

WEB 3.0 i sigurnost aplikacija



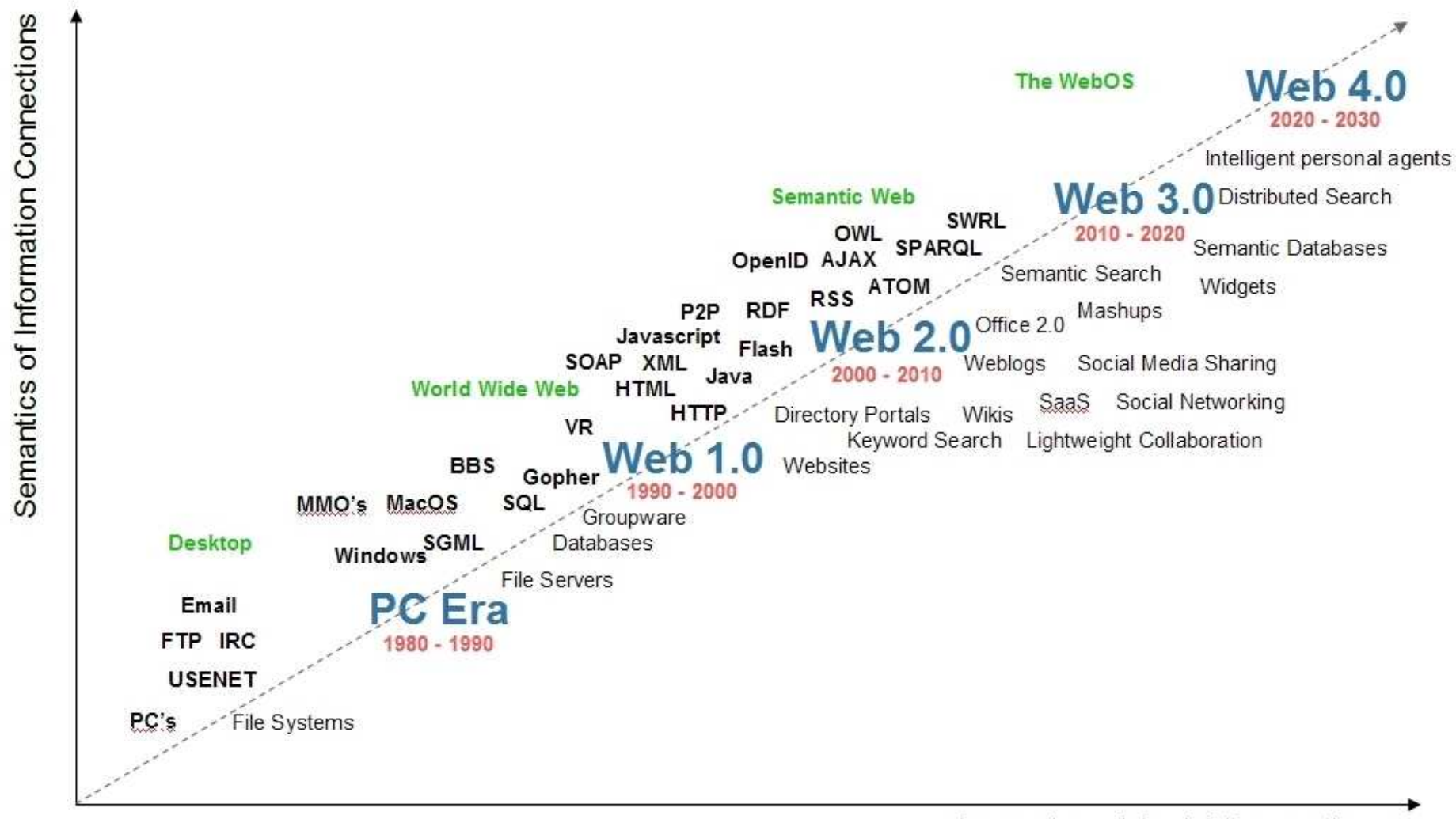
Goran Peteh

gopeteh@cisco.com

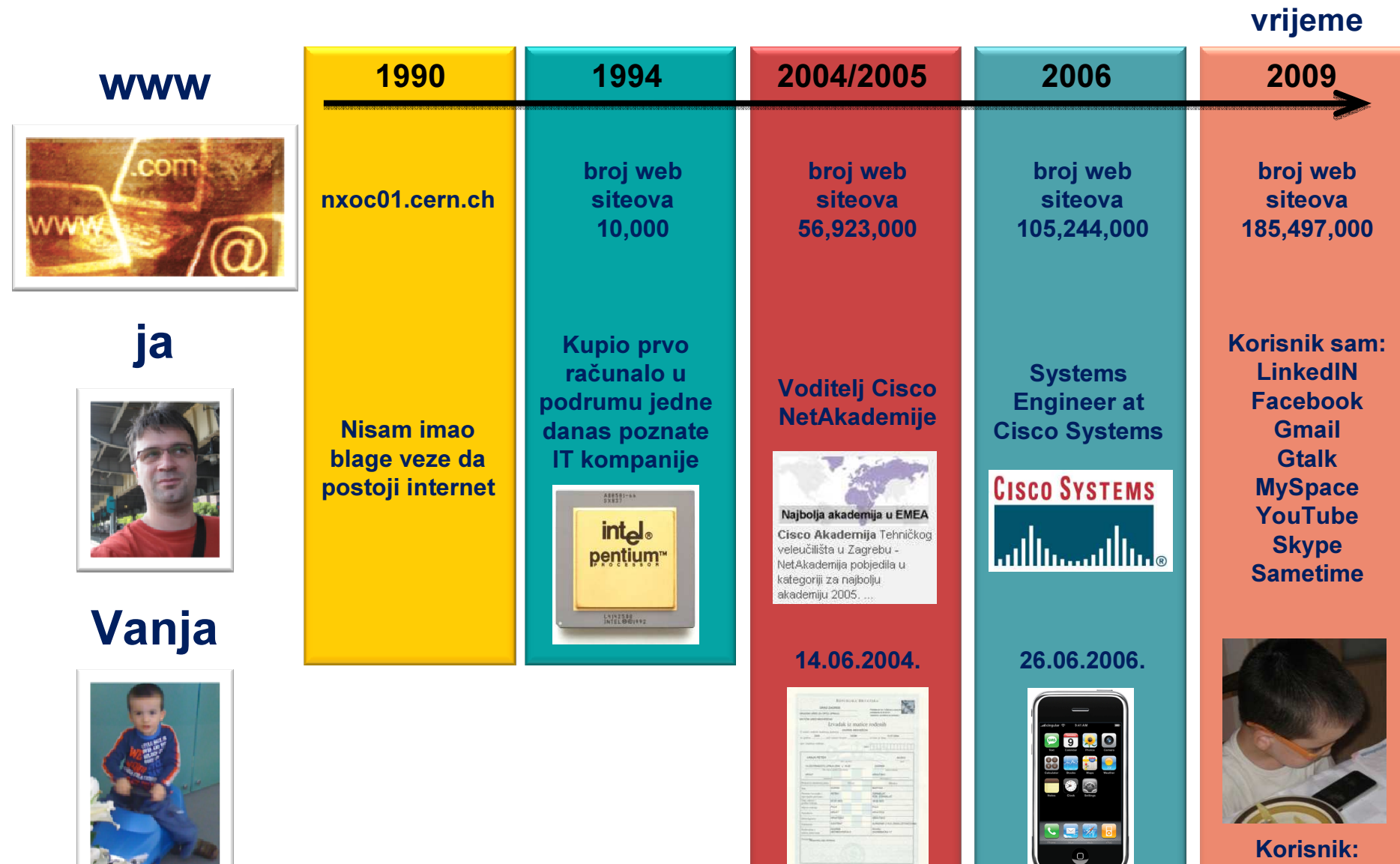
System Engineer, CCSP



WEB 3.0 i sigurnost aplikacija



My web history... nxoc01.cern.ch...



www.cisco.com



Cisco Connection ONLINE
WHAT'S NEW LOGIN REGISTER NAVIGATE HELP

Cisco Solutions
An introductory guide to Cisco products and services that meet your internetworking needs.

Corporate News & Information
Employment opportunities, acquisitions, contacts, news releases, newsletters, and



Cisco Connection Online
The Worldwide Leader in Networking for the Internet

HOW TO BUY LOGIN REGISTER SITE MAP COUNTRIES/LANGUAGES

Products Search
[Select a Category] Go [Advanced] [Help with Search]

Solutions
Service Providers, Large Enterprises, Corporate News & Information, About Cisco, Publications

Products & Ordering
General Information, Ordering Information, Software & Support, Technical Support, Software Center, Training, Seminars, Training, Cisco Co Events, Partners & Reseller, Log In, Become a Partner

Service & Support
Online Support Benefits, Technical Documents, Software Center, Contact/Service Management, Service/Support Programs

Training, Events, & Seminars
Training/Certifications, Networkers, Seminars, Events, E-Learning

Corporate News & Information
About Cisco, Contact Cisco, Investor Information, Find a Job, News/Press and Publications



Cisco Connection Online
The Worldwide Leader in Networking for the Internet

How to Buy Login Register Map/Help Countries/Languages

Search More Options Help
Concept Go
All COO

Solutions for Your Network
Overview, Large Corporations, Small/Medium Business, Service Providers, Home, Government, Education

Products & Technologies
Product Families, Products, Technologies

Ordering
Online Ordering, Ordering Information, Finance Your Network

Partners & Resell
Login, Become a Partner, Build Your Business, Find a Partner/Reseller, Strategic Alliance



Cisco
Powered Network
find recommended service providers

All contents copyright © 1992-1999 Cisco Systems, Inc.



Worldwide [change] Log In Account Register About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

Unify, Simplify, and Amplify
Discover how Cisco Unified Computing is changing the economics of the data center.

LATEST NEWS Cisco Unveils Unified Computing System - 16 Mar 2009 View All News QUICK LINKS

Information for:
Small Business
Enterprise
Service Provider
Consumer

Get Closer to Your Customers
Expertise on demand with 0 payments for 3 months.
Learn More

Cisco live!
June 27 - July 2, 2009
San Francisco, CA
Register Now

Contacts | Feedback | Help | Site Map
© 1992-2009 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Quick Links
Partner Locator
Find a Service Provider
Security Center
Documentation
Career Opportunities
Investor Relations
Discussion Forums
Annual Report

Download Software
All Software Downloads

2007 Online Annual Report
Read Now

Featured Product
Unified Workspace Licensing
Maximize productivity with a simple and affordable way to deliver Cisco Unified Communications to everyone.
Learn More

View All Products

Latest News
City of Bowling Green Improves Public Safety - 15 Oct 2007
Podcast: How Virtual Worlds are Helping to Evolve the Workplace - 11 Oct 2007
Blog: A New World of Communication and Collaboration - 10 Oct 2007
View All News

Direct Access
Software Downloads Industries
Resources For Large Enterprise Small & Medium Business Home & Home Office Service Provider Investor Government Press

Find a Service Provider
Security at Cisco Career-Specializations Discussion Forums

THIS IS THE POWER OF THE NETWORK. NOW.
LEARN MORE

News
Converged Optical Network Puts Hotel Group in Command - 25 Mar 2004
First Cisco Partner Summit in Vietnam - 25 Mar 2004
Interactive TV Services Enabled by Cisco's CMTS solution - 25 Mar 2004
Cisco Participates in 'Moovs' next-generation Internet Testing - 24 Mar 2004
Linksys Takes Wireless Home Networking Beyond the PC - 24 Mar 2004
More News

Warning – Disclaimer - Upozorenje

Neither Cisco or the presenter encourages the use of any methods and/or tools mentioned within this presentation without the expresses aproval and signed agreement with the owner of the IT infrastructure in question.

The unathorised usage of the aforementioned tools and/or methods could lead to legal prosecution and severe penalties.

Sigurnost jučer, danas, sutra



Sigurnost jučer, danas, sutra

www.remote-exploit.org



Sigurnost jučer, danas, sutra

www.metasploit.com

metasploit

ALWAYS HOT EXPLOITS . ALWAYS .

[HOME](#) [FRAMEWORK](#) [SHELLCODE](#) [OPCODEDB](#) [RESEARCH](#) [BLOG](#)



The Metasploit Project

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

Demo 1

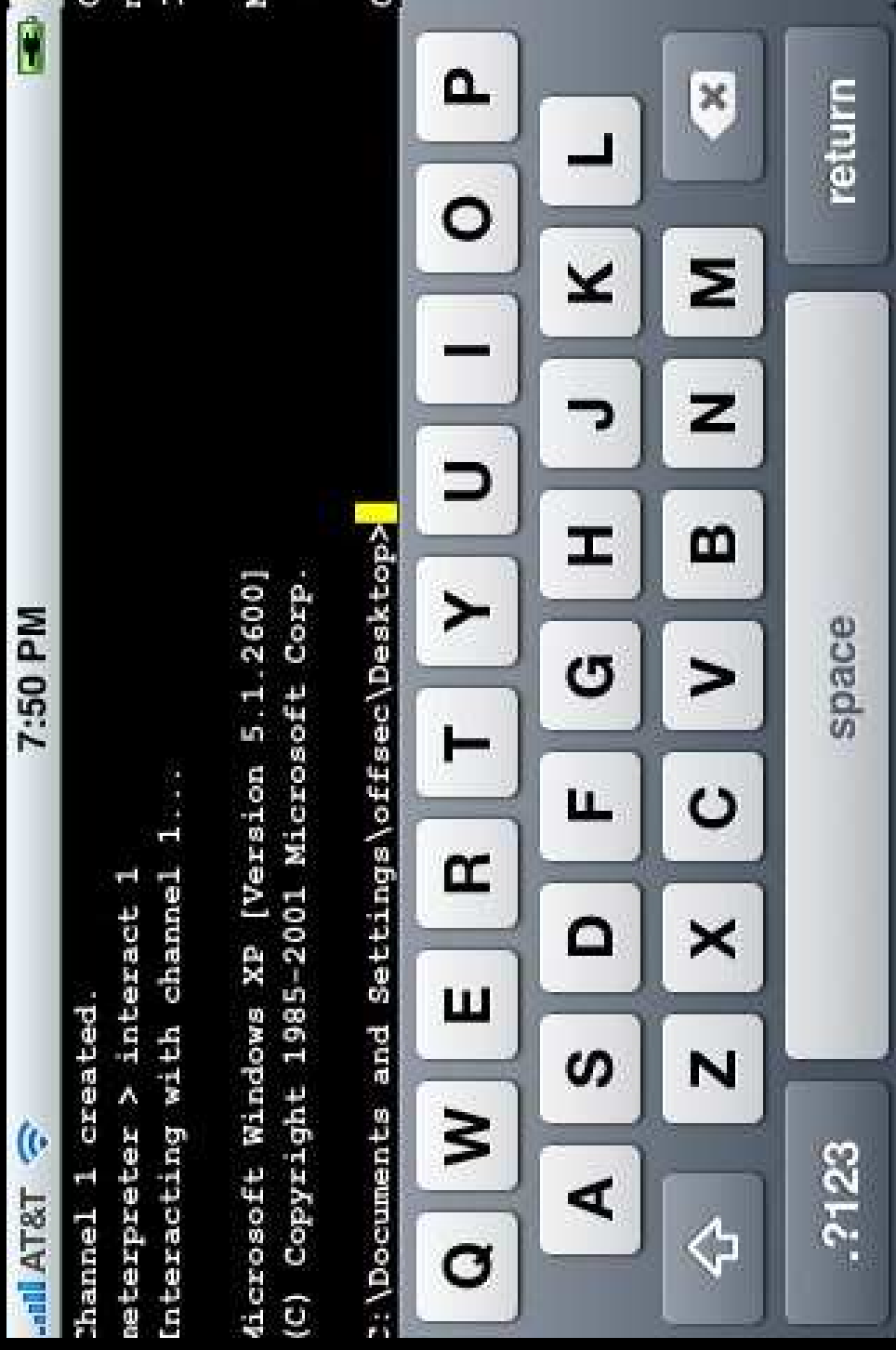
Demo 2 – buši, buši...

AT&T 7:41 PM

```
=[ msf v3.1-release  
t-- --=[ 262 exploits - 117 payloads  
t-- --=[ 17 encoders - 6 nops  
      =[ 46 aux
```

```
msf > use windows/browser/ms06_001_wmf_setabortproc  
msf exploit(ms06_001_wmf_setabortproc) > set
```





Introducing Cisco's ACE Web App Firewall

- Builds on top of industry-leading ACE XML Gateway platform
- Simple software upgrade to install Web Application Firewall



Web Application Firewall

Protects your custom HTTP/HTML applications
from high-impact web-borne attacks

SOA/Web Services/XML Threat Defense Secures and offload web services transactions

Enables HTTP/HTML/XML threat defense

Cross-Site Scripting (XSS) attacks

- **What is it?**

- A malicious script is echoed back into HTML returned from a trusted web site. The scripts executes locally on the client.
- Extremely widespread – some experts estimate 70%-80% of websites are vulnerable

- **What are the implications?**

- Web Site Defacement
- Session IDs stolen (cookies exported to hacker's site)
- Browser security compromised – control given to hacker
- All data sent between client and server potentially hijacked

Getting started with the Cisco ACE WAF

ACE XML Manager CISCO WEB APPLICATION FIREWALL administrator | Logout | Help

Subpolicy Shared Deploy Policy...

★ Manager Dashboard

Policy

- HTTP Ports & Hostnames
- Destination HTTP Servers
- Virtual Services**
 - Access Control
 - LDAP Servers
 - Exception Mapping Defaults
 - Denial-of-Service Protection
 - Content Screening Defaults
- Virtual Web Apps** >>
 - Web App Firewall Profiles
 - Web App Firewall Rules
- Policy Management
 - Subpolicies

Resources

Reports & Tools

- Message Traffic Log
- Web App Firewall Incidents
- Event Log
- Service Health
- Performance Monitor
- Cache Manager
- Compliance Report
- Service Directory

Administration

Virtual Web Apps > New Virtual Web App

NEW VIRTUAL WEB APP

Basic Virtual Web App Wizard

Web App URL:

Web App Group: test

Firewall Profile: Basic Profile

☐ Create in Monitor Mode

Save Changes Cancel

Specify the IP/name of the backend server

Call the WAF wizard

Monitor means the WAF alerts but doesn't block – extremely convenient if you're leery of deploying inline

Getting started with the Cisco ACE WAF

The screenshot displays the Cisco ACE XML Manager interface for configuring a new virtual web application. The top header shows the Cisco logo, 'ACE XML Manager', 'CISCO WEB APPLICATION FIREWALL', and user information 'administrator | Logout | Help'. The sidebar on the left contains navigation links for 'Manager Dashboard', 'Policy', 'Virtual Services', 'Virtual Web Apps', 'Policy Management', 'Resources', and 'Reports & Tools'. The main content area is titled 'Virtual Web Apps > New Virtual Web App' and includes a 'Deploy Policy...' button. The configuration sections are as follows:

- NEW VIRTUAL WEB APP**: Includes a 'Full Virtual Web App Editor' dropdown.
- Web App Group**: Set to 'test'.
- Virtual URL Request Filter**: Includes fields for 'Port/Hostname' (http://* (Default HTTP port)), 'Path' (/), 'Matching Mode' (prefix), 'Methods' (ignore), 'HTTP Headers' (ignore), and 'Parameters' (ignore).
- Destination Server**: Set to 'http://172.25.89.140 (172.25.89.140)'.
- Firewall Profile**: Includes a 'Profile' dropdown set to 'Basic Profile' and a 'Monitor Mode' checkbox. A red arrow points to the 'Profile' dropdown, which is highlighted with an orange box labeled 'Profile'.

At the bottom, there are 'Save Changes' and 'Cancel' buttons.

Protecting the web site from XSS

CISCO ACE XML Manager **CISCO WEB APPLICATION FIREWALL** Authenticated by Reactivity administrator | Logout | Help

Subpolicy: **Shared** [Deploy Policy...](#)

★ Manager Dashboard

Policy

- [HTTP Ports & Hostnames](#)
- [Destination HTTP Servers](#)
- Virtual Services**
 - [Access Control](#)
 - [LDAP Servers](#)
 - [Exception Mapping Defaults](#)
 - [Denial-of-Service Protection](#)
 - [Content Screening Defaults](#)
- Virtual Web Apps**
 - [Web App Firewall Profiles](#) >>
 - [Web App Firewall Rules](#)
- Policy Management**
 - [Subpolicies](#)

Resources

Reports & Tools

- [Message Traffic Log](#)
- [Web App Firewall Incidents](#)
- [Event Log](#)
- [Service Health](#)
- [Performance Monitor](#)
- [Cache Manager](#)
- [Compliance Report](#)
- [Service Directory](#)

Web App Firewall Profiles > Test profile ?

GENERAL [[EDIT](#)]

Name: Test profile
Description:

FIREWALL CONFIGURATION

Active Security

HTTP Header Processing	...	[edit]
HTTP Exception Mapping	not configured	[edit]
Referer Enforcement	disabled	[edit]
Cookie Security	cookies processing is disabled	[edit]
Data Overflow Defense	...	[edit]

Message Rewrite

CARDNUMBERREWRITING	-- disabled --	[edit]
-------------------------------------	----------------	--------------------------

Message Inspection

SSIINJECTION	-- disabled --	[edit]
COMMANDINJECTION	-- disabled --	[edit]
LDAPINJECTION	-- disabled --	[edit]
CROSSSITESCRIPTING	-- disabled --	[edit]
SQLINJECTION	-- disabled --	[edit]

[Exit to Profiles List](#) [Duplicate](#) [Remove](#)

XSS protection

Fine-tuning a security profile

The screenshot displays the Cisco ACE XML Manager interface for configuring a Web App Firewall profile. The top header shows the Cisco logo, 'ACE XML Manager', 'CISCO WEB APPLICATION FIREWALL', and user information 'administrator | Logout | Help'. The left sidebar contains navigation links under 'Manager Dashboard', 'Policy', 'Virtual Services', 'Virtual Web Apps', 'Policy Management', 'Resources', and 'Reports & Tools'. The main content area shows the configuration for 'Web App Firewall Profiles > Test profile > Configure' with the 'Rule Group: CROSSITESCRIPTING'. The configuration options include 'Mode: Enabled', 'Level: strict' (with a dropdown menu showing 'basic', 'moderate', and 'strict'), and 'Actions' with 'Event Log: Info-level Event' and 'Response: Return an HTTP Error Response - 400 Client Error'. Two orange callout boxes with red arrows point to the 'Level' dropdown and the 'Response' dropdown. A third orange callout box with a blue arrow points to the expanded 'Response' dropdown menu, which lists options: 'Return an HTTP Error Response - 400 Client Error', 'Return an HTTP Error Response - 500 Server Error', 'Return a Custom HTTP Error Response', and 'Allow Message'.

Subpolicy: **Shared** [Deploy Policy...](#)

★ **Manager Dashboard**

Policy [Web App Firewall Profiles](#) [Test profile](#) [Configure](#)

Rule Group: CROSSITESCRIPTING

RULE GROUP: CROSSITESCRIPTING

Mode: **Enabled**

Level: **strict** (dropdown menu showing: basic, moderate, strict)

crossSiteScripting1 [[details](#)]

Actions

Event Log: **Info-level Event**

Response: **Return an HTTP Error Response - 400 Client Error**

[Save Changes](#) [Cancel](#)

XSS rules level

Action to take when a XSS is detected

Return an HTTP Error Response - 400 Client Error
Return an HTTP Error Response - 500 Server Error
Return a Custom HTTP Error Response
Allow Message

Associate the profile to the web site

Virtual Web Apps > test

WEB APP GROUP		[EDIT]
Name: test		
Default Profile: Basic Profile		
VIRTUAL WEB APPS		[ADD A VIRTUAL WEB APP]
Virtual URL: http://*/		[edit] [delete]
Destination: http://foobarfoo2k.cisco.com		
+ Firewall Profile: <u>Test profile</u>		
+ Firewall Modifiers (1)		[add modifier]

Exit to Virtual Web Apps

Disable Virtual Web App

Switch to Monitor Mode

Turn Off Monitor Mode

View Logs

Remove

Profile "Test" mapped to our web site

Deploy the policy to the WAF gateway(s)

The screenshot shows the Cisco ACE XML Manager interface for the Cisco Web Application Firewall. The left sidebar contains a navigation menu with sections: Manager Dashboard, Policy, Virtual Services, Virtual Web Apps, Policy Management, Resources, Reports & Tools, and Administration. The main content area is titled 'Policy Manager > Deploy > Step 1 of 3: Review Changes'. It instructs the user to review changes before continuing. The changes are categorized into 'Changed' (differences between versions) and 'New' (items in the current version not in the previous one). Under 'WAFHANDLER', a 'Changed' item 'http://*/' is listed with a link to 'detailed differences'. Under 'WAFPROFILE', a 'New' item 'Test profile' is listed. At the bottom, there are buttons for 'Continue to Next Step >' and 'Exit to Policy Manager'. A red arrow points from an orange callout box to the 'Test profile' entry.

Changed - these are different between the previously deployed version and the current version:

- ! [http://*/](#) [detailed differences](#)

New - these exist in the current version, but not the previously deployed version:

- + [Test profile](#)

[Continue to Next Step >](#) [Exit to Policy Manager](#)

Deltas between current applied policy and proposed one are highlighted

Verification of successful deployment

ACE XML Manager CISCO WEB APPLICATION FIREWALL administrator | Logout | Help

Subpolicy **Shared** Deploy Policy...

★ Manager Dashboard

- Policy**
 - HTTP Ports & Hostnames
 - Destination HTTP Servers
 - Virtual Services**
 - Access Control
 - LDAP Servers
 - Exception Mapping Defaults
 - Denial-of-Service Protection
 - Content Screening Defaults
 - Virtual Web Apps**
 - Web App Firewall Profiles
 - Web App Firewall Rules
 - Policy Management** >>
 - Subpolicies
- Resources**
- Reports & Tools**
 - Message Traffic Log
 - Web App Firewall Incidents
 - Event Log
 - Service Health
 - Performance Monitor
 - Cache Manager
 - Compliance Report
 - Service Directory

Policy Manager > Deploy > Step 3 of 3: Compile and Deploy

This policy is compiled and can now be deployed. To deploy a different policy, load it from the [Policy History](#).

[[check all](#) | [unchecked all](#)]

	ACE XML Gateway	Version	Licensed	Compiled Policy Timestamp & ID	Policy Description	
				Feb 13 2008 01:24:20 AM PST ea6b569bce4cd863		
☐	171.69.45.233	6.0Alpha5-2008-02-05T19	yes	Deployed Policy Timestamp & ID Feb 13 2008 01:24:21 AM PST ea6b569bce4cd863	Deployed Policy Description	Status

Deploy To Selected Gateways UDDI Publishing... Refresh Status

timestamps

Policies can be deployed to N gateways

The web site is under attack!

Web App Firewall Incidents

Group by: Virtual Web App -- all records --

[Update View](#) Incident records are available for the last 12 minutes [CSV](#) [Export Raw Data](#)

Description	Incidents	%	
Incidents By Virtual Web App at Feb 13 2008 01:50:35 AM PST	4	100.0%	
test	4	100.0%	[events]
http://*/	4	100.0%	[events]
CrossSiteScripting	1	25.0%	[events]
Data Overflow	2	50.0%	[events]
SqlInjection	1	25.0%	[events]

Immediate incident
report view

Let's drill down

Event Log Viewer

Current Manager Event Logging alert, error, warning, notice [edit]
Current ACE XML Gateway Event Logging alert, error, warning, notice, info, debug [edit]

During last hour
search events logged on -- all hosts -- for events of type alert, error, warning, notice
with message GUID
category (e.g., /policy/access)
component (e.g., core or console)
description

Display a maximum of 500 events per page
Update

EVENT LOG SEARCH RESULTS AT FEB 18 2008 09:30:39 AM PST

First < Prev Displaying events 1 - 8 Next > (more recent events are shown at the top)

Time (PST)	Description	Message GUID	Host	Component	Category
Feb 18 2008 09:29:41.714 AM	W CROSSSITE SCRIPTING.CrossSiteScripting[1:52:REQUEST_POSTPARAM['name']] detected by rule; returning error.	45ABFA2D000014292D980A4F08849B2D	ciscowaf	reactor	/waf/incid
Feb 18 2008 09:29:41.714 AM	W Terminating HTTP session: 500 An error occurred	45ABFA2D000014292D980A4F08849B2D	ciscowaf	reactor	/session
Feb 18 2008 09:29:41.714 AM	W An error occurred for this request: An error occurred while handling the request.	45ABFA2D000014292D980A4F08849B2D	ciscowaf	reactor	/error

ID of the rule which caused the alert

The name of the attack vector is provided

Detailed security event drill down

EVENT LOG SEARCH RESULTS AT FEB 18 2008 09:34:51 AM PST	
First < Prev Displaying events 1 - 14 Next > (more recent events are shown at the top)	
Time (PST)	Description
Feb 18 2008 09:29:41.714 AM	D Awaiting new request on inbound connection
Feb 18 2008 09:29:41.714 AM	W CROSSSITESCRIPTING.CrossSiteScripting1:52:REQUEST_POSTPARAM['name'] detected by rule; returning error.
Feb 18 2008 09:29:41.714 AM	W Terminating HTTP session: 500 An error occurred
Feb 18 2008 09:29:41.714 AM	W An error occurred for this request: An error occurred while handling the request.
Feb 18 2008 09:29:41.714 AM	I No policy-specific error handler for WAF.CROSSSITESCRIPTING.CrossSiteScripting1:\$(SIG_MATCH_SIGID):\$(SIG_MATCH_INPUT_NAME):
Feb 18 2008 09:29:41.713 AM	I Checking limit 1
Feb 18 2008 09:29:41.713 AM	I Checking limit 0
Feb 18 2008 09:29:41.713 AM	I Checking 3 limits
Feb 18 2008 09:29:41.713 AM	I Accepted a new HTTP POST request from 171.69.141.0 for /SCRIPTS/xss.php
Feb 18 2008 09:29:41.713 AM	I HTTP POST request for /SCRIPTS/xss.php from 171.69.141.0 matched Port 'Default HTTP port'; checking for handler
Feb 18 2008 09:29:41.713 AM	I Performing normalization on '/SCRIPTS/xss.php' with mode 7211
Feb 18 2008 09:29:41.713 AM	D HTTP Trace IN: Content-Type: application/x-www-form-urlencoded Content-Length: 58 name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
Feb 18 2008 09:29:41.711 AM	D HTTP Trace IN: POST /SCRIPTS/xss.php HTTP/1.1 Host: foobarfoo2k.cisco.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12 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-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Connection: keep-alive Referer: http://foobarfoo2k.cisco.com/SCRIPTS/xss.php Cookie: cec_user_id=cpaggen; SMIDENTITY=zv5hvichtfb9t4nGfXC5vsozOJXocY3BBaWM0802bEHDUDb4mPvEBkbi0dOq+xO//TRZiz0UpMcRa3IWnmLDn3PaH5z74dxFY3ILl

Full dump of incoming request

What the user/hacker/victim sees



- The error message and HTTP return code are fully customizable! You can return your own HTML code and for example redirect the hacker to the main page.

I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network v
I will NOT leave my network

The background of the entire image shows a person's dark hair and back as they look towards a light-colored surface where the text is displayed. The text consists of seven lines of the same sentence, with the sixth line being partially cut off by the bottom edge of the frame.

