well to focus on fighting highly targeted attacks and protecting their Web and Microsoft Office application environments.

MORE REL

- Security

SC MAGAZINE

You are here: SC Magazine UK > News > Hackers steal pe

SC NEWS

Hackers steal personal info of 19,000

Dan Kaplan Aug 30 2006 18:30

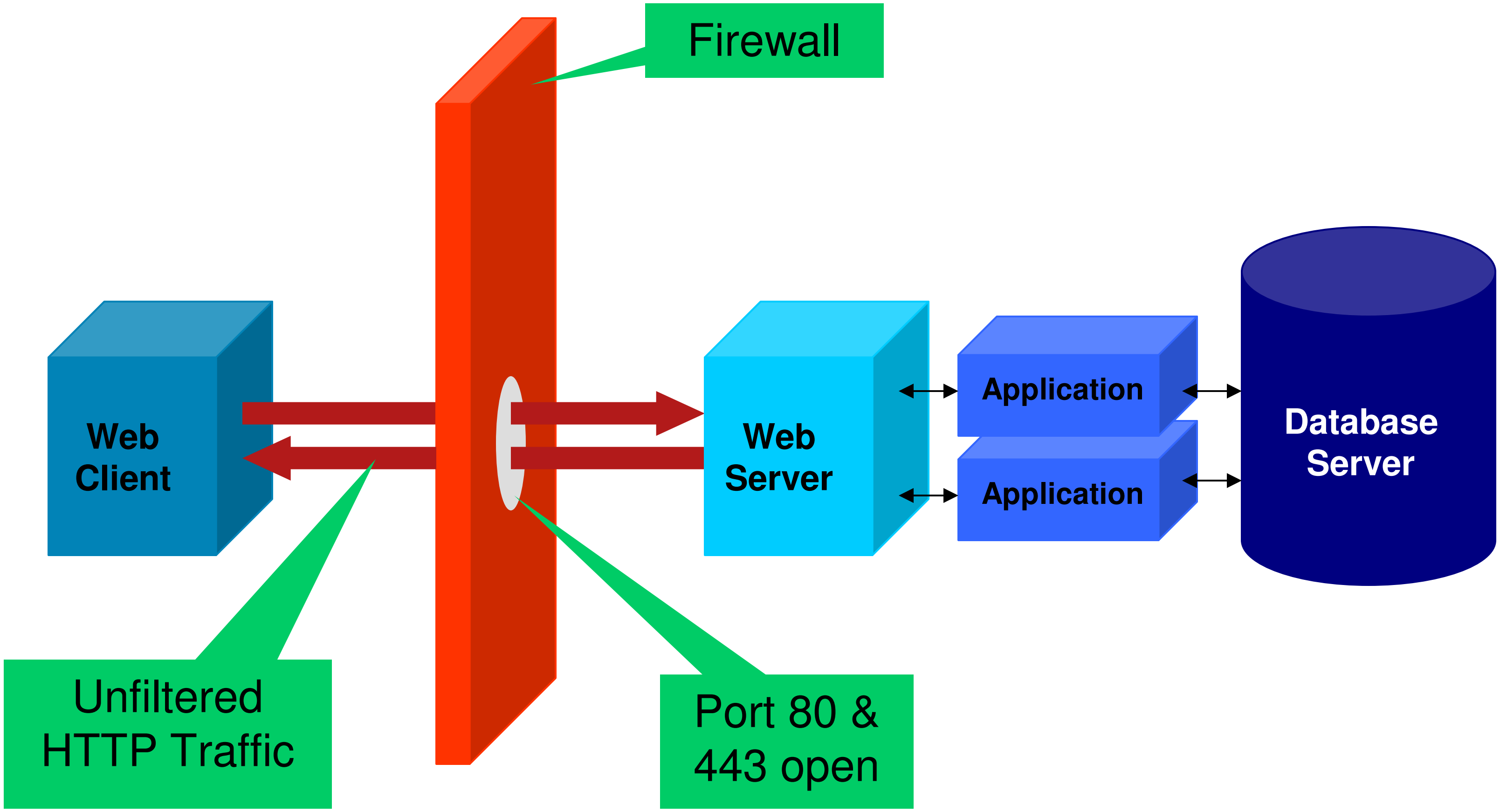
Hackers hijacked AT&T's computer system o weekend and accessed the personal informa 19,000 customers using the company's onlin telecom giant said late Tuesday.

The Register » Security » Spam »

Spammer charged in huge Acxiom personal data theft

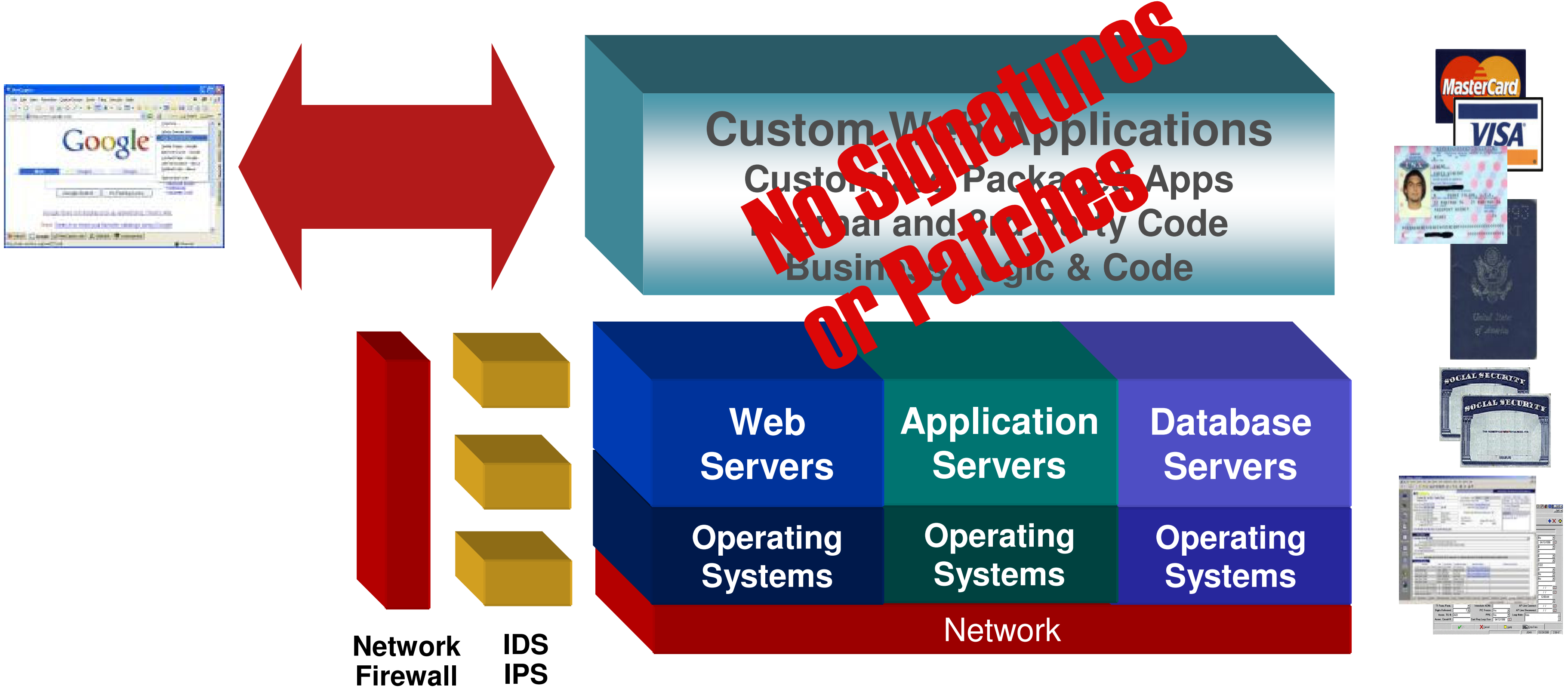
Hack to spam indictment

Existing Network Firewalls Can Not Adequately Inspect HTTP Protocol & Data



Focus of Attacks Moves the Application Layer

75% of Attacks Focused Here



Custom Web Applications
Customized Packaged Apps
Internal and 3rd Party Code
Business Logic & Code

No Signatures or Patches

Web Servers | Application Servers | Database Servers
Operating Systems | Operating Systems | Operating Systems
Network

Network Firewall

IDS IPS

Comprehensive Application Security is the Answer!

Why Not Just Fix the Code?

Every 1000 lines of code averages 15 critical security defects

(US Dept of Defense)

The average business app has 150,000-250,000 lines of code

(Software Magazine)

The average security defect takes 75 minutes to diagnose and 6 hours to fix

(5-year Pentagon Study)

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

Attacks!

OWASP’s Top 10 attacks

- A1 **Unvalidated Input**
- A2 Broken Access Control
- **A3 Broken Authentication and Session Management**
- A4 **Cross Site Scripting**
- A5 Buffer Overflow
- A6 **Injection Flaws**
- A7 Improper Error Handling
- A8 Insecure Storage
- A9 Application Denial of Service
- A10 Insecure Configuration Management

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#Top_Ten_Overview

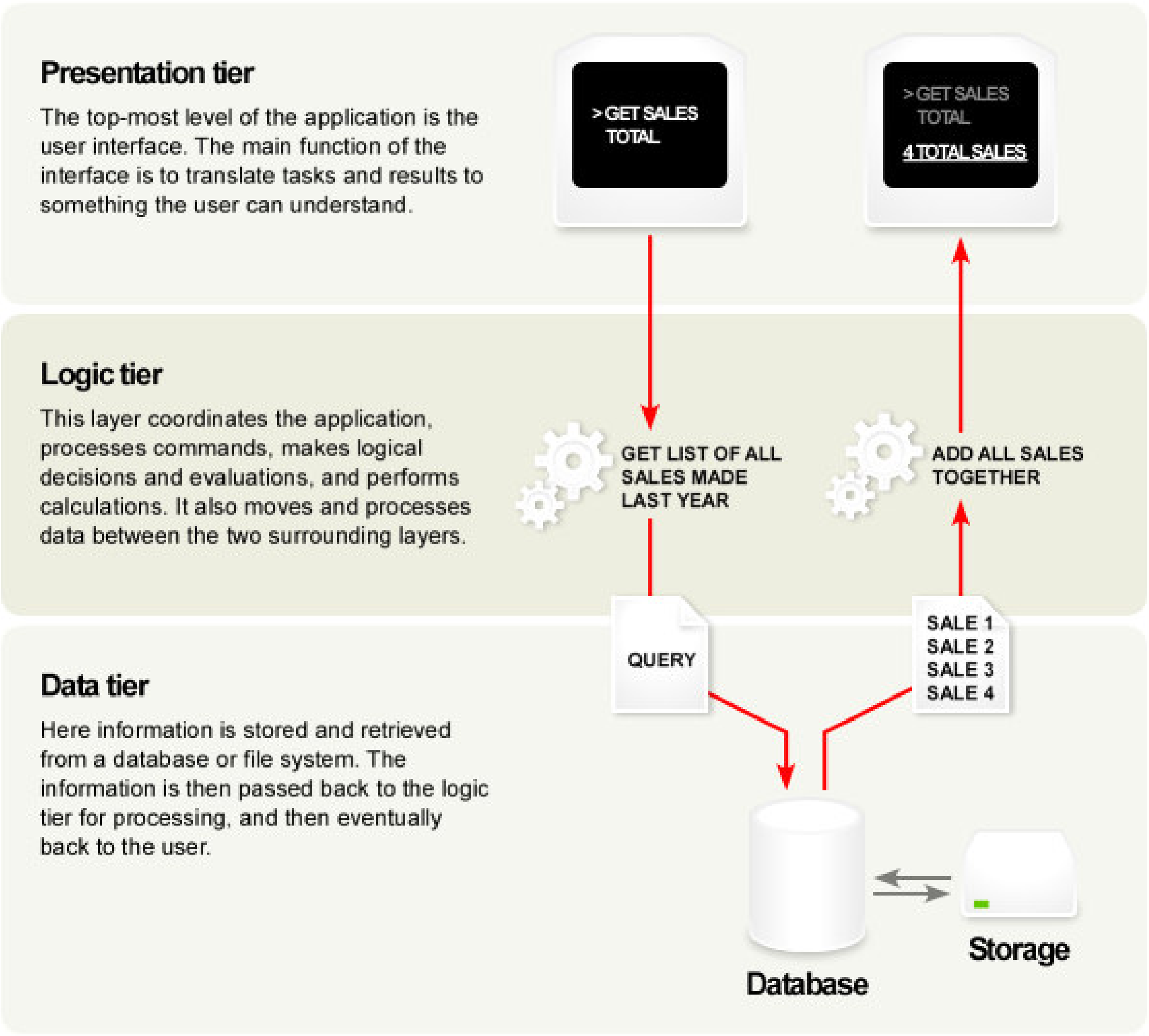
Attack #1: Unvalidated input

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.

Attack #1 – Unvalidated Input

What is it?

- Web Apps use parameters to obtain information from the client

How is this vulnerable?

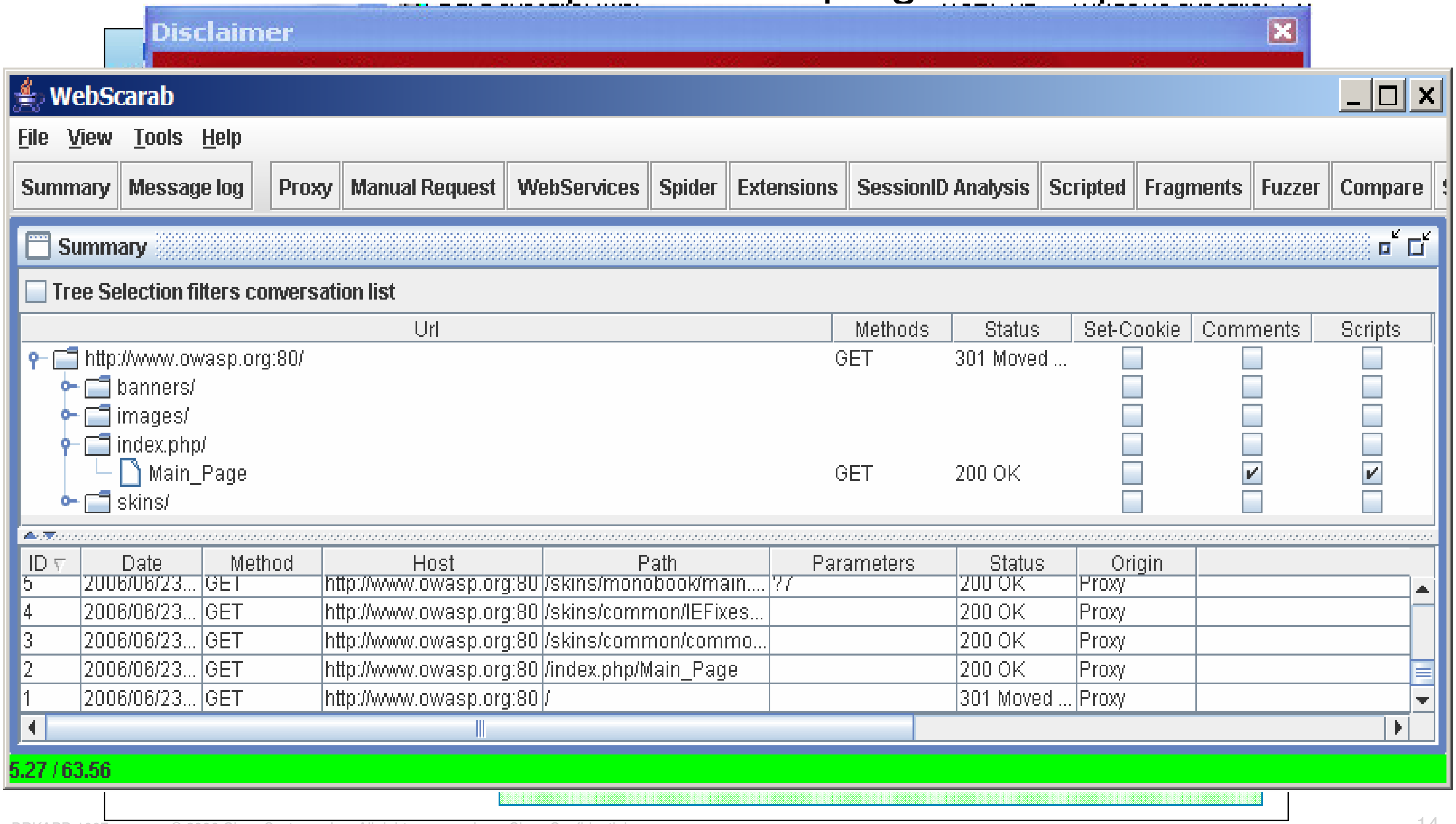
- Developers focus on the legal values of parameters and how they should be utilized
- Too much credit given to client-side browser validation
- Little if any attention is given to the effect of incorrect values

Result

- The application acts according to the changed information, potentially giving access to other user's accounts, confidential info, or anything else on the computer – vector for 90% of web-based attacks!

Attack #1 – Unvalidated Input

Client-side validation is pointless – plugins and proxies exist



☐ Tree Selection filters conversation list

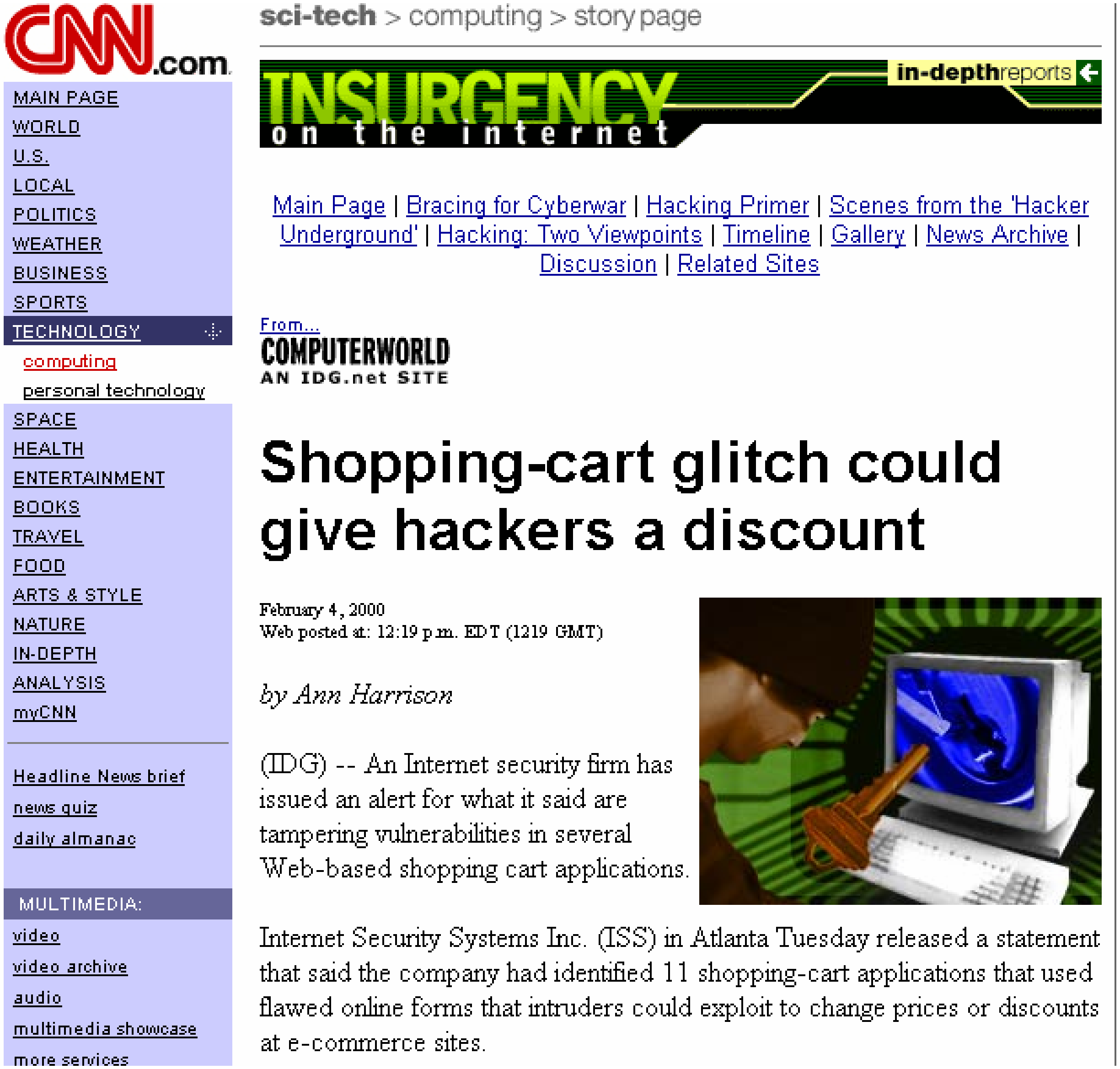
Url	Methods	Status	Set-Cookie	Comments	Scripts
http://www.owasp.org:80/	GET	301 Moved ...	☐	☐	☐
banners/			☐	☐	☐
images/			☐	☐	☐
index.php/			☐	☐	☐
Main_Page	GET	200 OK	☐	☑	☑
skins/			☐	☐	☐

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main....	??	200 OK	Proxy
4	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/IEFixes...		200 OK	Proxy
3	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/commo...		200 OK	Proxy
2	2006/06/23...	GET	http://www.owasp.org:80	/index.php/Main_Page		200 OK	Proxy
1	2006/06/23...	GET	http://www.owasp.org:80	/		301 Moved ...	Proxy

5.27 / 63.56

Attack #1: Parameter Tampering – Shopping Cart Exploit

- Although this is an old exploit, applications are still vulnerable to similar types of attacks.
- New technologies such as SOAP contain old exploits.



From...
COMPUTERWORLD
AN IDG.net SITE

Shopping-cart glitch could give hackers a discount

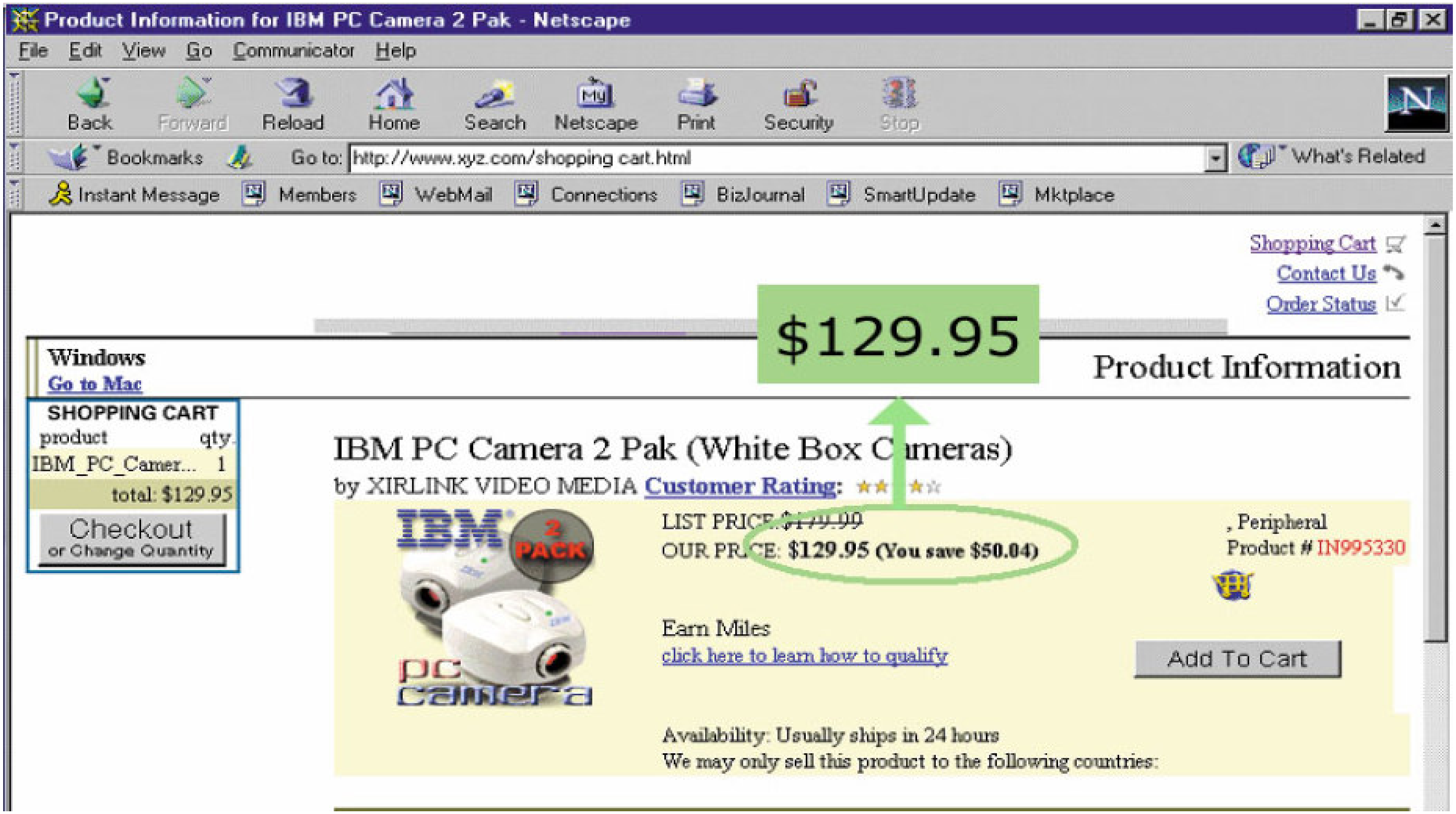
February 4, 2000
Web posted at: 12:19 p.m. EDT (1219 GMT)

by Ann Harrison

(IDG) -- An Internet security firm has issued an alert for what it said are tampering vulnerabilities in several Web-based shopping cart applications.

Internet Security Systems Inc. (ISS) in Atlanta Tuesday released a statement that said the company had identified 11 shopping-cart applications that used flawed online forms that intruders could exploit to change prices or discounts at e-commerce sites.

Attack #1: Parameter Tampering For Fun and Profit


Product Information for IBM PC Camera 2 Pak - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks
What's Related
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Shopping Cart
Contact Us
Order Status
Windows
Go to Mac
Checkout
or Change Quantity
Customer Rating:
Add To Cart
$129.95

Go to: http://www.xyz.com/shopping cart.html

SHOPPING CART

product	qty.
IBM_PC_Camer...	1
total: $129.95	

Product Information

IBM PC Camera 2 Pak (White Box Cameras)

by XIRLINK VIDEO MEDIA Customer Rating:

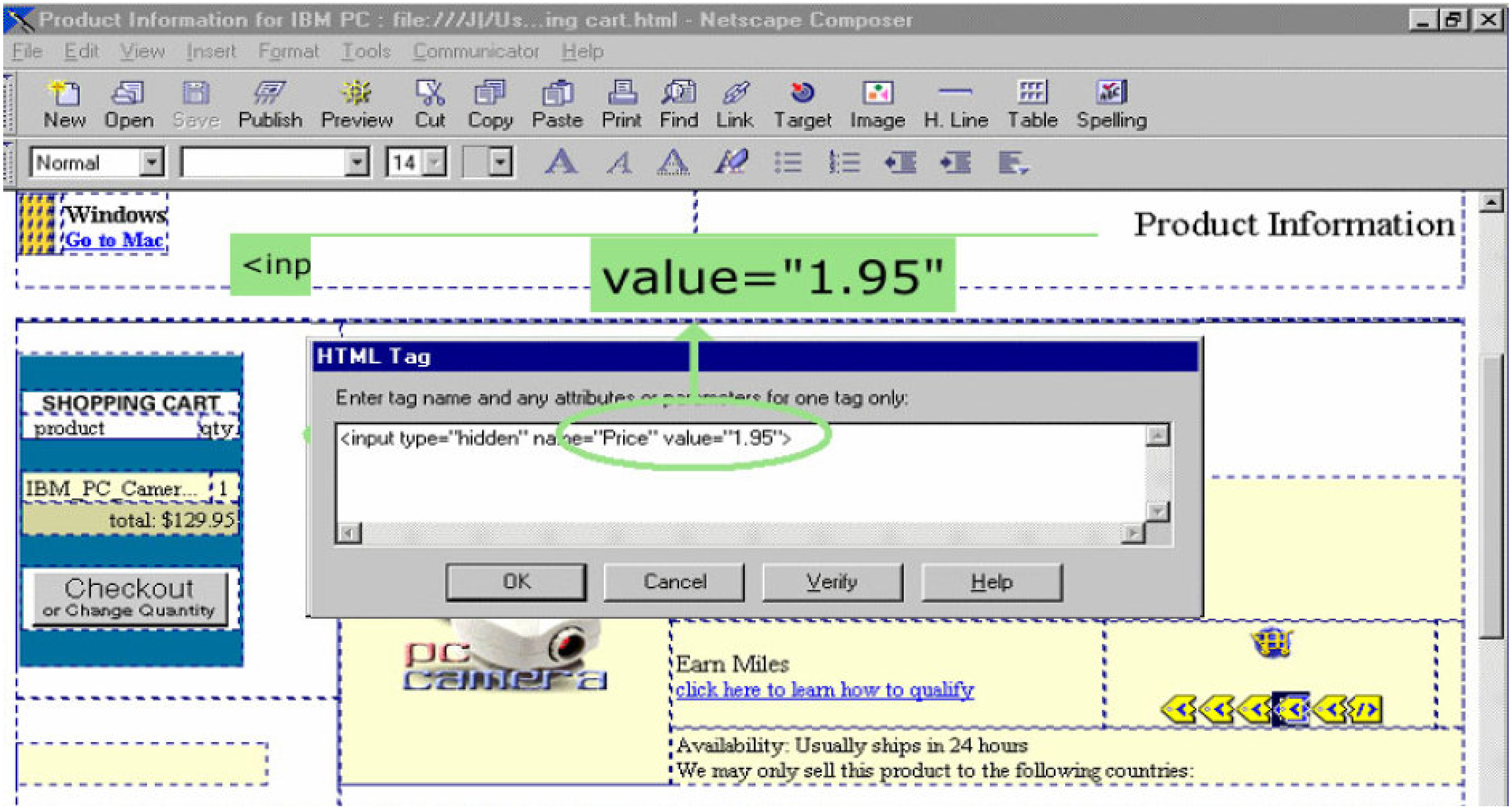
LIST PRICE: ~~$179.99~~
OUR PRICE: $129.95 (You save $50.04)

, Peripheral
Product # IN995330

Earn Miles
click here to learn how to qualify

Availability: Usually ships in 24 hours
We may only sell this product to the following countries:

Attack #1: Parameter Tampering For Fun and Profit



Product Information for IBM PC : file:///J|/Us...ing cart.html - Netscape Composer
File Edit View Insert Format Tools Communicator Help
New Open Save Publish Preview Cut Copy Paste Print Find Link Target Image H. Line Table Spelling
Normal
14
Windows
Go to Mac
Product Information
SHOPPING CART
product
qty
IBM_PC_Camer...
1
total: $129.95
Checkout
or Change Quantity
Earn Miles
click here to learn how to qualify
Availability: Usually ships in 24 hours
We may only sell this product to the following countries:
OK
Cancel
Verify
Help

<inp

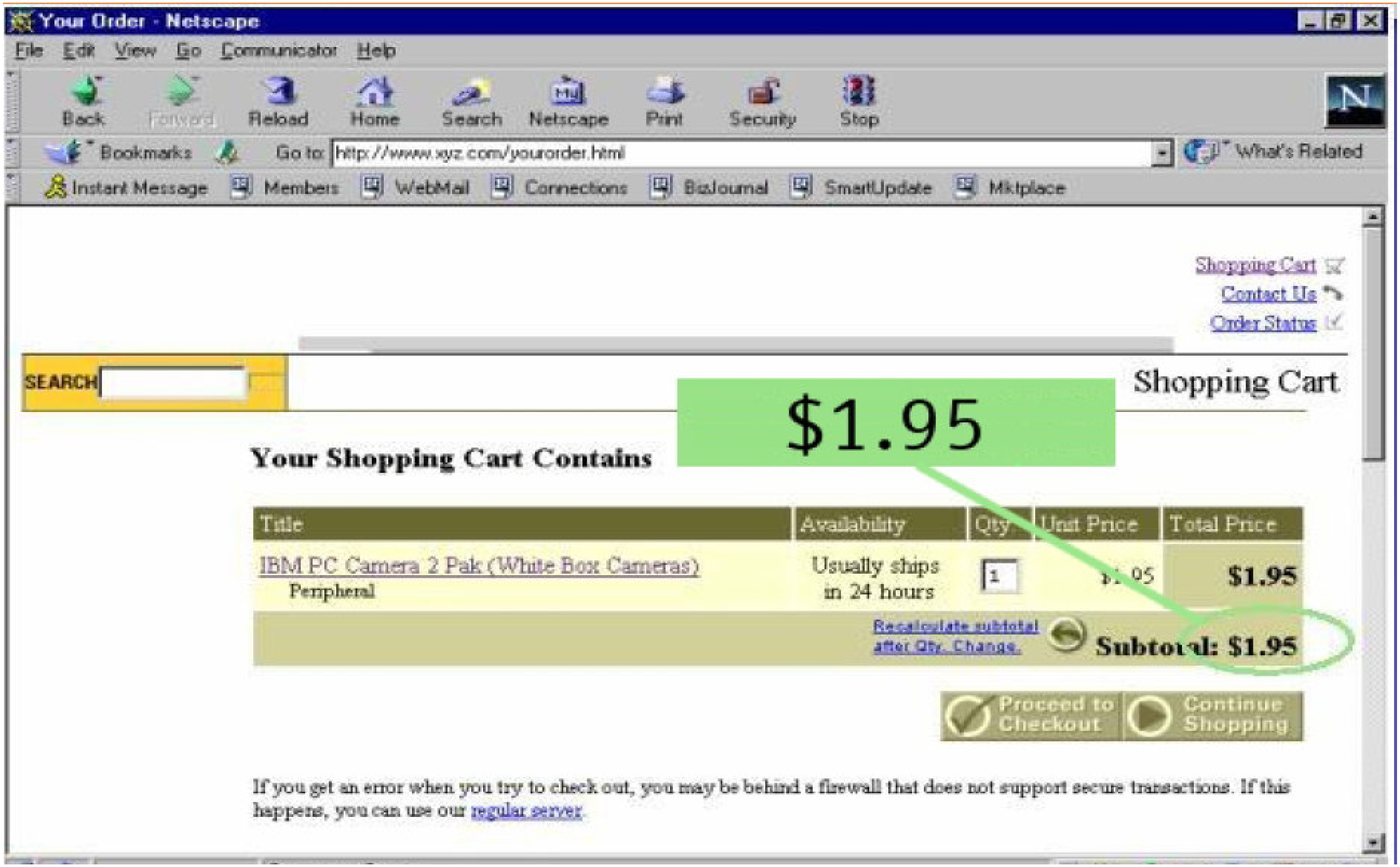
value="1.95"

HTML Tag

Enter tag name and any attributes or parameters for one tag only:

```
<input type="hidden" name="Price" value="1.95">
```

Attack #1: Parameter Tampering For Fun and Profit


Your Order - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to:
What's Related
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Shopping Cart
Contact Us
Order Status
SEARCH
$1.95
Recalculate subtotal after Qty. Change
Proceed to Checkout
Continue Shopping

Go to: http://www.xyz.com/yourorder.html

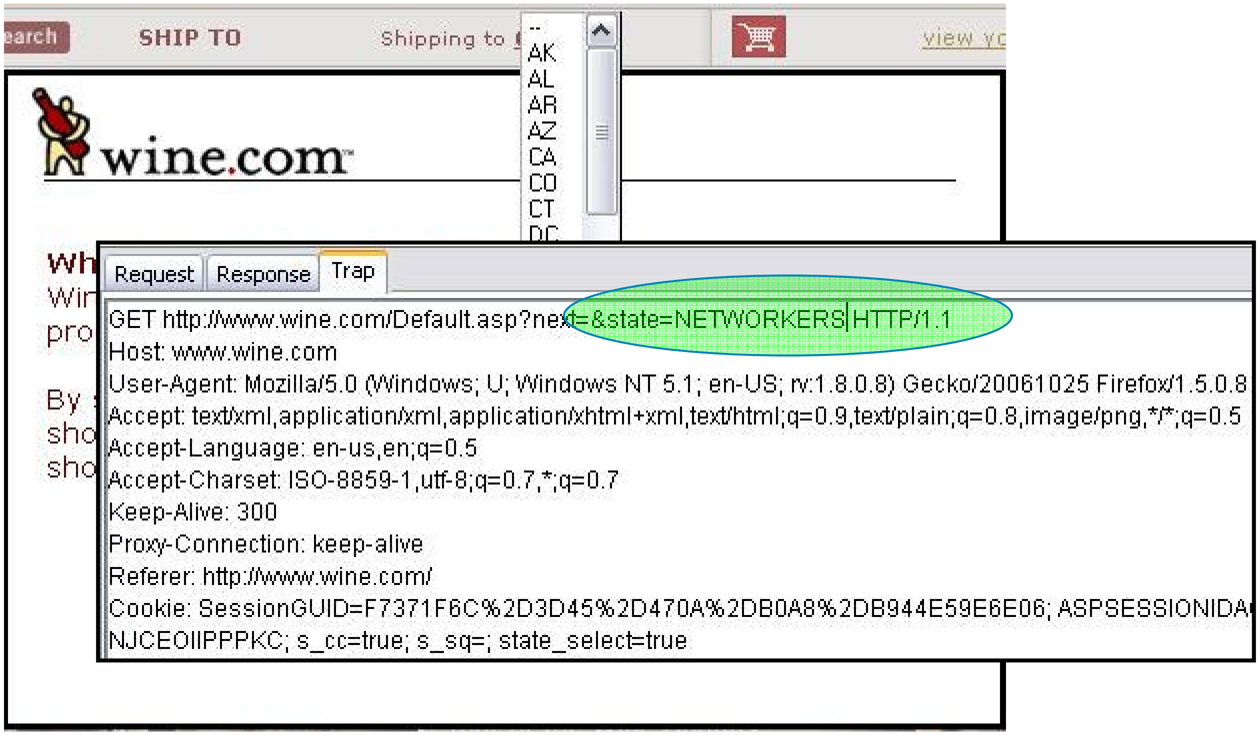
Shopping Cart

Your Shopping Cart Contains

Title	Availability	Qty	Unit Price	Total Price
IBM PC Camera 2 Pak (White Box Cameras) Peripheral	Usually ships in 24 hours	1	$1.95	**$1.95**
				Subtotal: $1.95

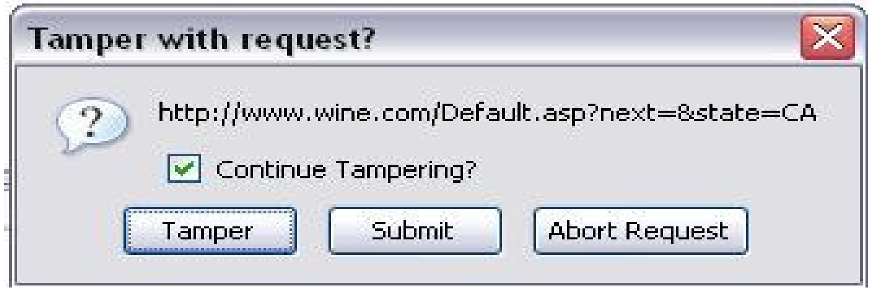
If you get an error when you try to check out, you may be behind a firewall that does not support secure transactions. If this happens, you can use our regular server.

Attack #1 – Unvalidated Input: What If?



```
GET http://www.wine.com/Default.asp?next=&state=NETWORKERS HTTP/1.1
Host: www.wine.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://www.wine.com/
Cookie: SessionGUID=F7371F6C%2D3D45%2D470A%2DB0A8%2DB944E59E6E06; ASPSESSIONIDA
NJCEOIIPPPKC; s_cc=true; s_sq=; state_select=true
```

- How will your application react to totally unexpected input?

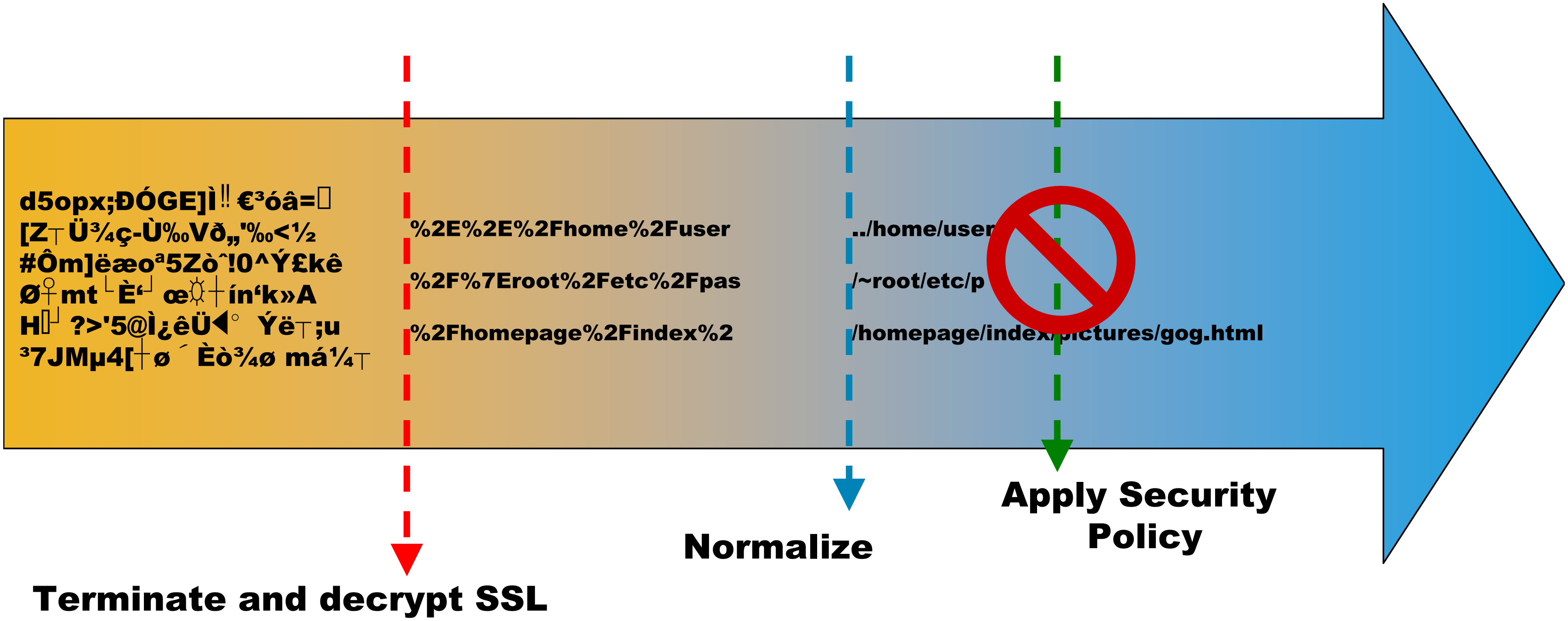

Tamper with request?

http://www.wine.com/Default.asp?next=&state=CA

☑ Continue Tampering?

Attack #1: Using Encoding To Bypass Server-Side Filters/Validation *(aka "thank you RFC2279")*

http://0306.0205.0333.0031/%6E%65%74%77%6F%72%6B%65%72%73



d5opx;ÐÓGE]Ì‼ €³óâ=
[Z┬Ü¾ç-Ù‰Vð„'‰<½
#Ôm]ëæoª5Zòˆ!0^Ý£kê
Ø♀mt└È‘┘ œ☼┼ín‘k»A
H┘ ?>'5@Ì¿êÜ◄° Ýë┬;u
³7JMµ4[┼ø ´ Èò¾ø má¼┬

%2E%2E%2Fhome%2Fuser
%2F%7Eroot%2Fetc%2Fpas
%2Fhomepage%2Findex%2

../home/user
/~root/etc/p
/homepage/index/pictures/gog.html

Terminate and decrypt SSL

Normalize

Apply Security Policy

URL canonicalization stops attacks disguised by encoding URLs

Unvalidated Input Attacks: Summary

How serious?

- The mother of two of the top attacks (XSS and SQL Injection)
- Series of browser-side tools, ranging from plugins to full-blown proxies

  Paros, Suru, Burp Suite, WebScarab, Fiddler

Damage potential?

- **Very High**

Countermeasures

- Always perform server-side input validation
- Be aware of evasion techniques using various encodings – see the encoding cheat sheet at http://ha.ckers.org/xss.html
- Cisco's Web Application Firewall can apply regexes and length checks to URL query parameters or POST data, it always canonicalizes URLs by default

Attack #2: 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

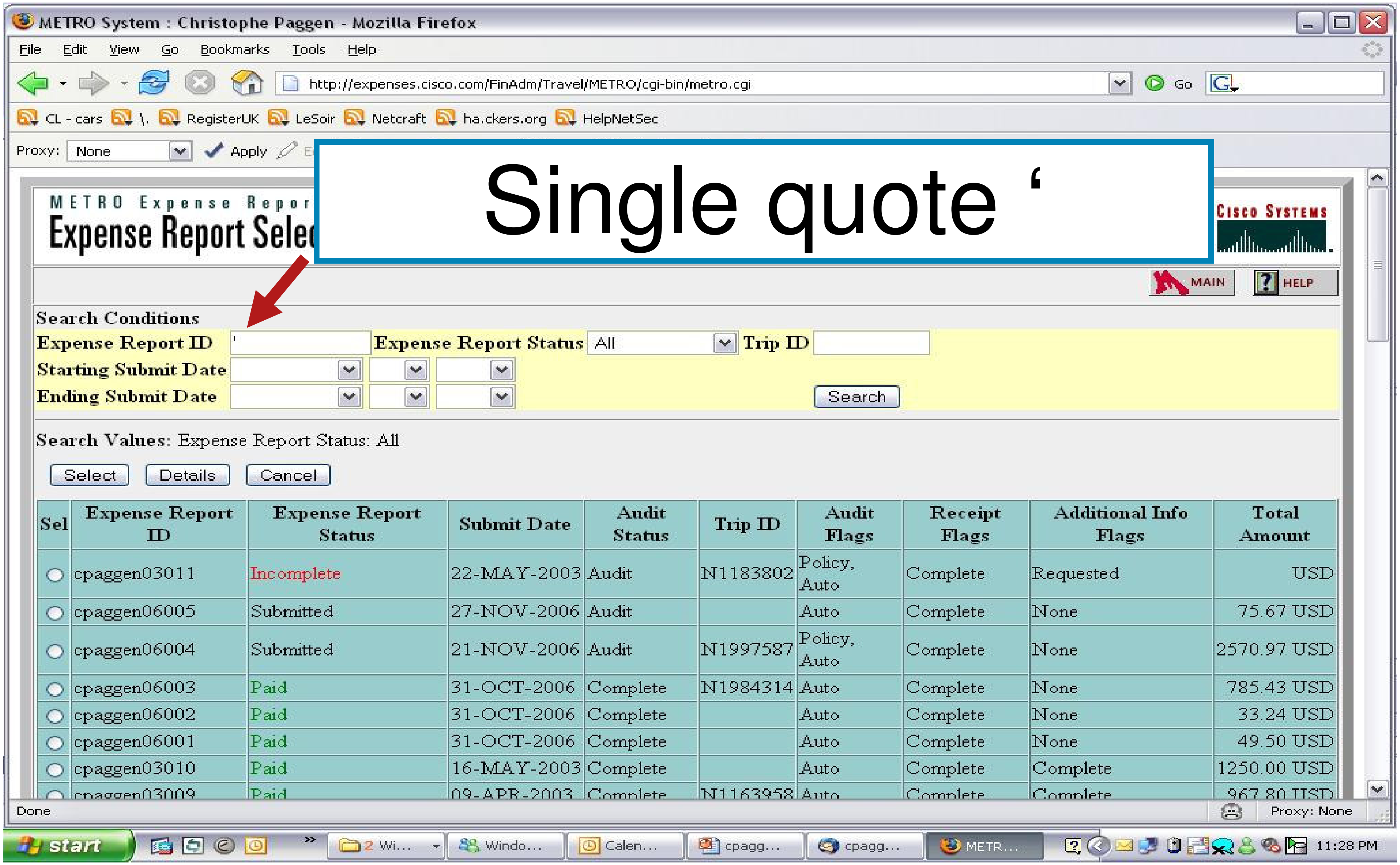
  insert new records in a database

  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 System : Christophe Paggen - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://expenses.cisco.com/FinAdm/Travel/METRO/cgi-bin/metro.cgi
Go
CL - cars
\.
RegisterUK
LeSoir
Netcraft
ha.ckers.org
HelpNetSec
Proxy: None
Apply
METRO Expense Repor
Expense Report Selec
Cisco Systems
MAIN
HELP

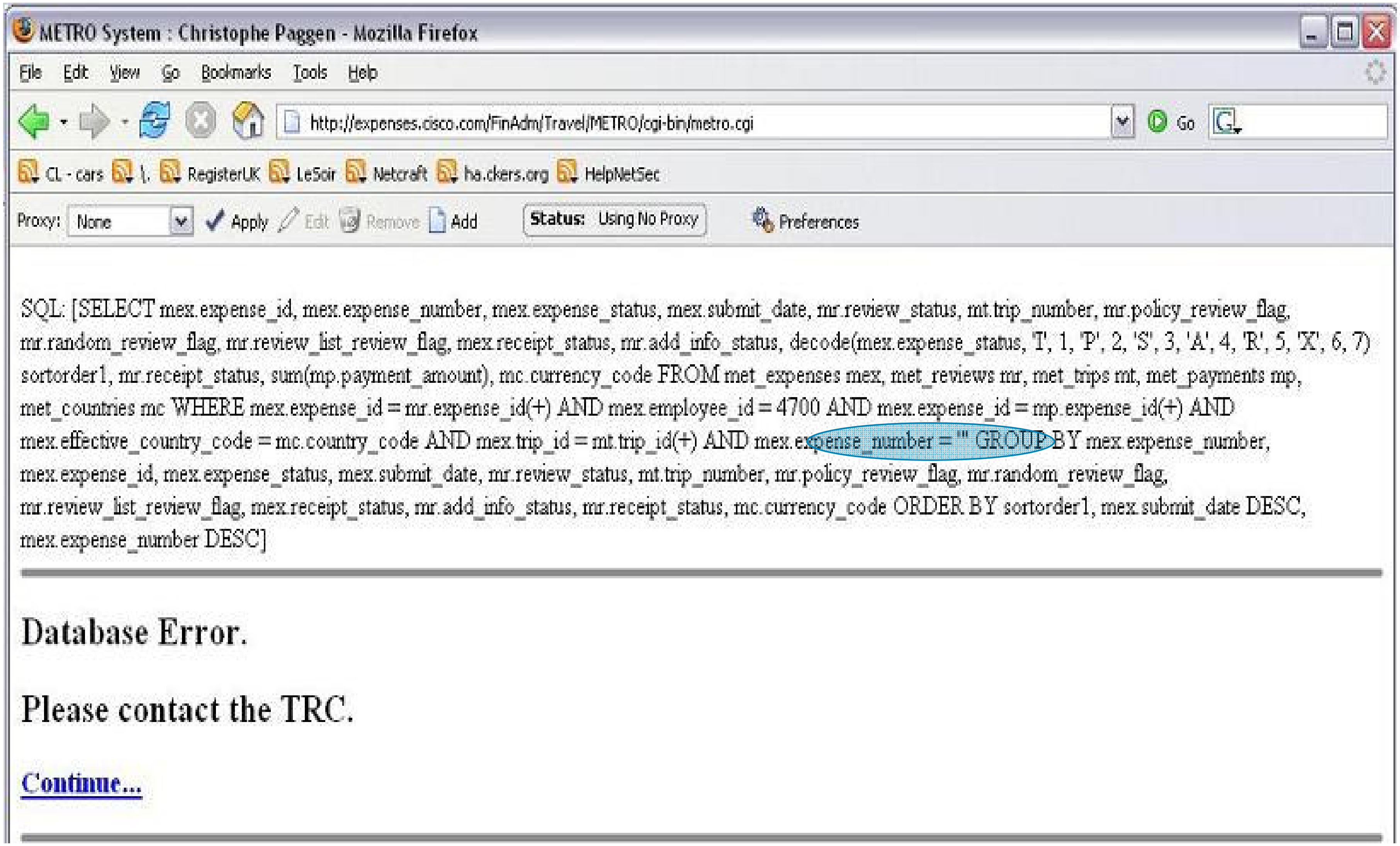
Search Conditions

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

Search Values: Expense Report Status: All

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
http://expenses.cisco.com/FinAdm/Travel/METRO/cgi-bin/metro.cgi
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...

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

Typical SQL query

```
SELECT * FROM users
WHERE login = 'victor'
AND password = '123'
```

Typical ASP/MS SQL Server login syntax

```
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.

SQL Injection Example

- Last year, hackers breached the computer files of merchant processor CardSystems Inc., exposing 40 million card accounts and directly affecting about 200,000. The breach eventually led to the sale of CardSystems' assets to Pay By Touch Inc.
- SQL injection was used by the attackers to install malicious script on the CardSystems web application database which where scheduled to run every four days, extract records, zip them and export them to an FTP site.

http://www.webappsec.org/projects/whid/list_class_sql_injection.shtml

SQL/Command Injection: Summary

How serious?

- Result of poor/inexistant input validation
- Extremely easy to carry out: just a browser is sufficient
- Major vector of identity theft, DB denial of service (shutdown the DB)

Damage potential?

- **Very High**

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 #3: XSS / Cross-site Scripting

Attack #3 – Cross Site Scripting

What is it?

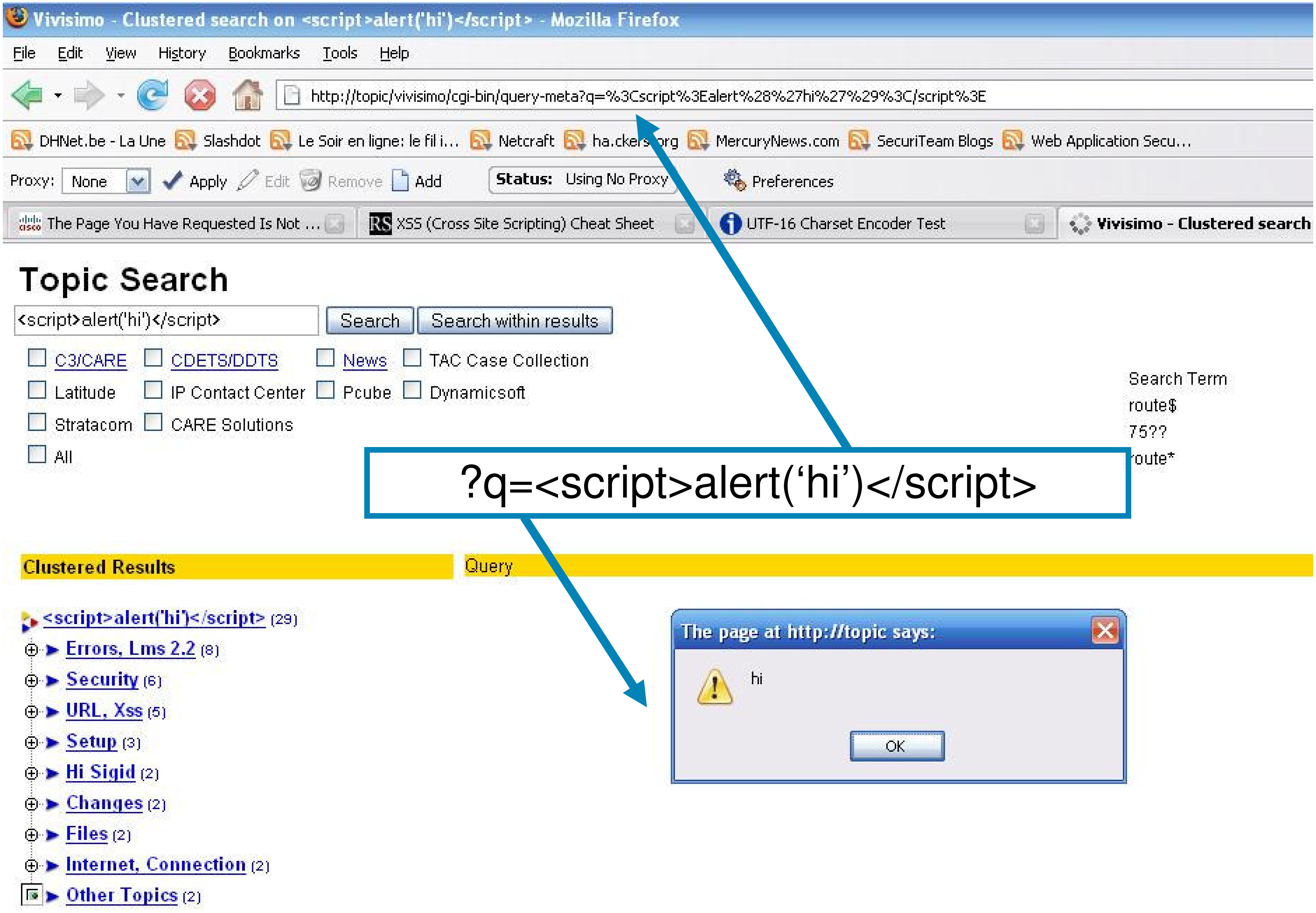
- User feeds data to the web application
- Web application doesn’t sanitize input and echoes back the query
- The unvalidated data contains a piece of JavaScript that is executed in the context of the user’s browser session.
- A carefully formed link sent to a victim (usually by mail) results in the JavaScript code being run in the victim’s browser, sending information to the hacker.

Why does Cross Site Scripting happen?

- Unvalidated input – example: html is permitted into query parameter
- Application blindly echoes request back to browser

Result

- “Virtual hijacking” of the session by stealing cookies
- Any information flowing between the legitimate user and site can be manipulated or transmitted to a 3rd party.


Vivisimo - Clustered search on <script>alert('hi')</script> - Mozilla Firefox
File Edit View History Bookmarks Tools Help
DHNet.be - La Une
Slashdot
Le Soir en ligne: le fil i...
Netcraft
ha.ckers.org
MercuryNews.com
SecuriTeam Blogs
Web Application Secu...
Proxy: None
Apply
Edit
Remove
Add
Status: Using No Proxy
Preferences
The Page You Have Requested Is Not ...
XSS (Cross Site Scripting) Cheat Sheet
UTF-16 Charset Encoder Test
Vivisimo - Clustered search

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

Topic Search

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

Search
Search within results

□ C3/CARE □ CDETS/DDTS □ News □ TAC Case Collection
□ Latitude □ IP Contact Center □ Pcube □ Dynamicsoft
□ Stratacom □ CARE Solutions
□ All

Search Term
route$
75??
route*

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

Clustered Results

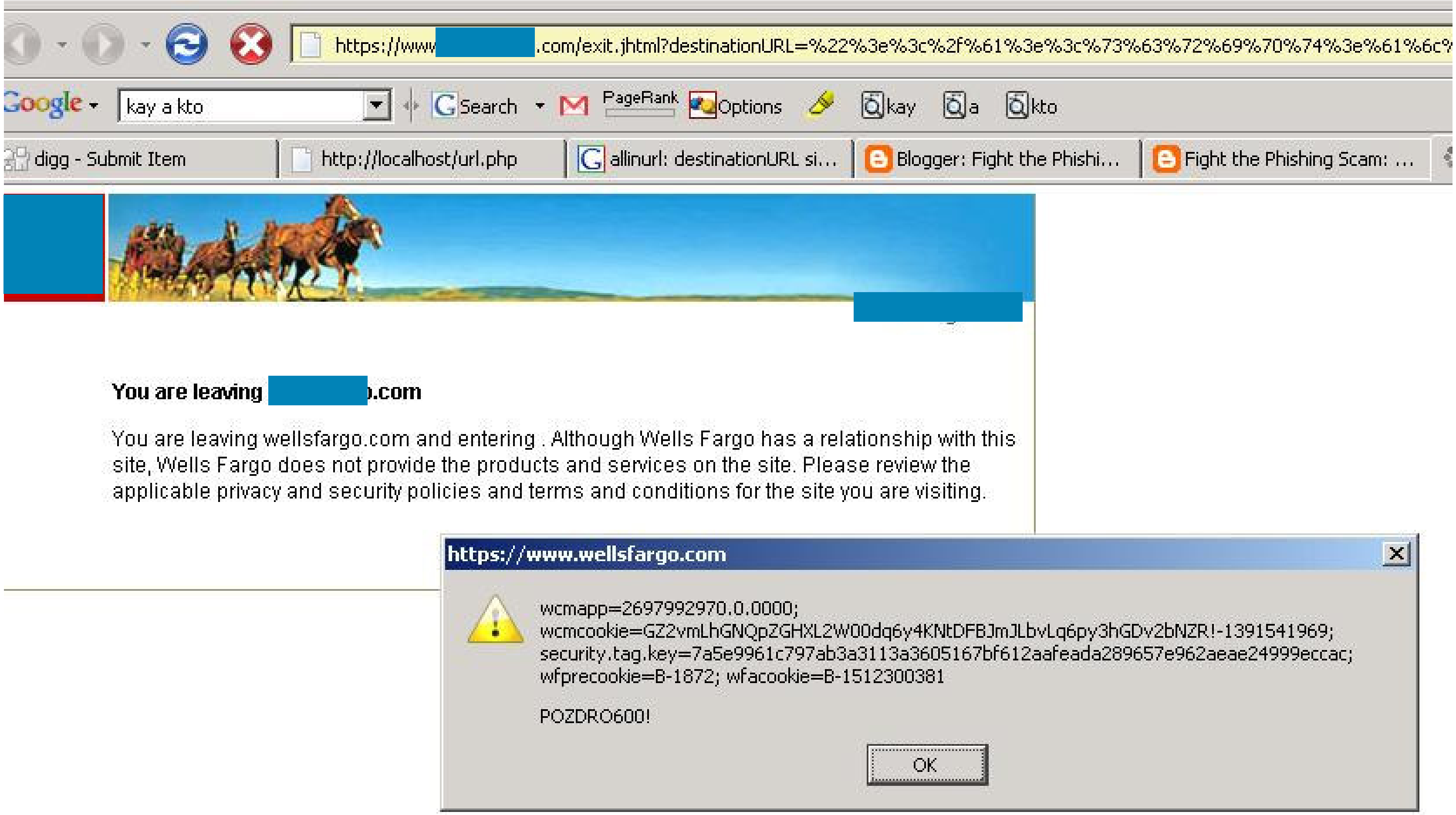
Query

- <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

Popular U.S. Bank—Live Example


Google
kay a kto
Search
PageRank
Options
kay
a
kto
digg - Submit Item
http://localhost/url.php
allinurl: destinationURL si...
Blogger: Fight the Phishi...
Fight the Phishing Scam: ...

https://www[redacted].com/exit.jhtml?destinationURL=%22%3e%3c%2f%61%3e%3c%73%63%72%69%70%74%3e%61%6c%

[redacted]

[redacted]

You are leaving [redacted].com

You are leaving wellsfargo.com and entering . Although Wells Fargo has a relationship with this site, Wells Fargo does not provide the products and services on the site. Please review the applicable privacy and security policies and terms and conditions for the site you are visiting.

https://www.wellsfargo.com

```
wcmapp=2697992970.0.0000;
wcmcookie=GZ2vmLhGNQpZGHXL2W00dq6y4KNtDFBJmJLbvLq6py3hGDv2bNZR!-1391541969;
security.tag.key=7a5e9961c797ab3a3113a3605167bf612aafeada289657e962aeae24999eccac;
wfprecookie=B-1872; wfacookie=B-1512300381

POZDRO600!
```

OK

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?

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

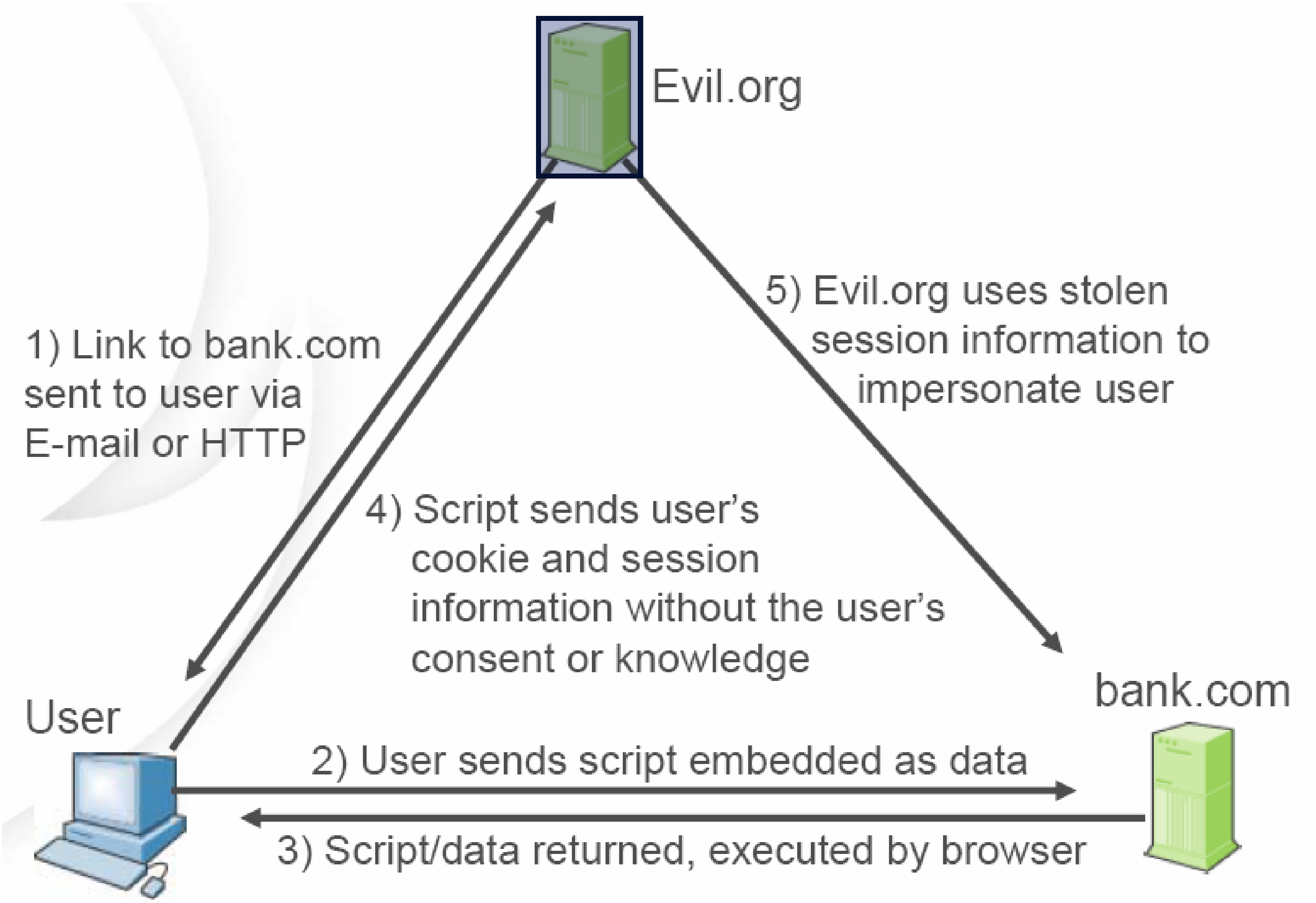
  -check your browsing history

  -scan your subnet for certain hosts

  -etc.

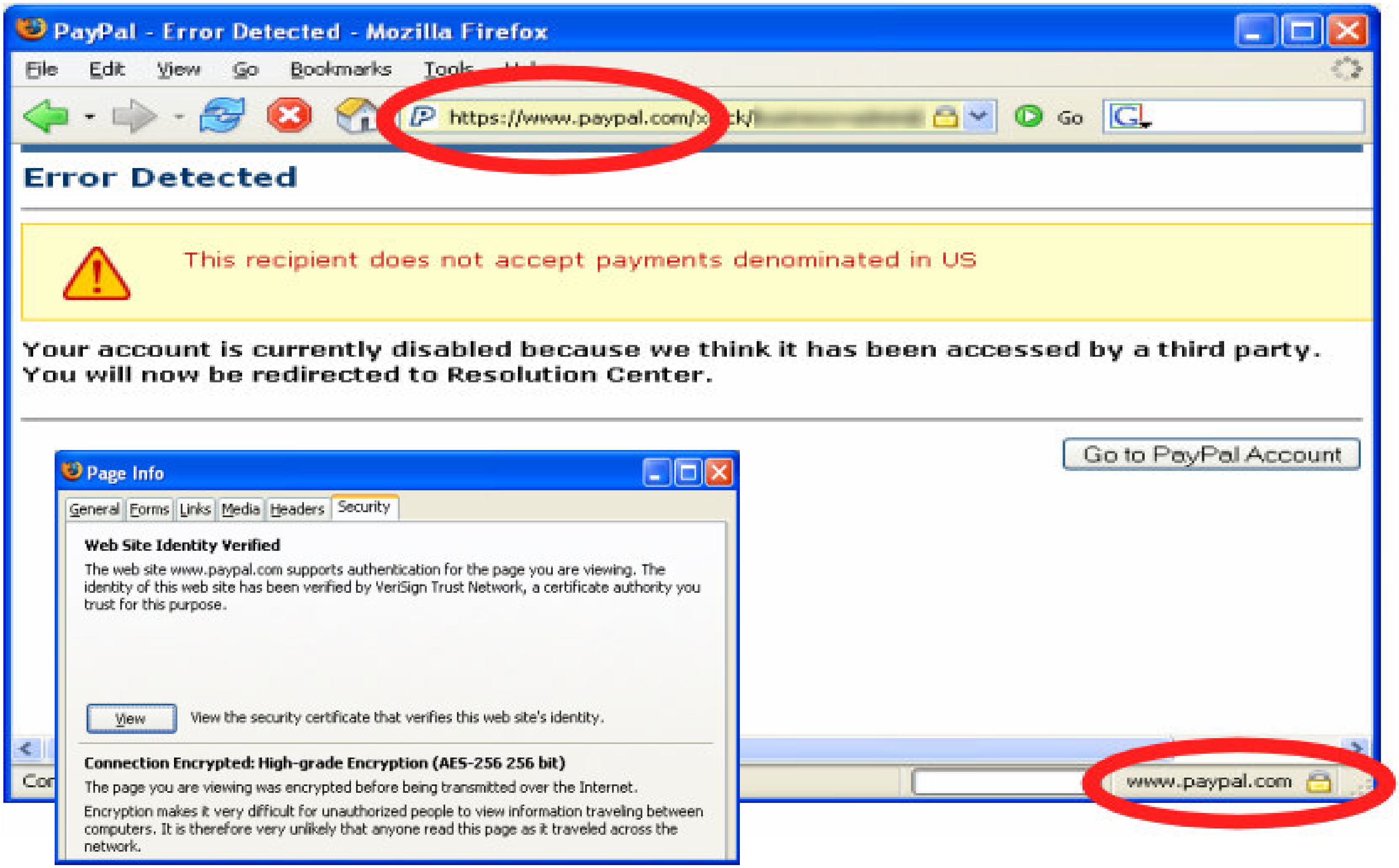
- Commonly used in Phishing emails
- Experts estimate 80% of web sites are vulnerable (http://www.whitehatsec.com/downloads/WHXSSThreats.pdf)

XSS In Action: Stealing Authentication Credentials



Evil.org
1) Link to bank.com sent to user via E-mail or HTTP
5) Evil.org uses stolen session information to impersonate user
4) Script sends user's cookie and session information without the user's consent or knowledge
User
bank.com
2) User sends script embedded as data
3) Script/data returned, executed by browser

Paypal 2006: victims redirected to hacker site via XSS


PayPal - Error Detected - Mozilla Firefox
File Edit View Go Bookmarks Tools
https://www.paypal.com/x ck/[redacted]
Go
Go to PayPal Account
www.paypal.com
Page Info
General Forms Links Media Headers Security
View

Error Detected

This recipient does not accept payments denominated in US

Your account is currently disabled because we think it has been accessed by a third party. You will now be redirected to Resolution Center.

Web Site Identity Verified

The web site www.paypal.com supports authentication for the page you are viewing. The identity of this web site has been verified by VeriSign Trust Network, a certificate authority you trust for this purpose.

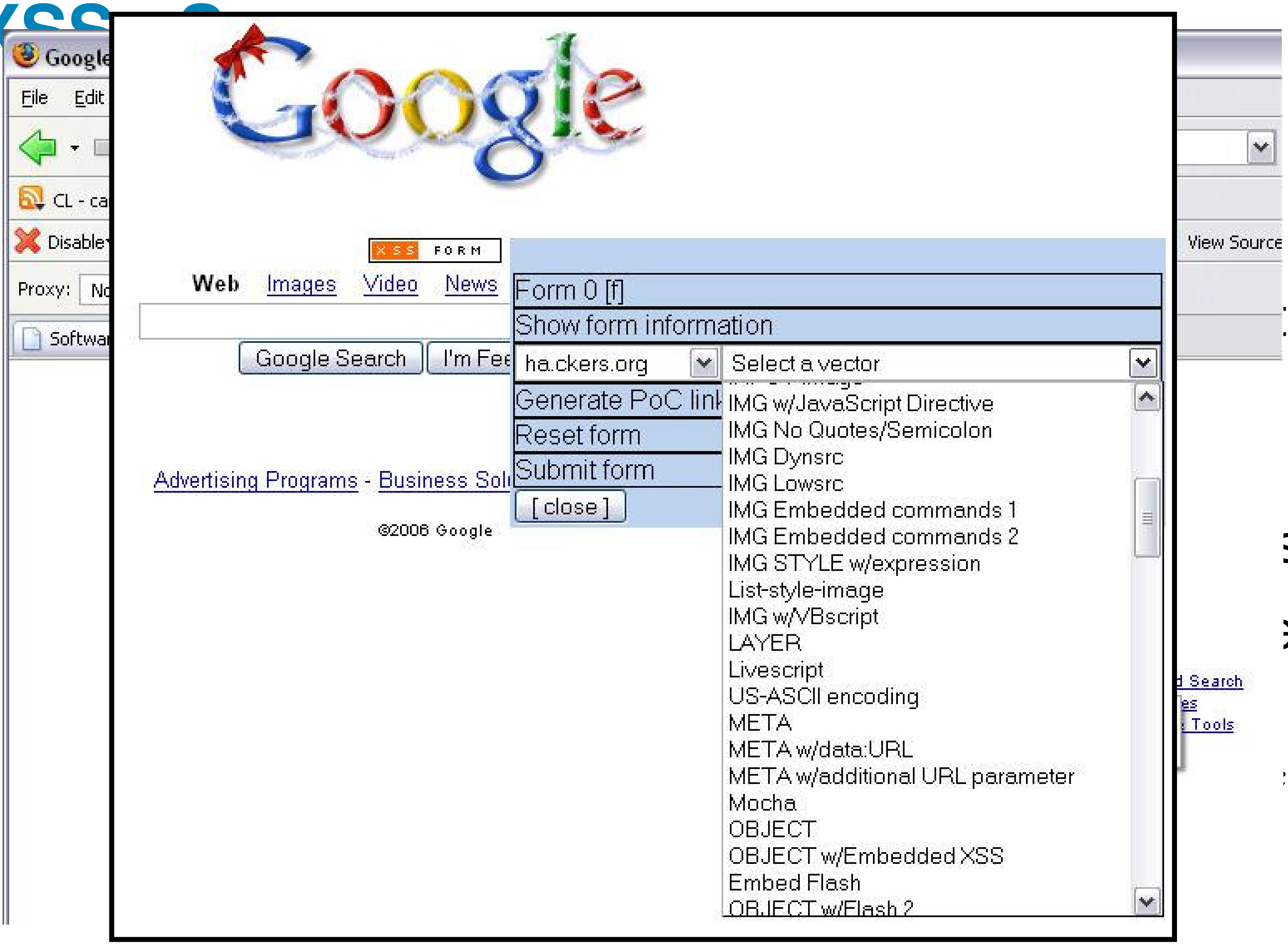
View the security certificate that verifies this web site's identity.

Connection Encrypted: High-grade Encryption (AES-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

XSS


Google
File
Edit
CL - ca
Disable
Proxy:
No
Softwar
View Source
XSS FORM
Web
Images
Video
News
Google Search
I'm Fee
Advertising Programs - Business Sol
©2006 Google
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
d Search
es
Tools

Attack #4: Cookie tampering

Attack #4 – Broken Authentication & Session Management using Cookie Tampering

What is it?

- A cookie that has had its value changed by the user
- Cookie storage is managed and controlled by the user.
- Cookies can be viewed and modified by the user.
- Cookies transferred in the open can be captured and modified by a 3rd party.

Why does it happen?

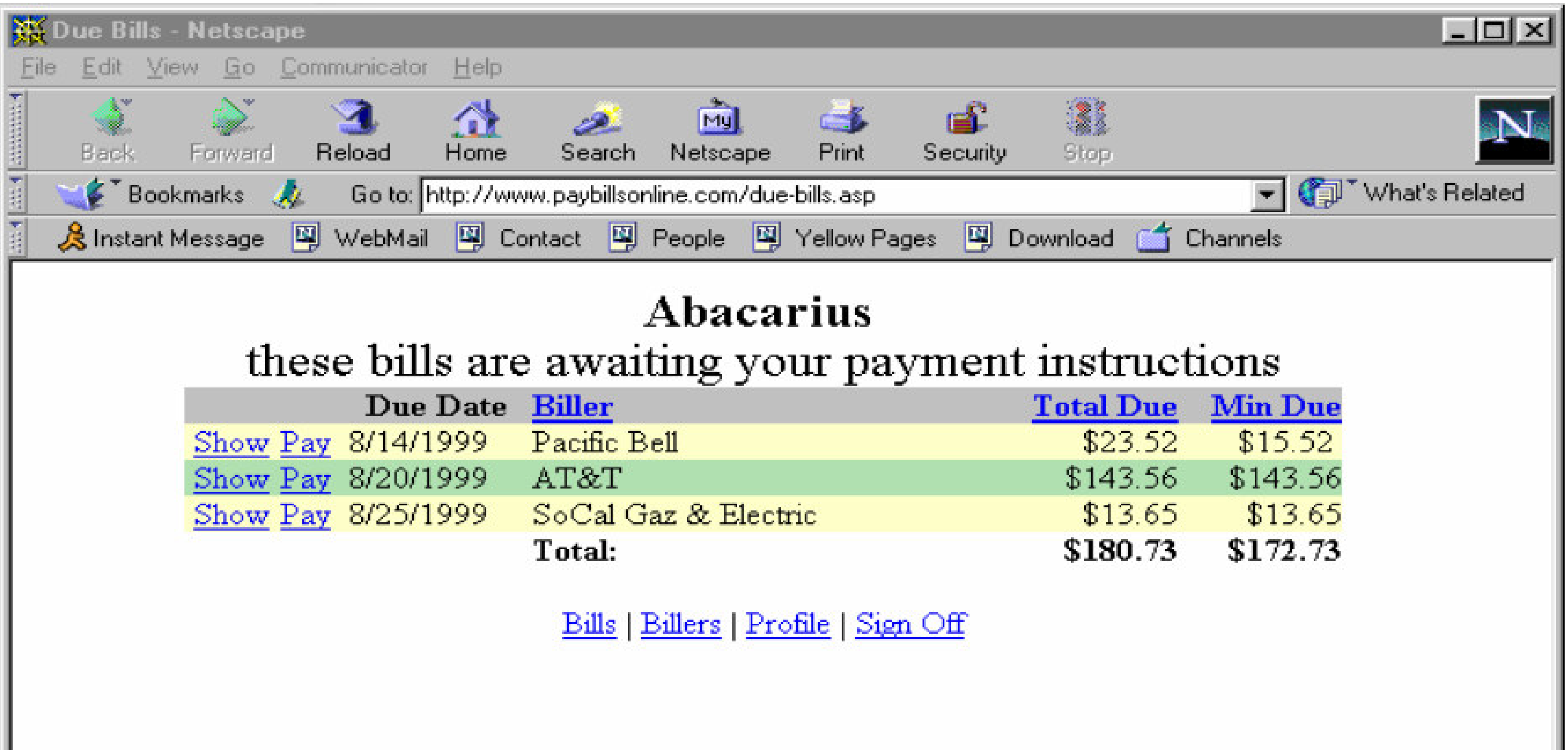
- Cookie information is weakly encrypted or hashed.
- Web application developers are unaware of the threat or lack the cryptographic expertise to prevent tampering.
- The cookie is assumed to contain a certain format of content –an assumption that isn’t verified.

Result

- Identity theft or impersonation by a 3rd party altering the session id or authorization information stored in the cookie.
- DoS or even remote command execution due to buffer overflows

Cookie Tampering – Assuming Another User's Identity

- User 'Abacarius' is paying his bills online



Due Bills - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks
Go to: http://www.paybillsonline.com/due-bills.asp
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels

Abacarius

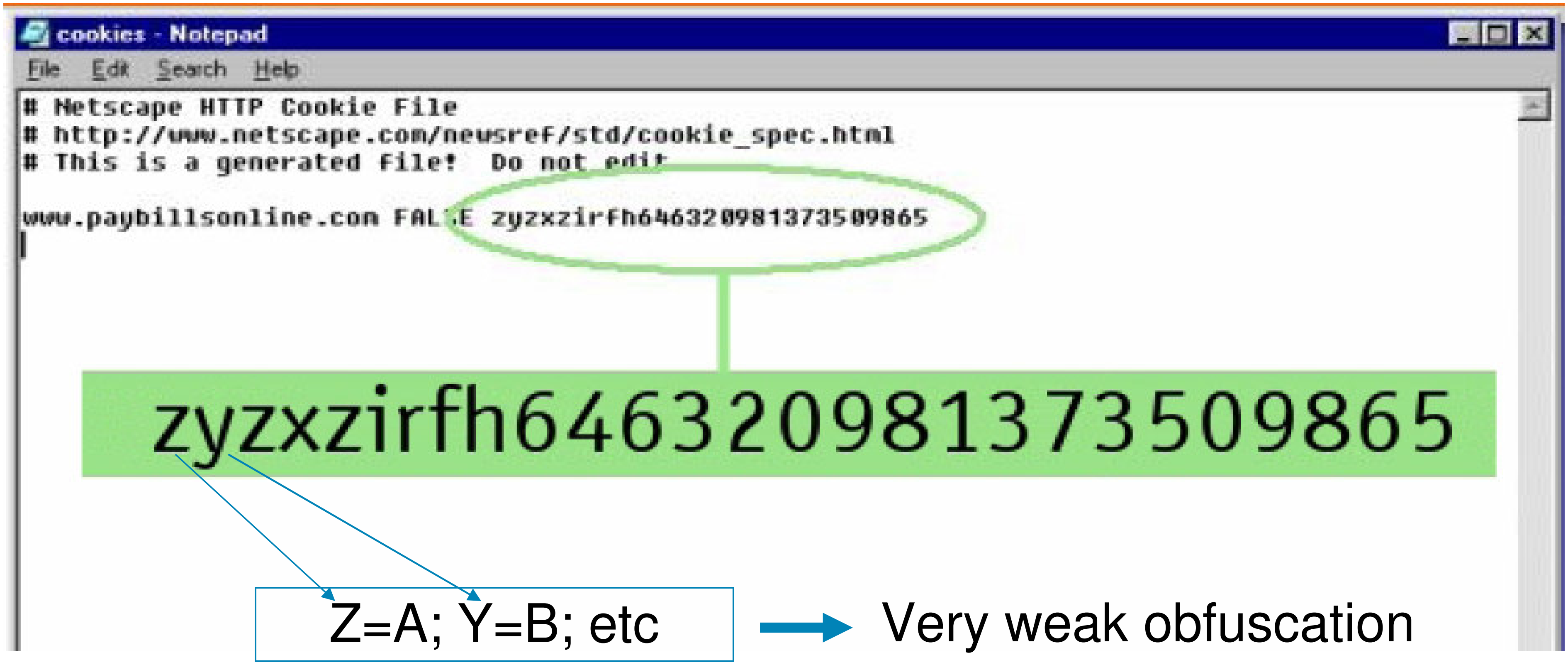
these bills are awaiting your payment instructions

	Due Date	Biller	Total Due	Min Due
Show Pay	8/14/1999	Pacific Bell	$23.52	$15.52
Show Pay	8/20/1999	AT&T	$143.56	$143.56
Show Pay	8/25/1999	SoCal Gaz & Electric	$13.65	$13.65
		Total:	**$180.73**	**$172.73**

Bills | Billers | Profile | Sign Off

Cookie Tampering – Assuming Another User’s Identity

- Abacarius gets bored and looks at the Cookie set by the application



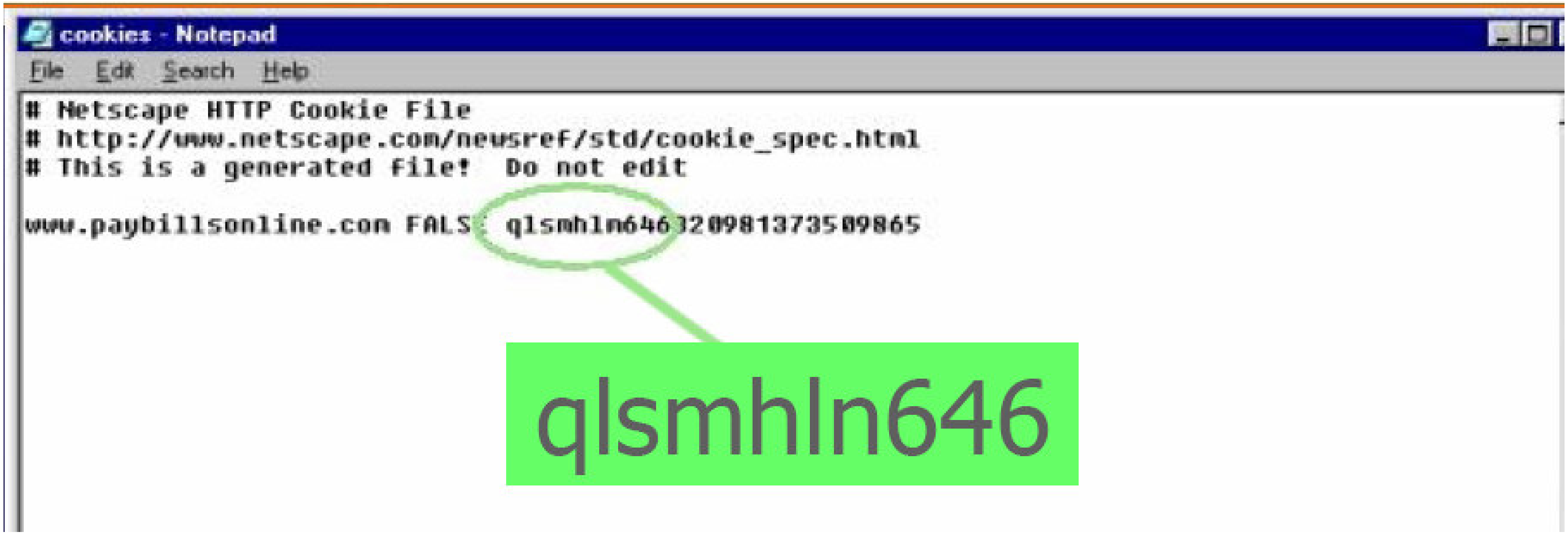
```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file!  Do not edit.

www.paybillsonline.com FALSE zyzxzirfh646320981373509865
```

zyzxzirfh646320981373509865

Z=A; Y=B; etc → Very weak obfuscation

Cookie Tampering – Assuming Another User’s Identity

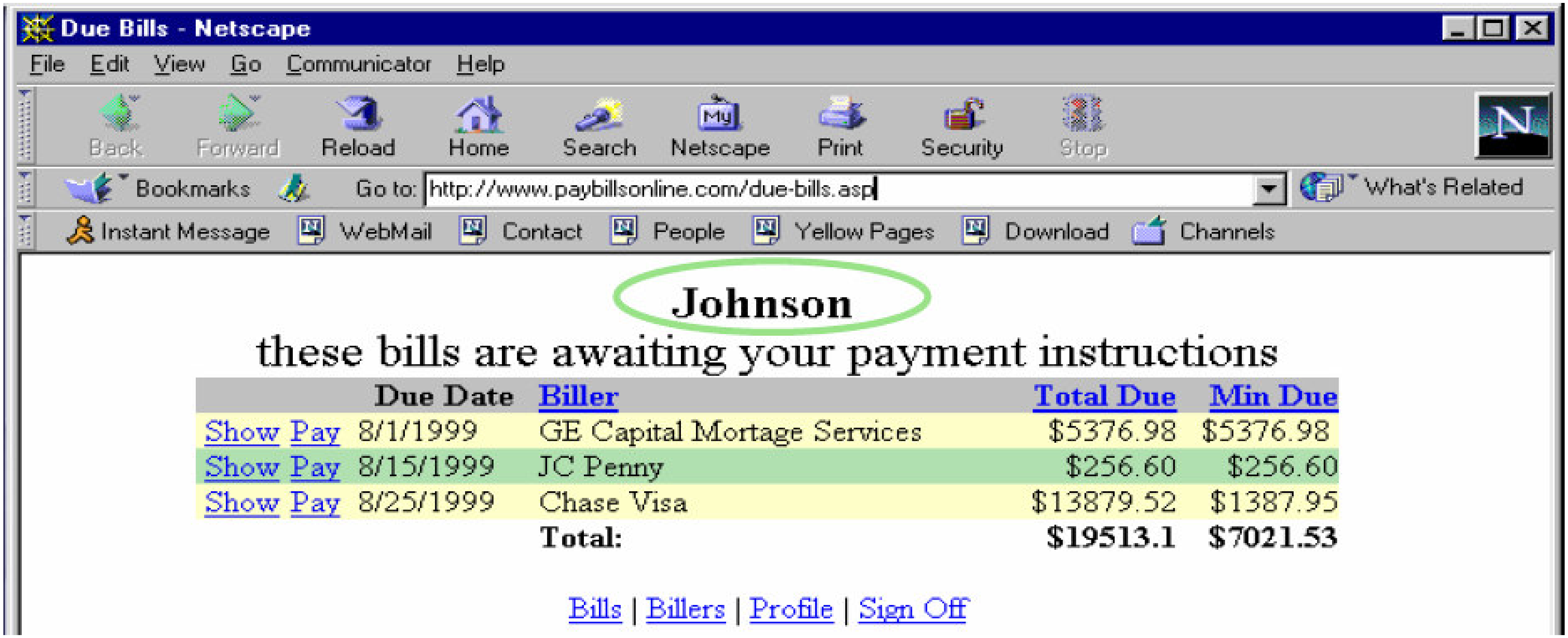
- Abacarius attempts to impersonate user “Johnson”



```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file!  Do not edit

www.paybillsonline.com FALSE qlsmhlm646320981373509865
```

Cookie Tampering – Assuming Another User's Identity

- The new cookie is sent to the web application which interprets it as user "Johnson"



Due Bills - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.paybillsonline.com/due-bills.asp
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels

Johnson

these bills are awaiting your payment instructions

		Due Date	Biller	Total Due	Min Due
Show	Pay	8/1/1999	GE Capital Mortage Services	$5376.98	$5376.98
Show	Pay	8/15/1999	JC Penny	$256.60	$256.60
Show	Pay	8/25/1999	Chase Visa	$13879.52	$1387.95
			Total:	$19513.1	$7021.53

Bills | Billers | Profile | Sign Off

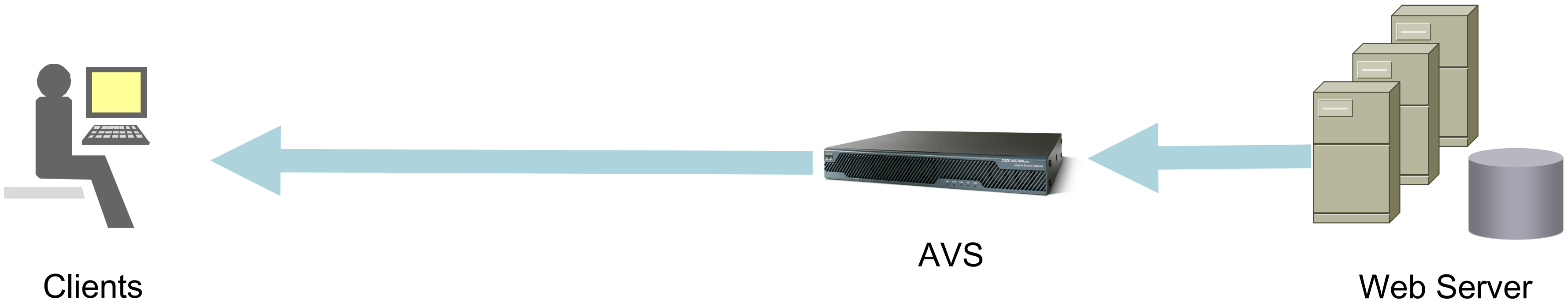
Cookie tampering: mitigation

- No need to reinvent the wheel – existing proven encryption algorithms available to web application developers
- Use modern development frameworks for session maintenance
- Cisco’s WAF can encrypt cookies, only sending an MD5 hash of the actual cookie

  →**immune to tampering**

  →**be aware that replay attacks are still possible**

Cookie Encryption
Example : Server to Client



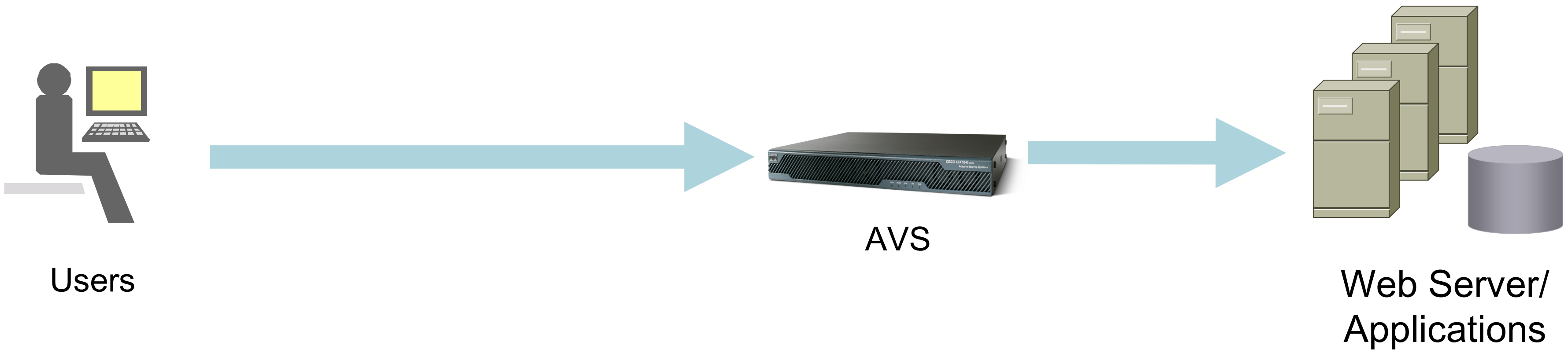
CP_EN-
e7a989b1f1b9e966e47d629eec63302d3571d1677b27fe1beb
ba48df648b2edc=
1-
0c49cd6655b1ffd32746970b5f21876c2c700e088b923d38d50
6fea0e7c15d7a;
expires=Mon, 15-Dec-2007 1:03:00 GMT; path=/;
domain=.google.com; secure

Cookie after processing by AVS for encryption

sess1=1800;
expires=Mon, 15-Dec-2007
1:03:00 GMT;
path=/;
domain=.google.com;
secure

Cookie from Server

Cookie Encryption
Example : Client to Server



CP_EN-
e7a989b1f1b9e966e47d629eec63302d3571d1677b27fe1be
bba48df648b2edc=
1-
0c49cd6655b1ffd32746970b5f21876c2c700e088b923d38d5
06fea0e7c15d7a

Cookie from Client

sess1=1800;

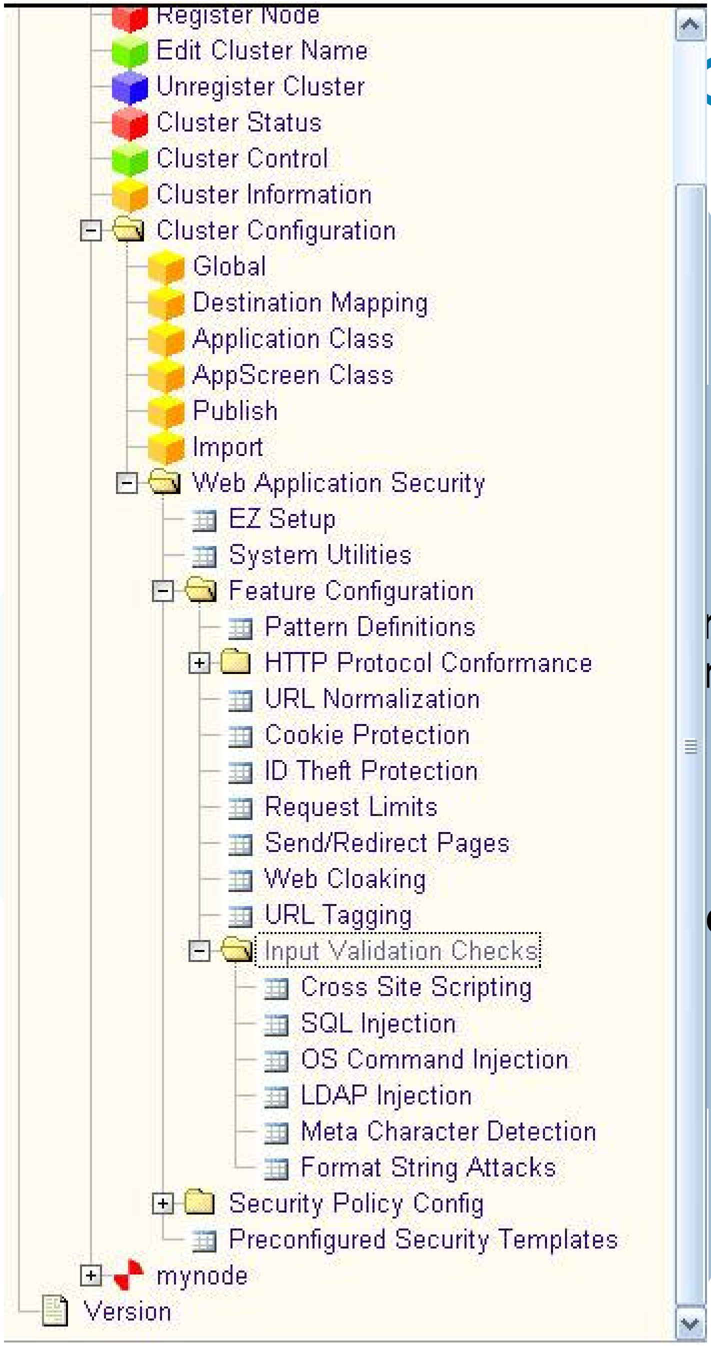
Cookie to Server after being processed and decrypted by AVS

Cisco's Web Application Firewall: AVS 6.0

What is Cisco’s WAF

- Application Velocity System (AVS) 6.0 and higher
- Delivers both app optimization and web app security, even for in-house apps
- Focuses 100% on HTTP
- Ships with hundreds of built-in regular expressions template to catch unvalidated input – users can create regexes too
- Other built-in features such as cookie encryption, SSL termination, URL rewrite, HTTP error code obfuscation, web cloaking
- Can operate as a gateway, an inline bridge, or in monitor mode (no action – just log) – meant to be deployed in front of web server

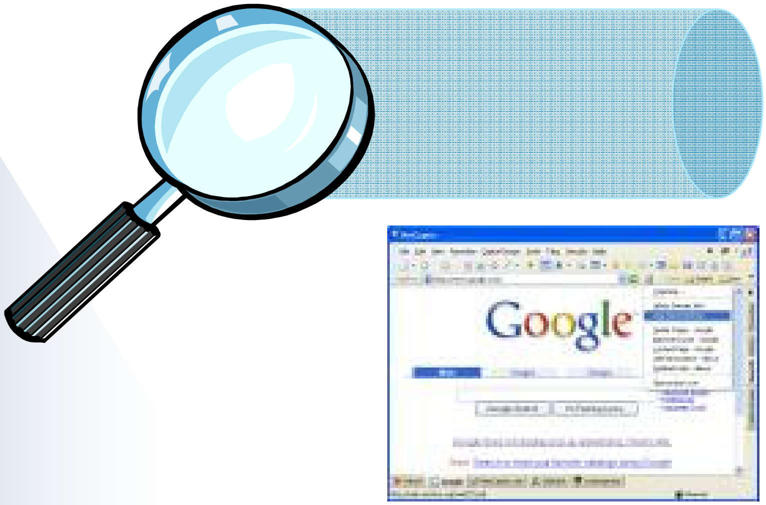
pplications Securely



- Register Node
- Edit Cluster Name
- Unregister Cluster
- Cluster Status
- Cluster Control
- Cluster Information
- Cluster Configuration
  - Global
  - Destination Mapping
  - Application Class
  - AppScreen Class
  - Publish
  - Import
  - Web Application Security
    - EZ Setup
    - System Utilities
    - Feature Configuration
      - Pattern Definitions
      - HTTP Protocol Conformance
      - URL Normalization
      - Cookie Protection
      - ID Theft Protection
      - Request Limits
      - Send/Redirect Pages
      - Web Cloaking
      - URL Tagging
      - Input Validation Checks
        - Cross Site Scripting
        - SQL Injection
        - OS Command Injection
        - LDAP Injection
        - Meta Character Detection
        - Format String Attacks
    - Security Policy Config
    - Preconfigured Security Templates
- mynode
- Version

ng
nce

oits



- Bi – Directional Deep Inspection and Rewrite capabilities
- Positive & Negative Security
- Protocol compliance and anomaly detection
- Transaction logging and report for application security forensics

Fingerprinting – Web Cloaking Protection

Users requesting Web pages
Web Applications

PROBLEM

Responses from the server could reveal software, their version and even topology

```
HTTP/1.1 200 OK
Date: Mon, 07 Jun 2004 14:31:03 GMT
Server: Apache/1.3.29 (Unix) mod_perl/1.29
Connection: close
```

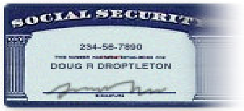
```
HTTP/1.1 200 OK
Date: Mon, 07 Jun 2004 14:31:03 GMT
Server: CISCO WEB SERVER
Connection: close
```

RFC warns against revealing server identity

The AVS can rewrite or hide specific headers in the reply

Data Theft Protection

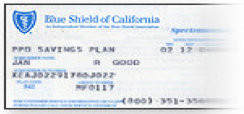
Credit Card
1234-5678-9012-3456



Social Security
123-45-6789

Driver’s License
A123456

Employee ID
S-924600

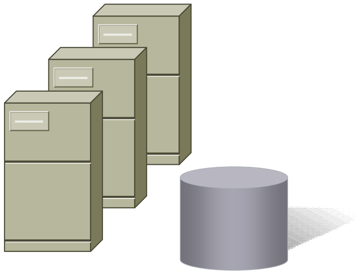


Patient ID
134-AR-627

Users

PROBLEM

Any web app that links to critical data may expose that data to hackers



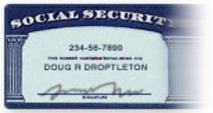
Web
Applications

Data Theft Protection

MASK

Credit Card
XXXX-XXXX-XXXX-3456

MASK



Social Security
XXX-XX-XXXX

BLOCK

Driver's License
A123456

MASK

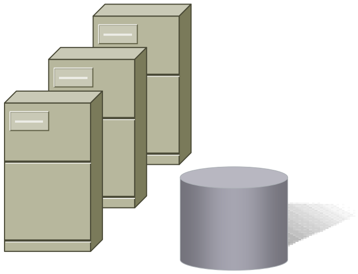
Employee ID
XXXX

BLOCK

Patient ID
134-AR-627

Users

AVS 3120



Web
Applications

Helps ensure compliance with regulations

Summary: So What is the Answer?

- **Do not trust input from the client**
- **Always perform input validation, restrict character set/encoding, escape suspicious patterns BEFORE sending to database**
- **Do not re-invent your own encryption or session management schemes, rely on modern web app dev frameworks**
- **and …**

Defense-in-Depth should include a web application firewall that can quickly, effectively and cost-effectively block attacks at Layer 7